RESEARCH CENTER
Nancy - Grand Est

FIELD

Activity Report 2012

Section New Results

Edition: 2013-04-24

ALGORILLE Project-Team

6. New Results

6.1. Structuring applications for scalability

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

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

6.1.1. Efficient linear algebra on accelerators.

Graphics Processing Units have evolved to fully programmable parallel vector-processor sub-systems. We have designed several parallel algorithms on GPUs, and integrated that level of parallelism into larger applications including several other levels of parallelism (multi-core, multi-node,...). In this context, we also have studied energy issues and designed some energy performance models for GPU clusters, in order to model and predict energy consumption of GPU clusters.

The PhD thesis of Wilfried Kirschenmann, has been a collaboration with EDF R&D and was co-supervised by S. Vialle and Laurent Plagne (EDF SINETICS). It has given rise to a DSEL based on C++ and to a unified generic library that adapts to multi-core CPUs, multi-core CPUs with vector units (SSE or AVX), and GPUs. This framework allows to implement linear algebra operations originating from neutronic computations, see [22].

The PhD thesis of Thomas Jost, co-supervised by S. Contassot-Vivier and Bruno Lévy (Alice INRIA team) deals with specific algorithms for GPUs, in particular linear solvers. He has also worked on the use of GPUs within clusters of workstations via the study of a solver of non-linear problems [17]. The defense of this thesis is planned in January 2013.

6.1.2. Combining locking and data management interfaces.

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; [21] extends distributed lock mechanisms and combines them with implicit data management.

A new implementation (ORWL) of our ideas of combining control and data management in C has been undertaken, see 5.5 . A first work has demonstrated its efficiency for a benchmark application [18]. Our current efforts concentrate on the 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 now able to handle such an application seamlessly and efficiently, a real alternative to home made interactions between MPI and CUDA.

6.1.3. Discrete and continuous dynamical systems.

The continuous aspect of dynamical systems has been intensively studied through the development of asynchronous algorithms for solving PDE problems. We have focused our studies on the interest of GPUs in asynchronous algorithms [17]. Also, we investigate the possibility to insert periodic synchronous iterations inside the asynchronous scheme in order to improve the convergence detection delay. This is especially interesting on small/middle sized clusters with efficient networks. Finally, we investigate other optimizations like load balancing. For this last subject, the SimGrid environment has revealed itself to be a precious tool to perform feasibility tests and benchmarks for this kind of algorithms on large scale systems. It has been successfully used to evaluate an asynchronous load balancing algorithm [37].

In 2011, the PhD thesis of Marion Guthmuller, supervised by M. Quinson and S. Contassot-Vivier, has started on the subject of model-checking distributed applications inside the SimGrid simulator [20]. This is also the opportunity of designing new tools to study more precisely the dynamics of discrete or continuous systems. See the simulation part in Section 6.3.2 for more details on this PhD.

6.2. Transparent resource management

6.2.1. Client-side cloud broker.

Integrating the 'pay-as-you-go' pricing model commonly used in IaaS clouds is an important question which profoundly changes the assumptions for job scheduling. From the observation that in most commercial solutions the price of a CPU cycle is identical, be the CPU a fast or slow one, several schedulings may be derived for a same price but with different makespans. Hence, in a context where resources can be started on-demand, scheduling strategies must include a decision process regarding the scaling (number of resources used) of the platform and the types of resources rented over time. In [24], we have studied the impact of these two factors on classic job scheduling strategies applied to bag-of-tasks workloads. The results show that shorter makespans can be achieved through scaling at no extra cost, while using quicker CPUs largely increases the price of the computations. More importantly, we show the difficulty to predict the outcomes of such decisions, which requires to design new provisioning approaches.

6.3. Experimental Methodologies

6.3.1. Overall improvement of SimGrid

2012 was the last year of the USS-SimGrid project granted by the ANR. We thus capitalized the results of the first project by properly releasing them in the public releases. Parallel simulation is now stable enough to be used in practice by our users. In addition, the framework is now able to simulate millions of processes without any particular settings in C. The java bindings were also improved to simulate several hundred thousand processes out of the box [25].

This year was also the first year of the SONGS project, also funded by the ANR. This project is much larger that the previous one, both in funding and targets. In surface, SONGS aims at increasing the scope of the SimGrid simulation framework by enabling the Cloud and HPC scenarios in addition to the existing Grid and P2P ones. Under the hood, it aims at providing new models specifically designed for these use cases, and also provide the necessary internal hooks so that users can modify the used models by themselves.

This project is well started, with three plenary meetings and a user conference organized over the year, but no new publication resulted of this work yet. The first work toward increasing the simulation versatility, initiated last year, was published this year[14]

6.3.2. Dynamic verification of liveness properties in SimGrid

A full featured model-checker is integrated to SimGrid since a few years, but it was limited to the verification of safety properties. We worked toward the verification of liveness properties in this framework. The key challenge is to quantify the state equality at state level, adding and leveraging introspection abilities to arbitrary C programs.

This constitutes the core of the PhD thesis of M. Guthmuller, started last year. A working prototype was developed during this year, described in an initial publication [20].

6.3.3. Grid'5000 and related projects

We continued to play a key role in the Grid'5000 testbed in 2012. Lucas Nussbaum, being delegated by the executive committee to follow the work of the technical team, was heavily involved in the recent evolutions of the testbed (network weathermaps, storage management, etc.) and in other activities such as the preparation of the Grid'5000 winter school. We were also involved in a publication [33] which is a follow-up to the workshop on *Supporting Experimental Computer Science* held during SC'11, and in another publication [32] describing the recent advances on the Grid'5000 testbed in order to support experiments involving virtualization at large scale.

More specifically, our involvement in the *OpenCloudWare* project led us to design several tools that ease the deployment of Cloud stacks on Grid'5000 for experimental purposes. Those tools were also used during an internship that was co-advised with the *Harmonic Pharma* start-up, exploring how complex bio-informatics workflows could be ported to the Cloud.

On the institutional side, we will also play a central role in the *Groupement d'Intérêt Scientifique* that is currently being set up, since Lucas Nussbaum is a member of both the *bureau* and of the *comité d'architectes*.

6.3.4. Distem – DISTributed systems EMulator

In the context of ADT Solfége, we continued our work on Distem. Three releases were made over the year, with several improvements and bug fixes, including support for variable CPU and network emulation parameters during an experiment. See http://distem.gforge.inria.fr/ for more information, or our paper accepted at PDP'2013 [26].

6.3.5. Kadeploy3 – scalable cluster deployment solution

Thanks to the support of ADT Kadeploy3, many efforts were carried out on Kadeploy3. Two releases were made, including many new features (many improvements to the handling of parallel commands and to the inner automaton for more fault-tolerant deployments; use of Kexec for faster deployments) as well as bug fixes.

Kadeploy3 was featured during several events (*journée 2RCE*, *SuperComputing 2012*), and in two publications: one unsuccessfully submitted to LISA'2012 [35], one accepted in USENIX *;login:* [13].

Finally, Kadeploy3 was also the basis of submissions to the *SCALE challenge held with CCGrid'2012*, of which we were finalists, and of the winner challenge entry at *Grid'5000 winter school 2012*.

6.3.6. Business workflows for the description and control of experiments

We are exploring the use of Business Process Modelling and Management for the description and the control of complex experiments. In [28], we outlined the required features for an experiment control framework, and described how business workflows could be used to address this issue. In [27] and [15], we described our early implementation of XPFlow, a experiment control engine relying on business workflows paradigms.

6.3.7. Towards Open Science for distributed systems research

One of our long term goal on experimental methodologies would be the advance of an Open Science in the research domain of Distributed Systems. Scientific tools would be sufficiently assessed and easily combined when necessary, and scientific experiments would be perfectly reproducible. These objectives are still very ambitious for the researches targeting distributed systems.

In order to precisely evaluate the path remaining toward these goals, and try addressing some of the challenges that they pose, we currently host Maximiliano Geier as an Inria intern. While most researchers try to answer brilliant scientific questions with simple scientific methodologies, he is asked to answer a simple question (on the adaptation of the BitTorrent protocol to high bandwidth networks) using an advanced scientific methodology. We are also surveying the experimental methodology used in top tier conferences to gain further insight on this topic.

In addition, we are organizing Realis, an event aiming at testing the experimental reproducibility of papers submitted to Compas'2013. Associated to the Compas'13 conference, this workshop aims 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.

ALICE Project-Team

5. New Results

5.1. A Runtime Cache for Interactive Procedural Modeling

Participant: Sylvain Lefebvre.

This work further explores hashing techniques that we developed over the past years. In particular, we considered modifying our hashing scheme to create a run-time cache. The cache avoids expensive computations when texturing implicit surfaces with complex procedural functions. This is a result from a collaboration with the Karlsruhe Institute of Technology which was funded by an Inria COLOR grant and has been published this year in the journal "Computers & Graphics" [14].

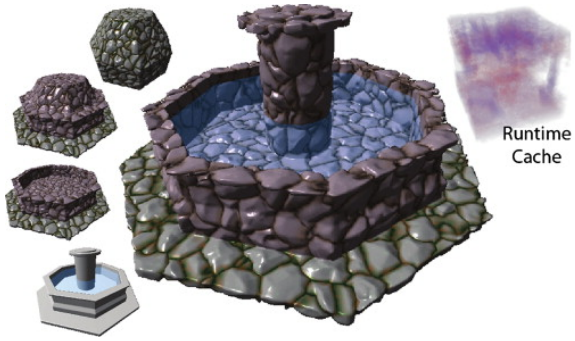

Figure 1. A Runtime Cache for Interactive Procedural Modeling.

5.2. Texture Synthesis

Participants: Sylvain Lefebvre, Bruno Jobard.

We continued investigating on Gabor Noise and considered fitting the parameters of our Gabor noise texturing technique from example images. This required a new formulation of our noise, allowing us to solve the problem as a basis pursuit denoising optimization. This is the result of a collaboration with the team REVES / Inria Sophia-Antipolis, the Katholieke Universiteit of Leuven and Université Paris Descartes. This work has been presented at the SIGGRAPH conference this year [8].

We also revisited techniques for texture synthesis explicitly copying and assembling large patches of an example image to form a new texture. We accelerate this process through a parallel implementation which both optimizes for the shape of the patches and a deformation along their boundary to better match edges. This work is part of the PhD thesis of Anass Lasram and has been presented this year at the Eurographics/ ACM SIGGRAPH Symposium on High Performance Graphics, [19].

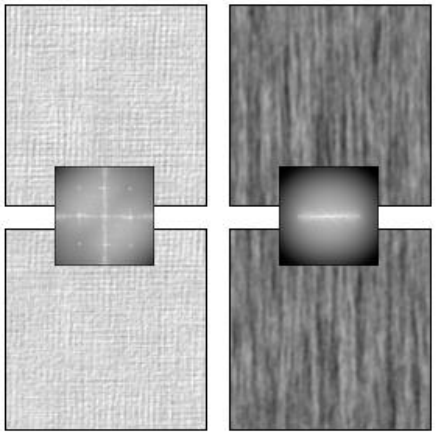

Figure 2. Gabor Noise by Example.

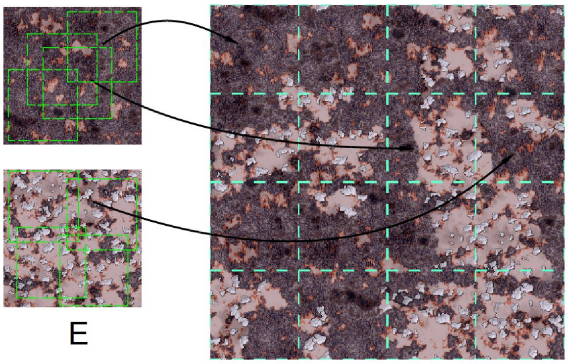

Figure 3. Parallel patch–based texture synthesis.

We also studied ways of helping the user to select the parameters of procedural texture generators, by proposing two contributions :

- We studied how to summarize the appearances generated by complex procedural textures in a small preview image. The challenge is to capture the large variety of appearances despite a limited pixel space. We formulate the problem as a layout of high-dimensional samples in a regular grid, and optimize for it through a modified Self Organizing Map algorithm. This work is part of the PhD thesis of Anass Lasram, and is a collaboration with our industrial partner Allegorithmic. This work has been published this year in the journal "Computer Graphics Forum", [10].
- The parameters of complex procedural textures are typically chosen through a slider-based interface. We augment this interface with preview images which predict how the texture will change when manipulating the slider. This greatly simplifies the process of choosing parameters for these textures. This work is part of the PhD thesis of Anass Lasram, and is a collaboration with our industrial partner Allegorithmic. This work has been published this year as EUROGRAPHICS short paper, [18].

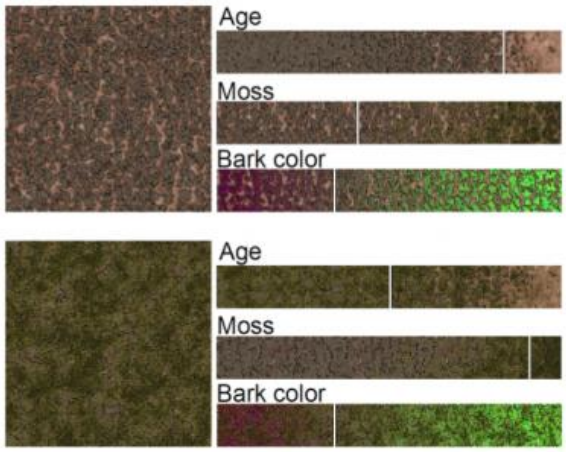

Figure 4. Scented Sliders for Procedural Textures.

5.3. Algorithms and analysis

Participants: Laurent Alonso, Samuel Hornus.

Data structure for fast witness complexes: Samuel Hornus is currently pursuing work started while a post-doc in Sophia Antipolis, on data structure for the fast construction of witness complexes; these are sub complexes of Delaunay triangulations that can be faster to compute for low dimensional data embedded in high dimensional ambiant space.

Analysis of Boyer and Moore's MJRTY Algorithm: Given a set of n elements each of which is either red or blue, Boyer and Moore's algorithm uses pairwise equal/not equal color comparisons to determine the majority color. We analyze the average behavior of their algorithm, proving that if all 2^n possible inputs are equally likely, the average number of color comparisons used is $n - \sqrt{2n/\pi} + O(1)$ and have variance in $\frac{\pi-2}{\pi}n - \frac{\sqrt{2\,n}}{\sqrt{\pi}} + O(1)$. This work has been submitted to SIAM Journal On Computing.

5.4. Visualizing $2D$ Flows with Animated Arrow Plots

Participants: Bruno Jobard, Nicolas Ray, Dmitry Sokolov.

Flow fields are often represented as a set of static arrows in illustration of scientific vulgarization, documentary, meteorology, etc. This simple and schematic representation lets an observer intuitively interpret the main properties of a flow: its orientation and velocity magnitude (Figure 5).

We have investigated how to automatically generate dynamic versions of such representations for $2D$ unsteady flow fields. As a result, we designed an algorithm able to smoothly animate arrows along the flow while controlling their density in the domain over time. Beside keeping an even distribution of arrows over time, we made significant efforts to remove disturbing rendering artefacts such as the apparition of a new arrow, the removing of existing arrows, and the representation of field where the velocity is null. This work has been published as a research report, [24].

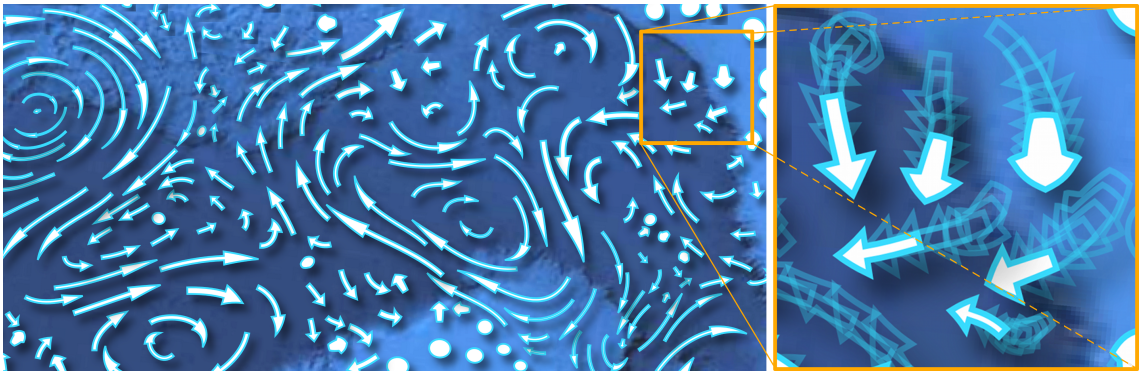

Figure 5. Ocean currents visualized with a set of dynamic arrows. The Close-up shows the arrow trajectories and the morphing of their glyphs.

5.5. Fixing normal constraints for generation of polycubes

Participants: Nicolas Ray, Dmitry Sokolov.

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

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

We have worked on a method able to determine if there exists a deformation of the surface that respects a given orientation constraint on each point. We have also design an automatic solution that can fix constraints that would prevent the existence of a deformation into a polycube (Figure 6).

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

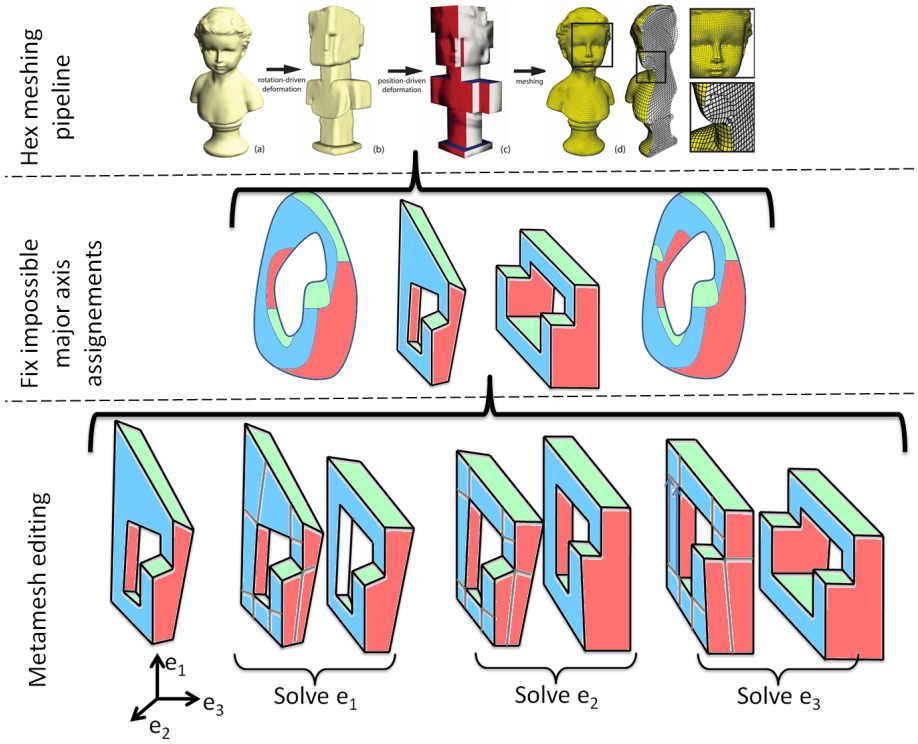

Figure 6. ***Upper row:*** *the surface is deformed to make its normals closer to major axis, but to reach an equality, we need to have a coherent "wished orientation" of the faces.* ***Middle row:*** *we define a valid deformation into a polycube by editing the "wished orientation".* ***Lower row*** *the resolution is performed a dimension at a time.*

5.6. Control of the differential behaviour of the joining curve between two fractal curves

Participants: Dmitry Sokolov, S. Podkorytov, C. Gentil, S. Lanquetin.

The general objective of our work is to create a geometric modeller based on iterative processes. Iterative processes can be used to describe a wide array of shapes inaccessible to standard methods such as fractal curves or sets. Our work is based on Boundary Controlled Iterative System (BCIFS). BCIFS upgrades the standard iterative process such as Iterated Function System (IFS) with B-Rep structure. We can describe objects with familiar B-rep structure, where each cell is a fractal object. For instance, if we consider a polyhedron, then each face is a fractal surface, and each edge is a fractal curve. Objects modelled with BCIFS not necessary have the fractal properties, objects such as B-splines curves and surfaces can be modelled as well. So with BCIFS formalism we can operate with both standard and fractal objects.

With this objective in mind, we have to provide tools that work with fractal objects in the same manner as with objects of classical topology. In this project we focus on the constructing of an intermediate curve between two other curves defined by different iterative construction processes. Similar problem often arises with subdivision surfaces, when the goal is to connect two surfaces with different subdivision masks. We start by dealing with curves, willing to later generalize our approach to surfaces. We formalise the problem with Boundary Controlled Iterated Function System model. Then we deduct the conditions that guaranties continuity of the intermediate curve. These conditions determine the structure of subdivision matrices. By studying the eigenvalues of the subdivision operators, we characterise the differential behaviour at the connection points between the curves and the intermediate one. This behaviour depends on the nature of the initial curves and coefficients of the subdivision matrices. We also suggest a method to control the differential behaviour by adding intermediate control points (Figure 7). This work was presented at the Symposium on Solid and Physical Modeling [23].

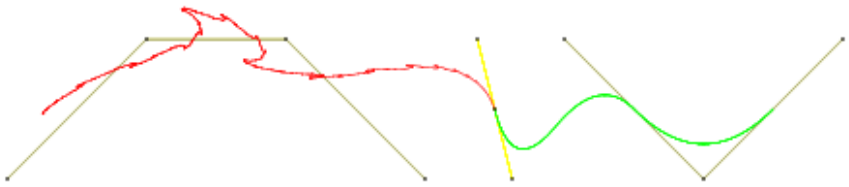

Figure 7. Two intermediate curves between the fractal curve and B-spline. Three control point are used to control the shape of the curve

5.7. Approximate convex hull of affine iterated function system attractors

Participants: Dmitry Sokolov, A. Mishkinis, C. Gentil, S. Lanquetin.

In this paper, we present an algorithm to construct an approximate convex hull of the attractors of an affine iterated function system (IFS). We construct a sequence of convex hull approximations for any required precision using the self-similarity property of the attractor in order to optimize calculations. Due to the affine properties of IFS transformations, the number of points considered in the construction is reduced. The time complexity of our algorithm is a *linear* function of the number of iterations and the number of points in the output convex hull. The number of iterations and the execution time increases logarithmically with increasing accuracy. In addition, we introduce a method to simplify the approximation of the convex hull without loss of accuracy. Figure 8 gives and illustration. This work was published at the Chaos, Solitons & Fractals journal [12].

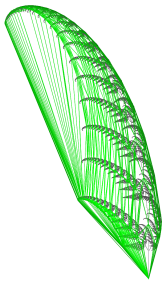

Figure 8. Approximate convex hull for a 3D IFS attractor.

5.8. Shift-Based Parallel Image Compositing on InfiniBand Fat-Trees

Participant: Xavier Cavin.

In this work, we propose a new parallel image compositing algorithm, called Shift-Based, relying on a well-known communication pattern called shift permutation. Indeed, shift permutation is one of the possible ways to get the maximum cross bisectional bandwidth provided by an InfiniBand fat-tree cluster. We show that our Shift-Based algorithm scales on any number of processing nodes (with peak performance on specific counts), allows overlapping communications with computations and exhibits contention free network communications. This is demonstrated with the image compositing of very high resolution images at interactive frame rates. This work is a collaboration with the SED service of Inria (Olivier Demengeon). It has been presented this year at the Eurographics Symposium on Parallel Graphics and Visualization, [17].

5.9. Multi view data processing

Participants: Rhaleb Zayer, Alejandro Galindo, Kun Liu.

Direct use of denoising and mesh reconstruction algorithms on point clouds originating from multi-view images is often oblivious to the reprojection error. This can be a severe limitation in applications which require accurate point tracking, e.g., metrology. we propose a method for improving the quality of such data without forfeiting the original matches. We formulate the problem as a robust smoothness cost function constrained by a bounded reprojection error. The arising optimization problem is addressed as a sequence of unconstrained optimization problems by virtue of the barrier method. Experimental results on synthetic and acquired data compare our approach to alternative techniques. This work has been presented this year at the 8th International Symposium on Visual Computing, [20].

5.10. Deformation modeling of slender objects

Participants: Rhaleb Zayer, Alejandro Galindo, Kun Liu.

A desirable property when modeling/editing slender curve-like objects is the ability to emulate the deformation behavior of natural objects (e.g. cables, ropes). Taking such physical considerations into account needs also to abide to editing requirements such as interactivity and full access and control of all degrees of freedom (positional and rotational constraints) during interaction. We regard editing as a static deformation problem but our treatment differs from standard finite element methods in the sense that the interpolation is based on deformation modes rather than the classic shape functions. A careful choice of these modes allows capturing the deformation behavior of the individual curve segments, and devising the underlying mathematical model from simple and tractable physical considerations. In order to correctly handle arbitrary user input (e.g.

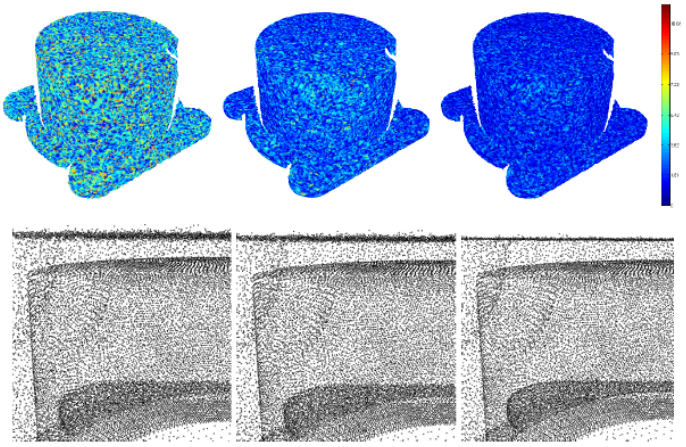

Figure 9. Example of denoising.

dragging vertices in a fast and excessive manner), our approach operates in the nonlinear regime. The arising geometric nonlinearities are addressed effectively through the modal representation without requiring complicated fitting strategies. In this way, we circumvent commonly encountered locking and stability issues while conveying a natural sense of flexibility of the shape at hand. Experiments on various editing scenarios including closed and non-smooth curves demonstrate the robustness of the proposed approach. This work has been published this year in the journal "Computers & Graphics", [15].

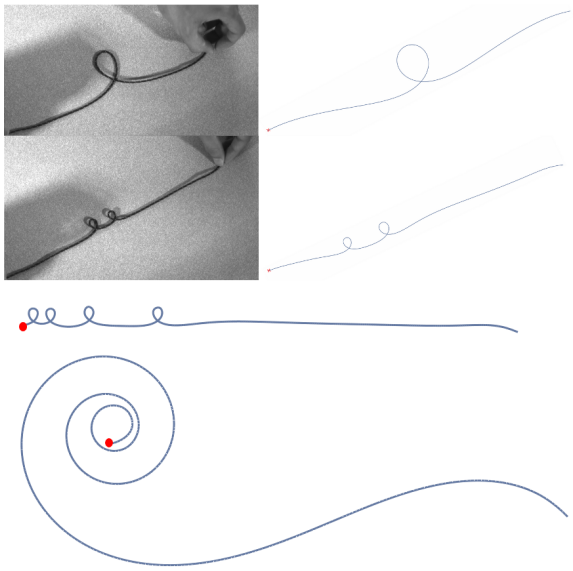

Figure 10. Example of curves.

5.11. Temporally consistent 3D meshing from video data

Participants: Dobrina Boltcheva, Phuong Ho, Bruno Lévy.

This work is a part of the ANR Morpho project (Morpho) which aims at combined analysis of human shapes and motions. In particular, the goal is to study how motions relate to human shapes or how shapes deform in typical motions. During this year, we addressed the first challenge which is building temporally consistent 3D meshes from silhouette images. We have already achieved a very fast meshing algorithm for each frame based on the Centroidal Voronoi Tessellation which has been previously developed in our team. Actually, we are investigating different ways for adding the temporal consistency within our optimisation framework. In particular, we are studding a strategy based on the optimal transport paradigm.

5.12. Re-meshing surfaces

Participants: Nicolas Bonneel, Bruno Lévy, David Lopez, Vincent Nivoliers, DongMing Yan.

In the frame of the ERC GOODSHAPE project, we continued to develop new methods to optimize the sampling of 3D objects. In particular, we studied how to sample a surface with generalized primitives, such as line segments and deformable graphs [11]. We also focused on the problem of remeshing a surface with quads, or fiting a polynomial surface to an input mesh. We proposed a method that minimizes an approximation of the integrated squared distance, based on a restricted Voronoi diagram [22]. Still on the same topic of mesh quadrangulation, we co-published a survey with other international experts of this field [16].

We also worked on anisotropic surface meshing, and developed a technique based on embedding into higher dimensional space and a fast computation of the restricted Voronoi diagram [21].

BIGS Project-Team

6. New Results

6.1. Modern methods of data analysis

Participants: R. Bar, B. Lalloué, J-M. Monnez, C. Padilla, D. Zmirou, S. Deguen.

In 2012, our contributions to data analysis in a Biological context are twofold:

- At a theoretical level, we have kept on working on the so-called online data analysis alluded to at the *Scientific Foundations* Section. Specifically we have carried on in [15] (see also [4]) the analysis of data whose characteristics such as mathematical expectation or covariance matrix may vary with time, a problem which arises very naturally in this context. Moreover, in order to save computation time and thus take into account more data, a method considering several data at each step (we talk about data blocks) is proposed. This technique can also be useful if data are sent and received block-wise. In parallel, a R package performing most of the methods of factorial analysis in an online way is under development.
- At a practical level, our efforts have focused (cf. [19]) on an interesting study concerning the construction of a socio-economic neighborhood index which might quantify health inequalities. While several socio-economic indices already exist in this application field, most of them are very simple both in term of methodological construction and of number of variables taken into account, and only a few use data mining techniques. In order to exploit the large data sets of socio-economic variables provided by censuses and create neighborhood socio-economic indices yielding a better highlight of social health inequalities, a procedure was set in order to automatically select the best indicators in a set of socio-economic variables and synthesize them in a quantitative index. Application to three French metropolitan areas allowed testing the procedure and confirming both its reproducibility on various urban areas and the quality of the neighborhood socio-economic indices we had created (according to field experts and study partners). In this context, our expertise in data analysis allows for a good prediction by means of rigorous methods. Eventually, in order to simplify the application of the creation procedure of a socio-economic index for non-statisticians, a R package called SesIndexCreatoR was created to implement it.
- Publication of the sharp results obtained in [8] on local regression techniques.

6.2. Tumor growth modeling

Participants: R. Keinj, T. Bastogne, P. Vallois.

Up to now, the treatment planning systems used in radiotherapy only use mathematical models to describe the delivery of physical doses of radiation within biological tissues but cannot accurately predict the biological damages caused by such treatments. One important bottleneck is to account for the cell damage heterogeneity in the treated tumor. To this aim we firstly introduced in [51] a stochastic model based on multi-state Markov chains able to describe both treatment damage and cell reparation process.

More recently, we have proposed another model describing the lifespan of heterogenous tumors treated by radiotherapy. It is a bi-scale model in which the cell and tumor lifespans are represented by random variables. First and second-order moments, as well as the cumulative distribution functions and confidence intervals are expressed for the two lifespans with respect to the model parameters. One interesting result is that the mean value of the tumor lifespan can be approached by a logarithmic function of the initial cancer cell number. Moreover, we show that TCP (Tumor Control Probability) and NTCP (Normal Tissue Complication Probability), used in radiotherapy to evaluate, optimize and compare treatment plans, can be derived from the tumor lifespan and the surrounding healthy tissue respectively. Finally, we propose a ROC curve, entitled ECT (Efficiency-Complication Trade-off), suited to the selection by clinicians of the appropriate treatment planning (see [10]).

One difference between photodynamic therapy (PDT) and radiotherapy (RT) is the irradiation signal (X ray in RT and light beam in PDT). Another one is the treatment planning: 10 to 30 daily sessions of treatment in RT against only one for PDT. To adapt the previous model to PDT, a continuous-time version was developed and proposed in [18]. The model has been implemented into Matlab and numerical simulations have emphasized the effects of the model parameters on the model output.

In the framework of a new collaboration with S. Niclou (NorLux Neuro-Oncology Laboratory, Department of Oncology, Centre de Recherche Public de la Santé, Luxembourg), we have extended our stochastic model of cell damage to describe the phenotypic heterogeneity in brain tumors. Preliminary results have recently been presented in [16]. Cancer stem cell (CSC) hypothesis suggests that tumor progression and recurrence rely on a small subpopulation of cancer cells with stem-like properties. The unresolved question is whether cancer stem cells lead to organisation of intratumoral phenotypic heterogeneity by hierarchical differentiation events or whether they represent one of the transitory phenotypic states. This is crucial not only for our understanding of tumor progression, but also for the successful design of novel therapeutic strategies targeting CSCs. Let us also highlight the fact that those studies are related to a more application oriented research synthesized in [3], [13], [21]

6.3. Piecewise deterministic Markov processes

Participants: A. Crudu, A. Debussche, A. Muller-Gueudin, O. Radulescu.

Piecewise deterministic Markov processes are models which feature in a prominent way in Biomedical applications. They appear in two contributions of our team this year.

(1)*Convergence of stochastic gene networks.* In [24], [5], we propose simplified models for the stochastic dynamics of gene network models arising in molecular biology. Those gene networks are classically modeled by Markov jump processes, which are extremely time consuming. To overcome this drawback, we study the asymptotic behavior of multiscale stochastic gene networks using weak limits of Markov jump processes.

We consider a set of chemical reactions R_r, $r \in \mathcal{R}$; $\mathcal{R}$ is supposed to be finite. These reactions involve species indexed by a set $S = 1, \cdots, M$, the number of molecules of the species i is denoted by n_i and $X \in \mathbb{N}^M$ is the vector consisting of the n_i's. Each reaction R_r has a rate $\lambda_r(X)$ which depends on the state of the system, described by X and corresponds to a change $X \to X + \gamma_r$, $\gamma_r \in \mathbb{Z}^M$.

Mathematically, this evolution can be described by the following Markov jump process. It is based on a sequence $(\tau_k)_{k\geq 1}$ of random waiting times with exponential distribution. Setting $T_0 = 0$, $T_i = \tau_1 + \cdots + \tau_i$, X is constant on $[T_{i-1}, T_i)$ and has a jump at T_i. The parameter of τ_i is given by $\sum_{r\in\mathcal{R}} \lambda_r(X(T_{i-1}))$:

$$\mathbf{P}(\tau_i > t) = \exp\left(-\sum_{r\in\mathcal{R}} \lambda_r(X(T_{i-1}))t\right).$$

At time T_i, a reaction $r \in \mathcal{R}$ is chosen with probability $\lambda_r(X(T_{i-1}))/\sum_{r\in\mathcal{R}} \lambda_r(X(T_{i-1}))$ and the state changes according to $X \to X + \gamma_r$: $X(T_i) = X(T_{i-1}) + \gamma_r$. This Markov process has the following generator:

$$Af(X) = \sum_{r\in\mathcal{R}} [f(X + \gamma_r) - f(X)]\, \lambda_r(X).$$

In the applications we have in mind, the numbers of molecules have different scales. Some of the molecules are in small numbers and some are in large numbers. Accordingly, we split the set of species into two sets C and D with cardinals M_C and M_D. This induces the decomposition $X = (X_C, X_D)$, $\gamma_r = (\gamma_r^C, \gamma_r^D)$. For $i \in D$, n_i is of order 1 while for $i \in C$, n_i is proportional to N where N is a large number. For $i \in C$, setting $\widetilde{n}_i = n_i/N$, $\widetilde{n}_i$ is of order 1. We define $x_C = X_C/N$ and $x = (x_C, X_D)$.

For this kind of system, we are able to give in [5] some relevant information on the asymptotic regime $N \to \infty$ when different type of reactions are involved. Depending on the time and concentration scales of the system we distinguish four types of limits:

- Continuous piecewise deterministic processes (PDP) with switching.
- PDP with jumps in the continuous variables.
- Averaged PDP.
- PDP with singular switching.

We justify rigorously the convergence for the four types of limits.

(2)*Variable length Markov chains.* A classical random walk $(S_n,\, n \in \mathbb{N})$ is defined by $S_n := \sum_{k=0}^{n} X_k$, where (X_k) are i.i.d. When the increments $(X_k)_{k\in\mathbb{N}}$ are a one-order Markov chain, a short memory is introduced in the dynamics of (S_n). This so-called "persistent" random walk is no longer Markovian and, under suitable conditions, the rescaled process converges towards the integrated telegraph noise (ITN) as the time-scale and space-scale parameters tend to zero (see [70], [71], [50]). The ITN process is effectively non-Markovian too. In [28] our aim has been to consider persistent random walks (S_t) whose increments are Markov chains with variable order which can be infinite.

Associated with a process (X_n) which takes its values in a finite set, we consider an integer valued process (M_n) so that (X_n, M_n) is Markov and M_n measures the size of the memory at time n. This variable memory is justified by a one-to-one correspondence between (X_n) and a suitable Variable Length Markov Chain (VLMC), since for a VLMC the dependency from the past can be unbounded. We prove in [28] that, under a suitable rescaling, (S_n, X_n, M_n) converges in distribution towards a time continuous process $(S^0(t), X(t), M(t))$. The process $(S^0(t))$ is a semi-Markov and Piecewise Deterministic Markov Process whose paths are piecewise linear.

Observe that, though our study in [28] is made at a theoretical level, it leads to potentially interesting applications in growth models for tumors. This kind of link will be developed in the next future.

6.4. Inference for Gaussian systems

Participants: T. Cass, S. Cohen, M. Hairer, C. Litterer, F. Panloup, L. Quer, S. Tindel.

As mentioned at the *Scientific Foundations* Section, the problem of estimating the coefficients of a general differential equation driven by a Gaussian process is still largely unsolved. To be more specific, the most general ($\mathbb{R}$-valued) equation handled up to now as far as parameter estimation is concerned (see [69]) 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:

$$X_t^\theta = a + \int_0^t b(\theta; X_u)\, du + \int_0^t \sigma(\theta; X_u)\, dB_t, \tag{1}$$

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 2012:

- An implementable numerical scheme for equations driven by irregular processes, which is one of the ingredients one needs in order to perform an accurate statistical estimation procedure (see [6]).
- A better understanding of the law of the solution X_t^θ to equation (1), carried out in [25]. This step allows to obtain smoothness of density for our equation of interest in a wide range of contexts, which is an essential prerequisite for a good estimation procedure.
- Another important preliminary step for likelihood estimates for stochastic equations is a good knowledge of their invariant measure in the ergodic case. This is the object of our article [27].
- Finally we have also progressed in our knowledge of noisy differential systems by extending the range of applications of rough paths methods [11], [14].

CALVI Project-Team

6. New Results

6.1. Mathematical analysis of kinetic models

6.1.1. Gyrokinetic and Finite Larmor radius approximations

Participants: Mihai Bostan, Céline Caldini, Emmanuel Frénod, Mathieu Lutz.

In a work in progress by E. Frénod and M. Lutz, the deduction of the Geometrical Gyro-Kinetic Approximation, which was originally obtained by Littlejohn in [75], [76], [77] using a physical approach which was mathematically formal, is done. The rigorous mathematical theory is built and explained in a form for providing it, especially, for analysts, applied mathematicians and computer scientists.

In the Note [16], we present the derivation of the finite Larmor radius approximation, when collisions are taken into account. We concentrate on the Boltzmann relaxation operator whose study reduces to the gyroaverage computation of velocity convolutions, which are detailed here. We emphasize that the resulting gyroaverage collision kernel is not local in space anymore and that the standard physical properties (i.e., mass balance, entropy inequality) hold true only globally in space and velocity. This work is a first step in this direction and it will allow us to handle more realistic collisional mechanisms, like the Fokker-Planck or Fokker-Planck-Landau kernels.

The subject matter of the paper [34] concerns the derivation of the finite Larmor radius approximation, when collisions are taken into account. Several studies are performed, corresponding to different collision kernels. The main motivation consists in computing the gyroaverage of the Fokker-Planck-Landau operator, which plays a major role in plasma physics. We show that the new collision operator enjoys the usual physical properties ; the averaged kernel balances the mass, momentum, kinetic energy and dissipates the entropy.

6.1.2. Singularities of the stationary Vlasov–Poisson system in a polygon

Participant: Simon Labrunie.

In collaboration with Fahd Karami (Université Cadi Ayyad, Morocco) and Bruno Pinçon (Université de Lorraine and project-team CORIDA), we conducted in [43] a theoretical and numerical study of the so-called "point effect" in plasma physics. The model (stationary Vlasov–Poisson system with external potential) corresponds a fully ionised plasma considered on a time scale much smaller than that of ions, but much larger than that of electrons. It appears as the relevant non-linear generalisation of the electrostatic Poisson equation. This may be a first step toward a quasi-equilibrium model valid on a larger time scale, where the equilibrium description of the electrons would be coupled to a kinetic or fluid model for the ions. This approximation is classical in plasma physics. We proved a general existence result for our model in a bounded domain $\Omega \subset \mathbb{R}^N$, which is not assumed to be smooth. When Ω is a polygonal domain of $\mathbb{R}^2$, we described the singular behavior of the solution near a reentrant corner. In the important case of the Maxwell–Boltzmann distribution, we established a link between various asymptotics of the problem and the (suitably extended) theory of large solutions to nonlinear elliptic problems (for a review of this theory, see e.g. [50]). This allowed us to determine the the dependence of the singularity coefficients on the parameters of the problem, such as the total mass of the distribution, or the boundary conditions of the potential. Numerical tests confirmed the theory.

6.2. Two-Scale Asymptotic-Preserving schemes

Participants: Nicolas Crouseilles, Emmanuel Frénod, Michaël Gutnic, Sever Hirstoaga.

In paper [20], we build a Two-Scale Macro-Micro decomposition of the Vlasov equation with a strong magnetic field. This consists in writing the solution of this equation as a sum of two oscillating functions with circumscribed oscillations. The first of these functions has a shape which is close to the shape of the Two-Scale limit of the solution and the second one is a correction built to offset this imposed shape. The aim of such a decomposition is to be the starting point for the construction of Two-Scale Asymptotic-Preserving schemes.

During CEMRACS 2011, we have started the project to test on a simplified model the Two-Scale Asymptotic-Preserving Schemes. The model, a two dimensional in phase space Vlasov-Poisson equation with small parameter, is used for a long time simulation of a beam in a focusing channel. This work was already done in [68] in the case where the solution is approximated by the two scale limit. The first goal is to improve this approximation, by going further, to the first order one; this was done in [41]. The second goal is to replace this approximation by an exact decomposition, using the macro-micro framework. This last approach will permit to treat the case of a not necessary small parameter. In order to accomplish the first task we have writen a Particle-In-Cell code in SeLaLib.

6.3. Development of numerical methods

Participants: Morgane Bergot, Anaïs Crestetto, Nicolas Crouseilles, Pierre Glanc, Michel Mehrenberger, Hocine Sellama, Eric Sonnendrücker, Christophe Steiner.

The work [19] is devoted to the numerical simulation of the Vlasov equation in the fluid limit using particles. To that purpose, we first perform a micro-macro decomposition as in [53] where asymptotic preserving schemes have been derived in the fluid limit. In [53], a uniform grid was used to approximate both the micro and the macro part of the full distribution function. Here, we modify this approach by using a particle approximation for the kinetic (micro) part, the fluid (macro) part being always discretized by standard finite volume schemes. There are many advantages in doing so: (i) the so-obtained scheme presents a much less level of noise compared to the standard particle method; (ii) the computational cost of the micro-macro model is reduced in the fluid regime since a small number of particles is needed for the micro part; (iii) the scheme is asymptotic preserving in the sense that it is consistent with the kinetic equation in the rarefied regime and it degenerates into a uniformly (with respect to the Knudsen number) consistent (and deterministic) approximation of the limiting equation in the fluid regime.

In [39] we present finite volumes schemes for the numerical approximation of the one-dimensional Vlasov-Poisson equation (FOV CEMRACS 2011 project). Stability analysis is performed for the linear advection and links with semi-Lagrangian schemes are made. Finally, numerical results enable to compare the different methods using classical plasma test cases.

In [40], we test an innovative numerical scheme for the simulation of the guiding-center model, of interest in the domain of plasma physics, namely for fusion devices. We propose a 1D Discontinuous Galerkin (DG) discretization, whose basis are the Lagrange polynomials interpolating the Gauss points inside each cell, coupled to a conservative semi-Lagrangian (SL) strategy. Then, we pass to the 2D setting by means of a second-order Strang splitting strategy. In order to solve the 2D Poisson equation on the DG discretization, we adapt the spectral strategy used for equally-spaced meshes to our Gauss-point-based basis. The 1D solver is validated on a standard benchmark for the nonlinear advection; then, the 2D solver is tested against the swirling deformation ow test case; finally, we pass to the simulation of the guiding-center model, and compare our numerical results to those given by the Backward Semi-Lagrangian method.

In [44] we have developed the guiding-center model in polar coordinates; numerical issues/difficulties can be tackled in such a test case which thus may be viewed as a first intermediate step between a classical center guide simulation in a 2D cartesian mesh and a 4D drift kinetic simulation.

In [25] and [28], we are interested in the numerical solution of the collisionless kinetic or gyrokinetic equations of Vlasov type needed for example for many problems in plasma physics. Different numerical methods are classically used, the most used is the Particle In Cell method, but Eulerian and Semi-Lagrangian (SL) methods that use a grid of phase space are also very interesting for some applications. Rather than using a uniform

mesh of phase space which is mostly done, the structure of the solution, as a large variation of the gradients on different parts of phase space or a strong anisotropy of the solution, can sometimes be such that it is more interesting to use a more complex mesh. This is the case in particular for gyrokinetic simulations for magnetic fusion applications. We develop here a generalization of the Semi-Lagrangian method on mapped meshes. Classical Backward Semi-Lagrangian methods (BSL), Conservative Semi-Lagrangian methods based on one-dimensional splitting or Forward Semi-Lagrangian methods (FSL) have to be revisited in this case of mapped meshes. We consider here the problematic of conserving exactly some equilibrium of the distribution function, by using an adapted mapped mesh, which fits on the isolines of the Hamiltonian. This could be useful in particular for Tokamak simulations where instabilities around some equilibrium are investigated. We also consider the problem of mass conservation. In the cartesian framework, the FSL method automatically conserves the mass, as the advective and conservative form are shown to be equivalent. This does not remain true in the general curvilinear case. Numerical results are given on some gyrokinetic simulations performed with the GYSELA code and show the benefit of using a mass conservative scheme like the conservative version of the FSL scheme. Inaccurate description of the equilibrium can yield to spurious effects in gyrokinetic turbulence simulations. Also, the Vlasov solver and time integration schemes impact the conservation of physical quantities, especially in long-term simulations. Equilibrium and Vlasov solver have to be tuned in order to preserve constant states (equilibrium) and to provide good conservation property along time (mass to begin with). Several illustrative simple test cases are given to show typical spurious effects that one can observes for poor settings. We explain why Forward Semi-Lagrangian scheme bring us some benefits. Some toroidal and cylindrical GYSELA runs are shown that use FSL.

In [12] we present the Semi-Lagrangian method which is composed by essentially two ingredients : the computation of the characteristics along which the distribution function is constant and the interpolation step. We analyse high order schemes in time based on directional splitting, which are a succession of linear transport steps. We then study the Semi-Lagrangian methods in this particular case and we make the link between different formulations. We also obtain a convergence theorem for the Vlasov-Poisson system in this framework, which remains valid in the case of small displacements. We then develop this type of methods in a more general framework, by using one dimensionnal conservative splitting. We also consider a discontinuous Galerkin variant of such schemes. In a last part, we study the gyroaverage operator which appears in plasma physics by taking care of finite Larmor radius corrections. Finally, we discuss the problematic of zero discrete divergence which gives a compatibility between field computations and the numerical method of transport.

6.4. Finite Element Methods

6.4.1. Gyrokinetic quasi-neutrality equation

Participants: Nicolas Crouseilles, Eric Sonnendrücker.

In [21], a new discretization scheme of the gyrokinetic quasi-neutrality equation is proposed. We discretised the gyrokinetic Poisson equation using arbitrary order spline finite elements which enables to accommodate more complex domains. Moreover in standard polar coordinates we developed a fast solver which is comparable in computational time to the original FFT-second order finite differences, but can become more efficient for higher order as fewer grid points are needed for the same accuracy.

6.4.2. Dissipative boundary conditions for finite element codes

Participants: Philippe Helluy, Laurent Navoret, Eric Sonnendrücker.

We are developing finite-element codes for the Vlasov-Poisson system that would be able to capture the filamentation phenomenon. The filamentation is a mechanism that transfers the space fluctuations of the distribution function to high frequency oscillations in the velocity direction. For stability purpose, most numerical schemes contain dissipation that may affect the precision of the finest oscillations that could be resolved. In [60], [61], [62] Eliasson constructs a non reflecting and dissipative condition for the Fourier-transformed Vlasov-Poisson system. The condition enables the high velocity-frequency oscillations to leave the computational domain in a clean way.

We are currently developing a finite-element code based on this dissipative boundary condition. The code is part of the Selalib library. We also propose an approximation of the Eliasson method, based on the Béranger's PML formalism. Contrary to the original boudary conditions that requires a space Fourier transformation, this method is local and thus could be extended to higher dimensionnal problems and more complex geometries.

6.4.3. High order finite element methods for Maxwell

Participants: Stéphanie Salmon, Eric Sonnendrücker.

In paper [23], we study high order discretization methods for solving the Maxwell equations on hybrid triangle-quad meshes. We have developed high order finite edge element methods coupled with different high order time schemes and we compare results and efficiency for several schemes. We introduce in particular a class of simple high order low dissipation time schemes based on a modified Taylor expansion.

6.5. Waterbag models: analysis and simulations

Participant: Nicolas Besse.

In paper [33], we revisit the linear theory of kinetic flute-like modes such as ionic instabilities by using the exact geometric reduction of Vlasov equation yielded by waterbag invariants which are reminiscent to the geometric Liouville invariants. The waterbag representation of the statistical distribution function of particles can be viewed as a special class of exact weak solution of the Vlasov equation, allowing to reduce this latter into a set of hydrodynamic equations (with the complexity of a multi-fluid model) while keeping its kinetic features (Landau damping and resonant wave-particle interaction). For high toroidal-number-mode, from ballooning transformation and multi-scale WKB-type analysis, we demonstrate that one can construct eigenmode solutions of the two-dimensional integro-differential gyrowaterbag operator by solving a nested one-dimensional Fredholm-type integral equation. Qualitatively, the solution of the nested one-dimensional Fredholm-type equation is equivalent to first solving for the mode structure along the field lines locally in radius, and then constructing the two-dimensional global mode structure through a radially weighted superposition of local solutions. The radial weighted function is solution of a Schrödinger equation or a Riccati equation in the dual space. Solving the linear turning points problem and using connection formulas, the global dispersion relation arises from the WKB-type phase integral quantization condition which involves the local eigenfrequency. Finally we perform the spectral analysis of the nested one-dimensional Fredholm-type operator which constitutes a meromorphic family of compact operators and extend all the results proved for unstable eigenmodes to stable and damped ones by analytic continuation.

In paper [36], we present two new codes devoted to the study of ion temperature gradient (ITG) driven plasma turbulence in cylindrical geometry using a drift-kinetic multi-water-bag model for ion dynamics. Both codes were developed to complement the Runge-Kutta semi-lagrangian multi-water-bag code GMWB3D-SLC described in [55]. The CYLGYR code is an eigenvalue solver performing linear stability analysis from given mean radial profiles. It features three resolution schemes and three parallel velocity response models (fluid, multi-water-bag, continuous Maxwellian). The QUALIMUWABA quasi-linear code is an initial value code allowing the study of zonal flow influence on drift-waves dynamics. Cross-validation test performed between the three codes show good agreement on both temporal and spatial characteristics of unstable modes in the linear growth phase.

In paper [32], we first present the derivation of the anisotropic Lagrangian averaged gyrowaterbag continuum (LAGWBC) equations. The gyrowaterbag continuum can be viewed as a special class of exact weak solution of the Vlasov-gyrokinetic equation, allowing to reduce this latter into an infinite dimensional set of hydrodynamic equations (i.e. an infinite dimensional hyperbolic system of first-order conservation laws in several space dimensions with non-local fluxes) while keeping its kinetic features (Landau damping and nonlinear resonant wave-particle interaction). These models are very promising because they reveal to be very useful for analytical theory (such as the resolution of the eigenvalue problem for analytical description of various instabilities) and numerical simulations (when the continuum is converted into a small finite set of "fluid" or waterbag, the problem has the complexity of a multifluid model instead of a kinetic one) of laser-plasma and gyrokinetic

physics (electrostatic turbulence problem). The gyrowaterbag waterbag continuum is derived from two phase-space variable reductions of the Vlasov equation through the existence of two underlying invariants. The first one, coming from physic properties of the dynamics (the fast gyromotion of particles around magnetic field lines) is adiabatic and called the magnetic moment. The second one, named "waterbag" and coming from geometric invariance property of the phase-space, is just the direct consequence of the Liouville Theorem and is reminiscent to the geometric Liouville invariant. In order to obtain the LAGWBC equations from the gyrowaterbag continuum we use an Eulerian variational principle and Lagrangian averaging techniques. Regarding to the original gyrowaterbag continuum, the LAGWBC equations show some additional properties and several advantages from the mathematical and physical viewpoints, which make this model a good candidate for describing accurately gyrokinetic turbulence in magnetically confined plasma. In the second part of this paper we prove local in time well-posedness of an approximated version of the anisotropic LAGWBC equations, that we call the "isotropic" LAGWBC equations, by using quasilinear PDE type methods and elliptic regularity estimates for several operators.

6.6. Simulations for Vlasov-Maxwell model

Participants: Anaïs Crestetto, Philippe Helluy.

In [37] (see also [11]), we present an implementation of a Vlasov-Maxwell solver for multicore processors. The Vlasov equation describes the evolution of charged particles in an electromagnetic field, solution of the Maxwell equations. We propose to solve the Vlasov equation by a Particle-In-Cell method (PIC), while the Maxwell system is computed by a Discontinuous Galerkin method. These methods are detailed, as well as the emission law for the particles and the implementation of the boundary conditions. We use the OpenCL framework, which allows our code to run on multicore processors or recent Graphic Processing Units (GPU). The key points of the implementation on this architecture are presented. We then study several numerical applications to two-dimensional test cases in cartesian geometry. The acceleration between the computation on a CPU and on a graphic card is very high, especially for the Maxwell part.

We have started a new software project called CLAC (for "Conservation Laws Approximation on many Cores"). This a 3D Discontinuous Galerkin solver, which runs on cluster of GPU's, thanks to the OpenCL environment and the MPI library. CLAC is open source and developed in collaboration with the AxesSim company, a SME near Strasbourg. For the moment, it is applied to the Maxwell equations. But we plan to apply it to the MHD equations or mixed kinetic/fluid plasma models.

6.7. Free-streaming ELM formulae vs. Vlasov simulations

Participants: Sever Hirstoaga, Giovanni Manfredi.

One of the main challenges for future tokamak operation, such as ITER, is constituted by the large heat load on the divertor plates. The divertor surfaces are constantly bombarded with high-energy particles and may see their lifetime considerably reduced. The intensity of the particles and energy fluxes is particularly high during transient events known as edge-localised modes (ELMs). Our purpose here is to propose and investigate a kinetic model for ELMs.

The free-streaming model [69] is a simple analytical model for ELM transport in the scrape-off layer (SOL) of a tokamak. It is a force-free Vlasov equation with a source term for the ions distribution function (the Coulomb forces are ignored). Even though this model reproduces with good accuracy some of the main features of an ELM signal, it has two main drawbacks: (i) the self-consistent electric potential is not accounted for and (ii) only solutions for the ion distribution are considered.

In this contribution [24] we propose a set of modified free-streaming equations in order to overcome the above drawbacks. More precisely, some hypotheses on the Maxwellian initial condition lead to a model that includes the self-consistent electric potential. Assuming quasinetrality and using energy conservation we could derive analytical formulae for the electron quantities. This augmented free-streaming model was benchmarked to the Vlasov-Poisson simulations reported in [78]. The match is encouragingly good, thus justifying the applicability of the free-streaming approach.

Finally, from a computational point of view, transport in the SOL was studied by means of three different approaches – fluid, Vlasov and particle-in-cell (PIC). In spite of kinetic effects due to fast electrons which are not captured in the fluid code, the overall agreement between the codes was found to be quite satisfactory [22].

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

Participants: Pierre Bertrand, Takashi Hattori, Simon Labrunie, Jean Rodolphe Roche.

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

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

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

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

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

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

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

During 2012 we have developed a domain decomposition method and a new behavior of the plasma density was considered in the code "FullWaveFEM". A analyze of the model considered, existence and unicity of solution, equivalence of the formulation for the domain decomposition formulation was completed in the frame of Takashi Hattori Phd thesis.

6.9. Nearby fields to plasma physics

6.9.1. Neutrino transport in supernova

Participant: Emmanuel Frénod.

In [31] we give an introduction to the Boltzmann equation for neutrino transport used in core collapse supernova models as well as a detailed mathematical description of the Isotropic Diusion Source Approximation (IDSA). Furthermore, we present a numerical treatment of a reduced Boltzmann model problem based on time splitting and finite volumes and revise the discretization of the IDSA for this problem. Discretization error studies carried out on the reduced Boltzmann model problem and on the IDSA show that the errors are of order one in both cases. By a numerical example, a detailed comparison of the reduced model and the IDSA is carried out and interpreted. For this example the IDSA modeling error with respect to the reduced Boltzmann model is numerically determined and localized.

In [30] we present Chapman–Enskog and Hilbert expansions applied to the O(v/c) Boltzmann equation for the radiative transfer of neutrinos in core collapse supernovae. Based on the Legendre expansion of the scattering kernel for the collision integral truncated after the second term, we derive the diffusion limit for the Boltzmann equation by truncation of Chapman–Enskog or Hilbert expansions with reaction and collision scaling. We also give asymptotically sharp results obtained by the use of an additional time scaling. The diffusion limit determines the diffusion source in the Isotropic Diffusion Source Approximation (IDSA) of Boltzmann's equation for which the free streaming limit and the reaction limit serve as limiters. Here, we derive the reaction limit as well as the free streaming limit by truncation of Chapman–Enskog or Hilbert expansions using reaction and collision scaling as well as time scaling, respectively. Finally, we motivate why limiters are a good choice for the definition of the source term in the IDSA.

6.9.2. Inverse problem governed by Maxwell equations

Participant: Jean Rodolphe Roche.

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

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

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

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

In a previous work we studied the inverse electromagnetic casting problem considering the case where the inductors are made of single solid-core wires with a negligible area of the cross-section. In a second paper we considered the more realistic case where each inductor is a set of bundled insulated strands. In both cases the number of inductors was fixed in advance, see [18]. In this year we aim to overcome this constraint, and look for configurations of inductors considering different topologies with the purpose of obtaining better results. In order to manage this new situation we introduce a new formulation for the inverse problem using a shape functional based on the Kohn-Vogelius criterion. A topology optimization procedure is defined by means of topological derivatives, a new method that simplifies computation issues was considered, see [35] and [29].

CAMUS Team

6. New Results

6.1. VMAD

Participants: Alexandra Jimborean, Philippe Clauss, Jean-François Dollinger, Aravind Sukumaran-Rajam, Juan Manuel Martinez Caamaño, Vincent Loechner.

The goal of the VMAD 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.

VMAD contains 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 templates, and callbacks to the runtime system. External modules associated to specific analyses and transformations are dynamically loaded when required at runtime. Dynamic information, such as memory locations of the modules entries, are patched at startup in the loaded executable.

VMAD uses sampling and multi-versioning to limit the runtime overhead (profiling, analysis, and code generation). At runtime, targeted codes are launched by successive chunks that can be either original, instrumented or optimized/parallelized versions. After each chunk execution, decisions can be taken relatively to the current optimization strategy. VMAD is handling advanced memory access profiling [17] through linear interpolation of the addresses, dynamic dependence analysis, version selection [17] and speculative polyhedral parallelization [19], [16].

Alexandra Jimborean defended her PhD thesis on this topic in 2012 [12]. In 2012, Aravind Sukumaran-Rajam started a PhD in our team to continue this work, especially on extending the dependence analysis to make it handle more general programs, keeping it fast and accurate. Jean-François Dollinger will extend the framework to handle heterogeneous architectures (GPGPUs). Juan Manuel Martinez Caamaño, a master student of University of Buenos Aires (associate team EA-Ancome) is also working on VMAD to make the code generation support tiling.

6.2. The Multifor programming construct

Participants: Philippe Clauss, Imèn Fassi, Yosr Slama, Matthieu Kuhn.

We have proposed a new programming control structure called “multifor”, allowing to take advantage of parallelization models that were not naturally attainable with the polytope model before. In a multifor-loop, several loops whose bodies are run simultaneously can be defined. Respective iteration domains are mapped onto each other according to a run frequency – the grain – and a relative position – the offset –. Execution models like dataflow, stencil computations or MapReduce can be represented onto one referential iteration domain, while still exhibiting traditional polyhedral code analysis and transformation opportunities. Moreover, this construct provides ways to naturally exploit hybrid parallelization models, thus significantly improving parallelization opportunities in the multicore era. Traditional polyhedral software tools are used to generate the corresponding code. Additionally, a promising perspective related to non-linear mapping of iteration spaces has also been developed, yielding to run a loop nest inside any other one by solving the problem of inverting “ranking Ehrhart polynomials”.

This work is the PhD work of Imèn Fassi, who started her work this year and who is co-advised by Yosr Slama, Assistant Professor at the University El Manar in Tunis, Tunisia, and Philippe Clauss. A first publication of this topic has been accepted at the IMPACT workshop that will be held in conjunction with the HIPEAC conference in Berlin, Germany, January 2013.

6.3. Parwiz: dynamic data dependence analysis

Participants: Alain Ketterlin, Philippe Clauss.

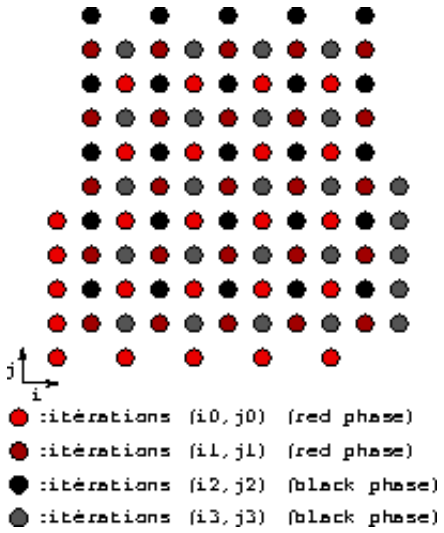

Figure 3. Red-Black Gauss-Seidel Multifor Iteration Space

We have continued working on dynamic data-dependence analysis during this year, especially on increasing the scope of our tool (called Parwiz). For instance, Parwiz is now able to suggest several program transformations (like loop distribution) that enable loop vectorization. It uses an algorithm known as *codegen* (developed by Allen & Kennedy), but the novelty is that it applies the algorithm to dependence graphs that are built empirically, by running the program on selected input data sets. As far as we know, Parwiz is the first tool able to suggest loop transformations.

We have also developed several other empirical analysis. One of these focuses on loops that are not parallel, but whose iterations present significant parallelism provided the program explicitly schedules the various iterations. This still lacks a suitable cost model to estimate the potential gain, but gives significant insight into the behavior of a given non-parallel loop.

This work has been presented at the MICRO-45 conference held in Vancouver on december 1–5 2012 [18].

6.4. Modeling the behavior of parallel traces

Participants: Alain Ketterlin, Stéphane Genaud.

We have started this year a project aiming at developing algorithms and tools to capture the behavior of parallel programs. Our initial goal is automatically obtain formal models of communicating MPI processes, in terms of message sends and receives and of synchronization events. Such models have various uses, the first of them being the visualization of the system's communications, for debugging, or plain understanding (see below, Figure 4). However, we expect to develop other applications, for example in optimizing the communication infrastructure (or routing algorithm) for specific applications.

Our modeling algorithm works in two phases. The first phase is local to each node, using our work on nested loop recognition [7]. This builds a sequence of loop nests providing a compact representation of all local communication events. At the end of the run, the various local models are merged, typically through a parallel reduction operation, to build the global model.

We plan to publish the first part of this work in the first half of 2013. Several experimental data have been collected already, but we would like to evaluate the overall task on significantly sized programs.

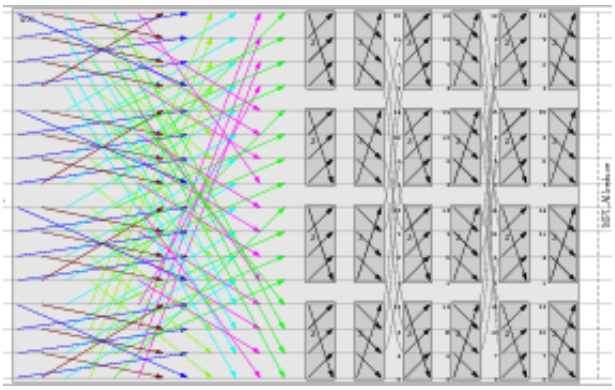

Figure 4. Visualizing parallel traces

Currently, the whole process is restricted to communication events. However, it can be immediately extended to trace including other kinds of events, like the addresses and sizes of memory buffers transmitted from process to process. This would provide a complete, run time description of the program, which could be used to evaluate the potential gain of various re-parallelization techniques. This aspect is the next goal on our agenda.

6.5. Certified polyhedral transformations into more and more concrete languages

Participants: Nicolas Magaud, Julien Narboux, Éric Violard.

We continued our work to complete the proof of polyhedral based transformations in the language *Loops* designed by Alexandre Pilkiewicz (see the proof scheme on Fig. 5). Our idea is to use once again a validator. The validation here consists in comparing two polyhedrons: the one (**pprogopt**) obtained from the non-optimized Loops program (**prog**), by translation to the polyhedral language (*Plang*) (**pprog**), and then optimization in *Plang*; and the one (**interprogopt**) obtained from the optimized Loops program (**progopt**) by translation into *Plang*. If these two polyhedrons are the same, then the validator returns true, otherwise it returns false. The proof that the non-optimized and optimized programs have the same behaviour lies on the deterministic property of the function that translates a program *Loops* into *Plang*. We obtained the proof in Coq that our scheme is correct. Now, we have to complete the implementation of our optimizing compiler for *Loops* by connecting our validator with the off the shell tools for polyhedral transformations. We will use the tool PLuTo[10] to find efficient code transformations and CLooG[11] to generate the loops from the polyhedral representation (we proposed an internship for this purpose).

We now have to connect the language *Loops* with more concrete languages (whose features and semantics have to be defined). We already showed how to deal with arithmetic overflows in a more concrete language where each loop variable is a machine integer [20]. Our approach is thus to incrementally add concrete features until joining an intermediate language of CompCert.

Since the members of our team have some skill in defining new languages and their semantics, we thought that it could be a good idea to exploit this and to define a formal semantics for the **Multifor** syntactic sugar proposed by Philippe Clauss. We aims at associating a rigorous mathematical meaning with this syntactic construct: first a denotational semantics and then an operational one. This work will serve as a base to prove correct the compilation process that translates this construct into intermediate code.

[10] http://pluto-compiler.sourceforge.net/
[11] http://www.cloog.org/

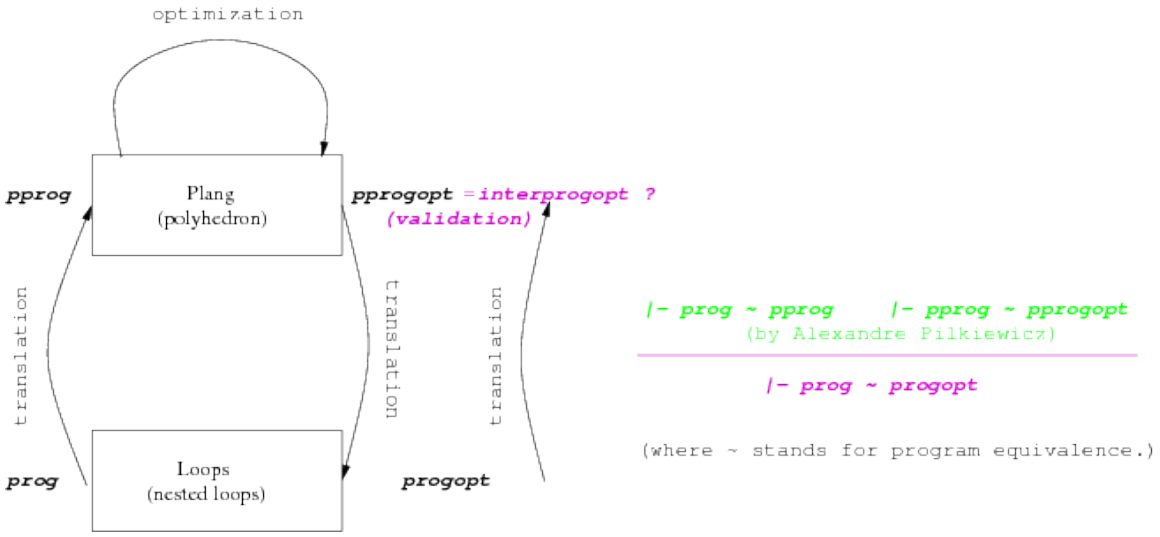

Figure 5. Our proof scheme for a certified compiler of Loops

CARAMEL Project-Team

6. New Results

6.1. Sieve for FFS

Participants: Jérémie Detrey, Pierrick Gaudry [contact], Marion Videau.

Jérémie Detrey, Pierrick Gaudry and Marion Videau have worked on the relation collection step of the Function Field Sieve and especially on its implementation. This is still an ongoing work but the first results have been accepted for publication [13] in the ARITH-2013 conference.

6.2. Bilinear Maps

Participants: Răzvan Bărbulescu, Jérémie Detrey, Nicolas Estibals, Paul Zimmermann [contact].

As a result of an internal working group in the team, we have found and published at the WAIFI conference a new algorithm to find optimal formulae for bilinear maps [8]. This algorithm enables one to rediscover Karatsuba's multiplication algorithm, but has many other applications, for example to matrix multiplication.

6.3. Number Field Sieve

Participants: Emmanuel Thomé, Paul Zimmermann [contact].

Together with Shi Bai (Australian National University), E. Thomé and P. Zimmermann used CADO-NFS to factor RSA-704, a 212-digit number, to check scalability of the software on large factorizations [10]. This is the second largest number factored by any GNFS software so far, and the largest one factored by CADO-NFS. This experiment was very helpful, since it demonstrated several weaknesses of the code, that have been addressed since then.

Together with Shi Bai (Australian National University), P. Zimmermann wrote a preprint describing the algorithm used in CADO-NFS for the size-optimization of sextic polynomials [11].

Alain Filbois, Shi Bai (Australian National University) and P. Zimmermann improved the polynomial selection code. With parameters used to find good polynomials for RSA-896, a total speedup by a factor 14 was obtained, with both algorithmic and implementation improvements.

6.4. Sparse linear algebra modulo p

Participants: Hamza Jeljeli, Emmanuel Thomé [contact].

The resolution of linear algebra problems with subexponential methods, which is the topic of the ANR-CATREL project (to begin in 2013) calls for the resolution of large sparse linear systems defined over finite fields. In preparation for this, H. Jeljeli has developed software for performing sparse matrix times vector multiplication on NVIDIA GPUS [16]. This code provides a very significant speedup over the use of CPUs for this task, and achieves this speedup by a clever use of a "residue number system" representation of the finite field elements.

As a complement, a recent re-implementation of Thomé's algorithm for the (matrix) Berlekamp-Massey step in the block Wiedemann algorithm has been done. This program can of course be special-cased to the simple non-matrix case. The GPU code above and this special case, together, form the needed software to have a sparse linear system solver over finite fields using Wiedemann's algorithm. This has been put to use, and led to the completion of a discrete logarithm record in $\mathbb{F}_{2^{619}}$, the linear system part taking only 17 hours in total on one GPU (plus 1 hour on one CPU for the Berlekamp-Massey step).

6.5. Using symmetries in elliptic curve discrete logarithm

Participant: Pierrick Gaudry.

In a joint work by Jean-Charles Faugère, Pierrick Gaudry, Louise Huot and Guénaël Renault, it has been shown that the geometric symmetries of an elliptic curve, in particular, the symmetries of an Edwards curve, could be used to speed up the index calculus attack for computing discrete logarithms in an elliptic curve defined over an extension field. The corresponding article [14] is currently under revision.

6.6. Galois properties of curves for ECM

Participants: Răzvan Bărbulescu, Cyril Bouvier.

In collaboration with Joppe Bos, Peter Montgomery and Thorsten Kleinjung, Răzvan Bărbulescu and Cyril Bouvier proved some divisibility properties of the group order of an elliptic curve, using the Galois structure of its division polynomial. It explains the good behaviour of some curves that have been experimentally found to factor more numbers than others, and gives a way to find new curves with this property. The corresponding article [7] was presented in ANTS-X.

6.7. Computation of CM class polynomials for genus 2 Jacobians

Participants: Sorina Ionica, Emmanuel Thomé [contact].

In collaboration with Andreas Enge, Emmanuel Thomé has developed software for computing class polynomials, in the context of complex multiplication theory in genus 2. The current computations set new records which are well above the previous state of the art. A publication is in the works.

Using similar underlying tools and theory, and based on work by Sorina Ionica [15], Sorina Ionica and Emmanuel Thomé have worked on the analysis of isogeny graphs in genus 2, when certain properties of the endomorphism ring are satisfied.

6.8. Filtering step for NFS and FFS

Participant: Cyril Bouvier.

Cyril Bouvier studied the filtering step for the Number Field Sieve. A better weight function, used during the clique removal step, was found which allows to construct smaller matrices for the linear algebra step. A preprint is avalaible [12]. The filtering step for the Function Field Sieve was written in CADO-NFS.

CARTE Project-Team

6. New Results

6.1. Dynamical systems

Participant: Mathieu Hoyrup.

Birkhoff theorem is a central result in ergodic theory. Consider a dynamical system $(X, T : X \to X)$, start with an initial condition $x \in X$ and construct the trajectory $(x, T(x), T^2(x), ...)$. How is this trajectory distributed in X? What is the limit frequency of visits of a set $A \subseteq X$? Ergodic theorems answer to these questions by showing (i) that the distribution of *almost every* point converges and (ii) by describing the possible distributions associated to trajectories.

For several years we have been working on the project of identifying the exact computational content of several ergodic theorems: can the speed of convergence of limit frequencies be computed? Can one distinguish between points with different limit frequencies? Can we construct (compute) points whose trajectory follow a prescribed distribution? How random (i.e. incompressible) a point has to be for the distribution of its trajectory to converge?

6.1.1. Limit frequencies

We have obtained new insight in the above questions by proving that random elements eventually reach effective closed sets of positive measure (while it was only known for a more restricted class of sets). The paper appeared in *Information and Computation* [11]. This result is a key tool in the proof of the result published in [23].

6.1.2. Information

A chaotic system is unpredictable because it has much more trajectories than observable initial conditions: hence many undistinguishable initial points lead to radically different trajectories. As there are many trajectories, most of them are complex in the sense that they can hardly be compressed, i.e. described in a shorter way than simply listing them. The Shannon-McMilan-Breiman theorem states that the compression-rate of most trajectories coincides with the entropy of the system.

We have been interested in the computational content of this theorem: how random a point has to be to generate a trajectory whose compression rate is the entropy? This question was raised in [71] and has been left open for 14 years. We have solved the problem by showing that Martin-Löf notion of randomness is sufficient. Our recent result presented in [11]is a key ingredient of our proof. We presented the result at *STACS* [23].

6.1.3. Decomposition

The ergodic decomposition theorem states that a dynamical system can always be uniquely decomposed into indecomposable subsystems, technically *ergodic* subsystems. We have been interested in the computability of the decomposition operation. It is known from [71] that this operation is not computable in general. Whether this operation is still not computable when the system can be decomposed into a *finite* number of subsystems was open. We raised the question and answer it negatively in [57]. More precisely, we prove the existence of ergodic measures P and Q such that neither P nor Q is computable relative to $P + Q$. In other words, the operation of splitting a non-ergodic process into ergodic components is not computable, even in the trivial case of a combination of 2 ergodic processes. The paper is currently in press and will appear in *Annals of Pure and Applied Logic* [14].

6.2. Computations

Participant: Mathieu Hoyrup.

6.2.1. Inversion of computable functions

We strengthen the preceding result by making P and Q computable. This result is a particular case of a more general problem. In many situations an operator $F \to Y$ can be computed but can hardly be reversed: given $F(x)$, x cannot always we recovered (computed) even when F is one-to-one. We introduce a strong notion of discontinuity for the inverse of F and prove that it entails the existence of a non-computable $x \in X$ such that $F(x)$ is computable. Our result on the ergodic decomposition can be derived by applying our general result to the operator $F(P, Q) = P + Q$ which is computable but difficult to reverse. At the same time we prove a significant improvement of a classical result of Pour-El and Richards [67] about the computability of linear operators. The paper [26] is currently submitted.

6.2.2. Computability and measure theory.

We study the constructive content of the Radon-Nikodym theorem, show that it is not computable in general and precisely locate its non-computability in the Weihrauch lattice. The paper [15] appeared in the first issue of the new journal *Computability*.

6.3. Computer virology

6.3.1. Behavioral analysis

Participants: Isabelle Gnaedig, Jean-Yves Marion.

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

We had previously proposed to abstract trace automata by rewriting them with respect to a set of predefined behavior patterns defined as a regular language described by a string rewriting system [32]. We then have increased the power of our approach on two aspects. We fist have modified the abstraction mechanism, keeping the abstracted patterns in the rewritten traces, which allows us to handle interleaved patterns. Second, we have extended the rewriting framework to express data constraints on action parameters by using term rewriting systems. An important consequence is that, unlike in [32], using the data-flow, we can now detect information leaks in order to prevent unauthorized disclosure or modifications of information.

We also have introduced model checking in our approach: the predefined behavior patterns, used to abstract program traces, have been defined by first order temporal logic formulas, as well as the reference suspicious behaviors, given in a signature. The infection problem can then be seen as the satisfaction problem of the formula of the signature by an abstracted trace of the program, which can be checked using existing model checking techniques. This work has been published at the ESORICS conference [20].

6.3.2. Analyzing cryptographic implementations

Participants: Joan Calvet, Jean-Yves Marion.

Analyzing cryptographic implementations has important applications, especially for malware analysis where they are an integral part both of the malware payload and the unpacking code that decrypts this payload. These implementations are often based on well-known cryptographic functions, whose description is publicly available. While potentially very useful for malware analysis, the identification of such cryptographic primitives is made difficult by the fact that they are usually obfuscated. Current state-of-the-art identification tools are ineffective due to the absence of easily identifiable static features in obfuscated code. However, these implementations still maintain the input-output (I/O) relationship of the original function. In a joint work with José M. Fernandez published in [22], we present a tool that leverages this fact to identify cryptographic functions in obfuscated programs, by retrieving their I/O parameters in an implementation-independent fashion, and comparing them with those of known cryptographic functions. In experimental evaluation, we successfully

identified the cryptographic functions TEA, RC4, AES and MD5 in obfuscated programs. In addition, our tool was able to recognize basic operations done in asymmetric ciphers such as RSA.

6.3.3. Self-replication

Participant: Jean-Yves Marion.

Self-replication is one of the fundamental aspects of computing where a program or a system may duplicate, evolve and mutate. Our point of view is that Kleene's (second) recursion theorem is essential to understand self-replication mechanisms. An interesting example of self-replication codes is given by computer viruses. This was initially explained in the seminal works of Cohen and of Adleman in the eighties. In fact, the different variants of recursion theorems provide and explain constructions of self-replicating codes and, as a result, of various classes of malware. None of the results are new from the point of view of computability theory. We just propose a self-modifying register machine as a model of computation in which we can effectively deal with self-reproduction and in which new offsprings can be activated as independent organisms. This work was published by Jean-Yves Marion in a special issue on the honor of Alan Turing [16].

6.3.4. Reverse engineering by morphological analysis

Participants: Guillaume Bonfante, Jean-Yves Marion, Fabrice Sabatier, Aurélien Thierry.

Let us suppose we are given some malware and we want to know what it is doing. One may run it, or one may analyze it more or less statically. Typically, an expert tries to guess the behavior of a malware through the analysis of its binary code (in tools such as Ida). The task is much simpler if the expert already knows some part of the code. We have shown that morphological analysis could be used in such a context. We have rediscovered the parts of the malware `Duqu` within `Stuxnet`. We have rediscovered the compilation options used to include OpenSSL's functions within `Waledac` [21].

CASSIS Project-Team

6. New Results

6.1. Automated Deduction

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

6.1.1. Building and verifying decision procedures

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

We have developed a methodology to build decision procedures by using superposition calculi which are at the core of equational theorem provers. We are interested in developing automated deduction techniques to prove properties about these superposition-based decision procedures. To this aim, we plan to further investigate the use of schematic superposition, which has been already applied to check the termination and the combinability of superposition-based procedures. We have been working on the development of a framework for specifying and verifying superposition-based procedures. In [52], we present an implementation in Maude of the two inference systems corresponding to superposition and schematic superposition. Thanks to this implementation we automatically derive termination of superposition for a couple of theories of interest in verification.

Until now, schematic superposition was only studied for standard superposition. In [62], we introduce a schematic superposition calculus modulo a fragment of arithmetics, namely the theory of Integer Offsets. This new schematic calculus is used to prove the decidability of the satisfiability problem for some theories extending Integer Offsets. We illustrate our theoretical contribution on theories representing extensions of classical data structures, e.g., lists and records. Our Maude-based implementation has been extended to incorporate this new schematic superposition calculus modulo Integer Offsets. It enables automatic decidability proofs for theories of practical use.

6.2. Security Protocol Verification

The design of cryptographic protocols is error-prone. Without a careful analysis, subtle flaws may be discovered several years after the publication of a protocol, yielding potential harmful attacks. In this context, formal methods have proved their interest for obtaining good security guarantees. Many analysis techniques have been proposed in the literature [72]. We have edited a book [65] where each chapter presents an important and now standard analysis technique. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees.

6.2.1. Equational theories of cryptographic primitives

Participant: Michaël Rusinowitch.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [76], we provide a list of such properties and attacks as well as existing formal approaches for analyzing cryptographic protocols under algebraic properties.

Encryption "distributing over pairs" is employed in several cryptographic protocols. We have shown that unification is decidable for an equational theory HE specifying such an encryption [15]. We model block chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element and present in [27] an algorithm for deciding the unification problem modulo this rewrite system. Potential applications of this unification procedure include flaw detection for protocols employing the CBC encryption mode. We have also studied a very simple property satisfied by the RSA-based implementation of the *blind signature scheme* and we have shown its unification problem is undecidable [28]. It is the simplest theory, to our knowledge, for which unification is undecidable.

In their seminal work Dolev and Yao used string rewriting to check protocol security against an active intruder. The main technical result and algorithm were improved by Book and Otto who formulated the security check in terms of an extended word problem for cancellation rules. We extend in [16] their main decidability result to a larger class of string rewrite systems called opt-monadic systems.

6.2.2. Voting protocols

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

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

- Helios is an open-source web-based end-to-end verifiable electronic voting system, used e.g. by UCL and the IACR association in real elections. We have discovered a vulnerability which allows an adversary to compromise the privacy of voters and we have presented a fixed version, showed to satisfy a formal definition of ballot secrecy using the applied pi calculus [21]. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We are now working on defining a variant of Helios that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authorities that provides credentials that the ballot box can verify but not forge. This new version is under implementation and we are proving computational security for both ballot secrecy (inherited from Helios) and full verifiability (due to our credentials).
- Norway has used e-voting in its last political election in September 2011, with more than 25 000 voters using the e-voting option. Using formal models, we have analyzed the underlying protocol w.r.t. privacy, considering several corruption scenarios [41].
- The Section 07 of CNRS (now split into Section 06 and Section 07) has proposed a voting protocol for Face-to-Face meetings to enhanced the verifiability of an election run through electronic devices. We have formally modeled this protocol and proved both ballot secrecy and verifiability.

Even a basic property like ballot secrecy is difficult to define formally and several definitions co-exist. The loss of privacy may not only come from the protocol but also from the tally function itself and depends on what needs to be kept private. We have proposed a general and quantitative definition of privacy, that captures two previously proposed definitions [35]. Security based on cryptography relies on the fact that certain operations (such as decrypting) are computationally infeasible. However, e-voting protocols should also guarantee privacy in the future, when computers will have an increased computational power and will be able e.g. to break nowadays keys. Such privacy in the future is called *everlasting privacy* and we have proposed a definition of *practical everlasting privacy*.

6.2.3. Other families of protocols

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

Securing routing Protocols. The goal of routing protocols is to construct valid routes between distant nodes in the network. If no security is used, it is possible for an attacker to disorganize the network by maliciously interacting with the routing protocols, yielding invalid routes to be built. That is why secure versions of routing protocols are now developed. The security model differs from standard protocols since the adversary can only control some nodes of the network. The security of a routing protocols therefore depends on the network topology. In [39], we show a simple reduction result: if there is an attack then there is an attack in a four nodes topology. It is therefore sufficient to study security for a finite number of distinct topologies, allowing to reuse existing tools such as ProVerif.

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 previously designed a generic API for key-management based on key hierarchy [77]. In [40], [60], we have extended our API to handle key-revocation such that the security tokens can still be used (it is not necessary to revoke the full token) and such that any key can be revoked (even upper keys in the hierarchy). In [64], we propose a universally composable key management functionality and show how to achieve a secure, distributed implementation on TRDs.

6.2.4. Automated verification of indistinguishability properties.

Participants: 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.

Static case. The YAPA tool [17] can check static equivalence for convergent equational theories. It is proved to terminate for a wide class of equational theories that includes subterm convergent theories (e.g. encryption, signatures, pairing and hash) and layered convergent theories (e.g. blind signatures). The procedure is generic in the sense that it remains sound and complete (but may not terminate) for any convergent theory. It has been implemented in the YAPA tool[3]. The KISS tool [19] is also able to verify static equivalence for convergent equational theories. Termination has been shown for subterm convergent equational theories (a subset of layered convergent theories) as well as several equational theories motivated by electronic voting protocols such as blind signatures and trap-door commitment schemes (which are out of the scope of YAPA).

In [20], we show how to *combine* decision procedures: if static equivalence and deduction are decidable for two disjoint equational theories then they are decidable for the union of the theories. In [25] we develop a method that allows us in some cases to simplify the task of deciding static equivalence in a multi-sorted setting, by removing a symbol from the term signature and reducing the problem to several simpler equational theories. We illustrate our technique at hand of bilinear pairings.

Active case. In [36] we present a novel procedure to verify equivalence properties for a bounded number of sessions which is able to handle a large class of equational theories. Although, we were unable to prove termination of the resolution procedure, the procedure has been implemented in a prototype tool and has been effectively tested on examples. We were able to verify properties such as guessing attacks in password protocols, strong flavors of confidentiality and anonymity properties, including fully automated checking of anonymity of an electronic voting protocol by Fujioka et al. which was outside the scope of existing tools.

In [42] we study this equivalence problem when cryptographic primitives are modeled using a group equational theory, a special case of monoidal equational theories. We reduce the problem to solving systems of equations over rings and provide several new decidability and complexity results, notably for equational theories which have applications in security protocols, such as exclusive or and Abelian groups which may additionally admit a unary, homomorphic symbol.

Rémy Chrétien has recently started a PhD on deciding trace equivalence for an unbounded number of sessions. His first findings show that for some classes of protocols, decidability of trace equivalence can be reduced to equivalence of deterministic pushdown automata (which is decidable [81]).

Note that for simple processes without branch nor replication observational equivalence can be reduced to checking whether two symbolic constraints (representing honest agents) are equivalent [75]. We have published a new proof that symbolic constraints equivalence is decidable for the large class of subterm convergent theories [18].

[3] http://www.lsv.ens-cachan.fr/~baudet/yapa/

6.2.5. Soundness of the Dolev-Yao Model

Participants: Véronique Cortier, Guillaume Scerri.

All the previous results rely on symbolic models of protocol executions in which cryptographic primitives are abstracted by symbolic expressions. This approach enables significantly simple and often automated proofs. However, the guarantees that it offers have been quite unclear compared to cryptographic models that consider issues of complexity and probability. A 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.

Existing soundness results for symmetric encryption are not satisfactory. This is due to the fact that dishonest keys may introduce many behaviors that cannot be easily captured in symbolic models. Guillaume Scerri has started a PhD thesis on designing more flexible symbolic models for cryptographic proofs. His first result is a computationally sound symbolic model in the presence of dishonestly generated keys, allowing a symbolic adversary to generate new equalities between terms, on-the-fly [38].

6.3. Model-based Verification

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

6.3.1. Algorithms for Tree Walking Automata

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

Tree walking automata are widely used to tackle data base algorithmic problems, particularly to analyse queries over XML documents. The emptiness problem for tree walking automata is known to be EXPTIME-complete. The general algorithm to solve this problem consists in transforming the tree walking automaton into a classical top-down tree automaton. The best known in the literature algorithm works in time $O(s2^{n^2})$ where n is the number of states of the tree walking automaton, and s is the size of the alphabet. In [24] we have proposed a new algorithm based on an *overloop* concept and working in time $O(2^{n^2})$. Then our approach has been improved for deterministic tree walking automata to have in this case a $O(2^{n \log n})$ time complexity. Finally, we have also proposed a polynomial-time approximation based semi-algorithm for the emptiness problem. The algorithms have been implemented and experimental results confirm the relevance of the approach.

6.3.2. Algorithms for Tree Automata with Global Constraints

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

Extending tree automata models to be able to compare different tree branches is an important and challening issue for systems' modeling and for verifying their properties. Several exetensions have been proposed in the litterature. Among them we are interested in the model of Tree Automata with Global Constraints (TAGED) introduced in 2009. The membership problem for this new model is known to be NP-complete, and the emptyness problem is known to be EXPTIME-complete. In [47] we have investigated some complexity results for tree automata with a bounded number of equality constraints. We have proved that with a unique constraint the emptyness problem is in PTIME and that it is EXPTIME-complete with only two constraints. For a bounded number of constraints, the membership problem is in PTIME.

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

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

In the regular model-checking framework, reachability analysis can be guided by temporal logic properties, for instance to achieve the counter example guided abstraction refinement (CEGAR) objectives. A way to perform this analysis is to translate a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and then to generate semi-decision procedures based on (approximations of) the rewrite proposition. In [46] we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and we have proposed a general scheme providing exact results for a fragment of LTL corresponding mainly to safety formulæ, and approximations for a larger fragment.

6.3.4. Rewriting-based Mathematical Model Transformations

Participants: Walid Belkhir, Alain Giorgetti.

We have pursued our collaboration 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) to automatically generate asymptotic models of large arrays of micro- and nanosystems. The goal is to provide engineers with an implementation of this mathematical tool inside a modeling software. We follow therefore a multidisciplinary approach which combines a generalization and formalization effort of mathematical asymptotic methods, together with rewriting-based formal transformation techniques. This approach is described in [53], together with an example and a presentation of the architecture of the software under design. A second contribution [34] is a detailed formal specification and analysis of lazy pattern-matching mechanism modulo associativity and commutativity, and its integration into a strategy language. The pattern-matching solutions are stored in a lazy list composed of a first substitution at the head and a non-evaluated object that encodes the remaining computations. Rule and strategy applications also produce a lazy list of terms. This contribution has been published in EPTCS as the proceedings of the 10th International Workshop on Reduction Strategies in Rewriting and Programming, where a lighter version was presented in 2011 [69].

6.4. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test. The test generation uses various underlying techniques such as symbolic animation of models [22] or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.4.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Elizabeta Fourneret, Jean-Marie Gauthier, Jonathan Lasalle.

We have introduced an original model-based testing approach that takes a behavioural view (modelled in UML) of the system under testing and automatically generates test cases and executable test scripts according to model coverage criteria. We continue to extended this result to SysML specifications for validating embedded systems [26]. To allow the test generation from SysML model, we study the transformation into a low level language more close of hardware in [44].

In the context of software evolution, we have worked on exploiting the evolution of requirements in order to classify test sequences, and precisely target the parts of the system impacted by this evolution. We have proposed to define the life cycle of a test via three test classes: (i) Regression, used to validate that unimpacted parts of the system did not change, (ii) Evolution, used to validate that impacted parts of the system correctly evolved, and (iii) Stagnation, used to validate that impacted parts of the system did actually evolve. The associated algorithms are under implementation in a dedicated prototype to be used in the SecureChange european project. A link with the security model proof has been started with partners of the project in [54] that allows to generate test needs associated to security properties verified on model.

6.4.2. Scenario-Based Verification and Validation

Participants: Fabrice Bouquet, Kalou Cabrera, Frédéric Dadeau, Elizabeta Fourneret.

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

We have designed a scenario based testing language for UML/OCL that can be either connected to a model animation engine or to a symbolic animation engine, based on a set-theoretical constraint solver [22]. In the context of the ANR TASCCC project, we are investigating the automation of test generation from Security Functional Requirements (SFR), as defined in the Common Criteria terminology. SFRs represent security functions that have to be assessed during the validation phase of security products (in the project, the Global Platform, an operating system for latest-generation smart cards). To achieve that, we are working on the definition of description patterns for security properties, to which a given set of SFRs can be related. These properties are used to automatically generate test scenarios that produce model based test cases. The traceability, ensured all along the testing process, makes it possible to provide evidences of the coverage of the SFR by the tests, required by the Common Criteria to reach the highest Evaluation Assurance Levels.

We have proposed a dedicated formalism to express test properties. A test property is first translated into a finite state automaton which describes a monitor of its behaviors. We have proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property.

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

6.4.3. *Mutation-based Testing of Security Protocols*

Participants: Frédéric Dadeau, Pierre-Cyrille Héam.

Verification of security protocols models is an important issue. Nevertheless, the verification reasons on a model of the protocol, and does not consider its concrete implementation. While representing a safe model, the protocol may be incorrectly implemented, leading to security flaws when it is deployed. We have proposed a model-based penetration testing approach for security protocols [9]. This technique relies on the use of mutations of an original protocol, proved to be correct, for injecting realistic errors that may occur during the protocol implementation (e.g. re-use of existing keys, partial checking of received messages, incorrect formatting of sent messages, use of exponential/xor encryption, etc.). Mutations that lead to security flaws are used to build test cases, which are defined as a sequence of messages representing the behavior of the intruder. We have applied our technique on protocols designed in HLPSL, and implemented a protocol mutation tool that performs the mutations. The mutants are then analyzed by the CL-Atse [82] front-end of the AVISPA toolset [66]. Experiments show the relevance of the proposed mutation operators and the efficiency of the CL-Atse tool to conclude on the vulnerability of a protocol and produce an attack trace that can be used as a test case for implementations.

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

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

In collaboration with the CEA we enhance the innovative verification technique SANTE (Static ANalysis and TEsting), combining value analysis, program slicing and test generation, with two novel, optimized and adaptive strategies of program slicing based on threat dependencies [37]. We study the properties of threat dependencies, introduce the notion of slicing-induced cover, and prove the underlying theoretical results. Compared to a basic usage of program slicing, our advanced strategies need only quadratic additional work in order to optimize the calls of costly dynamic analysis. We give a detailed evaluation of all slicing strategies and compare them with one another.

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 [43] based on various strategies, namely uniform random generation, bounded exhaustive generation and rule-coverage-based test generation.

6.4.5. Specification, implementation and validation of generation algorithms

Participant: Alain Giorgetti.

We have shown how to use logic programming and bounded-exhaustive testing to design and validate algorithms generating a family of combinatorial objects [45]. The focus is on computer assistance for the task of validation of an implementation with respect to a different implementation or a formal specification. Among the numerous perspectives, these generation algorithms can to their turn be embedded in bounded exhaustive testing tools, such as the one proposed in [43].

6.5. Verification of Collaborative Systems

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

6.5.1. Automatic Analysis of Web Services Security

Participants: 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. In [30] we present a tool that compiles the attack trace desribing the execution of a the mediator into its corresponding runnable code. For that the tool computes an executable specification of the mediator as prudent as possible of her role in the orchestration. This specification is expressed in ASLan language, a formal language designed for modeling Web Services tied with security policies that was developed in AVANTSSAR project. 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 compile the specification into a Java servlet that can be used by the mediator to execute the orchestration. This process has been implemented in AVANTSSAR Platform [29].

In [31] we give a decision procedure for the satisfiability problem of general deducibility constraints. Two cases are considered: the standard Dolev-Yao theory and its extension with an associative, commutative idempotent operator. The result is applied to solve the automated distributed orchestration problem for secured Web services.

Finall we show in [32] how to check satisfiability of negative deducibility constraints and we apply the result to the orchestration of secured services under non-disclosure policies. We show in particular how to handle separation-of-duty constraints in orchestration.

6.5.2. Secure Querying and Updating of XML Data

Participants: Abdessamad Imine, Houari Mahfoud, Michaël Rusinowitch.

Over the past years several works have proposed access control models for XML data where only read-access rights over nonrecursive DTDs are considered. A small number of works have studied the access rights for updates. In this work, we propose a general model for specifying access control on XML data in the presence of the update operations of W3C XQuery Update Facility [56], [48]. Our approach for enforcing such update specification is based on the notion of query rewriting. A major issue is that query rewriting for recursive DTDs is still an open problem [49], [55]. We show that this limitation can be avoided using only the expressive power of the standard XPath, and we propose a linear algorithm to rewrite each update operation defined over an arbitrary DTD (recursive or not) into a safe one in order to be evaluated only over the XML data which can be updated by the user. This work represents the first effort for securely XML updating in the presence of arbitrary DTDs (recursive or not) and a rich fragment of XPath. Finally, we study the interaction between read and update access rights to preserve the confidentiality and integrity of XML data.

We introduce an extension of hedge automata called bidimensional context-free hedge automata, proposing a new uniform representation of vertical and horizontal computation steps in unranked ordered trees. We also extend the parameterized rewriting rules used for modeling the W3C XQuery Update Facility in previous works, by the possibility to insert a new parent node above a given node. Since the rewrite closure of hedge automata languages with these extended rewriting systems is a computable context-free hedge language we can perform some static typechecking on these XML transformations [63].

6.5.3. On the Polling Problem in Social Networks

Participants: Bao Thien Hoang, Abdessamad Imine.

We tackle the polling problem in social networks where the privacy of exchanged information and user reputation are very critical. Indeed, users want to preserve the confidentiality of their votes and to hide, if any, their misbehaviors. Recent works proposed polling protocols based on simple secret sharing scheme and without requiring any central authority or cryptography system. But these protocols can be deployed safely provided that the social graph structure should be transformed into a ring-based structure and the number of participating users is perfect square. Accordingly, devising polling protocols regardless these constraints remains a challenging issue. In this work, we propose a simple decentralized polling protocol that relies on the current state of social graphs [58], [33]. More explicitly, we define one family of social graphs and show their structures constitute necessary and sufficient condition to ensure vote privacy and limit the impact of dishonest users on the accuracy of the output of the poll.

6.5.4. Access Control Models for Collaborative Applications

Participants: Fabrice Bouquet, Asma Cherif, Abdessamad Imine.

The importance of collaborative systems in real-world applications has grown significantly over the recent years. The most of new applications are designed in a distributed fashion to meet collaborative work requirements. Among these applications, we focus on Real-Time Collaborative Editors (RCE) that provide computer support for modifying simultaneously shared documents, such as articles, wiki pages and programming source code by dispersed users. Although such applications are more and more used into many fields, the lack of an adequate access control concept is still limiting their full potential. In fact, controlling access in a decentralized fashion in such systems is a challenging problem, as they need dynamic access changes and low latency access to shared documents. In [12], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We consider the propagation of authorizations and their interactions. We propose an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the selective undo approach in order to eliminate the effect of illegal document updates. Since, the safe undo is an open issue in collaborative applications. We investigate a theoretical study of the undo problem and propose a generic solution for selectively undoing operations. Finally, we apply our framework on a collaboration prototype and measure its performance in the distributed grid GRID'5000 to highlight the scalability of our solution.

We realize the verification of Ramos protocol for concurrent writing and reconfiguration for collaborative systems in [23]. The Ramos protocol implements a fault-tolerant, and a context consistency (ensuring a total order of write operations) based on an asynchronous message-passing model. Communication takes place via gossip messages, which are sent at any frequency between a dynamic set of nodes into the collaborative system.

CORIDA Project-Team

6. New Results

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

In [38], a new characteristics method for the discretization of the two dimensional fluid-rigid body problem is proposed in the case of different densities for the fluid and the solid. Convergence results are obtained for a fully-discrete finite element scheme.

In [35], controllability results are obtained for a low Reynolds number swimmer. The swimmer is undergoing radial and axi-symmetric deformations in order to propel itself in a viscous fluid.

The aim of the paper [51] is to tackle the time optimal controllability of an (n+1)-dimensional nonholonomic integrator. A full description of the optimal control and optimal trajectories are explicitly obtained.

In [25], we the interaction between a viscous incompressible fluid and an elastic structure immersed in the fluid.

In [30], weconsider the model composed by a rigid body immersed into a n incompressible perfect fluid and analyze the regularity of the trajectory of the rigid body and of the fluid particles.

In [39], we study the motion of a rigid body with a cavity filled with a viscous liquid.

In [34], we analyze a model of vesicle moving into a viscous incompressible fluid.

In [27], we obtain the identifiability of a rigid body moving in a stationary viscous fluid.

In [40] we study a mathematical model for the dynamics of vesicle membranes in a 3D incompressible viscous fluid. we show that, given $T > 0$, for initial data which are small (in terms of T), these solutions are defined on $[0, T]$ (almost global existence).

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

In [21] and [20], we propose an asymptotic analysis for the simple layer potential for multiple scattering at low frequencies.

In [19] we propose some strategies to solve numerically the difficult problem of multiple scattering by a large number of disks at high frequency. To achieve this, we combine a Fourier series decomposition with the EFIE integral equation. Numerical examples will be presented to show the efficiency of our method.

In [32], we are concerned with the convergence analysis of the iterative algorithm for solving initial data inverse problems from partial observations that has been recently proposed in Ramdani et al. More precisely, we provide a complete numerical analysis for semi-discrete (in space) and fully discrete approximations derived using finite elements in space and an implicit Euler method in time. The analysis is carried out for abstract Schrödinger and wave conservative systems with bounded observation (locally distributed).

In [23], we propose a strategy to determine the Dirichlet-to-Neumann (DtN) operator for infinite, lossy and locally perturbed hexagonal periodic media, using a factorization of this operator involving two non local operators. The first one is a DtN type operator and corresponds to a half-space problem, while the second one is a Dirichlet-to-Dirichlet (DtD) type operator related to the symmetry properties of the problem.

In [18], we investigate absorbing boundary conditions for the two-dimensional Schrödinger equation with a time and space varying exterior potential.

6.3. Observality, controllability and stabilzation in the time domain

In [17] we consider N Euler-Bernoulli beams and N strings alternatively connected to one another and forming a chain beginning with a string. We study the strong and polynomial stabilities of this system on this network and the spectrum of the corresponding conservative system.

In [37] we study the asymptotic behavior of the solution of the non-homogeneous elastic systems with voids and a thermal effect. Our main results concern strong and polynomial stabilities (since this system suffers of exponential stability).

In [12], we consider the approximation of two coupled wave equations with internal damping. Our goal is to damp the spurious high frequency modes by introducing a numerical viscosity term in the approximation schemes and prove the exponential or polynomial decay of the discrete scheme.

In [13], we show similar results as in [12] for an abstract second order evolution equations.

In [44] we consider a class of infinite dimensional systems involving a control function u taking values in $[0, 1]$ and we prove, when u is given in an appropriate feedback form and the system satisfies appropriate observability assumptions, that the system is weakly stable. The main example concerns the analysis and stabilization of a model of Boost converter connected to a load via a transmission line.

In [46] we present a course on stabilization of hyperbolic equations given at a CIME session on Control of PDE's in Italy in July 2010, including well-known results, together with recent ones including nonlinear stabilization, memory-damping and stabilization of coupled systems by a reduced number of controls. In particular, we present the optimal-weight convexity method (Alabau-Boussouira 2005, 2010) in both the finite dimensional and infinite dimensional framework and give applications to semi-discretization of hyperbolic PDE's.

In [41], we consider stabilization of coupled systems of wave-type, with localized couplings and either localized internal closed loop controls or boundary control. We establish polynomial decay rates for coupling and damping regions which do not intersect in the one-dimensional case. We also derive results in the multi-dimensional case, under multiplier type conditions for both the coupling and damping regions. The novelty and difficulty is to consider localized couplings.

In [15], we give a constructive proof of Gibson's stability theorem, some extension and further positive and negative applications of this result.

In [36] we prove that the boundary controls for the heat equation have the bang-bang property, at least in rectangular domains. This result is proved by combining methods from traditionally distinct fields: the Lebeau-Robbiano strategy for null controllability and estimates of the controllability cost in small time for parabolic systems, on one side, and a Remez-type inequality for Muntz spaces and a generalization of Turan's inequality, on the other side.

In [16] we prove exact controllability for symmetric coupled wave equations by a single control in the case of coupling and control regions which do not intersect. For this, we use and extend the two-level energy method introduced by Alabau-Boussouira (2001, 2003). Using transmutation, we derive null controllability results for coupled parabolic and Schrödinger equations. This is the first positive quantitative result, in a multi-dimensional framework with control and coupling regions with empty intersection.

In [14], we prove controllability results for abstract systems of weakly coupled N evolution equations in cascade by a reduced number of boundary or locally distributed controls ranging from a single up to N-1 controls. We give applications to cascade coupled systems of N multi-dimensional hyperbolic, parabolic and diffusive (Schrödinger) equations. The results are valid for control and coupling regions which do not necessarily intersect.

In [22], we study two notions of controllability, called respectively radial controllability and directional controllability. We prove that for families of linear vector fields, the two notions are actually equivalent.

In [24] we solve an optimization problem in convex geometry which, despite its seeming simplicity, offers a nice variety of solutions, some of them being unexpectable.

The paper [28] is devoted to prove that the union of two identical balls minimizes a non linear eigenvalue (related to the generalized Wirtinger inequality) among sets of given volume.

In [33] is considered a problem in population dynamics where we investigate the question of optimal location of the zone of control.

In [26], we give a rigorous proof, valid also for unbounded operators, of the widely used "rotating wave approximations" for bilinear Schrödinger equations.

In [42], we exploit the results of [26] on standard examples of bilinear quantum systems.

CORTEX Project-Team

6. New Results

6.1. Spiking neurons

Participants: Hana Belmabrouk, Dominique Martinez, Thierry Viéville, Thomas Voegtlin.

6.1.1. Mathematical modeling

In order to understand the dynamics of spiking neural networks under the influence of a modified synaptic dynamics of single neurons, we study the effect of tonic inhibition on the population activity in spiking neural networks. The aim is to derive mathematical relations of the population activity and some statistics estimated numerically from the simulation of networks [4], [8].

6.1.2. Biophysical modeling

Our understanding of the computations that take place in the human brain is limited by the extreme complexity of the cortex, and by the difficulty of experimentally recording neural activities, for practical and ethical reasons. The Human Genome Project was preceded by the sequencing of smaller but complete genomes. Similarly, it is likely that future breakthroughs in neuroscience will result from the study of smaller but complete nervous systems, such as the insect brain or the rat olfactory bulb. These relatively small nervous systems exhibit general properties that are also present in humans, such as neural synchronization and network oscillations. Our goal is therefore to understand the role of these phenomena by combining biophysical modelling and experimental recordings, before we can apply this knowledge to humans. In the last year, we have studied new aspects of our models of the insect olfactory system [7], [14].

6.1.3. Using event-based metric for event-based neural network weight adjustment

The problem of adjusting the parameters of an event-based network model is addressed here at the programmatic level. Considering temporal processing, the goal is to adjust the network units weights so that the outcoming events correspond to what is desired. The work of [18] proposes, in the deterministic and discrete case, a way to adapt usual alignment metrics in order to derive suitable adjustment rules. At the numerical level, the stability and unbiasness of the method is verified.

The key point, here, is the non-learnability of even-based , since it is proved that this problem is NP-complete, when considering the estimation of both weights in the general case, except for exact simulation. We show that we can "elude" this caveat and propose an alternate efficient estimation mechanism, inspired by alignment metrics used in spike train analysis, thus providing a complement of other estimation approaches, beyond usual convolution metric. At last, the proposed mollification *is* a series of convolution metric, but that converges towards the expected alignment metric.

6.1.4. Predictive learning

In collaboration with Sander Bohte (CWI, Netherlands) and Nicolas Fourcaud-Trocme (CNRS, Lyon), we are developing a model of predictive learning using oscillations in a population of spiking neurons. The model is based on previous work performed in the Cortex group. Our previous model suggested a possible role for neuronal synchronization in unsupervised, predictive-type learning. However, that model was not compatible with sustained oscillations observed in biological networks. We are extending our initial approach in order to allow the network to learn during a stable, steady-state oscillatory regime. This extension involves using type-2 neurons and two distinct types of inhibition.

6.2. Dynamic Neural Fields

Participants: Frédéric Alexandre, Yann Boniface, Laurent Bougrain, Georgios Detorakis, Hervé Frezza-Buet, Bernard Girau, Axel Hutt, Mathieu Lefort, Nicolas Rougier, Wahiba Taouali.

The work reported this year represents both extensions of previous works and new results linked to the notion of neural population, considered at (i) a formal level (theoretical studies of neural fields), (ii) a numerical level (study of functioning and learning rules) and (iii) a more embodied one (implementations of specific functions).

6.2.1. Formal Level

To study the effect of external stimuli on nonlinear neural population dynamics involving constant delays, the work aims to apply the center manifold theorem and derive expressions of the time-dependent centre manifold. It is observed that additive noise and external quasi-periodic driving change the stability of neural populations dependent on the delay [9], [10].

6.2.2. Numerical Level

At the numerical level, specific developments were carried out to assess our software platform, to master functioning rules and to study the performances of new learning rules:

- Adaptation of the BCM rule to multi-modality by adapting the dynamics of the threshold by the use of a feed-back signal generated by a neural field map [1], [26]
- We investigate the formation and maintenance of ordered topographic maps in the primary somatosensory cortex as well as the reorganization of representations after sensory deprivation or cortical lesion. We consider both the critical period (postnatal) where representations are shaped and the post-critical period where representations are maintained and possibly reorganized. We hypothesize that feed-forward thalamocortical connections are an adequate site of plasticity while cortico-cortical connections are believed to drive a competitive mechanism that is critical for learning. We model a small skin patch located on the distal phalangeal surface of a digit as a set of 256 Merkel ending complexes (MEC) that feed a computational model of the primary somatosensory cortex (area 3b). This model is a two-dimensional neural field where spatially localized solutions (a.k.a. bumps) drive cortical plasticity through a Hebbian-like learning rule. Simulations explain the initial formation of ordered representations following repetitive and random stimulations of the skin patch. Skin lesions as well as cortical lesions are also studied and results confirm the possibility to reorganize representations using the same learning rule and depending on the type of the lesion. For severe lesions, the model suggests that cortico-cortical connections may play an important role in complete recovery [6].

6.2.3. Embodied Level

6.2.3.1. Motion detection

We develop bio-inspired neural architectures to extract and segment the direction and speed components of the optical flow from sequences of images. Following this line, we have built additional models to code and distinguish different visual sequences. The structure of these models takes inspiration from the course of visual movement processing in the human brain, such as in area MT (middle temporal) that detects patterns of movement, or area FBA where neurons have been found to be sensitive to single spatio-temporal patterns. This work has been extended to complex movements: to fight, to wave, to clap, using real-world video databases [5].

6.2.3.2. Anticipatory mechanisms in neural fields

We have defined first models of neural fields that include anticipatory mechanisms through the integration of spatiotemporal representations into the lateral interactions of a dynamic neural field. In [20], the case of multiple anticipated trajectories is studied.

6.2.3.3. Action selection

Within the context of enaction and a global approach to perception, we focused on the characteristics of neural computation necessary to understand the relationship between structures in the brain and their functions. We first considered computational problems related to the discretization of differential equations that govern the studied systems and the synchronous and asynchronous evaluation schemes. Then, we investigated a basic functional level : the transformation of spatial sensory representations into temporal motor actions within the visual-motor system. We focused on the visual flow from the retina to the superior colliculus to propose a minimalist model of automatic encoding of saccades to visual targets. This model, based on simple local rules (CNFT and logarithmic projection) in a homogeneous population and using a sequential processing, reproduces and explains several results of biological experiments. It is then considered as a robust and efficient basic model. Finally, we investigated a more general functional level by proposing a computational model of the basal ganglia motor loop. This model integrates sensory, motor and motivational flows to perform a global decision based on local assessments. We implemented an adaptive process for action selection and context encoding through an innovative mechanism that allows to form the basic circuit for other cortico-basal loops. This mechanism allows to create internal representations according to the enactive approach that opposes the computer metaphor of the brain. Both models have interesting dynamics to study from whether a biological point of view or a computational numerical one [2], [12].

6.3. Higher level functions

Participants: Frédéric Alexandre, Laurent Bougrain, Octave Boussaton, Axel Hutt, Maxime Rio, Carolina Saavedra, Christian Weber.

Our activities concerned information analysis and interpretation and the design of numerical distributed and adaptive algorithms in interaction with biology and medical science. To better understand cortical signals, we choose a top-down approach for which data analysis techniques extract properties of underlying neural activity. To this end several unsupervised methods and supervised methods are investigated and integrated to extract features in measured brain signals. More specifically, we worked on Brain Computer Interfaces (BCI).

6.3.1. Using Neuronal States for Transcribing Cortical Activity into Muscular Effort

We studied the relations between the activity of corticomotoneuronal (CM) cells and the forces exerted by fingers. The activity of CM cells, located in the primary motor cortex is recorded in the thumb and index fingers area of a monkey. The activity of the fingers is recorded as they press two levers. The main idea of this work is to establish and use a collection of neuronal states. At any time, the neuronal state is defined by the firing rates of the recorded neurons. We assume that any such neuronal state is related to a typical variation (or absence of variation) in the muscular effort. Our forecasting model uses a linear combination of the firing rates, some synchrony information between spike trains and averaged variations of the positions of the levers [17].

6.3.2. From the decoding of cortical activities to the control of a JACO robotic arm: a whole processing chain

We realized a complete processing chain for decoding intracranial data recorded in the cortex of a monkey and replicates the associated movements on a JACO robotic arm by Kinova. We developed specific modules inside the OpenViBE platform in order to build a Brain-Machine Interface able to read the data, compute the position of the robotic finger and send this position to the robotic arm. More precisely, two client/server protocols have been tested to transfer the finger positions: VRPN and a light protocol based on TCP/IP sockets. According to the requested finger position, the server calls the associated functions of an API by Kinova to move the fingers properly. Finally, we monitor the gap between the requested and actual fingers positions. This chain can be generalized to any movement of the arm or wrist [22].

6.3.3. Wavelet-based Semblance for P300 Single-trial Detection

Electroencephalographic signals are usually contaminated by noise and artifacts making difficult to detect Event-Related Potential (ERP), specially in single trials. Wavelet denoising has been successfully applied to ERP detection, but usually works using channels information independently. This paper presents a new adaptive approach to denoise signals taking into account channels correlation in the wavelet domain. Moreover, we combined phase and amplitude information in the wavelet domain to automatically select a temporal window which increases class separability. Results on a classic Brain-Computer Interface application to spell characters using P300 detection show that our algorithm has a better accuracy with respect to the VisuShrink wavelet technique and XDAWN algorithm among 22 healthy subjects, and a better regularity than XDAWN [21].

6.3.4. Filter for P300 detection

According to recent literature, the most appropriate preprocessing to improve P300 detection is still unknown or at least there is no consensus about it. Research papers refer to different low-pass filters, high-pass filters, baseline, subsampling or feature selection. Using a database with 23 healthy subjects we compared the effect on the letter accuracy (single-trial detection) provided by a linear support vector machine of a high-pass filter with cutoff frequencies from 0.1 to 1 Hz and a low-pass filter with cutoff frequencies from 8 to 60 Hz. According to this study, the best combination is for a band-pass filter of 0.1 to 15 Hz [16].

6.3.5. Processing Stages of Visual Stimuli and Event-Related Potentials

Event-evoked potentials (ERP) in electroencephalograms reflect various visual processing stages according to their latencies and locations. Thus, ERP components such as the N100, N170 and the N200 which appears 100, 170 and 200 ms after the onset of a visual stimulus correspond respectively to a selective attention, the processing of color, shape and rotation (e.g. processing of human faces) and a degree of attention [24].

6.3.6. Exploring the role of the thalamus in visuomotor tasks implicating non-standard ganglion cells

Non-standard ganglion cells in the retina have specific loci of projection in the visuomotor systems and particularly in the thalamus and the superior colliculus. In the thalamus, they feed the konio pathway of the LGN. Exploring the specificities of that pathway, we discovered it could be associated to the matrix system of thalamo-cortical projections, known to allow for diffuse patterns of connectivity and to play a major role in the synchronization of cortical regions by the thalamus.

An early model [23] led to the design of the corresponding information flows in the thalamo-cortical system, that we are now expanding, in the framework of the Keops project § 7.2 , to be applied to real visuomotor tasks.

6.3.7. Formalization of input/output retinal transformation regarding non-standard gangion cells behavior

We propose to implement the computational principles raised by the study on the K-cells of the retina using a variational specification of the visual front-end, with an important consequence: In such a framework, the GC are not to be considered individually, but as a network, yielding a mesoscopic view of the retinal process.
Given natural image sequences, fast event-detection properties appears to be exhibited by the mesoscopic collective non-standard behavior of a subclass of the so-called dorsal and ventral konio-cells (K-cells) that correspond to specific retinal output.
We consider this visual event detection mechanism to be based on image segmentation and specific natural statistical recognition, including temporal pattern recognition, yielding fast region categorization. We discuss how such sophisticated functionalities could be implemented in the biological tissues as a unique generic two-layered non-linear filtering mechanism with feedback. We use computer vision methods to propose an effective link between the observed functions and their possible implementation in the retinal network.

The available computational architecture is a two-layers network with non-separable local spatio-temporal convolution as input, and recurrent connections performing non-linear diffusion before prototype based visual event detection.
The numerical robustness of the proposed model has been experimentaly checked on real natural images. Finally, model predictions to be verified at the biological level are discussed [25].

6.4. Embodied and embedded systems

Participants: Yann Boniface, Hervé Frezza-Buet, Bernard Girau, Mathieu Lefort.

6.4.1. InterCell

Our research in the field of dedicated architectures and connectionist parallelism mostly focuses on embedded systems (*cf.* §3.5). Nevertheless we are also involved in a project that considers coarse-grain parallel machines as implementation devices. The core idea of this InterCell project (*cf.*http://intercell.metz.supelec.fr) is to map fine grain computation (cells) to the actual structure of PC clusters. The latter rather fit coarse grain processing, using relatively few packed communication, which a priori contradicts neural computing. Another fundamental feature of the InterCell project is to promote interaction between the parallel process and the external world. Both features, cellular computing and interaction, allow to consider the use of neural architectures on the cluster on-line, for the control of situated systems, as robots.

6.4.2. Hardware implementations of neural models

In the field of dedicated embeddable neural implementations, we use our expertise in both neural networks and FPGAs so as to propose efficient implementations of applied neural networks on FPGAs, as well as to define hardware-friendly neural models.

- We currently intend to minimize the topological constraints of FPGA-embedded spiking neural fields using reduced neighborhoods but randomly propagating spikes. A preliminary result has been obtained so as to implement massively distributed pseudo-random number generators based on cellular automata that use minimal areas though they produce random streams that pass most randomness tests [19]. These results have also been applied to cellular aurtomata using randomnes in their transition rules [13].
- Researchers have proposed the concept of Central Pattern Generators (CPGs) as a neural mechanism for generating an efficient control strategy for legged robots based on biological locomotion principles. We have developed a reconfigurable hardware implementation of a CPG-based controller which is able to generate several gaits for quadruped and hexapod robots [3].

6.4.3. Towards brain-inspired hardware

Our activities on dedicated architectures have strongly evolved in the last years. We now focus on the definition of brain-inspired hardware-adapted frameworks of neural computation. Our current works aim at defining hardware-compatible protocols to assemble various perception-action modalities that are implemented and associated by different bio-inspired neural maps.

6.4.3.1. Multimodal learning through joint dynamic neural fields

This work relates to the development of a coherent multimodal learning for a system with multiple sensory inputs. We have modified the BCM synaptic rule, a local learning rule, to obtain the self organization of our neuronal inputs maps and we use a CNFT based competition to drive the BCM rule. In practice, we introduce a feedback modulation of the learning rule, representing multimodal constraints of the environment, and we introduce an unler-arning term in the BCM equation to solve the problem of the different temporalities between the raise of the activity within modal maps and the multimodal learning of the organization of the maps [1], [26].

6.4.3.2. Randomly spiking dynamic neural fields

We have defined a new kind of spiking neural field that is able to use only local links while transmitting spikes through the map by succesive random propagations. Such a model is able to be mapped onto FPGAs, while maintaining most properties of neural fields. Early results will be soon published.

MADYNES Project-Team

6. New Results

6.1. Android Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact].

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

During 2012, we have designed and developed a monitoring framework integrating observed network and system activities of a running application. We have developed an embedded NetFlow probe running on android devices to export observed network flow records observed to a collection point for their processing. Our embedded probe includes a new set of IPFIX information elements that we have designed [36] to encapsulate location information within exported flows using the IPFIX protocol.

We have also developed an embedded logging probe that exports available system logs to a collection point. The logs are then centrally processed and correlated with observed network flow records to extract an accurate behavior of an application including its network and in-device activities.

Our monitoring framework is different from available proposed solutions since we build a dynamic model to infer the running behavior of an Android application. This technique allows us to identify patched applications where a malicious activity has been added, cloned applications where the observed behavior is different from the expected behavior and privacy leaks where an application is contacting unexpected services.

6.2. Sensor networks monitoring

Participants: Alexandre Boeglin, Laurent Ciarletta, Olivier Festor, Abdelkader Lahmadi [contact], Emmanuel Nataf, Bilel Saadallah.

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

During the year 2012, we developed novel approaches for the monitoring of LLNs. We developed and designed a novel algorithm and a supporting framework [18] that improves a poller-pollee monitoring architecture. We empower the poller-pollee placement decision process and operation by exploiting available routing data to monitor nodes status. In addition, monitoring data is efficiently embedded in any messages flowing through the network, drastically reducing monitoring overhead. Our approach is validated through both simulation, implementation and deployment on a 6LoWPAN-enabled network. Both simulations and large-scale testbed experiments assess the efficiency of our monitoring scheme. Results also demonstrate that our approach is less aggressive and less resource consuming than its competitors.

We developed a first fully operational CCNx stack [40] on a wireless sensor network. We implemented CCNx as a native C experimental extension of Contiki, an operating system dedicated to Internet of Things applications. Our extension [33] is based on the reference implementation of CCNx modified to run as a network driver on top of different available MAC protocols implementations in Contiki. Our goal is to design a monitoring and configuration framework that benefits from the content-centric approach to efficiently collect desired management content and apply in-network processing functions for nodes configuration and monitoring. This includes extending naming schema with monitoring oriented processing functions, optimizing data interests to minimize the communication overhead.

6.3. Management and monitoring of P2P networks

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

In 2012, we have addressed operation, monitoring and security issues on several P2P target networks: KAD, BitTorrent and I2P.

Several large scale P2P networks operating on the Internet are based on a Distributed Hash Table. These networks offer valuable services, but they all suffer from a critical issue allowing malicious nodes to be inserted in specific places on the DHT for undesirable purposes (monitoring, distributed denial of service, pollution, etc.). While several attacks and attack scenarios have been documented, few studies have measured the actual deployment of such attacks and none of the documented countermeasures have been tested for compatibility with an already deployed network. In our work, we focus on the KAD network. Based on large scale monitoring campaigns, we demonstrated that the world-wide deployed KAD network suffers large number of suspicious insertions around shared contents and we quantify them. To cope with these peers, we proposed a new efficient protection algorithm based on analyzing the distribution of the peers ID found around an entry after a DHT lookup [3]. The evaluation of our solution showed that it detects the most efficient configurations of inserted peers with a very small false-negative rate, and that the countermeasures successfully filter almost all the suspicious peers. We demonstrate the direct applicability of our approach by implementing and testing our solution in real P2P networks

BitTorrent is a fast, popular, P2P filesharing application focused on fast propagation of content. Its trackerless approach uses a DHT based on Kademlia to search for sources when the hash of the metadata of the content to transfer is known. On the other hand, the eMule network uses the old ED2K protocol for filesharing including a system of priorized queues, but indexation is done through a solid Kademlia based DHT, named Kad. The Kad DHT stands for a search engine, wich provides an extra level to map keywords to file identifiers. We have designed an hybrid approach, compatible with both P2P file-sharing networks, which has the Kad advantages on indexation and the BitTorrent throughput for transfer while maintaining backward compatibility with both of these networks [42]. To validate our proposal we developed a prototype which supports content indexation provided by the Kad network and is able to transfer files using the BitTorrent protocol. Using this prototype, we measured the propagation of new content in clusters of aMule clients, BitTorrent clients, hybrid clients, and a mix of them.

In parallel, we continued our research about being anonymous when downloading from BitTorrent. Anonymous communications have been gaining more and more interest from Internet users as privacy and anonymity problems have emerged. Among anonymous enabled services, anonymous file-sharing is one of the most active one and is increasingly growing. Large scale monitoring on these systems allows us to grasp how they behave, which type of data is shared among users, the overall behavior in the system.

We presented the first monitoring study aiming to characterize the usage of the I2P network, a low-latency anonymous network based on garlic routing [23]. We characterized the file-sharing environment within I2P, and evaluated if this monitoring affects the anonymity provided by the network. We showed that most activities within the network are file-sharing oriented, along with anonymous web-hosting. We assessed the wide geographical location of nodes and network popularity. We also demonstrated that group-based profiling is feasible on this particular network [22].

Dedicated anonymous networks such as Freenet and I2P allow anonymous file-sharing among users. However, one major problem with anonymous file-sharing networks is that the available content is highly reduced, mostly with outdated files, and non-anonymous networks, such as the BitTorrent network, are still the major source of content. We showed that in a 30-days period, 21648 new torrents were introduced in the BitTorrent community, whilst only 236 were introduced in the anonymous I2P network, for four different categories of content. Therefore, how can a user of these anonymous networks access this varied and non-anonymous content without compromising its anonymity? In [24], we improved content availability in an anonymous environment by proposing the first internetwork model allowing anonymous users to access and share content in large public communities while remaining anonymous. We showed that our approach can efficiently interconnect I2P users and public BitTorrent swarms without affecting their anonymity nor their performance. Our model is fully implemented and freely usable.

6.4. Configuration security automation

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

The main research challenge addressed in this work is focused on enabling configuration security automation in autonomic networks and services. In particular our objective is to increase vulnerability awareness in the autonomic management plane in order to prevent configuration vulnerabilities. The continuous growth of networking significantly increases the complexity of management. It requires autonomic networks and services that are capable of taking in charge their own management by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. However, the operations and changes executed during these self-management activities may generate vulnerable configurations. A first part of our work in the year 2012 has been dedicated to the assessment of distributed vulnerabilities and to the elaboration of a collaborative management strategy for supporting their remediation. A configuration vulnerability is not necessarily local but can also be spread over several devices in the autonomic network. We have showed in [8] how such distributed vulnerabilities can be mathematically formalized and described in a machine readable manner, through the specification of the DOVAL (Distributed OVAL) language on top of OVAL (Open Vulnerability and Assessment Language). We have designed and evaluated a dedicated framework for exploiting these vulnerability descriptions, collecting device configurations and detecting distributed vulnerabilities using specific aggregation techniques. Once a vulnerability is identified in the autonomic network, several remediation actions can potentially be performed by the autonomic network over devices. For that purpose, we have introduced an XCCDF-based specification for expressing alternative treatments related to a distributed vulnerability. We have also proposed a collaborative scheme for selecting one of these treatments depending on the current context (device capabilities and willingness to participate) [6]. A second part of our work has focused on the extension of our solution to other environments. In particular we have worked on the integration of our vulnerability assessment strategy over the Android plateform [9]. We have put forward a mathematical model as well as an optimized method that provides solid foundations for this context. By maintaining low-consumption services monitoring the system, the proposed approach minimizes heavy task executions by only triggering assessment activities when configuration changes are detected or new vulnerability definitions are available. In light of this, we have developed a prototype that efficiently performs self-assessment activities, and also introduces dedicated web services for collecting OVAL descriptions and storing assessment results. We have performed an analytical evaluation of the proposed model as well as an extensive set of technical experiments that shows the feasibility of our solution. We are currently working on the issue of past hidden vulnerable states. A network compromised in the past by an unknown vulnerability at that moment may still constitute a potential security threat in the present. Accordingly, past unknown system

exposures are required to be taken into account. We are therefore investigating a novel strategy for identifying also such past hidden vulnerable configurations and increasing the overall security [9].

6.5. Cache Management in CCN

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

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

While the Internet was designed for -and still focuses on- host-to-host communication (IP), users are only interested in actual content rather than source location. Hence, new Information-Centric Networking architectures (ICN) such as CCN, NetInf, Pursuit have been proposed giving high priority to efficient content distribution at large scale. Among all these new architectures, Content Centric Networking (CCN) has attracted considerable attention from the research community [2].

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

As content is cached along the path, it is crucial to investigate the caching strategy for CCN Networks and to propose new schemes adapted to CCN. We therefore designed *Most Popular Content* (MPC), a new caching strategy for CCN network [10].

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

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

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

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

6.6. QoS in Wireless Sensor Networks

Participants: François Despaux, Abdelkader Lahmadi, Bilel Nefzi, Hugo Cruz-Sanchez, 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, but also high throughput with self-adaptation to dynamic traffic changes [21]. Our research on WSN QoS is thoroughly organized in three topics:

- MAC protocol design for both QoS and energy efficiency

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

The main result that we obtained in 2012 is a new hybrid CSMA/TDMA MAC protocol, called Queue-MAC, that dynamically adapts the duty-cycle according to the current network traffic. The queue length of nodes is used as the network traffic indicator. When the traffic increases, the active CSMA period is accordingly extended by adding dynamic TDMA slots, allowing thus to efficiently handle burst traffic under QoS constraints. This protocol is implemented on the STM32W108 SOC chips and compared with both a fixed duty-cycle reference protocol and an optimized IEEE802.15.4 MAC protocol. Through extensive experimental measurements, we showed that our queue-length aware hybrid CSMA/TDMA MAC protocol largely outperforms the compared protocols. The proposed protocol can be easily implemented through slight adaptation of the IEEE802.15.4 standard [25].

Many industrial WSN are based on IEEE802.15.4 standard. One of the critical issues is the scheduling of neighboring coordinators beacons. In [20], we presented TBoPS, a novel technique for scheduling beacons in the cluster-tree topology. TBoPS uses a dedicated period called beacon only period (BOP) to schedule beacons at the beginning of IEEE 802.15.4 superframe. The advantage of TBoPS is that every beacon-enabled node distributively selects a beacon schedule during association phase.

- QoS routing

  For supporting different QoS requirements, routing in WSN must simultaneously consider several criteria (e.g., minimizing energy consumption, hop counts or delay, packet loss probability, etc.). When multiple routing metrics are considered, the problem becomes a multi-constrained optimal path problem (MCOP), which is known as NP-complete. In practice, the complexity of the existing routing algorithms is too high to be implemented on the low cost and power constrained sensor nodes. Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. OC can be applied to solving MCOP problem with much lower complexity and can deal with dynamic topology changes (which is the case in duty-cycled WSN). The OC approach has been successfully applied to a concrete routing problem [13]. Its implementation over Contiki on TelosB motes has also been achieved, confirming thus its great potential for developing new QoS routing protocols for WSN.

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

  Probabilistic end-to-end performance guarantee may be required when dealing with real-time applications. For instance, in our ANR QUASIMODO project, we considered an intrusion detection and tracking scenario and analyzed the application requirements with respect to the network QoS. Assuming the use of the extended Kalman filter based tracking technique, we derived the tradeoff relationship between the tracking precision and the delay (from the target position and speed sampling to mobile nodes moving to cover the estimated next step area). In [5] we proposed a novel coordinative moving algorithm for autonomous mobile sensor networks to guarantee that the target can be detected in each observed step while minimizing the amount of moving sensors (so saving energy). In such kind of application context, we aim to provide methods for both network resource allocation and estimating the end-to-end delay in multi-hop WSN. Assuming IEEE802.15.4 WSN with cluster-tree routing, in [16] we addressed the problem of allocating and reconfiguring the available bandwidth using an Admission Control Manager that guarantees that the nodes respect their probabilistic bandwidth assignment when generating data traffic. It has been shown by simulation that using the proposed method, one can obtain desired probabilistic guarantee in both bandwidth and energy efficiency.

  In a more general context of meshed networks, we present an empirical support of an analytical approach, which employs a frequency domain analysis for estimating end-to-end delay in multi-hop networks. The proposed analytical results of the end-to-end delay distribution are validated through simulation and compared with queuing theory based analysis. Our results demonstrate that an analytical prediction schema is insufficient to provide an adequate estimation of the end-to-end

delay distribution function, but it requires to be combined with simulation methods for detailed link and node latency distribution [15].

6.7. Energy in Wireless Sensor Networks

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

The energy sources of sensors in a wireless network rely mainly on batteries and are very limited in their capacity. Several research efforts are focalized on trying to limit the energy consumption in such networks. This is particularly the case in protocol design. Indeed, the communication consumes a large majority of the available energy. To be realistic and efficient, all proposed approaches need to know the energy available at any time in the systems. Unfortunately, most sensors do not provide such information because it requires additional built-in hardware that would drastically increase their cost. Over the last decade very accurate physical battery models that encompass consumption and recovery have been designed. The complexity of these models is however too high to be implemented inside simple sensors. Recent research results have shown that this integration could be possible if some approximations are integrated in the models.

We have worked on integrating such an approcimated model in the sensor operating system. This work allows the simulation of such sensors and the deployement on real devices that will be aware of their remaining energy level without requiring any additionnal costly equipment. A first implementation on simulation tool has given very promising results; sensors can access their energy level and take decision based on this estimate. Firstly, we have studied energy consumption of a sensors network collecting and routing data toward a single destination. Energy cost of the network deployment has been computed and so the network life as a whole. An other result of our work is the comparison of several common link layer access protocols and several data rate transmits [31].

6.8. Online Risk Management

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

Telephony over IP has known a large scale deployment and has been supported by the standardization of dedicated signaling protocols. This service is however exposed to multiple attacks due to a lower confinement in comparison to traditional PSTN networks. While a large variety of methods and techniques has been proposed for protecting VoIP networks, their activation may seriously impact on the quality of such a critical service. Risk management provides new opportunities for addressing this challenge. In particular our work aims at performing online risk management for VoIP networks and services. The objective is to dynamically adapt the service exposure with respect to the threat potentiality, while maintaining a low security overhead. In the year 2012, we have pursued our work on online risk management and applied it to more distributed configurations. In that context we have defined in [14] an exposure control solution for P2PSIP networks where the registration and location servers are implemented by a distributed hash table. After having analyzed different attack scenarios, we have designed the underlying risk management architecture and modelled several dedicated countermeasures. We have evaluated the performance and scalability of our approach through extensive experiments performed with the OMNET++ simulator. We have also proposed a trust-based solution for addressing residual attacks in the RELOAD framework. This latter, complementary to our risk management approach, is a peer-to-peer signalling overlay using a central certificate enrolment server and supporting P2PSIP infrastructures. Self-signed certificates can also be used in closed networks, and connections amongst nodes can be secured using an encryption protocol such as TLS. While the RELOAD framework permits to reduce the exposure to threats, P2PSIP networks are still exposed to residual attacks related to the routing and storage activities. For instance, it is trivial for a malicious node to refuse to give the stored information, or to send false routing messages in the network. We have showed how trust mechanisms can be exploited to counter these attacks in an efficient manner. Our work on online risk management has also focused on VoIP services in the Cloud [30]. The integration of IP telephony in this environment permits the delivery and access of new resources and constitutes an important factor for its scalability. While the Cloud has recently served as a basis for security attacks targeting IP telephony, such as SIP brute force attacks from the Amazon EC2 Cloud

infrastructure, we consider that it also provides new possibilities for supporting the security of this service. We have analyzed the applicability of our online risk management approach in the Cloud, and evaluated to what extent security countermeasures may be outsourced as a service. We have mathematically defined a dedicated modelling and detailed different treatment strategies for applying countermeasures in the Cloud. Finally, we have quantified the benefits and costs of these strategies based on a set of experimental results.

6.9. Pervasive Computing

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

Vincent Chevrier(MAIA Team), Thomas Navarrette Gutierrez (MAIA Team) and Priyadrsi Nanda (Universit of Technology, Sydney) did contribute to part of this activity.

In Pervasive or Ubiquitous Computing, a growing number of communicating/computing devices are collaborating to provide users with enhanced and ubiquitous services in a seamless way. In a related field, Cyber Physical Systems also are technological systems that have to be considered within a physical world and its contraints. They are complex systems where several inter-related phenomena have to be considered. In order to be studied, modeled and evaluated, we propose the use of co-simulation and multimodeling. to be Madynes is focusing on the networking aspects of such systems. We cooperate with toher the Maia team to be able to encompass issues and research questions that combine both networking and cognitive aspects.

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

In 2012 we worked on the following research topics :

- Continuing the work on multi-modeling and co-simulation, we've participated with the MAIA team on the development of an architecture for the control of complex systems based on multi-agent simulation [32], [2], and a CPS co-simulation (next item), and continue working on the AA4MM framework (Agents and artefacts for Multiple heterogeneous Models).
- In Cyper Physical Systems, we have lead the design and implementation of the Aetournos (Airborne Embedded auTonomOUs Robust Network of Objects and Sensors) platform at Loria. The idea of AETOURNOS is to build a platform which can be at the same time a demonstrator of scientific realizations and an evaluation environment for research works of various teams of our laboratory. It is also its own research domain : building a completely autonomous and robust flock of collaborating UAVs.

  In Madynes, we focus on the CPS and their networks and applications. Those systems consist of numerous autonomous elements in sharp interaction which functioning require a tight coupling between software implementations and technical devices. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of such a system. Indeed, if we look at the level of each of the elements playing a role into this system, a certain number of challenges and scientific questions can be studied: respect of real-time constraints of calculations for every autonomous UAV and for the communication between the robots, conception of individual, embedded, distributed or global management systems, development of self-adaptative mechanisms, conception of algorithms of collective movement etc... Furthermore, the answers to each of these questions have to finally contribute to the global functioning of the system. Applying co-simulation technique we plan to develop a hybrid "network-aware

flocking behavior" / "behavior aware routing protocol". The platform is composed of several high-grade research UAVs (Pelican quadcopters and Firefly hexacopters) and lighter models (AR.Drone quacopters). We have provided a working set of tools : multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensor for location awareness, their own computing capabilities and several wireless networks.

This work is discribed in a position paper where a first implementation of a formation flight is detailed ([11]).

- Energy-constraint geolocalization, addressing, routing and management of wireless devices: a research collaboration with Fireflies RTLS was started in March 2009 and has ended in 2012. The initial work has been extended in a joint work with the former TRIO Team and a visiting professor from the University of Technology of Sydney. Its focus has been shiffted towards novel adressing and routing scheme minimizing a global energy-cost function in a wireless sensor network location systems [28]. We are proposing a global configuration tool for this matter in regards with given constraints (number of nodes, topology, QoS).

In 2013, we will continue working on the hybrid protocols and on the UAV platform, and apply our co-simulation work to Smart Grids.

MAGRIT Project-Team

6. New Results

6.1. Motion, scene and camera reconstruction

Participants: Marie-Odile Berger, Srikrishna Bhat, Christel Leonet, Gilles Simon, Frédéric Sur.

- **Enhancing the grid method for in-plane strain measurements**
  This work is motivated by a problem from experimental solid mechanics. The grid method permits to measure the heterogeneous strains on the surface of specimens subjected to mechanical tests. Among full-field measurement techniques, the grid method consists in transferring a regular grid on the surface of the specimen and in taking images of the grid before and after deformation. Windowed Fourier analysis then gives an estimate of the surface displacement and strain components. In a collaboration with Institut Pascal (Université Blaise Pascal, Clermont Ferrand), we have shown that the estimations obtained by this technique are approximately the convolution of the actual values with the analysis window. We have also characterized how the noise in the grid image impairs the displacement and strain maps [18]. This study has allowed us to improve the metrological performance of the grid method with deconvolution algorithms. A numerical and experimental study can be found in [17].
- **Visual words for pose computation**
  Visual vocabularies are standard tools in the object/image classification literature, and are emerging as a new tool for building point correspondences for pose estimation. Within S. Bhat's PhD thesis, we have proposed several methods for visual word construction dedicated to point matching, with structure from motion and pose estimation applications in view. The three dimensional geometry of a scene is first extracted with bundle adjustment techniques based on keypoint correspondences. These correspondences are obtained by grouping the set of all SIFT descriptors from the training images into visual words using transitive closure (TC) techniques. We obtain a more accurate 3D geometry than with classical image-to-image point matching. In a second on-line step, these visual words serve as 3D point descriptors that are robust to viewpoint change, and are used for building 2D-3D correspondences on-line during application, yielding the pose of the camera by solving the PnP problem. Several visual word formation techniques have been compared with respect to robustness to viewpoint change between the learning and the test images. Our experiments showed that the adaptive TC visual words are better in many ways when compared to other classical techniques such as K-means.

  More specifically, the work of this year has focused on improving pose estimation from visual words with respect to strong viewpoint changes. 2D-3D correspondences are actually difficult to establish if there are too large viewpoint changes between the image whose pose is sought and the images that yielded the visual words attached to 3D points. We assessed several viewpoint simulation techniques in order to enrich the visual word description of the 3D points.
- **Acquisition of 3D calibrated data**
  Christel Leonet joined the team in October 2010 as an Inria assistant engineer with the aim of building an integrated 3D acquisition system. More specifically, the objective of her work is to combine an IMU (Inertial Measurement Unit), a GPS receiver, a laser rangefinder and a video camera for ground truth data acquisitions of camera movements and scene structures. These data will be useful to validate several algorithms developed in our team. This year, a new visual pan tracking method has been designed and implemented. We considered spherical environments made of sparse video images instead of fully-covered environment maps which often suffer from geometric and photometric misalignments. The scanning process has been improved in order to increase the accuracy of the recovered polygons and allow for visual assessments of this accuracy. The 3D laser pointer has been validated in several indoor environments. Finally, the GPS has been integrated to the system and preliminary results have been obtained in outdoor environments.

6.2. Medical imaging

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

- **Vessel reconstruction with implicit surfaces**
  This research activity is led in collaboration with Shacra project-team from Inria Lille-Nord Europe and the Department of Interventional Neuroradiology from Nancy University Hospital. It was pursued this year in the context of the SOFA-InterMedS Inria Large-Scale Initiative (http://www.sofa-framework.org/).

  Our objective is to offer the interventional radiologists with a patient-based interactive simulator [16]. The medical applications are training to endovascular procedures, planning the intervention, and augmenting the intra-operative images with 3D simulated data. Our contributions address vasculature modeling from patient data, namely 3D rotational angiography (3DRA) volumes. The segmentation should be both user friendly and generate a vascular surface model that is compliant with the computing constraints set in interactive simulation. Within A. Yureidini's PhD thesis, a new model was developed consisting of a tree of local implicit blobby models. The algorithm consists of two steps: first, a vessel tracking step to extract the vessel topology and, second, fitting local surface data points with implicit blobby models at each node point on the vessel centerline.

  An extensive validation of our RANSAC-based vessel tracking algorithm was performed [14], by comparison with state of the art Multiple Hypothesis Testing [19] on 10 patient data. Fitting the implicit model to patient data relies on the minimization of a multi-termed energy. A closed form solution was derived, and a blob selection and subdivision heuristic was described to implement an efficient energy minimization algorithm. Both the geometric accuracy and compactness of the resulting vascular models were shown to be excellent [15].

  Our current goals are: first, to further enhance model compactness by relying on the robustness and versatility of the modeling algorithm and using sparser vascular centerline trees; second, to mathematically ensure the continuity between neighboring local implicit models; and third, to reintroduce the raw image data for a more accurate energy computation, with the aim to design a blobby deformable model.

  This model was implemented in Sofa simulation platform, enabling interactive simulation time and thereby showing an impressive realism during tool navigation. On-going preliminary medical evaluation is being carried on by our fellow interventional radiologist in the framework of intervention planning.

- **Designing respiration models for patient based simulators**
  The work presented here has been done within a collaboration with Imperial College of London, Bangor University and Inria Aviz team.

  Respiratory models could be a key component in increasing realism in medical simulators. We have previously developed such kind of model. However finding the good parameters to tune the model so that it corresponds to a real patient behavior is not an easy task.

  This year, we have studied methods to automatically tune the elasticity of soft-tissues and the respiratory model parameters based on patient data. The estimation is based on two 3D Computed Tomography scans of the same patient at two different time steps. The parametrization of the model is considered as an inverse problem. Optimization techniques have then been deployed to solve the problem.

  In [13], we used a random search algorithm to generate a given number of sets of 15 random parameters. The set of parameters that provides the lowest fitness is extracted and corresponds to the solution of the optimization problem.

In [9], we have made use of an ad-hoc evolutionary algorithm that is able to explore a search space with 15 dimensions. Our method is fully automatic and auto-adaptive. A compound fitness function has been designed to account for various quantities that have to be minimized. The algorithm efficiency was experimentally analyzed on several real test-cases: i) three patient datasets have been acquired with the "breath hold" protocol, and ii) two datasets corresponds to 4D CT scans. The performance was compared with two traditional methods (downhill simplex and conjugate gradient descent), our random search method and a basic real-valued genetic algorithm. The results showed that our evolutionary scheme provides more significantly stable and accurate results.

- **Physics-based augmented reality**
  The development of AR systems for use in the medical field faces one major challenge: the correct superposition of pre-operative data onto intraoperative images. This task is especially difficult when laparospic surgery is considered since superposition must be achieved on deformable organs. Most existing AR systems only consider rigid registration between the pre and intraoperative data and the transformation is often computed interactively or from markers attached to the patient's body. In cooperation with the Shacra team, we have introduced an original method to perform augmented or mixed reality on deformable objects. Compared to state-of-the-art techniques, our method is able to track deformations of volumetric objects and not only surfacic objects. A flexible framework that relies on the combination of 3D motion estimation obtained from stereoscopic data and a physics-based deformable model used as a regularization and interpolation step allows us to perform non-rigid and robust registration between the pre and intraoperative images [10].

MAIA Project-Team

6. New Results

6.1. Decision Making

6.1.1. Accounting for Uncertainty in Penetration Testing

Participants: Olivier Buffet, Jörg Hoffmann.

Carlos Sarraute (Core Security Technologies) is an external collaborator.

Core Security Technologies is an U.S.-American/Argentinian company providing, amongst other things, tools for (semi-)automated security checking of computer networks against outside hacking attacks. For automation of such checks, a module is needed that automatically generates potential attack paths. Since the application domain is highly dynamic, a module allowing to declaratively specify the environment (the network and its configuration) is highly advantageous. For that reason, Core Security Technologies have been looking into using AI Planning techniques for this purpose. After consulting by Jörg Hoffmann, they are now using a variant of Jörg Hoffmann's FF planner in their product. While that solution is satisfactory in many respects, it also has weaknesses. The main weakness is that it does not handle the incomplete knowledge in this domain – figuratively speaking, the attacker is assumed to have perfect information about the network. This results in high costs in terms of runtime and network traffic, for extensive scanning activities prior to planning.

We are currently working with Core Security's research department to overcome this issue, by modeling and solving the attack planning problem as a POMDP instead. A workshop paper detailing the POMDP model has been published at SecArt'11. While such a model yields much higher quality attacks, solving an entire network as a POMDP is not feasible. We have designed a decomposition method making use of network structure and approximations to overcome this problem, by using the POMDP model only to find good-quality attacks on single machines, and propagating the results through the network in an appropriate manner. This work has been published in ICAPS'12 [34].

6.1.2. Searching for Information with MDPs

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

In the context of Mauricio Araya's PhD, we are working on how MDPs —or related models— can search for information. This has led to various research directions, such as extending POMDPs so as to optimize information-based rewards, or actively learning MDP models. This year, we have focused on a novel optimistic Bayesian Reinforcement Learning algorithm –as described below– and on Mauricio's dissertation.

Exact or approximate solutions to Model-based Bayesian RL are impractical, so that a number of heuristic approaches have been considered, most of them relying on the principle of "optimism in the face of uncertainty". Some of these algorithms have properties that guarantee the quality of their outcome, inspired by the PAC-learning (Probably Approximately Correct) framework. For example, some algorithms provably make in most cases the same decision as would be made if the true model were known (PAC-MDP property).

We have proposed a novel optimistic algorithm, BOLT, that is

- appealing in that it is (i) optimistic *about* the uncertainty in the model and (ii) deterministic (thus easier to study); and
- provably PAC-BAMDP, i.e., makes in most cases the same decision as a perfect BRL algorithm would.

This work has been published in ICML'12 [9] and (in French) in JFPDA'12 [30], additional details appearing in [40].

6.1.3. Scheduling for Probabilistic Realtime Systems

Participant: Olivier Buffet.

Maxim Dorin, Luca Santinelli, Liliana Cucu-Grosjean (Inria, TRIO team), and Rob Davies (U. of York) are external collaborators.

In this collaborative research work (mainly with the TRIO team), we look at the problem of scheduling periodic tasks on a single processor, in the case where each task's period is a (known) random variable. In this setting, some job will necessarily be missed, so that one will try to satisfy some criteria depending on the number of deadline misses.

We have proposed three criteria: (1) satisfying pre-defined deadline miss ratios, (2) minimizing the worst deadline miss ratio, and (3) minimizing the average deadline miss ratio. For each criterion we propose an algorithm that computes a provably optimal fixed priority assignment, i.e., a solution obtained by assigning priorities to tasks and executing jobs by order of priority.

This work has been presented in RTNS'11, and an extended version is currently in preparation.

6.1.4. Adaptive Management with POMDPs

Participant: Olivier Buffet.

Iadine Chadès, Josie Carwardine, Tara G. Martin (CSIRO), Samuel Nicol (U. of Alaska Fairbanks) and Régis Sabbadin (INRA) 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 BRL.

Here, we consider that a number of experts provide us with one possible model each, assuming that one of them is the true model. This allows making decisions by solving a *hidden model MDP* (hmMDP). An hmMDP is essentially a simplified mixed observability MDP (MOMDP), where the hidden part of the state corresponds to the model (in cases where all other variables are fully observable).

From a theoretical point of view, we have proved that deciding whether a finite-horizon hmMDP problem admits a solution policy of value greater than a pre-defined threshold is a PSPACE-complete problem. We have also conducted preliminary studies of this approach, using the scenario of the protection of the Gouldian finch, and focusing on the particular characteristics that could be exploited to more efficiently solve this problem. These results have been presented in AAAI'12 [14].

6.1.5. 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 actionable cameras. This problem is difficult since the set of cameras cannot cover simultaneously the whole environment, since some persons can be hidden by obstacles or by other persons, and since the behavior of each person is governed by internal variables which can only be inferred (such as his motivation or his hunger).

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

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

6.1.6. Scaling Up Decentralized MDPs Through Heuristic Search

Participant: Jilles Dibangoye.

External collaborators: Christopher Amato, Arnaud Doniec.

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). The transition and observation independent Dec-MDP is a general subclass that has been shown to have complexity in NP, but optimal algorithms for this subclass are still inefficient in practice. We first provide an updated proof that an optimal policy does not depend on the histories of the agents, but only the local observations. We then present a new algorithm based on heuristic search that is able to expand search nodes by using constraint optimization. We show experimental results comparing our approach with the state-of-the-art Dec-MDP and Dec-POMDP solvers. These results show a reduction in computation time and an increase in scalability by multiple orders of magnitude in a number of benchmarks.

This work was presented in UAI'2012 [16].

6.1.7. Approximate Modified Policy Iteration

Participant: Bruno Scherrer.

External collaborators: Victor Gabillon, Mohammad Ghavamzadeh and Matthieu Geist.

Modified policy iteration (MPI) is a dynamic programming (DP) algorithm that contains the two celebrated policy and value iteration methods. Despite its generality, MPI has not been thoroughly studied, especially its approximation form which is used when the state and/or action spaces are large or infinite. We have proposed three implementations of approximate MPI (AMPI) that are extensions of well-known approximate DP algorithms: fitted-value iteration, fitted-Q iteration, and classification-based policy iteration. We have provided an error propagation analysis that unifies those for approximate policy and value iteration. For the classification-based implementation, we have developed a finite-sample analysis that shows that MPI's main parameter allows to control the balance between the estimation error of the classifier and the overall value function approximation.

This work was presented in JFPDA'2012 [35] and ICML'2012 [45].

6.1.8. A Dantzig Selector Approach to Temporal Difference Learning

Participant: Bruno Scherrer.

External collaborators: Matthieu Geist, Mohammad Ghavamzadeh and Alessandro Lazaric.

LSTD is one of the most popular reinforcement learning algorithms for value function approximation. Whenever the number of samples is larger than the number of features, LSTD must be paired with some form of regularization. In particular, L_1-regularization methods tend to perform feature selection by promoting sparsity and thus they are particularly suited in high-dimensional problems. Nonetheless, since LSTD is not a simple regression algorithm but it solves a fixed-point problem, the integration with L_1-regularization is not straightforward and it might come with some drawbacks (see e.g., the P-matrix assumption for LASSO-TD). We have introduced a novel algorithm obtained by integrating LSTD with the Dantzig Selector. In particular, we have investigated the performance of the algorithm and its relationship with existing regularized approaches, showing how it overcomes some of the drawbacks of existing solutions.

This work was presented at JFPDA'2012 [33] and ICML'2012 [20].

6.1.9. On the Use of Non-Stationary Policies for Stationary Infinite-Horizon Markov Decision Processes

Participants: Bruno Scherrer, Boris Lesner.

In infinite-horizon stationary γ-discounted Markov Decision Processes, it is known that there exists a stationary optimal policy. Using Value and Policy Iteration with some error ϵ at each iteration, it is well-known that one can compute stationary policies that are $\frac{2\gamma}{(1-\gamma)^2}\epsilon$-optimal. After having shown that this guarantee is tight, we have developed variations of Value and Policy Iteration for computing non-stationary policies that can be up to $\frac{2\gamma}{1-\gamma}\epsilon$-optimal, which constitutes a significant improvement in the usual situation when γ is close to 1. Surprisingly, this shows that the problem of "computing near-optimal non-stationary policies" is much simpler than that of "computing near-optimal stationary policies".

This work was presented and selected for a full oral presentation at NIPS'2012 [28].

6.1.10. Developmental Reinforcement Learning

Participant: Alain Dutech.

External collaborators: Matthieu Geist (IMS Supelec), Olivier Pietquin (IMS Supelec)

Reinforcement Learning in rich, complex and large sensorimotor spaces is a difficult problem mainly because the exploration of such a huge space cannot be done in an extensive way. The idea is thus to adopt a developmental approach where the perception and motor skills of the robot can grow in richness and complexity during learning, as a consequence the size of the state and action spaces grows progressively when the performances of the learning agent increases. The learning framework relies on function approximators with specific properties (continuous input space, life-long adaptation, knowledge transfer). Architectures based on "reservoir learning" and "dynamical self-organizing maps" kind of artificial neural networks have been investigated [32], [18].

6.1.11. Dialog and POMDPs

Participant: Lucie Daubigney.

Reinforcement learning (RL) is now part of the state of the art in the domain of spoken dialog systems (SDS) optimization. The best performing RL methods, such as those based on Gaussian Processes, require to test small changes in the policy to assess them as improvements or degradations. This process is called on policy learning. Nevertheless, it can result in system behaviors that are not acceptable by users. Learning algorithms should ideally infer an optimal strategy by observing interactions generated by a non-optimal but acceptable strategy, that is learning off-policy. Such methods usually fail to scale up and are thus not suited for real-world systems. In this work, a sample-efficient, on-line and off-policy RL algorithm is proposed to learn an optimal policy [15]. This algorithm is combined to a compact non-linear value function representation (namely a multilayer perceptron) enabling to handle large scale systems. One of the application domain is the teaching of a second language [31].

6.1.12. SAP Speaks PDDL: Exploiting a Software-Engineering Model for Planning in Business Process Management

Participant: Jörg Hoffmann.

Ingo Weber (NICTA) and Frank Michael Kraft (bpmnforum.net) are external collaborators.

Planning is concerned with the automated solution of action sequencing problems described in declarative languages giving the action preconditions and effects. One important application area for such technology is the creation of new processes in Business Process Management (BPM), which is essential in an ever more dynamic business environment. A major obstacle for the application of Planning in this area lies in the modeling. Obtaining a suitable model to plan with – ideally a description in PDDL, the most commonly used planning language – is often prohibitively complicated and/or costly. Our core observation in this work is that this problem can be ameliorated by leveraging synergies with model-based software development. Our application at SAP, one of the leading vendors of enterprise software, demonstrates that even one-to-one model re-use is possible.

The model in question is called Status and Action Management (SAM). It describes the behavior of Business Objects (BO), i.e., large-scale data structures, at a level of abstraction corresponding to the language of business experts. SAM covers more than 400 kinds of BOs, each of which is described in terms of a set of status variables and how their values are required for, and affected by, processing steps (actions) that are atomic from a business perspective. SAM was developed by SAP as part of a major model-based software engineering effort. We show herein that one can use this same model for planning, thus obtaining a BPM planning application that incurs no modeling overhead at all.

We compile SAM into a variant of PDDL, and adapt an off-the-shelf planner to solve this kind of problem. Thanks to the resulting technology, business experts may create new processes simply by specifying the desired behavior in terms of status variable value changes: effectively, by describing the process in their own language.

This work has been published in JAIR [6].

6.1.13. Resource-Constrained Planning: A Monte Carlo Random Walk Approach

Participant: Jörg Hoffmann.

Hootan Nakhost and Martin Müller (University of Alberta) are external collaborators.

The need to economize limited resources, such as fuel or money, is a ubiquitous feature of planning problems. If the resources cannot be replenished, the planner must make do with the initial supply. It is then of paramount importance how constrained the problem is, i.e., whether and to which extent the initial resource supply exceeds the minimum need. While there is a large body of literature on numeric planning and planning with resources, such resource constrainedness has only been scantily investigated. We herein start to address this in more detail. We generalize the previous notion of resource constrainedness, characterized through a numeric problem feature $C \leq 1$, to the case of multiple resources. We implement an extended benchmark suite controlling C. We conduct a large-scale study of the current state of the art as a function of C, highlighting which techniques contribute to success. We introduce two new techniques on top of a recent Monte Carlo Random Walk method, resulting in a planner that, in these benchmarks, outperforms previous planners when resources are scarce (C close to 1). We investigate the parameters influencing the performance of that planner, and we show that one of the two new techniques works well also on the regular IPC benchmarks.

This work has been published in ICAPS-12 [26].

6.1.14. How to Relax a Bisimulation?

Participants: Michael Katz, Jörg Hoffmann.

Malte Helmert (Basel University) is an external collaborator.

Merge-and-shrink abstraction (M&S) is an approach for constructing admissible heuristic functions for cost-optimal planning. It enables the targeted design of abstractions, by allowing to choose individual pairs of (abstract) states to aggregate into one. A key question is how to actually make these choices, so as to obtain an informed heuristic at reasonable computational cost. Recent work has addressed this via the well-known notion of bisimulation. When aggregating only bisimilar states – essentially, states whose behavior is identical under every planning operator – M&S yields a perfect heuristic. However, bisimulations are typically exponentially large. Thus we must relax the bisimulation criterion, so that it applies to more state pairs, and yields smaller abstractions. We herein devise a fine-grained method for doing so. We restrict the bisimulation criterion to consider only a subset K of the planning operators. We show that, if K is chosen appropriately, then M&S still yields a perfect heuristic, while abstraction size may decrease exponentially. Designing practical approximations for K, we obtain M&S heuristics that are competitive with the state of the art.

This work has been published in ICAPS-12 [22], and as Inria research report RR-7901 [42].

6.1.15. Semi-Relaxed Plan Heuristics

Participants: Emil Keider, Jörg Hoffmann.

Patrik Haslum (ANU) is an external collaborator.

Heuristics based on the delete relaxation are at the forefront of modern domain-independent planning techniques. Here we introduce a principled and flexible technique for augmenting delete-relaxed tasks with a limited amount of delete information, by introducing special fluents that explicitly represent conjunctions of fluents in the original planning task. Differently from previous work in this direction, conditional effects are used to limit the growth of the task to be linear, rather than exponential, in the number of conjunctions that are introduced, making its use for obtaining heuristic functions feasible. We discuss how to obtain an informative set of conjunctions to be represented explicitly, and analyze and extend existing methods for relaxed planning in the presence of conditional effects. The resulting heuristics are empirically evaluated, and shown to be sometimes much more informative than standard delete-relaxation heuristics.

This work has been published in ICAPS-12 [24].

6.1.16. Structural Patterns Beyond Forks: Extending the Complexity Boundaries of Classical Planning

Participants: Michael Katz, Emil Keider.

Tractability analysis in terms of the causal graphs of planning problems has emerged as an important area of research in recent years, leading to new methods for the derivation of domain-independent heuristics (Katz and Domshlak 2010). Here we continue this work, extending our knowledge of the frontier between tractable and NP-complete fragments. We close some gaps left in previous work, and introduce novel causal graph fragments that we call the hourglass and semi-fork, for which under certain additional assumptions optimal planning is in P. We show that relaxing any one of the restrictions required for this tractability leads to NP-complete problems. Our results are of both theoretical and practical interest, as these fragments can be used in existing frameworks to derive new abstraction heuristics. Before they can be used, however, a number of practical issues must be addressed. We discuss these issues and propose some solutions.

This work has been published in AAAI-12 [23].

6.2. Understanding and mastering complex systems

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

Participants: Vincent Chevrier, Tomas Navarrete.

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

Complex systems are present everywhere in our environment: internet, electricity distribution networks, transport networks. These systems have the following characteristics: a large number of autonomous entities, dynamic structures, different time and space scales and emergent phenomena. This 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[1] 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.

6.2.2. Multi Modeling and multi-simulation

Participants: Vincent Chevrier, Christine Bourjot, Benjamin Camus.

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

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 [56] is to build a society of models, simulators and simulation softwares that solves the core challenges of multimodelling and simulation coupling in an homogeneous perspective.

This year we focused on systems that naturally involve entities at different levels of description: micro and macro levels with their dynamics and and their articulations : emergence (upward causation, from micro to macro levels) and immergence (downward causation, from macro to micro levels). We relied on Bourgine's generic view of the relationship between complex phenomenon's levels and their temporal evolution [50]. We proposed an extension of the AA4MM concepts[13] in order to adapt them to emergence and immergence specifications. A simple example of multi-level modeling of a flocking phenomenon has been implemented to illustrate our proposal.

6.2.3. Robustness of Cellular Automata and Reactive Multi-Agent Systems

Participants: Olivier Bouré, Vincent Chevrier, Nazim Fatès.

Our research on emergent collective behaviours focuses on robustness analysis, that is the behavioural resistance to perturbations in collective systems. We progressed in the knowledge of how to tackle this issue in the case of cellular automata (CA) and multi-agent systems (MAS).

The density classification problem was taken as a simple example for studying how decentralised computations can be carried out with simple cells. Although it is known that this problem can not be solved perfectly, we derived analytic calculations to understand how stochastic cellular automata provide good solutions [3]. A collaboration with mathematicians lead us to study how to extend this result to the infinite-space case [25] and to the 2D finite case [19].

Two papers resulting from the Amybia projects were published : experimental results on phase transitions obtained with FPGAs [7] and the description on a robotics experiment that demonstrates the robustness of a bio-inspired aggregation method [5].

The results on asynchronous information transmission in cellular automata were consolidated [2]. Original definitions of asynchronism were also developed in lattice-gas cellular automata [11], which allows us to complete our spectrum of models for which robustness can be studied analytically and with numerical simulations.

6.2.4. Robotics Systems and Ambiant Intelligence

6.2.4.1. Robotics systems : autonomy, cooperation, robustness

6.2.4.1.1. Local control based platooning

Participants: Alexis Scheuer, Olivier Simonin, François Charpillet, Jano Yazbeck.

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

In order to reduce the tracking error (*i.e.* the distance between each follower's path and the path of its predecessor), we developed both an innovative approach [58] and a new lateral control law. This lateral control law reduces the tracking error faster than other existing control laws. This control law, and the experimental results obtained with it, has been submitted to 2013 IEEE International Conference on Robotics and Automation. Its integration with a previously defined secure longitudinal control law [55] has also been studied, and will be submitted soon to 2013 IFAC Intelligent Autonomous Vehicles Symposium.

6.2.4.1.2. Adaptation of autonomous vehicle traffic to perturbations

Participants: Mohamed Tlig, Olivier Simonin, Olivier Buffet.

In the context of the European project InTraDE, the problem studied in the context of Mohamed Tlig's PhD thesis is to handle the displacements of numerous IAVs (Intelligent Autonomous Vehicles) in a seaport. Here we assume a supervisor planning the routes of the vehicles in the port. 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.

We started focusing on a first important sub-problem of space resource sharing among multiple agents: how to ensure the crossing of two opposed flows of vehicles on a road when one of the two paths is blocked by an obstacle. To overcome this problem, blocked vehicles have to coordinate with vehicles of the other side to share the road and manage delays. The objective is to improve traffic flow and reduce the emergence of traffic jam. After formalizing this problem, we have defined and studied in simulation two decision rules that produce two different strategies: the first one alternates between two vehicles from each side of the road, and the second one gives priority to the vehicle with the highest delay. This work has been presented in ICTAI'12 [29].

We are now considering more complex situations, e.g., when multiple flows of vehicles share more than one crossroad.

6.2.4.1.3. Multi-robot exploration and mapping : The Carotte Challenge

Participants: Olivier Simonin, François Charpillet, Antoine Bautin, Nicolas Beaufort.

In the context of the ANR/DGA Carotte Challenge, we study since 2009 new strategies and algorithms for multi-robot exploration and mapping. The proposed models are experimented with real autonomous mobile robots at LORIA and every year at the Carotte challenge. Our consortium, called "Cart-o-matic", is composed of members from Université d'Angers (LISA) and from Maia team-project (our industrial partner has left the consortium in 2011).

The year 2012 produced several results :

- In June, **we won the final edition of the Carotte challenge !** This result was obtained in particular by the efficiency and the robustness of the multi-robot strategy we proposed. Our system also provided one of the best map of the contest.
- We developed a software platform, including SLAM, Planning and multi-robot explorations algorithms. These softwares have been protected by copyrights (APP), see 5.4 .
- We presented the results in different publications : RIA revue [8], ICIRA'2012 International Conference [10] (Finalist for the Best student paper).
- Antoine Bautin wrote his PhD thesis, that he will defend in the beginning of year 2013. This work proposes new frontier assignation algorithms for multi-robot exploration. We defined a new heuristics, based on counting the robots towards a frontier rather than considering only the distance between robots and frontiers. For these purpose we developed algorithms based on wavefronts computations (artificial potential fields).We measured on benchmarks that our algorithm outperforms the two classical approaches *closest frontier* and *Greedy assignation*.
- In Oct. 2012, Nassim Kaldé started a PhD thesis (MENRT scholarship), advised by F. Charpillet and O. Simonin. We aim at continuing the work of the Cartomatic project, under new hypothesis and constrains on communications and complexity of the environment to explore.

6.2.4.2. Intelligent environments and health assistance

6.2.4.2.1. Spatial computing: iTiles network

Participants: Olivier Simonin, François Charpillet, Lionel Havet, Mihai Andries.

Olivier Rochel (Inria research engineer, SED Nancy) is an external collaborator.

In the context of ambient intelligence and robotic assistance, we explore the definition of an active floor composed of connected nodes, forming a network of cells. We consider different way of computation, as spatial calculus, to define robust and self-adaptive functions in the environment. We aim at dealing with walk analysis, surveillance of people activity (actimetry) and assistance (control of assistant robots, etc.).

This work can be summarized in several points :

- We asked Hikob company to design the iTile model we defined at the end of year 2011. In 2012, a network of 90 iTiles has been installed on the floor of the smart apartment of the center. This apartment is an experimental platform developed in the context of the "Situated Computer Science" Action of the CPER MISN (Lorraine region, Inria and government fundings). See InfoSitu.
- Each iTile is composed of one node connected to embedded sensors and to its neighboring tiles. A tile holds 4 weight sensors, an accelerometer and 16 LEDs. A simulator of the iTile network has been developed by Olivier Rochel. This tools makes easier the development on the real tiles.
- Several functions have been developed and are currently under experiments: (i) detection of a person walking on the floor (ii) tracking of feet position (iii) propagation and display of information in the network.
- We are involved since 2010 in the PAL Inria large scale initiative (Personally Assisted Living). In this context, Mihai Andries started a PhD thesis in oct. 2012 (funded by Inria-PAL). This PhD. aims at studying the iTiles model and its possibility for assistance functions. We also study models allowing robots to interact and to use the iTile network.

6.2.4.2.2. Center of pressure and Step Detection of a person walking on our intelligent floor

Participants: Amandine Dubois, François Charpillet.

It is quite easy to estimate in realtime the center of pressure of a person walking on the intelligent floor described above. From a sequence of center of pressure, we conceived a system categorizing the set of measures into two sets :

- foot: the measure belongs to the pressure trace left by a foot on the floor,
- transition: the center of pressure corresponds to what happens when the person passes his right leg or left from backwards to forwards.

This has been done in a first time using an heuristic algorithm and then using an HMM. From this categorization it's then easy to estimate classical gait parameters such as length of the steps or speed of the walk.

6.2.4.2.3. Pose estimation of several kinects

Participants: Nicolas Beaufort, François Charpillet.

Tracking one or several persons using several Kinects required to solved the calibration, i.e estimation of the pose of each kinect in the scene, knowing that the area covered by each Depth camera don't overlap with other (because of interference). We have addressed this issue using a SLAM approach implemented within a GPU.

6.2.4.2.4. Fall prevention and Fall detection

Participants: Amandine Dubois, François Charpillet.

A major problem of public health is the loss of autonomy of elderly people usually caused by the falls. Since 2003 one of the goal of MAIA team is to develop a system allowing to detect falls and also to analyze the gait deterioration to prevent falls. A first approach consisted in developing a markerless human motion capture system estimating the 3D positions of the body joints over time. This system used a dynamic Bayesian network and a factored particle filtering algorithm. Since 2011, we used a new approach using Microsoft Kinect camera which allows to acquire at the same time a RGB and a depth image to deal of the problem of the gait. After the extraction of the human from the background, we calculate the gait parameters from the center of mass of a person. Some parameters, as the length and the time of steps, the speed of the gait, allow to predict a deterioration of the gait of a person and an increase of the risk of falls [17].

Another use of the extraction of center of mass of a person from the Kinect camera is to determine the activity of a person. The method uses a Hidden Markov Model to distinguish eight activities of the daily life (sitting, walking, lying (on a couch, on a bed), lying down, falling, going up on the obstacles, squatting and bending). We set up an experiment in a smart room to validate our results. Concerning the gait parameters we compare them to the real values obtained making the young subjects wake with pads soaked with ink under the shoes on the paper. The results show that there is a difference of 3-4cm between length provided by our Kinect algorithm and the real length provided by the paper. Concerning the detection of the activity, we ask to 28 subjects to perform eight situations (corresponding to the eight states of the HMM). The results showed that each situation is recognized exept “bending”, falls are detected correctly and there are no false positives except “sitting” and “qqsquatting” which are detected instead of “bending”.

MASAIE Project-Team

5. New Results

5.1. Robustness and $\mathcal{R}_0$

We have obtained new results about the relation between Robustness and the basic reproduction number $\mathcal{R}_0$.
It is now well admitted that the basic reproduction ratio $\mathcal{R}_0$ is a key concept in mathematical epidemiology and the literature devoted to this concept is now quite important, see [20], [40], [19], [22], [23], [24], [26], [28], [30], [34] and references therein.
This number is a threshold parameter for bifurcation of an epidemic system : for a general compartmental disease transmission model, if $\mathcal{R}_0 < 1$, the disease free equilibrium (DFE) is locally asymptotically stable; whereas, if $\mathcal{R}_0 > 1$, the DFE is unstable.
It is said in some papers that $\mathcal{R}_0$ is a measure to gauge the amount of uniform effort needed to eliminate infection from a population [22], [24], [25], [31], [30].
The concept of robustness, coming from control theory, is associated to uncertainty. Usually the parameters of a system are known within a certain margin. A question is, how some properties, e.g. stability, can be ascertained with uncertainty on the parameters. In control theory "stability margin" is an important concept. Another way to formulate this problem is to analyze the effect of perturbations, unstructured or structured. This problem is also related to the so-called pseudo-spectrum [36], [37], [35].
We found that the basic reproduction number of an epidemic system is not an accurate gauge of the distance from the Jacobian J of this system, computed at the disease free equilibrium, to the set of stable matrices (if J in unstable), respectively to the set of unstable matrices (if J is stable). The same conclusion arises for another indicator, introduced by Heestebeck et al. [24], [31], [30], the type-reproduction number.

5.2. Wolbachia and Dengue

Wolbachia is a genus of bacteria which infects arthropod species, including a high proportion of insects. It is one of the world's most common parasitic microbes and is possibly the most common reproductive parasite in the biosphere. *Wolbachia* is a maternally inherited endosymbiont of a large number of insects and other arthropods that induces various effects on host reproductive biology. Estimated to infect more than 60% of all insect species *Wolbachia* species are present in mature eggs, but not mature sperm. Only infected females pass the infection on to their offspring. Another consequence of infection is cytoplasmic incompatibility, i.e., the inability of *Wolbachia*-infected males to successfully reproduce with uninfected females.
The successful introduction of a life-shortening strain of *Wolbachia* into the dengue vector *Aedes aegypti* that halves adult lifespan has recently been reported.
Mosquitoes carrying this *Wolbachia* strain show around a 50% reduction in adult female lifespan compared to uninfected mosquitoes. It has been reported that wMel and wMelPop-CLA strains block transmission of dengue serotype 2 (DENV-2) in *Aedes aegypti*, forming the basis of a practical approach to dengue suppression. Infection by *Wolbachia* has a triple effect : reduction of recruitment, increasing of mortality for the mosquitoes and reduction of dengue transmission.
With our colleague of Brazil (see International cooperation) we built and study different models for the introduction of *Wolbachia* in a population of *Aedes aegypti*. These models are epidemiological models with vertical transmission only, which is quite new. We found that bistabilty does exist : three equilibria are present. We show that the coexistence equilibrium is unstable. We show that the equilibrium without infection and the equilibrium with the whole population infected are asymptotically stable. Numerical experimentation shows that the basin of the second equilibrium is appreciable. This indicates that introduction of *Wolbachia* is feasible. The connection of theses models with transmission models of dengue is under investigation by the French-Brazilian team.

5.3. Bilharzia

Schistosomiasis or bilharzia is a water-borne parasitic disease that affects 200 million people and poses a treat to 600 million in more than 76 countries [39]. It is caused by blood-dwelling fluke worms of the genus *Schistosoma*. The transmission cycle requires contamination of surface water by excreta, specific freshwater snails as intermediate hosts, and human water contact [21]. Schistosome are transmitted via contact with contaminated water containing cercaria the infective stage of the parasite [39], [32].
In connection with EPLS, a research NGO based in Saint-Louis (Senegal), and Pasteur Institute of Lille, we investigate a spatially deterministic metapopulation model in which infectious agents persist within a network of connected environments. This model accounts for human population age and behavior structure. We completely analyses the asymptotic behavior of this model. We give a formula for computing the basic reproduction ratio $\mathcal{R}_0$. If $\mathcal{R}_0 \leq 1$ we prove that the disease free equilibrium is globally asymptotically stable. If $\mathcal{R}_0 > 1$, with an hypothesis on connectedness, we prove that there exists a unique positive endemic equilibrium, which is globally asymptotically stable.
The validation of this model, using data of EPLS, is under investigation and is the subject of a Phd thesis. The defense will occur at the beginning of 2013. We explore the identification of key parameters using different kind of observers.

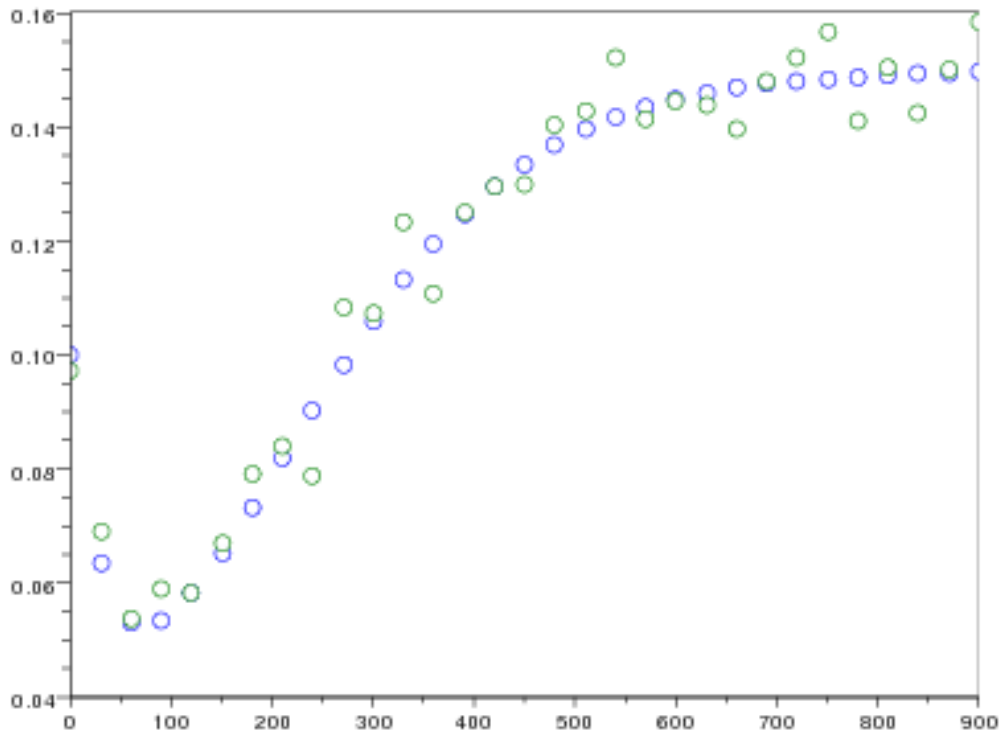

Figure 1. Noisy and discrete measure of host prevalence

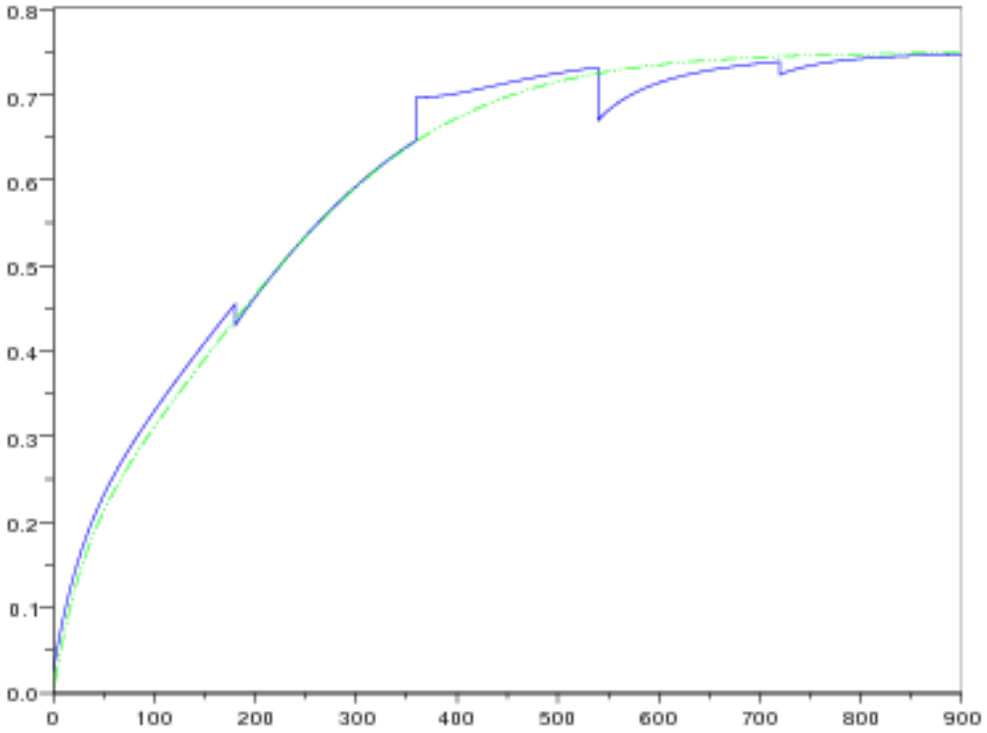

Figure 2. Reconstruction of the snail prevalence from preceding data

ORPAILLEUR Project-Team

6. New Results

6.1. The Mining of Complex Data

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

formal concept analysis, relational concept analysis, pattern structures, search for frequent itemsets, association rule extraction, mining of complex data, graph mining, skylines, sequence mining, FCA in spatial and temporal reasoning

Formal concept analysis, together with itemset search and association rule extraction, are suitable symbolic methods for KDDK, that may be used for real-sized applications. Global improvements may be 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 working on extensions of such symbolic data mining methods to be applied on complex data such as biological or chemical data or textual documents, involving objects with multi-valued attributes (e.g. domains or intervals), n-ary relations, sequences, trees and graphs.

6.1.1. FCA, RCA, and Pattern Structures

Recent advances in data and knowledge engineering have emphasized the need for Formal Concept Analysis (FCA) tools taking into account structured data. 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 [116]. The RCA process takes as input a collection of contexts and of inter-context relations, and yields a set of lattices, one per context, whose concepts are linked by relations. RCA has an important role in KDDK, especially in text mining [86], [85].

Another extension of FCA is based on Pattern Structures (PS) [94], which allows to build a concept lattice from complex data, e.g. nominal, numerical, and interval data. In [101]), pattern structures are used for building a concept lattice from intervals, in full compliance with FCA, thus benefiting of the efficiency of FCA algorithms. Actually, the notion of similarity between objects is closely related to these extensions of FCA: 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). Various results were obtained in the study of the relations existing between FCA with an embedded explicit similarity measure and FCA with pattern structures [100]. Moreover, similarity is not a transitive relation and this lead us to the study of tolerance relations. In addition, a new research perspective is aimed at using frequent itemset search methods for mining interval-based data being guided by pattern structures and biclustering as well.

6.1.2. Advances in FCA and Pattern Mining

In the context of environmental sciences, research work is in concern with the mining of complex hydroecological data with concept lattices. In particular, Florence Le Ber –as a member of UMR 7517 Lhyges, Strasbourg– is the scientific head of an ANR project named “FRESQUEAU” (2011–2014) dealing with FCA and data mining and hydroecological data (see http://engees.unistra.fr/site/recherche/projets/anr-fresqueau/).

In this framework, concept lattices based on multi-valued contexts have been used for characterizing macroinvertebrate communities in wetland and their seasonal evolution [19]. Within the ANR Fresqueau project we are studying tools for sequential pattern extraction taking into account spatial relations [56], [43].

From another point of view, miscanthus is a perennial crop used for biomass production. Its implantation is rather new, and there is few farms cultivating miscanthus in France. Understanding the farmers' choices for allocating miscanthus in their farmland is a main challenge. The CBR model is investigated for modeling these choices from farm surveys, including spatial reasoning aspects [20], [47] [41].

For completing the work on FCA and itemset search, there is still on-going work on frequent and rare itemset search, for being able to build lattices from very large data and completing the algorithm collection of the Coron platform. Work is still in progress on the design of an integrated and modular algorithm for searching for closed and generators itemsets, and equivalence classes of itemsets, thus enabling the construction of the associated lattice [121]. This research aspect is also linked to the research carried on within a the PICS CaDoE research project (see Section 8.1.1.3). In addition, there is also research work carried on different aspects involving the management of big data in the context of the BioIntelligence Project and the Quaero Project.

6.1.3. Skylines, sequential data, privacy and E-sports analytics

Pattern discovery is at the core of numerous data mining tasks. Although many methods focus on efficiency in pattern mining, they still suffer from the problem of choosing a threshold that influences the final extraction result. One goal is to make the results of pattern mining useful from a user-preference point of view. That is, take into account some domain knowledge to guide the pattern mining process. To this end, we integrate into the pattern discovery process the idea of skyline queries in order to mine *skyline patterns* in a threshold-free manner. This forms the basis for a novel approach to mining skyline patterns. The efficiency of our approach was illustrated over a use case from *chemoinformatics* and we showed that small sets of dominant patterns are produced under various measures that are interesting for chemical engineers and researchers.

Sequence data is widely used in many applications. Consequently, mining sequential patterns and other types of knowledge from sequence data has become an important data mining task. The main emphasis has been on developing efficient mining algorithms and effective pattern representation.

However, important fundamental problems still remained open: (i) given a sequence database, can we have an upper bound on the number of sequential patterns in the database? (ii) Is the efficiency of the sequence classifier only based on accuracy? (iii) Do the classifiers need the entire set of extracted patterns or a smaller set with the same expressiveness power?

In the field of the management of sequential date in medicine, analysis of health care trajectories led to the development of a new sequential pattern mining method [42]. The MMISP algorithm is able to efficiently extract sequential patterns composed of itemsets and multidimensional items. The multidimensional items can be described with additional taxonomic knowledge, allowing mining with appropriate levels of granularity. In parallel, a new measure has been created to compute the similarity between sequences of itemsets [78].

Orpailleur is one of the few project-teams working on privacy challenges which are becoming a core issue with different scientific problems in computer science. With technology infiltrating more and more every aspect of our lives, each human activity leaves a digital trace in some repository. Vast amounts of personal data are implicitly or explicitly created each day, and rarely one is aware of the extent of information that is kept, processed and analyzed without his knowledge or consent. These personal data give rise to significant concerns about user privacy, since important and sensitive details about private life are collected and exploited by third parties. The goal of privacy preservation technologies is to provide tools that allow greater control over the dissemination of user data. A promising trend in the field is Privacy Preserving Data Publishing (PPDP), which allows sharing of anonymized data. Anonymizing a dataset is not limited to the removal of direct identifiers that might exist in a dataset, e.g. the full name or the Social Security Number of a person. It also includes removing secondary information, e.g. like age, zip code that might lead indirectly to the true identity of an individual.

Existing research on this problem either perturbs the data, publishes them in disjoint groups disassociated from their sensitive labels, or generalizes their values by assuming the availability of a generalization hierarchy. In a recent work, we proposed a novel alternative [54]. Our publication method also puts data in a generalized

form, but does not require that published records form disjoint groups and does not assume a hierarchy either. Instead, it employs generalized bitmaps and recasts data values in a nonreciprocal manner.

One of the most fascinating challenges of our time is understanding the complexity of the global interconnected society we inhabit. Today we have the opportunity to observe and measure how our society intimately works, by analyzing the big data. i.e, the digital breadcrumbs of human activities sensed as a by-product of the ICT systems that we use. These data describe the daily human activities: for instance, automated payment systems record the tracks of our purchases, search engines record the logs of our queries for finding information on the web, social networking services record our connections to friends, colleagues and collaborators, wireless networks and mobile devices record the traces of our movements and our communications. These social data are at the heart of the idea of a knowledge society, where decisions can be taken on the basis of knowledge in these data.

Social network data analysis raises concerns about the privacy of related entities or individuals. We theoretically establish that any kind of structural identification attack can effectively be prevented using random edge perturbation and show that, surprisingly, important properties of the whole network, as well as of subgraphs thereof, can be accurately calculated and hence data analysis tasks performed on the perturbed data, given that the legitimate data recipient knows the perturbation probability as well [53].

"Electronic-sport" (E-Sport) is now established as a new entertainment genre. More and more players enjoy streaming their games, which attract even more viewers. In fact, in a recent social study, casual players were found to prefer watching professional gamers rather than playing the game themselves. Within this context, advertising provides a significant source of revenue to the professional players, the casters (displaying other people's games) and the game streaming platforms. In a recent work with Mehdi Kaytoue, we started focusing on the huge amount of data generated by electronic games. We crawled, during more than 100 days, the most popular among such specialized platforms: Twitch.tv.

Thanks to these gigabytes of data, we proposed a first characterization of a new Web community, and we showed, among other results, that the number of viewers of a streaming session evolves in a predictable way, that audience peaks of a game are explainable and that a Condorcet method can be used to sensibly rank the streamers by popularity [45]. This work should bring to light the study of E-Sport and its growing community for computer scientists and sociologists. They indeed deserve the attention of industrial partners (for the large amount of money involved) and researchers (for interesting problems in social network dynamics, personalized recommendation, sentiment analysis, etc.).

6.1.4. KDDK in Text Mining

Ontologies help software and human agents to communicate by providing shared and common domain knowledge, and by supporting various tasks, e.g. problem-solving and information retrieval. In practice, building an ontology depends on a number of "ontological resources" having different types: thesaurus, dictionaries, texts, databases, and ontologies themselves. We are currently working on the design of a methodology and the implementation of a system for ontology engineering from heterogeneous ontological resources. This methodology is based on both FCA and RCA, and was previously successfully applied in contexts such as astronomy and biology. At present, an engineer is implementing a robust system being guided by the previous research results and preparing the way for some new research directions involving trees and graphs (see also the work on the ANR Hybride project).

6.2. KDDK in Life Sciences

Participants: Yasmine Assess, Emmanuel Bresso, Thomas Bourquard, Adrien Coulet, Marie-Dominique Devignes, Anisah Ghoorah, Renaud Grisoni, Jean-François Kneib, Florence Le Ber, Bernard Maigret, Jean-François Mari, Amedeo Napoli, Violeta Pérez-Nueno, Dave Ritchie, Malika Smaïl-Tabbone.

The Life Sciences constitute a challenging domain in which to implement knowledge-guided approaches for knowledge discovery. Biological data are complex from many points of views: voluminous, high-dimensional, deeply inter-connected, etc. Analyzing such data and extracting hidden knowledge has become a crucial issue in important domains such as health, environment and agronomy. More and more bio-ontologies are available and can be used to enhance the knowledge discovery process [88], [117]. In the next few years, the experience of the Orpailleur team in KDDK applied to the Life Sciences will be further developed in two directions: the use of bio-ontologies to improve approaches for data integration and mining when applied to real-world data, and the study of the synergy between numeric and symbolic data-mining methods in life-science applications.

6.2.1. Relational data mining applied to complex biological object characterization and prediction

Inductive Logic Programming (ILP) is a learning method which allows expressive representation of the data and produces explicit first-order logic rules. However, any ILP system returns a single theory based on heuristic user-choices of various parameters and learning biases, thus ignoring potentially relevant rules. Accordingly, we propose an approach based on Formal Concept Analysis for effective interpretation of reached theories with the possibility of adding domain knowledge. Our approach was applied to the characterization of three-dimensional (3D) protein-binding sites, namely phosphorylation sites, which are the protein portions on which interactions with other proteins take place [33]. In this context, we defined a logical representation of 3D patches and formalized the problem as a concept learning problem using ILP. Another application of this KDDK methodology concerns the characterization and prediction of drug side-effect profiles (Journal manuscript in preparation). In this case, maximal frequent itemsets are extracted and allow us to propose relevant side-effect profiles of drugs which are further characterized by ILP.

6.2.2. Functional classification of genes using semantic similarity matrix and various clustering approaches

In the last report, we proposed a measure called IntelliGO which computes semantic similarity between genes for discovering biological functions shared by a set of genes (e.g., showing the same expression profile). This measure takes into account domain knowledge represented in Gene Ontology (GO) [83].

Functional classification aims at grouping genes according to their molecular function or the biological process they participate in. Evaluating the validity of such unsupervised gene classification remains a challenge given the variety of distance measures and classification algorithms that can be used. We evaluated functional classification of genes with the help of reference sets. Overlaps between clusters and reference sets are estimated by the F-score metric. We test the IntelliGO measure with hierarchical and fuzzy C-means clustering algorithms and we compare results with the state-of-the-art DAVID functional classification method (Database for Annotation Visualization and Integrated Discovery). Finally, study of best matching clusters to reference sets leads us to propose a method based on set-differences for discovering missing information.

The IntelliGO-based functional clustering method was tested on four benchmarking datasets consisting of biological pathways (KEGG database) and functional domains (Pfam database) [13]. The IntelliGO measure is usable on line (see http://bioinfo.loria.fr/Members/benabdsi/intelligo_project/).

We are currently investigating the clustering problem when objects are not represented as feature vectors in a vector space but as a pairwise similarity matrix. In biology such similarity measures are often computationally expensive or incompatible with *bona fide* distance definition. Embedding techniques of pairwise data into Euclidean space aim at facilitating subsequent clustering of the objects [115]. Spectral clustering methods are also relevant in this case [127]. We are conducting comparative and large-scale gene clustering evaluation using the Intelligo measure and reference sets.

6.2.3. Analysis of biomedical data annotated with ontologies

Annotating data with concepts of an ontology is a common practice in the biomedical domain. Resulting annotations define links between data and ontologies that are key for data exchange, data integration and data analysis tasks. In 2011 we collaborated with the National Center for Biomedical Ontologies (NCBO) to

develop of large repository of annotations named the NCBO Resource Index [99]. The resulting repository contains annotations of 34 biomedical databases annotated with concepts of 280 ontologies of the BioPortal [2]. We proposed a comparison of the annotations of a database of biomedical publications (Medline) with two databases of scientific funding (Crisp and ResearchCrossroads) to profile disease research [18]. The annotation of these three databases with a unique ontology about diseases enable to consider their content conjointly and consequently to analyze and compare, for distinct disease (or family of diseases), trends in term of number of publications and funding amounts.

We started a new project that aims at exploring biomedical annotations with FCA techniques. One main challenge here is to develop a knowledge discovery approach that consider the knowledge represented in the ontologies employed for the annotations.

6.2.4. Connecting textual biomedical knowledge with the Semantic Web

A large amount of biomedical knowledge is in the form of text embedded in published articles, clinical files or biomedical public databases. It is consequently of high interest to extract and structure this knowledge to facilitate its consideration when processing biomedical data. We benefited from advances in Natural Language Processing (NLP) techniques to extract fine-grained relationships mentioned in biomedical text and subsequently published such relationships on line in the form of RDF triples [91], [90]. In a collaborative work with the Health Care and Life Science (HCLS) interest group of the W3C, we demonstrated how biomedical knowledge extracted from text, along with Semantic Web technologies has high potential for recommendation systems and knowledge discovery in biomedicine [118].

6.3. Structural Systems Biology

Participants: Thomas Bourquard, Marie-Dominique Devignes, Anisah Ghoorah, Van-Thai Hoang, Bernard Maigret, Violeta Pérez-Nueno, Dave Ritchie, Malika Smaïl-Tabbone.

knowledge discovery in life sciences, bioinformatics, biology, chemistry, gene

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

6.3.1. Accelerating protein docking calculations using graphics processors

We have recently adapted the *Hex* protein docking software [113] to use modern graphics processors (GPUs) to carry out the expensive FFT part of a docking calculation [114]. Compared to using a single conventional central processor (CPU), a high-end GPU gives a speed-up of 45 or more. This software is publicly available at http://hex.loria.fr. A public GPU-powered server has also been created (http://hexserver.loria.fr) [105]. The docking server has performed some 12,000 docking runs during 2012. A book chapter describing the Hex docking algorithm has been published [75]. Our docking work has facilitated further developments on modeling the assembly of multi-component molecular structures using a particle swarm optimization technique [25], and on modeling protein flexibility during docking [24].

6.3.2. KBDOCK: Protein docking using Knowledge-Based approaches

In order to explore the possibilities of using structural knowledge of protein-protein interactions, Anisah Ghoorah recently developed the KBDOCK system as part of her doctoral thesis project. KBDOCK combines residue contact information from the 3DID database [119] with the Pfam protein domain family classification [92] together with coordinate data from the Protein Data Bank [87] 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 [96] for template-based docking using 73 complexes from the Protein Docking Benchmark [98]. KBDOCK is available at http://kbdock.loria.fr. Anisah Ghoorah successfully defended her thesis in November 2012 [10].

[2] http://bioportal.bioontology.org/

6.3.3. Kpax: A new algorithm for protein structure alignment

We have developed a new protein structure alignment approach called Kpax [6]. 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 [126]. The Kpax program is available at http://kpax.loria.fr/.

6.3.4. gEMpicker and gEMfitter: GPU-accelerated tools for cryo-electron microscopy

Solving the structures of large protein assemblies is a difficult and computationally intensive task. Multiple two-dimensional (2D) images must be processed and classified to identify protein particles in different orientations. These images may then be averaged and stacked to deduce the three-dimensional (3D) structure of a protein. In order to help accelerate the first of these tasks we have recently developed a novel and highly parallel algorithm called "gEMpicker" which uses multiple graphics processors to detecting 2D particles in cryo-electron microscopy images. We have also developed a 3D shape matching algorithm called "gEMfitter" which also exploits graphics processors, and which will provide a useful tool for the final 3D assembly step. Both programs will soon be made publicly available, and two manuscripts describing our approach are in preparation.

6.3.5. DOVSA: Developing new algorithms for virtual screening

In 2010, Violeta Pérez-Nueno joined the Orpailleur team thanks to a Marie Curie Intra-European Fellowship (IEF) award to develop new virtual screening algorithms (DOVSA). The aim of this project is 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 [111]. The main disease target in this project is the acquired immune deficiency syndrome (AIDS), caused by the human immuno-deficiency virus (HIV) [109]. However, the approach will be quite generic and will be broadly applicable to many other diseases. Good progress has been made on calculating and clustering spherical harmonic "consensus shapes" which represent rather well the essential features of groups of active molecules [110]. The approach has since been extended to provide a rapid way to cluster drug families according to the Gaussian distributions of their surface shapes, and to predict possible cross-interactions of drug families [21]. We have also published a review on the state of the art in 3D virtual drug screening [15].

6.4. Around the Taaable research project

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

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

The Taaable project (http://taaable.fr) has been originally created as a challenger of the Computer Cooking Contest (ICCBR Conference). A candidate to this contest is a system whose goal is to solve cooking problems on the basis of a recipe book (common to all candidates), where each recipe is a shallow XML document with an important plain text part. The size of the recipe book (about 1500 recipes) prevents from a manual indexing of recipes: this indexing is performed using semi-automatic techniques.

Beyond its participation to the CCCs, the Taaable project aims at federating various research themes: case-based reasoning, information retrieval, knowledge acquisition and extraction, knowledge representation, minimal change theory, ontology engineering, semantic wikis, text-mining, etc. Case-based reasoning is used to perform adaptation of recipe to user constraints. The reasoning process uses a cooking domain ontology (especially hierarchies of classes) and adaptation rules. The knowledge base used by the inference engine is encoded within a semantic wiki, which contains the recipes, the domain ontology, and adaptation rules.

The most important original features of this version are:

Modules for computing adaptation knowledge. Using adaptation knowledge, and especially adaptation rules, is a way to better adapt cooking recipes to user constraints. A previous work for extracting adaptation rules has been performed in 2011 [93]. In this work, variation of ingredients between couple of recipes are mined using closed itemsets extraction. The adaptation rules come from the interpretation of closed itemsets whose items correspond to the ingredients that have to be removed, kept, or added. This approach has been integrated as a wiki extension, providing a collaborative environment in which humans and machines may now collaborate to better acquire adaptation rules [38]. Humans (expert in cooking) may trigger automatic processes (knowledge discovery processes) and and may validate, using a specific user interface, proposition of adaptation rules as adaptation knowledge, which is then added to the knowledge base. In the same way, this environment integrates also the results of a new work on knowledge extraction where specific cooking adaptation rules (i.e. that can be applied to a single recipe) are generalized using close itemsets into generic adaptation rules, to make them usable on other recipes [60].

A module for acquiring a process semantic representation. While a process for acquiring cases from recipe preparation texts exists, the results are not perfect. In order for valid case representations to be available in the semantic wiki, a semi-automatic case acquisition tool was created [59]. This tools presents the user with a graphical interface through which it is able to interact with the case acquisition process. In order to limit the effort required, each correction entered by the user is propagated by the tool to the rest of the case representation.

Some other theoretical studies have been carried out that should be applied to some future versions of Taaable:

- The combination of workflows and interval algebras to represent procedural knowledge [55].
- The revision-based adaptation of cases represented in a qualitative algebra [41].
- The study of taxonomy merging [39]: several versions of the taxonomies used in Taaable (such as the food hierarchy) can be incoherent one with the others and a merging process is defined in order to obtain a consistent merged taxonomy.
- A continuous knowledge extraction process to ensure the non regression of the reasoning system according to the ontology evolution [50].

PAREO Project-Team

6. New Results

6.1. Model transformation

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

In [10], we have proposed a general method to transform high level models by using *Tom* strategies. High-level models we consider are *EMF-ECore* models that we represent by terms whose mappings have been generated by the *Tom-EMF* tool. The proposed method consists in decomposing a complex transformation into many elementary transformations (*definitions*) encoded by *Tom* strategies. These *definitions* are applied on a source model without any consideration of execution order. Therefore, we proposed a mechanism to address the problem of dependency between elementary transformations without introducing any scheduling between rewriting rules. This mechanism relies on the use of temporary elements which play the roles of the target elements until the last part of the transformation : the *Resolve* phase. The goal of this phase is to find and replace all temporary elements by real target ones, and therefore to reconnect all partial target models obtained during elementary transformations to build the resulting model.

In [11], [15], we presented a first proposal of a high-level transformation language included in *Tom* which implements the aforementioned general method. We used this language to implement an avionic case study — AADL2Fiacre — which was proposed by Airbus for the *quarteFt* project.

6.2. Improvements of theoretical foundations

6.2.1. Termination under strategies

Participants: Horatiu Cirstea, Pierre-Etienne Moreau.

Several approaches for proving the confluence and the termination of term rewriting systems have been proposed [16] and the corresponding techniques have been implemented in tools like Aprove [23] and TTT2 [32]. 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 [21] 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 tool 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.

6.2.2. Automatizing the certification of induction proofs

Participant: Sorin Stratulat.

Largely adopted by proof assistants, the conventional induction methods based on explicit induction schemas are non-reductive and local, at schema level. On the other hand, the implicit induction methods used by automated theorem provers allow for lazy and mutual induction reasoning. In collaboration with Amira Henaien [13], we devised a new tactic for the Coq proof assistant able to perform automatically implicit induction reasoning. By using an automatic black-box approach, conjectures intended to be manually proved by the certifying proof environment that integrates Coq are proved instead by the `Spike` implicit induction theorem prover. The resulting proofs are translated afterwards into certified Coq scripts.

As a case study, conjectures involved in the validation of a non-trivial application [35] have been successfully and directly certified by Coq using the `Spike` tactic. The proofs of more than 60% of them have been performed completely automatically, i.e., the Coq user does not need to provide any argument to the tactic. On the other hand, its application is limited to Coq specifications transformable into conditional specifications whose axioms can be oriented into rewrite rules.

6.2.3. Cyclic proofs by induction methods

Participant: Sorin Stratulat.

In a first-order setting, two different 'proof by induction' methods are distinguished: the conventional induction, based on explicit induction schemas, and the implicit induction, based on reductive procedures. In [14], we proposed a new cycle-based induction method that keeps their best features, i.e., performs local and non-reductive reasoning, and naturally fits for mutual and lazy induction. The heart of the method is a proof strategy that identifies in the proof script the subset of formulas contributing to validate the application of induction hypotheses. The conventional and implicit induction are particular cases of our method.

6.3. Integration of formal methods in programming languages

6.3.1. Multi-focus strategies

Participants: Jean-Christophe Bach, Christophe Calvès, Horatiu Cirstea, Pierre-Etienne Moreau.

Like most rewriting engines, *Tom* patterns combined with traversal strategies, gives the possibility to match and rewrite at any position in a given term. We have extended this classical approach with multi-focus strategies which enable us to match and rewrite several positions simultaneously. More precisely, the action performed at a given position can depend on the other positions involved in the corresponding strategy. This extension is particularly well-suited for programming-language semantics specification, semantics which usually require gathering several subterms (code, memory, input/output channels, ...) to perform one action.

The multi-focus library is a conservative extension of *Tom* standard strategies and provides combinators to handle multi-position traversal, matching and rewriting. Compared to the original *Tom* strategy library, the multi-focus version provides global backtracking. The library is available at http://gforge.inria.fr/projects/tom.

6.3.2. Formal islands grammars parsing

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

Extending a language by embedding within it another language presents significant parsing challenges, especially if the embedding is recursive. The composite grammar is likely to be nondeterministic as a result of tokens that are valid in both the host and the embedded language. In [9], we examined the challenges of embedding the *Tom* language into a variety of general-purpose high level languages. The current parser of *Tom* is complex and difficult to maintain. In this paper, we described how *Tom* can be parsed using island grammars implemented with the Generalised LL (*GLL*) parsing algorithm. The grammar is, as might be expected, ambiguous. Extracting the correct derivation relies on a disambiguation strategy which is based on pattern matching within the parse forest. We described different classes of ambiguity and proposed patterns to solve them.

6.4. Security policies specification and analysis

Participants: Horatiu Cirstea, Hélène Kirchner, Pierre-Etienne Moreau.

Access control policies, a particular case of security policies should guarantee that information can be accessed only by authorized users and thus prevent all information leakage. We proposed [12] a framework where the security policies and the systems they are applied on are specified separately but using a common formalism. This separation allows not only some analysis of the policy independently of the target system but also the application of a given policy on different systems. In this framework, we propose a method to check properties like confidentiality, integrity or confinement over secure systems based on different policy specifications.

PAROLE Project-Team

6. New Results

6.1. Speech Analysis and Synthesis

Participants: Anne Bonneau, Vincent Colotte, Dominique Fohr, Yves Laprie, Joseph di Martino, Slim Ouni, Sébastien Demange, Fadoua Bahja, Agnès Piquard-Kipffer, Utpala Musti.

Signal processing, phonetics, health, perception,articulatory models, speech production, learning language, hearing help, speech analysis, acoustic cues, speech synthesis

6.1.1. Acoustic-to-articulatory inversion

6.1.1.1. Annotation of X-ray films and construction of articulatory models

Two databases have been annotated this year: one composed of 15 short sentences representing more than 1000 X-ray images and a second about CVCVs which has already been annotated by hand on sheets of papers. In the latter case we adapted tools of Xarticul software in order to enable a fast processing of these annotations.

Since images of the first database have been digitized from old films there are several spurious jumps and we thus developed tools to remove them during the construction of articulatory models. The big difference with previous databases processed is the presence of more consonants.

The articulatory model is supplemented by a clipping algorithm in order to take into account contacts between tongue and palate.

6.1.1.2. Articulatory copy synthesis

Acoustic features and articulatory gestures have always been studied separately. Articulatory synthesis could offer a nice solution to study both domains simultaneously. We thus explored how X-ray images could be used to synthesize speech. The first step consisted of connecting the 2D geometry given by mediosagittal images of the vocal tract with the acoustic simulation. Last year we thus developed an algorithm to compute the centerline of the vocal tract, i.e. a line which is approximately perpendicular to the wave front. The centerline is then used to segment the vocal tract into elementary tubes whose acoustic equivalents are fed into the acoustic simulation.

The frequency simulation enables the impact of local modifications of the vocal tract geometry to be evaluated easily. This is useful to investigate the contribution of the sagittal to area transformation in the synthetic speech spectrum. However, the sequence of area functions alone does not suffice to synthesize speech since consonants involve very fine temporal details (closure of the vocal tract and then release of the constriction for stops and fricatives for instance) which additionally have to be synchronized with the temporal evolution of the glottis area. Scenarii have thus been designed for VCV sequences and more generally for any consonant clusters. The idea consists of choosing relevant X-ray images near the VCV to be synthesized. These images can be duplicated just before the closure of the vocal tract, modified to simulate the constriction release for a stop...

This procedure has been applied successfully to copy sentences and VCV for four X-ray films of the DOCVACIM database http://www2i.misha.fr/flora/jsp/index.jsp. The next objective will be to develop a complete articulatory synthesis system.

6.1.1.3. Inversion from cepstral coefficients

The two main difficulties of inversion from cepstral coefficients are: (i) the comparison of cepstral vectors from natural speech and cepstral vectors generated by the articulatory synthesizer and (ii) the access to the articulatory codebook.

Last year we developed a bilinear frequency warping optimized to compensate for the articulatory model mismatch. However, the spectral tilt was not taken into account. We thus combined it with affine adaptation of the very first cepstral coefficients in order to take into account the spectral tilt. It turns out that the new adaptation enables a more relevant comparison of cepstral vectors since the geometric precision of the best solution is less than 1mm.

The second difficulty consists of exploring the articulatory codebook efficiently. Indeed, only a small number of hypercuboids could correspond to the input cepstral vector. The issue is to eliminate all cuboids, which cannot give rise to the input cepstral vector. This is easy when using formants as input data since all cuboids can be indexed easily with extreme values of formants. But this becomes impossible with cepstral vectors because the effect of the excitation source cannot be removed completely from cepstral coefficients. We thus use spectral peaks to access the codebook. However, there exist some spurious spectral peaks, and at the same time some peaks can be absent. We thus designed a lax matching between spectral peaks, which enables the comparison of a series of spectral peaks of the original speech with peaks calculated on synthetic speech. This matching algorithm allows the exploration to focus on 5% of the codebook instead of 40% when using only the peak corresponding to F2 is used.

6.1.1.4. Acoustic-to-articulatory inversion using a generative episodic memory

We have developed an episodic based inversion method. Episodic modeling is interesting for two reasons. First, it does not rely on any assumption about the mapping relationship between acoustic and articulatory, but rather it relies on real synchronized acoustic and articulatory data streams. Second, the memory structurally embeds the naturalness of the articulatory dynamics as speech segments (called episodes) instead of single observations as for the codebook based methods. Estimating the unknown articulatory trajectories from a particular acoustic signal, with an episodic memory, consists in finding the sequence of episodes, which acoustically best explains the input acoustic signal. We refer to such a memory as a concatenative memory (C-Mem) as the result is always expressed as a concatenation of episodes. Actually a C-Mem lacks from generalization capabilities as it contains only several examples of a given phoneme and fails to invert an acoustic signal, which is not similar to the ones it contains. However, if we look within each episode we can find local similarities between them. We proposed to take advantage of these local similarities to build a generative episodic memory (G-Mem) by creating inter-episodes transitions. The proposed G-Mem allows switching between episodes during the inversion according to their local similarities. Care is taken when building the G-Mem and specifically when defining the inter-episodes transitions in order to preserve the naturalness of the generated trajectories. Thus, contrary to a C-Mem the G-Mem is able to produce totally unseen trajectories according to the input acoustic signal and thus offers generalization capabilities. The method was implemented and evaluated on the MOCHA corpus, and on a corpus that we recorded using an AG500 articulograph. The results showed the effectiveness of the proposed G-Mem which significantly outperformed standard codebook and C-Mem based approaches. Moreover similar performances to those reported in the literature with recently proposed methods (mainly parametric) were reached.

The paradigm of episodic memories was also used for speech recognition. We do not extend the acoustic feature with any explicit articulatory measurements but instead we used the articulatory-acoustic generative episodic memories (G-mem). The proposed recognizer is made of different memories each specialized for a particular articulator. As all the articulators do not contribute equally to the realization of a particular phoneme, the specialized memories do not perform equally regarding each phoneme. We showed, through phone string recognition experiments that combining the recognition hypotheses resulting from the different articulatory specialized memories leads to significant recognition improvements.

6.1.2. Using Articulography for Speech production

Since we have an articulograph (AG500, Carstens Medizinelektronik) available, we can easily acquire articulatory data required to study speech production. The articulograph is used to record the movement of the tongue (this technique is called electromagnetography - EMA). The AG500 has a very good time resolution (200Hz), which allows capturing all articulatory dynamics. It has also a good precision. In fact, we performed recently an comparative study to assess the precision of the articulograph AG500 in comparison to a concurrent

articulograph NDI Wave. In this study, we found that both systems presented similar results. We showed also that the accuracy is relatively independent of the sensor velocity, but decreases with the distance from magnetic center of the system [31].

To make the best use of the articulograph, we developed an original visualization software, VisArtico, which allows displaying the data acquired by an articulograph. It is possible to display the tongue contour and the lips contour animated simultaneously with acoustics. The software helps to find the midsagittal plane of the speaker and find the palate contour. In addition, VisArtico allows labeling phonetically the articulatory data[30].

We continuousely work on the usage this platform to acquire articulatory data that were used for articulatory-to-acoustic inversion but also to study the co-variation of speech clarity and coarticulatory patterns in Arabic [18]. The results revealed evident relationship between speech clarity and coarticulation: more coarticulation in formal speech and in strong prosodic position.

6.1.3. Speech synthesis

Visual data acquisition was performed simultaneously with acoustic data recording, using an improved version of a low-cost 3D facial data acquisition infrastructure. The system uses two fast monochrome cameras, a PC, and painted markers, and provides a sufficiently fast acquisition rate to enable an efficient temporal tracking of 3D points. The recorded corpus consisted of the 3D positions of 252 markers covering the whole face. The lower part of the face was covered by 70% of all the markers (178 markers), where 52 markers were covering only the lips so as to enable a fine lip modeling. The corpus was made of 319 medium-sized French sentences uttered by a native male speaker and corresponding to about 25 minutes of speech,.

We designed a first version of the text to acoustic-visual speech synthesis based on this corpus. The system uses bimodal diphones (an acoustic component and a visual one) and unit selection techniques (see 3.2.4). We have introduced visual features in the selection step of the TTS process. The result of the selection is the path in the lattice of candidates found in the Viterbi algorithm, which minimizes a weighted linear combination of three costs: the target cost, the acoustic joined cost, and the visual joined cost. Finding the best set of weights is a difficult problem by itself mainly because of their highly different nature (linguistic, acoustic, and visual considerations). To this end, we developed a method to determine automatically the weights applied to each cost, using a series of metrics that assess quantitatively the performance of synthesis.

The visual target cost includes visual and articulatory information. We implemented and evaluated two techniques: (1) Phonetic category modification, where the purpose was to change the current characteristics of some phonemes which were based on phonetic knowledge. The changes modified the target and candidate description for the target cost to better take into account their main characteristics as observed in the audio-visual corpus. The expectation was that their synthesized visual speech component would be more similar to the real visual speech after the changes. (2) Continuous visual target cost, where the visual target cost component is now considered as real value, and thus continuous, based on the articulatory feature statistics. This year, we continued working on improving the quality of the synthesis. This was done by continuously testing new strategies of weight tuning and improving our selection technique [26].

6.1.4. Phonemic discrimination evaluation in language acquisition and in dyslexia and dysphasia

6.1.4.1. Phonemic segmentation in reading and reading-related skills acquisition in dyslexic children and adolescents

Our computerized tool EVALEC was published [56] after the study of reading level and reading related skills of 400 hundred children from grade 1 to grade 4 (from age 6 to age 10) [58]. This research was supported by a grant from the French Ministery of Health (Contrat 17-02-001, 2002-2005). This first compurerized battery of tests in French language assessing reading and related skills (phonemic segmentation, phonological short term memory) comparing results both to chronological age controls and reading level age control in order to diagnostic Dyslexia. Both processing speed and accuracy scores are taken into account. This battery of tests is used by speech and langage therapists. We keep on examining the reliability (group study) and the prevalence (multiple case study) of 15 dyslexics' phonological deficits in reading and reading related skills in comparaison with a hundred reading level children [57], and by the mean of longitudinal studies of children

from age 5 to age 17 [55]. This year, we started the development of a project which examined multimodal speech both with SLI, dyslexics and control children (30 children). Our goal is to examine visual contribution to speech perception accross differents experiments with a natural face (syllables with several conditions). Our goal is to search what can improve intelligibility in children who have sévère langague acquisition difficulties.

6.1.4.2. Langage acquisition and langage disabilities (deaf chidren, dysphasic children)

Providing help for improving French language acquisition for hard of hearing (HOH) children or for children with language disabilities was one of our goal : ADT (Action of Technological Development) Handicom [piquardkipffer:2010:inria-00545856:2]. The originality of this project was to combine psycholinguistical and speech analyses researchs. New ways to learn to speak/read were developed. A collection of three digital books has been written by Agnès Piquard-Kipffer for both 2-6, 5-9, 8-12 year old children (kindergarten, 1-4th grade) to train speaking and reading acquisition regarding their relationship with speech perception and audio-visual speech perception. A web interface has been created (using Symfony and AJAX technologies) in order to create others books for language impaired children. A workflow which transforms a text and an audio source in a video of digital head has been developed. This worklow includes an automatic speech alignment, a phonetic transcription, a speech synthetizer, a French cued speech coding and speaking digital head. A series of studies (simple cases studies, 5 deaf children and 5 SLI children and group studies with 2 kindergarten classes) were proposed to investigate the linguistical, audio-visual processing.... presumed to contribute to language acquisition in deaf children. Publication are submitted.

6.1.5. Enhancement of esophageal voice

6.1.5.1. Detection of F0 in real-time for audio: application to pathological voices

The work first rested on the CATE algorithm developed by Joseph Di Martino and Yves Laprie, in Nancy, 1999.The CATE (Circular Autocorrelation of the Temporal Excitation) algorithm is based on the computation of the autocorrelation of the temporal excitation signal which is extracted from the speech log-spectrum. We tested the performance of the parameters using the Bagshaw database, which is constituted of fifty sentences, pronounced by a male and a female speaker. The reference signal is recorded simultaneously with a microphone and a laryngograph in an acoustically isolated room. These data are used for the calculation of the contour of the pitch reference. When the new optimal parameters from the CATE algorithm were calculated, we carried out statistical tests with the C functions provided by Paul BAGSHAW. The results obtained were very satisfactory and a first publication relative to this work was accepted and presented at the ISIVC 2010 conference. At the same time, we improved the voiced / unvoiced decision by using a clever majority vote algorithm electing the actual F0 index candidate. A second publication describing this new result was published at the ISCIT 2010 conference. Recently we developed a new algorithm based on a wavalet transform applied to the cepstrum excitation. The resuts obtained were satisfactory. This work has been published in the ICMCS 2012 conference [14].

6.1.5.2. Voice conversion techniques applied to pathological voice repair

Voice conversion is a technique that modifies a source speaker's speech to be perceived as if a target speaker had spoken it. One of the most commonly used techniques is the conversion by GMM (Gaussian Mixture Model). This model, proposed by Stylianou, allows for efficient statistical modeling of the acoustic space of a speaker. Let "x" be a sequence of vectors characterizing a spectral sentence pronounced by the source speaker and "y" be a sequence of vectors describing the same sentence pronounced by the target speaker. The goal is to estimate a function F that can transform each source vector as nearest as possible of the corresponding target vector. In the literature, two methods using GMM models have been developed: In the first method (Stylianou), the GMM parameters are determined by minimizing a mean squared distance between the transformed vectors and target vectors. In the second method (Kain), source and target vectors are combined in a single vector "z". Then, the joint distribution parameters of source and target speakers is estimated using the EM optimization technique. Contrary to these two well known techniques, the transform function F, in our laboratory, is statistically computed directly from the data: no needs of EM or LSM techniques are necessary. On the other hand, F is refined by an iterative process. The consequence of this strategy is that the estimation of F is robust and is obtained in a reasonable lapse of time. This interesting result was published and presented at the ISIVC

2010 conference. Recently,we realized that one of the most important problems in speech conversion is the prediction of the excitation. In order to solve this problem we developed a new strategy based on the prediction of the ceptrum excitation pulses. This interesting result has been published in the SIIE 2012 conference [13].

6.1.5.3. Signal reconstruction from short-time Fourier transform magnitude spectra

Joseph Di Martino and Laurent Pierron developed in 2010 an algorithm for real-time signal reconstruction from short-time Fourier magnitude spectra. Such an algorithm has been designed in order to enable voice conversion techniques we are developing in Nancy for pathological voice repair. Recently Mouhcine Chami, an assistant-professor of the INPT institute at Rabat (Morocco) proposed a hardware implementation of this algorithm using FPGAs. This implementation has been publised in the SIIE 2012 conference [17].

6.1.6. Perception and production of prosodic contours in L1 and L2

6.1.6.1. Language learning (feedback on prosody)

A corpus, made up of 8 English sentences and 40 English isolated words has been recorded. Thirty three speakers pronounced the corpus under different conditions : without any audio feedback (first condition), with audio feedback (second condition, experiment realized one week after the first one). In order to test the permanence of the improvement due to feedback, a set of words and all the sentences were then pronounced without feedback (third condition, experiment realized after the second one). An English teacher helped us in the composition of the corpus and recorded it. Parts of this corpus have already been used to test the automatic speech alignment methods developed under the framework of ALLEGRO and implemented in jsnoori (ADT). The feedback will be progressively transferred from Winsnoori to Jsnoori.

6.1.6.2. Production of prosodic contour

The study of French contours (various types of continuations, end of sentences ...) confirmed the existence of patterns which are typical of French prosody. In order to determine the impact of French (the native language) on a second language pronunciation (English), a series of prosodic contours extracted from English sentences uttered by French speakers have been compared to French prosodic countours. To that purpose, French speakers recorded similar sentences in French and in English. Analysis of results is in progress. First results tend to show the impact of the native language ([15] and [10]).

6.1.7. Pitch detection

Over the last two years, we have proposed two new real time pitch detection algorithms (PDAs) based on the circular autocorrelation of the glottal excitation, weighted by temporal functions, derived from the CATE [53] original algorithm (Circular Autocorrelation of the Temporal Excitation), proposed initially by J. Di Martino and Y. Laprie. In fact, this latter algorithm is not constructively real time because it uses a post-processing technique for the Voiced/Unvoiced (V/UV) decision. The first algorithm we developed is the eCATE algorithm (enhanced CATE) that uses a simple V/UV decision less robust than the one proposed later in the eCATE+ algorithm.

We propose a recent modified version called the eCATE++ algorithm which focuses especially on the detection of the F0, the tracking of the pitch and the voicing decision in real time. The objective of the eCATE++ algorithm consists in providing low classification errors in order to obtain a perfect alignment with the pitch contours extracted from the Bagshaw database by using robust voicing decision methods. The main improvement obtained in this study concerns the voicing decision, and we show that we reach good results for the two corpora of the Bagshaw database. This algorithm is under a submission process in an international journal.

6.2. Automatic Speech Recognition

Participants: Sébastien Demange, Dominique Fohr, Christian Gillot, Jean-Paul Haton, Irina Illina, Denis Jouvet, Odile Mella, Luiza Orosanu, Othman Lachhab.

telecommunications, stochastic models, acoustic models, language models, automatic speech recognition, training, robustness

6.2.1. Core recognition

6.2.1.1. Broadcast News Transcription

A complete speech transcription system, named ANTS (see section 5.6), was initially developed in the framework of the Technolangue evaluation campaign ESTER for French broadcast news transcription. This year, in the context of the ETAPE evaluation campaign about transcription of radio and TV debates, the speech transcription system was improved. Large amounts of text data have been collected over the web. This new collected web data, plus new text and speech resources have made possible the creation and training of new acoustic models and new language models. Moreover new processing steps have been included in the transcription system, leading to much better performance than with the initial system. Several system variants have been developed, and for the ETAPE evaluation campaign, their results have been combined.

Extensions of the ANTS system have been studied, including the possibility to use the sphinx recognizers, and unsupervised adaptation processes. Training scripts for building acoustic models for the Sphinx recognizers are now available and take benefit of parallel computations on the computer cluster for a rapid optimization of the model parameters The Sphinx models are also used for speech/text alignment on both French and English speech data. A new speech transcription program has been developed for efficient decoding on the computer cluster, and easy modification of the decoding steps (speaker segmentation and clustering, data classification, speech decoding in one or several passes, ...). It handles both the Julius and Sphinx (versions 3 and 4) decoders.

This year, in the context of the ETAPE evaluation campaign, which deals with the transcription of radio and TV shows, mainly debates, the Julius-based and Sphinx-based transcription systems have been improved. Several system variants have been developed (relying on different features, and/or different normalization schemes, different processing steps, and different unsupervised adaptation processes); and, combining the output of the various systems led to significantly improved performance.

The recently proposed approach to grapheme-to-phoneme conversion based on a probabilistic method: Conditional Random Fields (CRF) was investigated further. CRF gives a long term prediction, and assumes a relaxed state independence condition. The proposed system was validated in a speech recognition context. Our approach compared favorably with the performance of the state-of-the-art Joint-Multigram Models (JMM) for the quality of the pronunciations, and it was also shown that combining the pronunciation variants generated by both the CRF-based and the JMM-based apporaches improves performance [21].

Concerning grapheme-to-phoneme conversion, a special attention was paid to infering the pronunciation variants of proper names [34], and the usage of additional information corresponding to the language origin of the proper name was investigated.

6.2.1.2. Non-native speakers

The performance of automatic speech recognition (ASR) systems drastically drops with non native speech. The main aim of non-native enhancement of ASRs is to make available systems tolerant to pronunciation variants by integrating some extra knowledge (dialects, accents or non-native variants).

Our approach is based on acoustic model transformation and pronunciation modeling for multiple non-native accents. For acoustic model transformation, two approaches are evaluated: MAP and model re-estimation. For pronunciation modeling, confusion rules (alternate pronunciations) are automatically extracted from a small non-native speech corpus. We presents [9] a novel approach to introduce confusion rules in the recognition system which are automatically learned through pronunciation modelling. The modified HMM of a foreign spoken language phoneme includes its canonical pronunciation along with all the alternate non-native pronunciations, so that spoken language phonemes pronounced correctly by a non-native speaker could be recognized. We evaluate our approaches on the European project HIWIRE non-native corpus which contains English sentences pronunced by French, Italian, Greek and Spanish speakers. Two cases are studied: the native language of the test speaker is either known or unknown. Our approach gives better recognition results than the classical acoustic adaptation of HMM when the foreign origin of the speaker is known. We obtain 22% WER reduction compared to the reference system.

6.2.1.3. Language Model

Christian Gillot has defended his Ph.D. thesis on the 17th September 2012. In his thesis, he proposes a new approach to estimate the language model probabilities for an automatic speech recognition system. The most commonly used language models in the state of the art are based on n-grams smoothed with Kneser-Ney method. Such models make use of occurrence counts of words sequences up to a maximum length (typically 5 words). These counts are computed on a huge training corpus. Christian's Ph.D. thesis starts by an empirical study of the errors of a state-of-the-art speech recognition system in French, which shows that there are many regular language phenomena that are out of reach of the n-gram models. This thesis thus explores a dual approach of the prevailing statistical paradigm by using memory models that process efficiently specific phenomena, in synergy with the n-gram models which efficiently capture the main trends in the corpus. The notion of similarity between long n-grams is studied in order to identify the relevant contexts to take into account in a first similarity language model. The data extracted from the corpus is combined via a Gaussian kernel to compute a new score. The integration of this non-probabilistic model improves the performance of a recognition system. A second model is then introduced, which is probabilistic and thus allows for a better integration of the similarity approach with the existing models. This second model improves the performance on texts in terms of perplexity. Some future works are further described, where the memory-based paradigm is transposed from the estimation of the n-gram probability up to the language model itself. The principle is to combine individual models together, where each model represents a specific syntactic structure, and also to combine these specific models with a standard n-gram model. The objective is to let specific models compensate for some weaknesses of n-gram models, which cannot capture sparse and rare phenomena, nor patterns that do not occur at all in the the training corpus. This approach hence opens new interesting perspectives in particular for domain adaptation.

6.2.1.4. Speech recognition for interaction in virtual worlds

Automatic speech recognition was investigated for vocal interaction in virtual worlds, in the context of serious games in the EMOSPEECH project. For training the language models, the text dialogs recorded by the TALARIS team (Midiki corpus) on the same serious game (but in a text-based interaction), have been manually corrected and used on addition of available broadcast news corpus. Different language models have then been created using different vocabulary sizes. The acoustic models were adapted from the radio broadcast news models, using state-of-the-art Maximum A Posteriori adaptation algorithm. This reduces the mismatch in recording conditions between the game devices and the original models trained on radio streams. A client-server speech recognition demonstrator has been developed. The client runs on an iPad; it records the speech input, sends it to the server, waits for the speech recognition answer, and finally displays the results. The server runs on a PC, relies on the sphinx4 decoder for decoding the received speech signal, and then sends the results to the iPad client.

6.2.2. Speech recognition modeling

Robustness of speech recognition to multiple sources of speech variability is one of the most difficult challenge that limits the development of speech recognition technologies. We are actively contributing to this area via the development of the following advanced modeling approaches.

6.2.2.1. Detailed modeling

Detailed acoustic modeling was further investigated using automatic classification of speaker data. With such an approach it is possible to go beyond the traditional four class models (male vs female, studio quality vs telephone quality). However, as the amount of training data for each class gets smaller when the number of classes increases, this limits the amount of classes that can efficiently be trained. Hence, we have investigated introducing a classification marging in the classification process. With such a marging, which handle boundary classification uncertainty, speech data at the class-boundary may belong to several classes. This increases the amount of training data in each class, which makes the class acoustic model parameters more reliable, and finally improved the overall recognition performance [22]. Combining maximum likelihood linear regression (MLLR) and maximum a posteriori (MAP) adaptation techniques leads to better speech recognition performance, and makes it possible to use more classes [35].

The approach was later improved by introducing a classification process which relies on phonetic acoustic models and the Kullback Leibler divergence measure to build maximally dissimilar clusters. This approach lead to better recognition results than the likelihood based classification approach used in previous experiments [20].

These class-based speech recognition systems were combined with more traditional gender-based system in the ETAPE campaign for the evaluation of speech transcription systems on French radio and TV shows.

6.2.2.2. Training HMM acouctic models

At the beginning of his second internship at Inria Nancy research laboratory, Othman Lachhab focused on the finalization of a speech recognition system based on context-independent HMMs models, using bigram probabilities for the phonotactic constraints and a model of duration following a normal distribution $\mathcal{N}(\mu, \sigma^2)$ incorporated directly in the Viterbi search process. Currently, he built a reference system for speaker-independent continuous phone recognition using Context- Independent Continuous Density HMM (CI-CDHMM) modeled by Gaussian Mixture Models (GMMs). In this system he developed his own training technique, based on a statistical algorithm estimating the classical optimal parameters. This new training process compares favorably with already published HMM technology on the same test corpus (TIMIT) and has been published in the ICMCS 2012 conference [23].

6.2.3. Speech/text alignment

6.2.3.1. Evaluation of speech/text alignment tools

Speech-text alignment tools are frequently used in speech technology and research: for instance, for training or assessing of speech recognition systems, the extraction of speech units in speech synthesis or in foreign language learning. We designed the software CoALT (Comparing Automatic Labelling Tools) for comparing two automatic labellers or two speech-text alignment tools, ranking them, and displaying statistics about their differences.

The main feature of CoALT is that a user can define its own criteria for evaluating and comparing the speech-text alignment tools since the required quality for labelling depends on the targeted application. Beyond ranking, our tool provides useful statistics for each labeller and above all about their differences and can emphasize the drawbacks and advantages of each labeller. We have applied our software for the French and English languages [19] but it can be used for another language by simply defining the list of the phonetic symbols and optionally a set of phonetic rules.

6.2.3.2. Alignment with non-native speech

Non-native speech alignment with text is one critical step in computer assisted foreign language learning. The alignement is necessary to analyze the learner's utterance, in view of providing some prosody feedback (as for example bad duration of some syllables - too short or too long -). However, non-native speech alignement 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. Moreover, these pronunciation deviations are strongly speaker dependent (i.e. they depend on the mother tongue of the speaker, and on its fluency in the target foreign lanaguage) which makes their prediction difficult.

However, the first step in automatic computer assisted language learning is to check that the pronunced word or utterance corresponds to the expected sentence, otherwise, if the user has not pronunced the correct words it is useless to proceed further with a detailed analysis of the pronunciation to check for possible misspronunciations. In order to decide if the pronunced utterance corresponds to the expected word or sentence, a force phonetic alignment of the sentence is compared to free decoding of the same sentence. Several comparison features are then defined, such as the number of matching phonemes, the percentage of frames having the save category label, ..., as well as the likelihood ratio. A classifier is then used to decide whether text and speech utterance match or not [36], [28].

These non-native phonetic alignments processes developed in the framework of the ALLEGRO project are currently under implementation in the JSNOORI software, and the processing should be completed by the developpement of automatic feedback procedures.

6.3. Speech-to-Speech Translation and Langage Modeling

Participants: Kamel Smaïli, David Langlois, Sylvain Raybaud, Motaz Saad, Denis Jouvet, Cyrine Nasri.

machine translation, statistical models

Sylvain Raybaud has just defended his thesis untitled "De l'utilisation de mesures de confiance en traduction automatique : évaluation, post-édition et application à la traduction de la parole.". His contributions are the following: study and evaluation of confidence measures for Machine Translation, an original algorithm to automatically build an artificial corpus with errors for training the confidence measures, development of an entire speech-to-text translation system.

In the scope of Confidence Measures, we participated to the World Machine Translation evaluation campaign (WMT2012 http://www.statmt.org/wmt12/quality-estimation-task.html). More precisely, we proposed a Quality Estimation system to the Quality Estimation shared task. The goal was to predict the quality of translations generated by an automatic system. Each translated sentence is given a score between 1 and 5. The score is obtained using several numerical or boolean features calculated according to the source and target sentences. We perform a linear regression of the feature space against scores in the range [1:5]. To this end, we use a Support Vector Machine. We experiment with two kernels: linear and radial basis function. In our system we use the features from the shared task baseline system and our own features (based on the work from the Sylvain Raybaud's thesis). This leads to 66 features. To deal with this large number of features, we propose an in-house feature selection algorithm. Our system came 5th among 19 systems. This work was publish in [24]. In the continuation of this research, we contributed to the development of a Quality Estimation tool (quest: https://github.com/lspecia/quest). For that, David Langlois was invited by Lucia Specia at University of Sheffield, Computer Sciences department, Natural Language Processing group. We added our own features into quest. This tool is dedicated to be available for the research community.

Another objective of our research work, with the Cyrine Nasri's Phd thesis, is to retrieve bilingual phrases for machine translation. As in fact, current statistical machine translation systems usually build an initial word-to-word alignment before learning phrase translation pairs. This operation needs many matching between different single words of both considered languages. We propose a new approach for phrase-based machine translation which does not need any word alignments. It is based on inter-lingual triggers determined by Multivariate Mutual Information. This algorithm segments sentences into phrases and finds their alignments simultaneously. Inspite of the youth of this method, experiments showed that the results are competitive but needs some more efforts in order to overcome the one of state-of-the-art methods.

Another aspect of the research of the group is to work on under resourced language related to Arabic. In fact, in several countries through the Arabic world, only few people speak the modern standard Arabic language. People speak something which is inspired from Arabic but could be very different from the modern standard Arabic. This one is reserved for the official broadcast news, official discourses and so on. The study of dialect is more difficult than any other natural language because it should be noted that this language is not written. A preliminary work has been done knowing that our final objective is to propose a machine translation between the different Arabic dialects and modern standrad Arabic. This issue is very difficult and challenging because no corpus does exist, vernaculars are different even within the same country, etc.

Last, Motaz Saad has started his thesis in November 2011. His objective is to work on opinion analysis in multilingual documents from internet. During this year, he retrieved comparable corpus from the web, and proposed a method to align these corpora at document level. He proposed algorithms to measure the degree of comparability between documents. He submitted his work to the International Conference on Corpus Linguistics (CICL2013).

In the framework of the ETAPE evaluation campaign a new machine learning based process was developed to select the most relevant lexicon to be used for the transcription of the speech data (radio and TV shows). The approach relies on a neural network trained to distinguish between words that are relevant for the task and those that are not. After training, the neural network (NN) is applied to each possible word (extracted from a very large text corpus). Then the words that have the largest NN output score are selected for creating the speech recognition lexicon. Such an approach can handle counts of occurences of the words in various data subsets, as well as other complementary informations, and thus offer more perspectives than the traditional unigram-based selection procedures.

SCORE Team

6. New Results

6.1. Collaborative Data Management

6.1.1. A Framework to Design Conflict-Free Replicated Data Types

Participants: Mehdi Ahmed-Nacer, Stéphane Martin, Pascal Urso.

Design new eventually consistent data types is difficult and error-prone as demonstrated by the numerous proposed approaches that fail to resolve conflicts for simple plain text document. Moreover, more the data type is complex, more conflicts types must be resolved. We have presented a layered approach to design new eventually consistent data types [21], [15]. This approach decouples eventual consistency management from data type constraints satisfaction. We compose one or several existing replicated data types which ensure eventual consistency, and adaptation layers to obtain a new eventually consistent data type. Each layer or replicated data type can be freely substituted by one providing the same interface. We have demonstrated that our approach is implementable and obtains acceptable performances. Our experiments and implementation are publicly available and re-playable (https://github.com/score-team/replication-benchmarker).

6.1.2. Enhancing Rich Content Wikis with Real-Time Collaboration

Participants: Luc André, Claudia-Lavinia Ignat, Gérald Oster.

Wikis are one of the most important tools of Web 2.0 allowing users to easily edit shared data. WYSIWYG editors for wiki pages avoid the impediments of learning wiki syntax. However, wikis offer poor support for merging concurrent contributions on the same pages. Users have to manually merge concurrent changes and there is no support for an automatic merging. As real-time collaborative editing reduces the number of conflicts as the time frame for concurrent work is very short, we proposed extending wiki systems with real-time collaboration [23]. We propose an automatic merging solution adapted for rich content wikis. Our solution is integrated as an extension of XWiki system (http://extensions.xwiki.org/xwiki/bin/view/Extension/RealTime+Wiki+Editor).

6.1.3. Rapid and Round-free Multi-pair Asynchronous Push-Pull Aggregation

Participants: Claudia-Lavinia Ignat, Hyun-Gul Roh.

In the context of STREAMS project we investigated gossip-based dissemination mechanisms in peer-to-peer real-time collaboration adapted for consistency maintenance algorithms based on CRDT (Commutative Replicated Data Types). These dissemination mechanisms need to compute the size of the network and therefore a suitable rapid protocol that aggregates data over network is essential. Iterative aggregation protocols, especially push-pull style aggregations, generally need prior configurations to synchronize rounds over all nodes, and messages should be exchanged in a synchronous/blocking way in order to ensure accurate estimates in push-pull or push-sum protocols. We proposed a multi-pair asynchronous push-pull aggregation (MAPPA) [22], which frees the push-pull aggregations from the synchronization constraints, and therefore accelerates the aggregation speed. MAPPA is resilient to network churns, and thus suitable for dynamic peer-to-peer networks.

6.1.4. Trustworthy contract based collaboration

Participants: Claudia-Lavinia Ignat, Hien Thi Thu Truong.

Availability of trustworthy environments is one of the main conditions that would lead to a greater acceptance and reliance on collaborative systems. In the context of large scale multi-synchronous collaboration where users work in parallel on different streams of activities a ”hard” security that would forbid many actions is unusable. We adopt instead a “soft” security where rather than adopting an a priori strict enforcement of security rules, access is given first to data without control but with restrictions that are verified a posteriori. We proposed a contract-based collaboration model [2], [4] where we establish and adjust trust in users based on detective enforcement of basic usage control requirements. Usage control requirements are specified as contracts. Contracts are specified by data owners when they share data in accordance with user trust levels. Observation of adherence to or violation of contracts is used to adjust trust levels. Our contract-based collaboration model allows the specification of contracts, merging of data and contracts and resolution of conflicting contracts. A trust metric for computing user trust levels was proposed based on auditing user compliance to the given contracts.

Multi-synchronous collaboration maintains multiple, simultaneous streams of activity which continually diverge and converge. These streams of activity are represented by means of logs of operations, i.e. user modifications. A malicious user might tamper his log of operations. At the moment of synchronization with other streams, the tampered log might generate wrong results. A trustworthy collaboration environment should detect if logs were tampered. We proposed a mechanism for establishment of trusted logs relying on hash-chain based authenticators [17], [18], [2]. Our solution ensures the authenticity, the integrity of logs, and the user accountability. We proposed algorithms to construct authenticators and verify logs. We proved their correctness and provided theoretical and practical evaluations.

6.1.5. Distributed activity management in crisis situation

Participants: François Charoy, Joern Franke.

Crisis management has been a very fruitful domain to investigate new approaches for high value, human driven activity coordination in a multi organisational setting. Our work benefits from a large amount of use cases and detailed accounts of previous dramatic events to analyse requirements and confront our proposals. This paper present the final part of this work on the problem of replication of activities between several workspaces [3]. We are now looking for new vehicles to continue this research at an international level.

6.2. Data Centered Service Oriented Computing

6.2.1. Business process distribution on a SaaS architecture

Participants: Walid Fdhila, Claude Godart, Elio Goettelmann, Samir Youcef.

The objective of this work is to support the deployment of a business process as a set of distributed services provided partially or totally off-premises or even in the cloud. Direct applications in our target are:

- A methodological approach for choreographies elicitations and monitoring[12].
- An algorithm for optimized service providers selection (including cloud) [11], [9], [10].

In this objective, we have deployed two approaches. A first is based on heuristics (*greedy* algorithm to compute an initial solution, combined with a *tabu search*) for optimizing the selection of services assigned to activities in a decentralized composite service, both in terms of the overall QoS of the composite service and the communication overhead; in output, the initial business process model is translated in a set of interconnected business process fragments.

A second approach uses operational research techniques for optimizing a cloud selection taking into account two conflicting objectives, namely: the execution time (makespan) and the overall cost incurred using a set of resources. We proposed in [9] three complementary approaches to deal with the matching and scheduling scientific workflow tasks in Cloud computing environments. An extension of this first study was presented in [11], [10]. More precisely, we have extended the three proposed approaches to consider: (i) the business workflows and (ii) the concurrent access to resources by multiple instances of a given process. To achieve this goal, we proposed to use a predictive models in order to estimate the availability of the used resources. We

are currently working on the business processes execution in Cloud computing context taking into account workflow patterns such as *sequence, switch, multi-choice, etc.* patterns. Moreover, we plan to extend the proposed work to take into account others criteria like carbon emission and energy cost.

6.2.2. Alignment between Business Process and Service Architecture

Participants: François Charoy, Karim Dahman, Claude Godart.

In the continuation of work done previously on change management during process execution, we are conducting work on the governance of change at the business level and on its implications at the architecture and infrastructure level of an information system. Last year was devoted to the definition of the transformation rules that allowed to go from a business model to an IT model, i.e. a transformation between model based on different paradigms. During this year, a great deal of effort has been done in order to extend our work on Business to IT alignment management. Our goal is still to maintain this alignment at the lowest possible cost when the business process are changing. Further than that we are trying to describe and validated an engineering method to help designer to maintain this alignment. Karim Dahman has defended is PhD on this matter in october 2012.

6.2.3. Monitoring and violations detections of choreographies or distributed compositions of services

Participants: Aymen Baouab, Ehtesham Zahoor, Olivier Perrin, Walid Fdhila, Claude Godart.

The dynamic nature of the cross-organizational business processes poses various challenges to their successful execution. Services choreographies or distributed compositions of services help to reduce such complexity by providing means for describing complex systems at a higher level. However, this does not necessarily guarantee that erroneous situations cannot occur due to inappropriately specified interactions. In [7], [6], we propose an approach for decentralized monitoring of cross-organizational choreographies, using a runtime event-based approach to deal with the problem of monitoring conformance of interaction sequences. Our approach allows for an automatic and optimized generation of rules. After parsing the choreography graph into a hierarchy of *canonical* blocks, tagging each event by its block ascendancy, an optimized set of monitoring queries is generated. We evaluate the concepts based on a scenario showing how much the number of queries can be significantly reduced. These results use our previous results about event-based framework DISC [33].

SEMAGRAMME Team

6. New Results

6.1. Syntax-Semantics Interface

6.1.1. Graph Rewriting

Bruno Guillaume and Guy Perrier have proposed a system for annotating the French Treebank with semantic dependencies [12], [14]. This system (Synsem_FTB) is based on Graph Rewriting. Graph Rewriting is a framework which is well-suited for syntax-semantic interface because it allows for a modular development of large systems. Each modelled linguistic phenomenon is described by a small set of local rewriting rules. The whole transformation is then described by a sequence of modules to apply successively to the input structure. Another benefit of the Graph Rewriting formalism is that it handles the ambiguity in a natural way with the use of non confluent rewriting systems.

The Synsem_FTB system produces a semantic annotation in the framework of DMRS starting from an annotation with surface syntactic dependencies. It contains 34 modules that can be split in two main parts; the first part produces a deep syntax annotation of the input and the second one rewrites deep syntax to semantics.

With respect to previous works, the system of rewriting rules itself has been improved: it has a larger coverage (causative constructions, rising verbs, ...) and the order between modules has been studied in a more systematic way.

The rewriting calculus has been enriched on two points: the use of rules to make a link with lexicons, especially with the lexicon of verbs Dicovalence, and the introduction of filters to discard inconsistent annotations at some computation steps.

This system has been experimented on the whole French Treebank with the Grew software, which implements the used rewriting calculus.

6.1.2. Passive Sentences

Chris Blom, Philippe de Groote, Yoad Winter, and Joost Zwarts have proposed a unified syntactic-semantic account of passive sentences and sentences with an unspecified object [18]. For both constructions, they use *option types* for introducing implicit arguments into the syntactic-semantic categorial mechanism. They show the advantages of this approach over previous proposals in the domains of scope and unaccusatives. Unlike pure syntactic treatments, option types immediately derive the obligatory narrow scope of existential quantification over an implicit argument's slot. Unlike purely semantic, event-based treatments, their solution naturally accounts for syntactic contrasts between passives and unaccusatives.

6.1.3. Intensionalization

Makoto Kanazawa and Philippe de Groote have defined a general *intensionalization* procedure that turns an extensional semantics for a language into an intensionalized one that is capable of accommodating *truly intensional* lexical items without changing the compositional semantic rules [48]. They have proved some formal properties of this procedure and have clarified its relation to the procedure implicit in Montague's PTQ.

6.1.4. Plural

Sai Qian and Maxime Amblard have modeled the semantics of plurality in continuation semantics [13]. Two types of discourse antecedents formations, inherited from the classical treatment, namely summation and abstraction, are studied in detail. Solutions for each phenomenon are provided respectively by introducing two new functions `Sum` and `Abs`, for obtaining the semantic interpretations.

6.2. Discourse Dynamics

In a joint work with a psycho-linguistist (Michel Musiol, ATILF) and a philosopher (Manuel Rebuschi, Archives Poincaré), are developing a formal analysis of pathological conversations involving schizophrenic speakers [16]. Such conversations give rise to manifest incongruities or ruptures that can be seen as mere contradictions by any "normal" speaker. Our analysis relies both on semantic and pragmatic features of conversation. We propose a SDRT-inspired [20] account of pathological conversations, and we apply it to two relevant excerpts. We conclude with a short discussion about the localization of inconsistencies by schizophrenics, either in semantics or in pragmatics, and its importance for our understanding of thought disorders.

SHACRA Project-Team

6. New Results

6.1. Non-Rigid Augmented Reality for Hepatic Surgery

Hepatic resection and tumors removal approaches remains a major challenge. Despite the use of new minimally invasive techniques which has several advantages such as precision, decreased blood loss, quicker healing time and less pain, the lack of informations due to poor depth perception and direct contact lost leads the surgeons and the research groups to use Augmented Reality to overcome these issues. Augmented Reality is the visual overlay of computers-generated images over real world images. This technique can be used to overlay vessels, tumors and cutting planes performed on the pre-operative data (3D reconstruction from CT or MR scan) onto the laparoscopic video per-operatively. However, current techniques are limited to a rigid registration of the pre-operative liver anatomy onto the intra-operative image, and often this registration is not performed automatically. Our objective is to develop a real-time, non-rigid registration and tracking of the intra and pre-operative liver data.

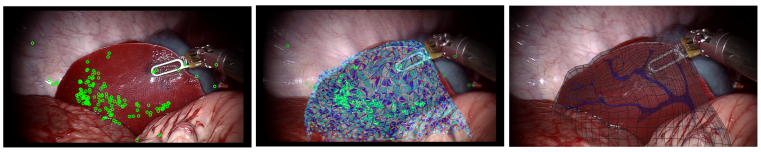

Figure 5. Non-rigid augmentation of a vascular network of a porcine liver : (left) The liver tracking. (Middle) Biomechanical model of the liver under deformation. (Right) Overlaid vascular network.

6.2. Implicit Modeling of Vascular Trees

Many clinical applications require a vessel segmentation process that is able to both extract the centerline and the surface of the blood vessels. However, noise and topology issues (such as kissing vessels) prevent existing algorithms from being able to easily retrieve such a complex system as the brain vasculature. We propose a new blood vessel tracking algorithm that 1) detect the vessel centerline; 2) provide a local radius estimate; and 3) extracts a dense set of points at the blood vessel surface. This algorithm is based on a RANSAC-based robust fitting of successive cylinders along the vessel. Our method was validated against the Multiple Hypothesis Tracking (MHT) algorithm on 10 3DRA patient data of the brain vasculature. Over 30 blood vessels of various sizes were considered for each patient. Our results demonstrated a greater ability of our algorithm to track small, tortuous and touching vessels (96% success rate), compared to MHT (65% success rate). The computed centerline precision was below 1 voxel when compared to MHT. Moreover, our results were obtained with the same set of parameters for all patients and all blood vessels, except for the seed point for each vessel, also necessary for MHT. The proposed algorithm is thereafter able to extract the full intracranial vasculature with little user interaction.

In the context of computer-based simulation, contact management requires an accurate, smooth, but still efficient surface model for the blood vessels. A new implicit model is proposed, consisting of a tree of local implicit surfaces generated by skeletons (*blobby models*). The surface is reconstructed from data points by minimizing an energy, alternating with an original blob selection and subdivision scheme. The reconstructed models are very efficient for simulation and were shown to provide a sub-voxel approximation of the vessel surface on 5 patients.

6.3. Riskmaps in DBS

As discussed in previous sections, Deep Brain Stimulation is a neurosurgical treatment that provides remarkable benefits in neurological movement and affective disorders. It consists in the implantation of a wired electrode deep into the brain. However, the accuracy of the placement is difficult due to brain shifts occuring during the procedure. Due to a potential risk of hemorrhage during the implantation, we specially investigated the brain shift induced motion of the vascular structures. We proposed a method to estimate this motion, based on a physics simulation that consider brain deformation, cerebrospinal fluid and multiple interactions, such as brain-skull contacts etc. The aim is to take it into account during the pre-operative planification step. Thus, we developped a brain-shift aware risk map. It estimate the risk for a trajectory to dissect a vessel. It could help surgeons to choose a safer trajectory for the electrode, and then avoid hemorrhages. The next steps is the use of more complex deformation models.

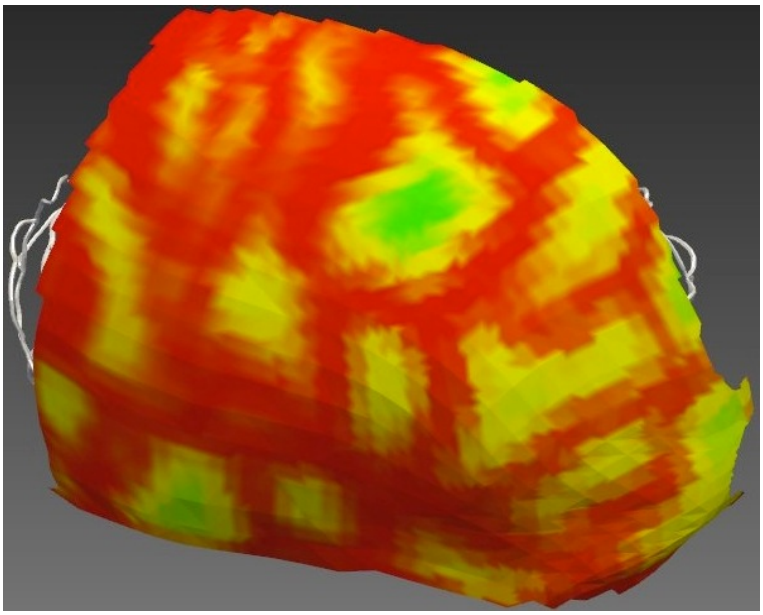

Figure 6. Brain-shift aware risk map

6.4. Electro Physiology

Cardiac arrhythmia is a very frequent pathology that comes from an abnormal electrical activity in the myocardium. This Ph.D. aims at developing a training simulator for interventional radiology and thermo-ablation of these arrhythmias. The latest improvements lead on electrophysiology simulation (using GPU computing) allowed us to reach real-time performance. The issue of fast electrophysiology was a major bottleneck in the development of our simulator.

This new result enabled us to couple the cardiac eletrophysiology with cardiac mechanical models, thus leading to an interactive framework. Our tractable simulation can therefore simulate a patient-specific electrophysiology and then compute the associated cardiac motion using an electromechanical model.

Moreover, the electrophysiology simulation has been also coupled with a navigation simulation. This is still a work in progress. The implementation of more complex models, such as bidomain models, is also in progress.

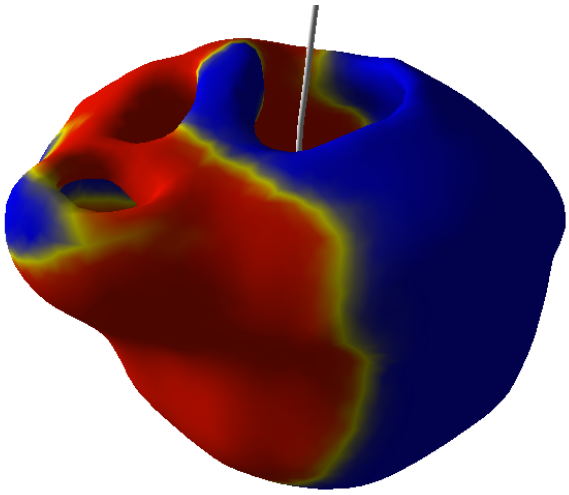

Figure 7. Cardiac electrophysiology computed on a patient-specific geometry

6.5. Shells

Many tissues in human body have thin structure and may be seen as surfaces or at least be modeled as such. Deformation modeling of surfaces is a topic with wide area of applications especially in computer graphics. However, many of the previously presented techniques are not applicable to the area of surgical simulations where a more physically based approach is desired.

To address this problem we present a new model of shell elements based on the formulation of Bézier triangles. To reduce the number of necessary degrees of freedom a kinematic link between nodes inside the element is defined. Furthermore, using implicit integration scheme allows us to achieve interactive frame rate of the simulation.

The applicability of the model has been validated on a prototype of simulator for preoperative planning of surgery of congenital heart diseases.

6.6. Interaction simulation between fluid film and deformable solids

Body fluids are a major constituent of the human body as well by their volume as by their functions. Besides the blood and the lymphatic liquid, many other liquids are present in the body and they have important functions such as lubrication or shock absorption. In this work, we are more particularly interested in the fluids being in the interface between two anatomical structures. We present a method making it possible to simulate the phenomena of interaction between a fluid film and surfaces between which it is forced. The approach that we propose is based on a fluid model and its mechanical coupling with deformable surfaces. According to the pressure of the fluid and the stiffness of the deformable solids in contact with the fluid, various behaviours are expected. Our preliminary results show that it is possible to simulate the main features of these behaviours. Furthermore, the approaches chosen for the fluid model, the deformable model and the coupling between both, are compatible with real time simulations.

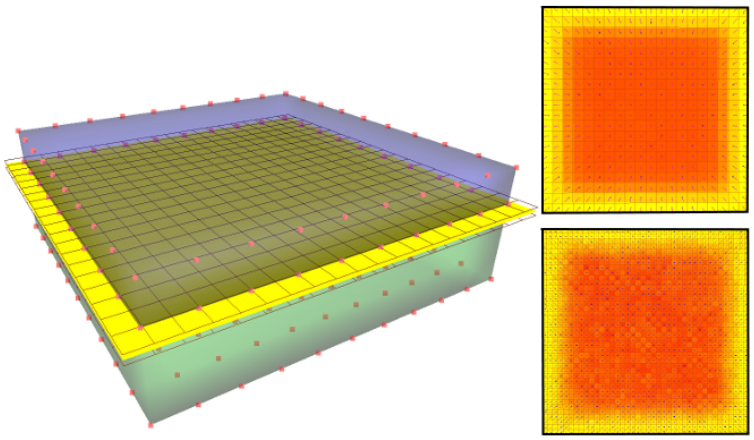

Figure 8. The fluid is between a rigid solid (green) and a deformable solid (blue). The deformable solid is constraint at the edges. Right: the height map of the fluid (yellow minimum and red maximum height).

TOSCA Project-Team

6. New Results

6.1. Probabilistic numerical methods, stochastic modelling and applications

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

6.1.1. Published works and preprints

- In collaboration with P.-E. Jabin (University of Maryland), J.-F. Jabir and J. Fontbona (CMM and Universidad de Chile, Santiago de Chile), M. Bossy have studied the link between the Lagrangian version of divergence free constraint (and the uniform density constraint), with an additional potential term in the Lagrangian equation, having some similarity with the role of the Eulerian pressure term. They obtained the local existence of analytical solutions to an incompressible Lagrangian stochastic model in periodic domain. The paper is in positive revision for publication in *Communications in Partial Differential Equations* [33]. http://hal.inria.fr/hal-00691712
- N. Champagnat worked with A. Lambert (Univ. Paris 6) on splitting trees with Poissonian mutations. Assuming that each mutation is neutral and gives a new type in the population, they obtained in [13], [14] large time convergence results on the sizes of the largest families and the ages of the oldest families in the population. http://hal.inria.fr/inria-00515481, http://hal.inria.fr/inria-00616765. In collaboration with Mathieu Richard (Ecole Polytechnique, Palaiseau), they also extended some of these results to the case of splitting trees with mutations occuring at birth of individuals [15], http://hal.inria.fr/hal-00736036.
- N. Champagnat obtained with P. Diaconis (Stanford Univ.) and L. Miclo (Univ. Toulouse 3) the full spectral decomposition of the transition matrix of two-dimensional Markov chains $(X_n, Y_n)_{n\geq 0}$ in $\mathbb{Z}_+^2$, without immigration or mutation, which are *neutral* in the sense that $(X_n + Y_n)_{n\geq 0}$ is a Markov process. Because of the specific form of the eigenvectors, they were also able to characterize all the Dirichlet eigenvectors in subdomains of $\mathbb{Z}_+^2$ of the form $\{(i,j) \in \mathbb{Z}_+^2 : i + j \geq d\}$ for all $d \geq 0$. As an application, they could determine the quasi-stationary and quasi-limiting distributions of such processes [12], http://hal.inria.fr/hal-00672938.
- N. Champagnat studied with F. Campillo (EPI MODEMIC, Inria Sophia Antipolis — Méditerrannée) individual based models of clonal plants where plants interact through the network formed by the rizhomes or stolons linking plants. In the limit of large population, they obtained a PDE governing the dynamics of population densities in space [11], http://hal.inria.fr/hal-00723209.
- M. Deaconu and S. Herrmann introduced a new method for the simulation of the hitting times of nonlinear boundaries for Bessel processes. This method combines the method of images and the random walk on spheres method. They construct the so called walk on moving spheres algorithm. This approach can be applied for the hitting time of a given level for the Cox-Ingersoll-Ross process and thus be used in models coming from finance and neuroscience [17], http://hal.inria.fr/hal-00636056/en. This work is part of the ANR MANDy project.
- J. Inglis and E. Tanré studied with F. Delarue and S. Rubenthaler (Univ. Nice – Sophia Antipolis) the global solvability of a networked system of integrate-and-fire neurons proposed in the neuroscience literature. In the mean-field limit the equation resembles a McKean-Vlasov equation, but is highly non-standard and previous attempts at rigorous analysis were not satisfactory. They here bridge this gap, and shed light on a surprisingly complicated problem [35], http://hal.inria.fr/hal-00747565.

- A. Lejay continued his long term investigations on probabilistic interpretations and Monte Carlo simulations of interfaces conditions, such as ones arising in discontinuous media. With G. Pichot (IRISA, Rennes), he has developed a series of tests and benchmarks regarding one-dimensional Monte Carlo methods, such as the ones proposed in [19], http://hal.inria.fr/hal-00649170. He has also developed a new family of stochastic diffusion processes, called the *snapping out Brownian motion*, in order to take into account an interface condition where the concentration of the fluid is proportional to its gradient. Finally, A. Lejay and S. Maire also proposed new methods and tested a few ones to deal with the locally isotropic case for multidimensional problems [18], http://hal.inria.fr/hal-00689581.
- With A. Kohatsu-Higa (Ristumeikan University) and K. Yasuda (Hosei university), A. Lejay has continued his work [25] on the simulation of SDE with a discontinuous drift. http://hal.inria.fr/hal-00670123
- With L. Coutin (University of Toulouse), A. Lejay has developed an appropriate framework to deal with linear rough differential equations, extending some results (Magnus formula, Dyson series...) to this case. Using theses properties, they have studied the sensitivites of solutions of rough differential equations with respect to the signal, the vector field or the starting point. They have provided new results such as the Hölder continuity of the derivative of the so called Itô map which transforms a rough path to the solution of a rough differential equation [34]. http://hal.inria.fr/hal-00722900
- S. Maire and C. Prissette (Univ. du Sud – Toulon – Var) have developed in [21] a stochastic algorithm to solve Sudoku puzzles using estimation of distribution coupled with restart techniques. http://hal.inria.fr/inria-00591852
- S. Maire and E. Tanré have generalised the spectral methods for elliptic PDEs developed in [42], [43] to the case of pure Neumann boundary conditions. Some additional difficulties occur because the stochastic representation of the solutions is defined only up to an additive constant and as a limit involving local time approximations [40]. By taking into account these additional properties, they still obtained a spectral matrix having a condition number converging to one [36]. http://hal.inria.fr/hal-00677529
- C. Graham (Ecole Polytechnique) and D. Talay wrote the first volume [27] of their series of books published by Springer on the Foundations of Stochastic Simulations. They started to write the second volume.
- D. Villemonais wrote with S. Méléard (École Polytechnique) a survey on quasi-stationary distributions and Q-processes for stochastic models of population dynamics. This survey also contains a detailed numerical study of the behaviour of classical models with extinction [23]. http://hal.inria.fr/hal-00653834
- D. Villemonais worked on the empirical distribution of Fleming-Viot type particle systems. Using couplings with reflected diffusion processes, he proved the uniform tightness of such empirical distributions and deduced the non-degeneracy of the law of diffusion processes conditioned not to hit a boundary [39]. http://hal.inria.fr/hal-00681601
- D. Villemonais proved in [38] a general approximation method for Markov processes conditioned not be killed. The method is based on a mean field interacting particles system which is easy to simulate. The study also details the particular case of time/environment dependent diffusion processes. http://hal.archives-ouvertes.fr/hal-00598085

6.1.2. Other works in progress

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

- N. Champagnat and D. Villemonais work on time-reversal of absorbed processes, which allow to characterize the path to extinction in extinct populations which are known to be non-extinct at some time in the past. They plan to apply these results on practical ecological situations.
- J. Claisse continued his PhD. under the supervision of N. Champagnat and D. Talay on stochastic control of population dynamics. He completed a finite-horizon and an infinite-horizon optimal control problem on a birth-death process. He is currently working on a finite-horizon optimal control problem on a branching-diffusion process. In addition, he is working on modelling of a pH-mediated cancer treament.
- M. Deaconu and S. Herrmann continue the study of the hitting times for Bessel processes in the situation of noninteger dimensions and also in the application of this method to the simulation of the Brownian hitting time,
- M. Deaconu starts a collaboration with L. Beznea (Simion Stoilow Institute of Mathematics of the Romanian Academy) on coagulation-fragmentation models and their connection with branching processes.
- M. Deaconu studies in collaboration with F. Nobile and F. Tesei (EPFL) a pollution model by using hitting times of stochastic processes.
- S. Herrmann and E. Tanré worked on a scheme to construct an efficient algorithm to simulate the first hitting time of curves by a one dimensional Brownian motion. They apply the result to estimate the spiking time of leaky integrate fire models in neuroscience. This work is part of the ANR MANDy project.
- S. Larnier joined the team in September as a post-doctoral researcher and began working with A. Lejay on data assimilation in order to predict the ocean wave energy from the knowledge of near-shore incoming waves. They started a collaboration on video data with R. Almar (LEGOS, Toulouse) and R. Cienfuegos (Pontificia Universidad Católica de Chile).
- S. Maire works with M. Simon (Mainz Univ.) on electrical impedance tomography problems using new Monte Carlo schemes that deal with Robin and transmission boundary conditions.
- S. Maire develops with I. Dimov (Bulgarian academy of sciences) a Monte Carlo method called the walk on equations to solve linear systems of algebraic equations.
- S. Niklitschek has continued his PhD. work under the supervision of D. Talay. They were able to extended their first work in which they gave a probabilistic interpretation of a parabolic equation with discontinuous drift and proved the weak rate of convergence of the Euler method using the accurate pointwise estimates obtained for the derivatives of the solution, to the case in which both drift and diffusion coefficients are discontinuous. Both results are consistent with each other, and also with the results obtained by M. Martinez and D. Talay in [22].
- N. Perrin continued his PhD. on stochastic methods in molecular dynamics under the supervision of M. Bossy, N. Champagnat and D. Talay. This year, he studied a stochastic interpretation of parabolic PDEs with divergence form operators involved in the Poisson-Boltzmann PDE of molecular dynamics, and the associated numerical Monte Carlo method. He also continued his study of a method due to P. Malliavin (French Academy of Science) based on the Fourier analysis of covariance matrices with delay in order to identify the fast and slow components of a molecular dynamics.
- P. Guiraud (University of Valparaiso) and E. Tanré study the effect of noise in the phenomenon of spontaneous synchronisation in a network of full connected integrate-and-fire neurons. They detail cases in which the phenomenon of synchronization persists in a noisy environment, cases in which noise permits to accelerate synchronization, and cases in which noise permits to observe synchronization while noiseless model does not have synchronization.
- P. Orio (Centro Interdisciplinario de Neurociencia de Valparaiso) and E. Tanré work on the comparison of global properties of the solution of mathematical models and the associated measurements obtained by experiments.

- L. Violeau continued his PhD. on *Stochastic Lagrangian Models and Applications to Downscaling in Fluid Dynamics* under the supervision of M. Bossy and A. Rousseau (MOISE team, Inria Sophia Antipolis – Méditerranée, Montpellier). Laurent studied this year the rate of convergence of the Nadaraya-Watson conditional estimator for "linear" kinetic processes. He is currently working on the rate of convergence of the particle approximation of kinetic conditional McKean-Vlasov stochastic models.
- P-E. Jabin and D. Talay continue to develop their innovating approach, which combines stochastic analysis and PDE analysis, for the time varying Hamilton-Jacobi-Bellman-McKean-Vlasov equations of the Lasry and Lions mean-field stochastic control theory.
- D. Talay is working with J. Bion-Nadal (Ecole Polytechnique) on applications of risk measures to the calibration of stochastic models, with N. Touzi (Ecole Polytechnique) on the stochastic control of stochastic differential equations with weighted local times, and with O. Bardou (GDF) on Edgeworth expansions for the Central Limit Theorem for Brownian martingales whose integrands depend on ergodic diffusion processes.

6.2. Financial Mathematics

Participants: Mireille Bossy, Paul Charton, Dalia Ibrahim, Denis Talay, Etienne Tanré.

- Mireille Bossy, in collaboration with H. Quinteros (Univ. Chile) worked on the rate of convergence of non Lipschitz diffusion processes discretized with the symetrized Milstein scheme. Under the same kind of hypotheses than in [41] on the symetrized Euler scheme, they obtained the expected improvement of the strong rate of convergence, when the diffusion coefficient is of the form $\sigma(x) = x^\alpha$, with $\alpha \in [1/2, 1[$.

  A preprint is being written.
- P. Charton continued his PhD. under the supervision of M. Deaconu and A. Lejay. He studied some storage strategies for wind farms.
- **Mathematical modelling for technical analysis techniques** Since November 2009, D. Ibrahim has been working on her PhD. thesis on Mathematical modeling of technical analysis in finance, under supervision of D. Talay and E. Tanré. The aim of her work is to study the performances of a technical analysis tool designed to detect changes in the volatility term: The Bollinger Bands. She studied the performances of this indicator in a modified Black-Scholes model such that the volatility is equal to σ_0 up to a random time τ, independent of the Brownian motion governing the prices. After τ, the volatility is equal to σ_1. She proved that Bollinger Bandwidth indicator can detect the time change (at which the volatility changes its value), in the case of small and large volatilities. She has also exhibited a mathematical optimal allocation strategy, by decomposing the initial allocation problem into an allocation problem before the change time τ and an allocation problem after τ, in order to circumvent some technical problems brought from the change of volatility.

  This work is part of the contract with FINRISK.
- In collaboration with C. Michel (CA-CIB) and V. Reutenauer (Citi), D. Talay and E. Tanré worked on the
  - the study of the liquidity risk in the interest rate options market;
  - the minimization of the hedging error in interest rates Gaussian models by means of strategies designed in an effective way by using stochastic optimization algorithms.
- P. Protter (Columbia University) and D. Talay continue to work on bubbles time evolution models, which leads them to try to extend Feller's results on explosion times for stochastic differetential equations.

TRIO Project-Team

6. New Results

6.1. Evaluation and optimal dimensioning of real-time systems

- **Code analyses and advanced visualization of software in real-time**

  Participants: Pierre Caserta, Olivier Zendra

  Last years, strong developments for our instrumentation, tracer and analyzer, had been performed, allowing us to really enter the experimental phase and getting first interesting results. A thorough state of the art had also been written.

  This state of the art paper had finally been published in TVCG, a leading journal in computer visualization. Thanks to the experimental setup efforts of previous years, we had been able in 2011 to conduct good experiments. We had designed and implemented a new way to visualize relations between software elements. These relations include static relations (is-a, direct heir, caller, callee, etc.) and dynamic ones (runtime caller, runtime callee). Our new relation visualization comprises a new way of placing way points so as to significantly decrease spatial and visual clutter when visualizing software systems with large numbers (thousands up to millions) of relations. This had lead to a publication in VISSOFT, one of the most recognized conferences in the software visualization domain, as well as a Best Poster in ECOOP, one of the most recognized conferences in the object-oriented domain. The important design and implementation work we had realized on the tracing and analysis software also lead to the publication of our method in ICOOOLPS 2011.

  This year, in 2012, we published our instrumentation and tracing method in Elsevier's Science of Computer Programming journal [9].

  Work has been going onto analyze polymorphism in Java programs, answering an apparently simple yet so far unanswered question: how much polymorphism is there actually in Java programs. This is of paramount importance, since a lot of work occur around polymorphism, which is an important concept, but no one is currently able to tell how much it impact programs in real life. We have begun writing this paper in cooperation with the LIRMM lab in Montpellier. In addition, we are in the process of finishing work pertaining to analyzing program evolutions, looking at differences between versions, and analyzing how dynamic metrics and static metrics correlate to evolution rate.

  Work in this domain has also lead to the writing and successful defense of Pierre Caserta's PhD thesis, titled "Analyse statique et dynamique de code et visualisation des logiciels via la métaphore de la ville : contribution à l'aide à la compréhension des programmes", on 7th December 2012 [7].

  A web site was also designed to publicize our work on the VITRAIL project.

- **Open Power and Energy Optimization PLatform and Estimator**

  Participants: Fabrice Vergnaud, Jérôme Vatrinet, Kévin Roussel, Olivier Zendra.

  Work in this domain was performed in the context of the ANR Open-PEOPLE (Open Power and Energy Optimization PLatform and Estimator) project, financed since the very end of 2008. Inria Nancy Grand Est is responsible for the software part of the platform and is involved in memory management for low-power issues. Work in this project begun in April 2009 (kick-off meeting). We have finished setting up the very important infrastructure for the software part of the Open-PEOPLE platform. We have finished expressing the requirements for the platform, in order to start the actual developments and the actual integration of tools provided by the different partners. In 2011, we have finished expressing the platform architecture and user interface (GUI). We have also finished implementing the part of the software platform that is the remote control to the hardware platform. We finally have finished implementing the core of the software platform and canonical

models handling. This work lead to several technical and the several presentations and posters in conferences.

This year was the result harvesting for our project, in terms of development. We finished the design and implementation of the PCMD (Power Consumption Model Development) and the PCAO (Power Consumption Analysis and Optimization) parts of the software platform, as well as the external tools integration work. We also designed and implemented the Open-PEOPE model sharing website. Again, several demos and publications in conferences resulted [13], [21], [22].

- **Operator calculus and conceptation of algorithms for optimisatio of multi-constraints problems**

  Participants: Jamila Ben Slimane, Hugo Cruz-Sanchez, Bilel Nefzi, René Schott, Ye-Qiong Song

  R. Schott and G. Stacey Staples proposed a solution based on operator calculus for graphs with multi-constraints [26]. These constraints are not necessarily linear or positive. This approach was developed for realistic problems like:

  – configuration of satellites proposing a high-quality coverage [14];
  – optimal utilisation of ressources in hospitals;
  – optimal management in sensor networks [25].

  This work was the result of the collaboration of our team with MADYNES team, LPMA (Laboratoire de Probabilités et Modèles Aléatoires, Paris 6 et 7) and University of Illinois at Edwardsville.

6.2. Real-time analysis

- **Scheduling of tasks in automotive multicore ECUs**

  Participants: Aurélien Monot, Nicolas Navet, Françoise Simonot-Lion.

  As the demand for computing power is quickly increasing in the automotive domain, car manufacturers and tier-one suppliers are gradually introducing multicore ECUs in their electronic architectures. Additionally, these multicore ECUs offer new features such as higher levels of parallelism which ease the respect of safety requirements such as the ISO 26262 and the implementation of other automotive use-cases. These new features involve also more complexity in the design, development and verification of the software applications. Hence, car manufacturers and suppliers will require new tools and methodologies for deployment and validation. We address the problem of sequencing numerous elementary software components, called runnables, on a limited set of identical cores. We show how this problem can be addressed as two sub-problems, partitioning the set of runnables and building the sequencing of the runnables on each core, which problems cannot be solved optimally due to their algorithmic complexity. We then present low complexity heuristics to partition and build sequencer tasks that execute the runnable set on each core, and derive lower bounds on their efficiency (i.e., competitive ratio). Finally, we address the scheduling problem globally, at the ECU level, by discussing how to extend this approach in the case where other OS tasks are scheduled on the same cores as the sequencer tasks. An article providing a summary of this line of work has been published in IEEE TII [12].

- **Probabilistically analysable real-time system**

  Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Luca Santinelli, Dorin Maxim and Cristian Maxim.
  The adoption of more complex hardware to respond to the increasing demand for computing power in next- generation systems exacerbates some of the limitations of static timing analysis for the estimation of the worst-case execution time (WCET) estimation. In particular, the effort of acquiring (1) detail information on the hardware to develop an accurate model of its execution latency as well as (2) knowledge of the timing behaviour of the program in the presence of varying hardware conditions, such as those dependent on the history of previously executed instructions. These

problems are also known as the timing analysis walls. The probabilistic timing analysis, a novel approach to the analysis of the timing behaviour of next-generation real-time embedded systems, provides answers to timing analysis walls. In [10], [15] we have showed how the probabilistic timing analysis attacks the timing analysis walls. We have also presented experimental evidence that shows how probabilistic timing analysis reduces the extent of knowledge about the execution platform required to produce probabilistically-safe and tight WCET estimations.

Based on existing estimations of WCET or minimal inter-arrival time, we may propose different probabilistic schedulability analyses [19], [11].

- **Statistical analysis of real-time systems**

  Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Lu Yue, Thomas Nolte [Malardelan University], Rob Davis, Ian Bate [University of York], Michael Houston, Guillem Bernat [Rapita].

  The response time analysis of real-time systems usually needs the knowledge of WCET estimation and this knowledge is not always available, e.g., because of intelectual property issues. This problem may be avoided by estimating statistically either the WCET of a task [18], the inter-arrival time [17] or the response time of each task [23].

- **Probabilistic Component-based ApproachesParticipants:** Luca Santinelli, Patrick Meumeu Yomsi, Dorin Maxim, Liliana Cucu-Grosjean.

  We have proposed a probabilistic component-based model which abstracts in the interfaces both the functional and non-functional requirements of such systems. This approach allows designers to unify in the same framework probabilistic scheduling techniques and compositional guarantees that go from soft to hard real- time. We have provided sufficient schedulability tests for task systems using such framework when the scheduler is either preemptive fixed-priority or earliest deadline first. These results were published in [16].

VEGAS Project-Team

5. New Results

5.1. Classical computational geometry

5.1.1. Complexity analysis of random geometric structures made simpler

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

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

5.1.2. On the monotonicity of the expected number of facets of a random polytope

Let K be a compact convex body in R^d, let K_n be the convex hull of n points chosen uniformly and independently in K, and let $f_i(K_n)$ denote the number of i-dimensional faces of K_n.

In a joint work with Olivier Devillers and Marc Glisse (Inria GEOMETRICA) and Matthias Reitzner (Univ. Osnabruck) [21], we showed that for planar convex sets, $E(f_0(K_n))$ is increasing in n. In dimension $d \geq 3$ we prove that if $lim_{n\to\infty} \frac{E(f_{d-1}(K_n))}{An^c} = 1$ for some constants A and $c > 0$ then the function $E(f_{d-1}(K_n))$ is increasing for n large enough. In particular, the number of facets of the convex hull of n random points distributed uniformly and independently in a smooth compact convex body is asymptotically increasing. Our proof relies on a random sampling argument.

5.1.3. Embedding geometric structures

We continued working this year on the problem of embedding geometric objects on a grid of $\mathbb{R}^3$. Essentially all industrial applications take, as input, models defined with a fixed-precision floating-point arithmetic, typically doubles. As a consequence, geometric objects constructed using exact arithmetic must be embedded on a fixed-precision grid before they can be used as input in other software. More precisely, the problem is, given a geometric object, to find a similar object representable with fixed-precision floating-point arithmetic, where similar means topologically equivalent, close according to some distance function, etc. We are working on the problem of rounding polyhedral subdivisions on a grid of $\mathbb{R}^3$, where the only known method, due to Fortune in 1999, considers a grid whose refinement depends on the combinatorial complexity of the input, which does not solve the problem at hand. This project is joint work with Olivier Devillers (Inria Geometrica) and William Lenhart (Williams College, USA) who was in sabbatical in our team in 2012.

5.2. Non-linear computational geometry

5.2.1. Geometry of robotic mechanisms

Parallel manipulators are a family of mechanisms, the geometry of which is difficult to compute in general. The use of algebraic methods allowed us to describe precisely the geometry of the configurations of different specific parallel manipulators, in collaboration with researchers from the IRCCyN laboratory in Nantes.

More precisely, moving a parallel robot toward specific parametric values can break it. A challenge is to describe this set of singularities. This was adressed for a planar mechanism with three degrees of freedom in [16] and a spatial mechanism with six degrees of freedom in [12].

Then, a more challenging question arises naturally. Given a familly of mechanisms parametrized by some construction variables, is it possible to find a mechanism that has no singularities? A method based on Gröbner bases was proposed in [17] for a specific family of planar parallel robot with two degrees of freedom.

5.2.2. Solving bivariate systems and topology of algebraic curves

In the context of our algorithm Isotop for computing the topology of algebraic curves [28], we study the bit complexity of solving a system of two bivariate polynomials of total degree d with integer coefficients of bitsize τ. 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.

We work on an algorithm for computing RURs with worst-case bit complexity in $O(d^8 + d^7\tau + d^5\tau^2)$ (where polylogarithmic factors are omitted). In addition, we show that certified approximations of the real solutions can be computed from this representation with $O(d^8 + d^7\tau)$ bit operations. It should be stressed that our algorithm is deterministic and that it makes no genericity assumption.

When $\tau \in O(d^2)$, this complexity decreases by a factor d^2 the best known upper bound for computing Rational Univariate Representations of such systems and it matches the recent best known complexity (Emeliyanenko and Sagraloff, 2012) for "only" computing certified approximations of the solutions. This shows, in particular, that computing RURs of bivariate systems is in a similar class of (known) complexity as computing certified approximations of *one* of the variables of its real solutions.

This work is on-going and is done in collaboration with Fabrice Rouillier (Inria Ouragan).

5.3. Combinatorics and combinatorial geometry

5.3.1. Multinerves and Helly numbers of acyclic families

The nerve of a family of sets is a simplicial complex that records the intersection pattern of its subfamilies. Nerves are widely used in computational geometry and topology, because the nerve theorem guarantees that the nerve of a family of geometric objects has the same topology as the union of the objects, if they form a good cover.

In a joint work with Éric Colin de Verdière (CNRS-ENS) and Grégory Ginot (Univ. Paris 6) we relaxed the good cover assumption to the case where each subfamily intersects in a disjoint union of possibly several homology cells, and we proved a generalization of the nerve theorem in this framework, using spectral sequences from algebraic topology. We then deduced a new topological Helly-type theorem that unifies previous results of Amenta, Kalai and Meshulam, and Matoušek. This Helly-type theorem is used to (re)prove, in a unified way, bounds on transversal Helly numbers in geometric transversal theory.

This work was presented at SoCG 2012 [18], where it received one of the two "best paper" awards.

5.3.2. Set systems and families of permutations with small traces

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

This work was published in the European Journal of Combinatorics [13].

5.3.3. Simplifying inclusion-exclusion formulas

Let $F = \{F_1, F_2, ..., F_n\}$ be a family of n sets on a ground set X, such as a family of balls in R^d. For every finite measure μ on X, such that the sets of F are measurable, the classical inclusion-exclusion formula asserts that $\mu(F_1 \cup F_2 \cup \bullet\bullet\bullet \cup F_n) = \sum_{I:\varnothing\neq I\subseteq[n]} (-1)^{|I|+1}\mu(\cap_{i\in I} F_i)$; that is, the measure of the union is expressed using measures of various intersections. The number of terms in this formula is exponential in n, and a significant amount of research, originating in applied areas, has been devoted to constructing simpler formulas for particular families F.

In a joint work with Jiří Matoušek, Pavel Paták, Zuzana Safernová and Martin Tancer (Charles Univ., Prague) [22] we provided the apparently first upper bound valid for an arbitrary F: we showed that every system F of n sets with m nonempty fields in the Venn diagram admits an inclusion-exclusion formula with $m^{O((\log n)^2)}$ terms and with ± 1 coefficients, and that such a formula can be computed in $m^{O((\log n)^2)}$ expected time. We also constructed systems of n sets on n points for which every valid inclusion-exclusion formula has the sum of absolute values of the coefficients at least $\Omega(n^{3/2})$.

VERIDIS Project-Team

6. New Results

6.1. Automated and Interactive Theorem Proving

6.1.1. Combination of decision procedures

Participants: Pascal Fontaine, Simon Halfon, Stephan Merz, Christoph Weidenbach.

SMT solvers, combination, decision procedures, theorem proving

We investigate the theoretical limits of combining decision procedures and reasoners, as these are important for the development of the veriT solver (see section 5.1). It has long been known that it is possible to extend any decidable language (subject to a minor requirement on cardinalities) with predicates described by a Bernays-Schönfinkel-Ramsey theory (BSR). A formula belongs to the BSR decidable fragment if it is a conjunction of universal, function-free formulas. As a consequence of this theoretical result, it is possible to extend a decidable quantifier-free language with sets and set operators, relations, orders and similar concepts. This can be used to significantly extend the expressivity of SMT solvers. In previous work, we generalized this result to the decidable first-order class of monadic predicate logic, and to the two-variable fragment. In subsequent joint work with Carlos Areces from Universidad Nacional de Córdoba, Argentina, we showed that two other important decidable fragments (namely the Ackermann fragment, and several guarded fragments) are also easily combinable. In 2012, we considered, in the same spirit, the combination of theories that are not necessarily decidable [18]. In particular, we considered combinations of decision procedures and refutationally complete semi-decision procedures, as well as black-box combinations of different refutationally complete theorem provers, together with finite model finders. These results in particular yield theoretical foundations for how FOL provers can be combined with SMT techniques in a black-box style of integration.

6.1.2. Using symmetries in SMT

Participants: Pascal Fontaine, Stephan Merz.

theorem proving, SMT solvers, decision procedures, symmetry

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

In 2012, we designed a more general approach, based on graph isomorphism, for symmetry detection in the SMT context. Experimental analysis indicates that many formulas from the SMT-LIB repository exhibit symmetries that are left unexploited by the previous techniques. Finding new techniques to exploit these is the subject of ongoing work with the University of Cordoba in Argentina; we expect that breaking those symmetries will yield again some significative efficiency improvement.

6.1.3. Encoding TLA+ proof obligations for SMT solvers

Participants: Stephan Merz, Hernán-Pablo Vanzetto.

system verification, SMT solving, TLA

The TLA$^+$ proof system TLAPS (see section 5.2) is being developed within a project at the MSR-Inria Joint Centre to which we contribute. Proof obligations that arise during the verification of typical TLA$^+$ specifications require reasoning about the principal TLA$^+$ data structures such as sets, functions, arithmetic, tuples, and records. None of the backend provers present in the initial versions of TLAPS was able to reason effectively about steps involving several of these features, and in 2011 we started developing an improved backend for translating TLA$^+$ proof obligations to SMT-Lib, the generic input language of SMT solvers. The main challenge was to design a sound translation from untyped TLA$^+$ to the multi-sorted first-order logic that underlies SMT-Lib, and our original proposal was based on deriving type assignments to TLA$^+$ expressions in a custom type system useful for SMT-Lib. This approach sometimes failed to derive types for subexpressions or required stronger typing assumptions than those required by the semantics of untyped TLA$^+$.

In 2012, based on a suggestion by Ken McMillan, we investigated a different approach whose main idea is to embed SMT sorts such as integers in the global universe of TLA$^+$ values, and to axiomatically define operations such as addition or multiplication on the image of that embedding. This approach effectively delegates type inference to the SMT solver and can therefore handle arbitrary TLA$^+$ expressions. However, it generates many quantified background axioms that may render SMT solvers ineffective, and we developed powerful pre-processing techniques for replacing quantified axioms by their required ground instances. The SMT backend in the current release of TLAPS is based on a hybrid approach to translation, where type inference is used whenever possible in order to obtain simpler SMT input. The two translation techniques have been published in 2012 [19], [20], and they have been validated over many case studies in TLAPS. For example, it enables proving the correctness of simple mutual-exclusion algorithms essentially without user interaction, and of the Paxos consensus algorithm in just 130 interactions, whereas a previous proof attempt using the traditional backend provers was unsuccessful.

6.1.4. Compression of SMT proofs

Participants: Pascal Fontaine, Stephan Merz.

theorem proving, SMT solvers, decision procedures, combination of decision procedures

Integrating an SMT solver in a certified environment such as TLAPS or an LF-style proof assistant requires the solver to output proofs. Unfortunately, those proofs may be quite large, and the overhead of rechecking the proof may account for a significant fraction of the proof time. In previous work, we proposed a technique for reducing the size of propositional proofs based on the analysis of resolution graphs, which were justified in an algebra of resolution. Unfortunately, the complexity of these techniques turned out to be prohibitive, but we proposed practical and efficient algorithms for more restricted compression techniques. We continue to develop this line of work with our partners at TU Wien.

6.1.5. Augmenting the Expressiveness of Spass

Participants: Evgeny Kruglov, Arnaud Fietzke, Daniel Wand, Christoph Weidenbach.

automated theorem proving, superposition, linear arithmetic, proof assistants

In 2012 we focused on bridging the gap between the input logic of SPASS and more expressive logics as they are used by systems supporting full-fledged verification such as Isabelle and TLAPS. Main contributions were a specific version of an order-sorted language that can be eventually translated in a many-sorted logic. The latter is implemented in Spass in a prototypic way and first experiments showed significant improvements on proof obligations out of Isabelle/HOL. Actually, the enhancements allowed Spass to become the most powerful automated theorem proving system supporting Isabelle [14]. We are currently working on a coupling with TLAPS (see section 5.2).

A second important branch is the integration of arithmetic into SPASS and the development of the respective hierarchic superposition calculus. In the past [31], [38] we experimented with a black box integration of LP solvers and Z3 to delegate arithmetic reasoning tasks. Now we started our own white box implementation for linear arithmetic and could achieve significant speed-ups. Our own reasoning procedure, dedicated to the specific form of the arithmetic proof obligations generated by SPASS is 50 to 200 times faster than any black box integration [29]. On the calculus side we could prove hierarchic superposition modulo linear arithmetic

to be a decision procedure for the ground case, thus strictly generalizing the DPLL(LA) set up, and to be a decision procedure [39], [40] for timed automata reachability and extensions thereof [17].

6.1.6. Verification of linear hybrid automata

Participant: Uwe Waldmann.

automated theorem proving, superposition, linear arithmetic, proof assistants

We propose an improved symbolic algorithm for the verification of linear hybrid automata with large discrete state spaces. Large discrete state spaces arise naturally in industrial hybrid systems, due to the need to represent discrete inputs, counters, sanity checkbits, possibly multiple concurrent state machines, system-degradation modes, and finite switching variables. To prove safety properties of such systems, it is necessary to combine techniques for analyzing a complex dynamic behaviour with state space exploration methods that can deal with hundreds of discrete variables. In our approach, we represent both the discrete part and the continuous part of the hybrid state space symbolically using a variant of AIGs (And-Inverter-Graphs). Key components of our method are redundancy elimination (to maintain a compact symbolic representation by deleting superfluous linear constraints) and constraint minimization (exploiting the fact that states already reached in previous iterations of the model-checking algorithm can be interpreted as "don't cares" in later steps). A journal article describing the technique appeared in Science of Computer Programming [9].

6.2. Proved development of algorithms and systems

6.2.1. Incremental development of distributed algorithms

Participants: Dominique Méry, Manamiary Andriamiarina.

distributed algorithms, refinement, verification, distributed protocols

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 works help to formalize pre-existing algorithms, develop new algorithms, as well as develop models for distributed systems.

Our research was initially (until 2010) carried out within the ANR project RIMEL, in joint work with Mohammed Mosbah and Mohammed Tounsi from the LABRI laboratory, and we are maintaining a joint project B2VISIDIA with LABRI on these topics. More concretely, we aim at an integration of the correct-by-construction refinement-based approach into the *local computation* programming model. The team of LABRI develops an environment called VISIDIA that provides a toolset for developing distributed algorithms expressed as a set of rewriting rules of graph structures. The simulation of rewriting rules is based on synchronization algorithms and we have developed these algorithms by refinement.

More precisely, we show how state-based models can be developed for specific problems and how they can be simply reused by controlling the composition of state-based models through the refinement relationship. Consequently, we obtain a redevelopment of existing distributed algorithms in the *correct-by-construction* approach, and a framework for deriving new distributed algorithms (by integrating models) whose correctness is ensured by construction. Traditionally, distributed algorithms are supposed to run on a fixed network, whereas we consider a network with a changing topology. We have illustrated our methodology with the study of the protocol ANYCAST RP.

The contribution is related to the development of proof-based patterns providing effective help to the developer of formal models of applications, such as dynamic routing or the snapshot problem [13]. In fact, we have developed patterns for simplifying the development of distributed systems using refinement. The applicability of a pattern for routing has been reapplied to the development of a network on chip [12] with our partners of the French-Algerian cooperation described in section 8.3 .

6.2.2. Modeling and verifying the Pastry routing protocol

Participants: Tianxiang Lu, Stephan Merz, Christoph Weidenbach.

distributed hash table, peer-to-peer protocol, Pastry, model checking, theorem proving

As a significant case study for the techniques that we are developing within VeriDis, we are modeling and verifying the routing protocol of the Pastry algorithm [36] for maintaining a distributed hash table in a peer-to-peer network. As part of his PhD work, Tianxiang Lu has developed a TLA$^+$ model of the Pastry routing protocol, which has uncovered several issues in the existing presentations of the protocol in the literature, and in particular a loophole in the join protocol that had been fixed by the algorithm designers in a technical report that appeared after the publication of the original protocol.

As a first step towards proving correctness of the Pastry routing protocol, we identified in 2011 a number of candidate invariants and formally proved in TLAPS (see section 5.2) that these implied the high-level correctness property. In 2012, we consolidated these invariants and proved them correct for our model under the strong assumption that no node ever leaves the network, and the minor assumption that any active node can at any time only allow one new node to join the network. It is still not clear at the moment to which extent nodes can be allowed to leave the network without breaking the virtual ring maintained by Pastry. The invariant proofs contain almost 15000 interactions and constitutes the largest case study carried out so far using TLAPS. We have more recently been able to obtain better automation using the new SMT backend (see section 6.1). The proof was presented at the TLA workshop of FM 2012 [23].

6.2.3. *Verification of distributed algorithms in the Heard-Of model*

Participants: Henri Debrat, Stephan Merz.

theorem proving, distributed algorithms, round-based computation, Byzantine failures

Distributed algorithms are often quite subtle, both in the way they operate and in the assumptions required for their correctness. Formal models are important for unambiguously understanding the hypotheses and the properties of a distributed algorithm. We focus on the verification of round-based algorithms for fault-tolerant distributed systems expressed in the Heard-Of model of Charron-Bost and Schiper [37], and have previously established a reduction theorem that allows to pretend that nodes operate synchronously.

In 2012, we have consolidated our formal proofs in Isabelle/HOL. In particular, we have finished the formal proof of the reduction theorem within Isabelle, produced a generic encoding of the Heard-Of model as a locale in Isabelle/HOL, and used this representation for verifying six different Consensus algorithms: three algorithms tolerating benign failures and three others designed for malicious failures, such as corrupted values. Our Isabelle theories have been published at the Archive of Formal Proofs [27]. The proof of the reduction theorem required formalizing the notion of stuttering invariance, which can be of independent interest and that has also been accepted at the Archive of Formal Proofs [28].

As a significant extension of this work, we have studied the formal verification of probabilistic Consensus algorithms in the Heard-Of model, in particular the Ben-Or algorithm.

6.2.4. *Model checking within SimGrid*

Participants: Marie Duflot-Kremer, Stephan Merz.

model checking, distributed algorithms, message passing, communication primitives, partial-order reduction

For several years we have cooperated with Martin Quinson from the AlGorille project team on adding model checking capabilities to the simulation platform SimGrid for message-passing distributed C programs. The expected benefit of such an integration is that programmers can complement simulation runs by exhaustive state space exploration in order to detect errors such as race conditions that would be hard to reproduce by testing. As part of the thesis work of Cristián Rosa (defended in 2011), a stateless model checker was implemented within the SimGrid platform that can be used to verify safety properties of distributed C programs that communicate by message passing. The ongoing thesis of Marion Guthmuller builds upon this work and aims to extend it for verifying certain liveness properties. This requires rethinking the stateless design, as well as adapting the dynamic partial-order reduction algorithm that is essential to limiting the part of the state space that must actually be explored.

6.2.5. Modeling Medical Devices

Participant: Dominique Méry.

Formal modelling techniques and tools have attained sufficient maturity for formalizing highly critical systems in view of improving their quality and reliability, and the development of such methods has attracted the interest of industrial partners and academic research institutions. Building high quality and zero-defect medical software-based devices is a particular domain where formal modelling techniques can be applied effectively. In [21], we present a methodology for developing critical systems from requirement analysis to automatic code generation based on a standard safety assessment approach. This methodology combines refinement, proof, model checking, and animation, and ultimately can automatically generate source code. This approach is intended to contribute to further the use of formal techniques for developing critical systems with high integrity and to verify complex properties. An assessment of the proposed methodology is given through developing a standard case study: the cardiac pacemaker.

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. In [24] we present a methodology for modelling a biological system, such as the heart. The heart model is based mainly on electrocardiography analysis, which provides a model at the cellular level. Combining this environment model with a formal model of the pacemaker, we obtain a closed-loop model over which the overall correctness can be verified.

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. In [25] we use the Event-B modeling language to represent guidelines for subsequent validation. Our main contributions are: to apply mathematical formal techniques to evaluate real-life medical protocols for quality improvement, to derive verification proofs for the protocol and properties according to medical experts, and to publicize the potential of this approach. An assessment of the proposed approach is given through a case study, relative to a real-life reference protocol concerning ECG interpretation, for which we uncovered several anomalies.

Finally, we propose a refinement-based methodology [10] for complex medical systems design, which possesses the required key features. A refinement-based combined approach of formal verification, model validation using a model-checker and refinement chart is proposed in this methodology for designing a high-confidence medical device. Furthermore, we show the effectiveness of this methodology for the design of a cardiac pacemaker system.

6.2.6. Fundamentals of Network Calculus in Isabelle/HOL

Participant: Stephan Merz.

networked systems, min-plus algebra, formal proof

The design of networked and embedded systems has traditionally been accompanied by formal methods for design and analysis. Network Calculus [42] is a well-established theory, based on the $(\min, +)$ dioid, that is designed for computing delay and memory bounds in networks. The theory is supported by several commercial and open-source tools and has been used in major industrial applications, such as the design and certification of the Airbus A380 AFDX backbone. Nevertheless, it is difficult for certification authorities to assess the correctness of the computations carried out by the tools supporting Network Calculus, and we propose the use of *result certification* techniques for increasing the confidence in the Network Calculus toolchain. In joint work with Marc Boyer from ONERA in Toulouse, and with Loïc Fejoz and Nicolas Navet from the RealTime at Work (RTaW) company, we have supervised the master thesis of Etienne Mabille to evaluate the feasibility of the approach. Parts of the theory underlying Network Calculus were formalized in the proof

assistant Isabelle/HOL, and this encoding was used to formally derive theorems that underly the computation of bounds in network servers. The Network Calculus tool produced by RTaW was instrumented to generate traces of its computation, and the correctness of simple systems could in this way be certified by Isabelle. A publication of this work is in preparation, and we intend to continue and extend it in a future joint project.

6.2.7. Bounding message length in attacks against security protocols

Participant: Marie Duflot-Kremer.

security protocols, verification

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. Together with Myrto Arapinis, we have shown [32] that, under a syntactic and reasonable condition of "well-formedness" on the protocol, we can get rid of the infinitely branching part. Following this conference publication, we are preparing a journal version of this result extending the set of security properties to which the result is applicable, in particular including authentication properties.

6.2.8. Evaluating and verifying probabilistic systems

Participant: Marie Duflot-Kremer.

verification, probabilistic systems, performance evaluation

Since its introduction in the 1980s, model checking has become a prominent technique for the verification of complex systems. The aim was to decide whether or not a system was fulfilling its specification. With the rise of probabilistic systems, new techniques have been designed to verify this new type of systems, and appropriate logics have been proposed to describe more subtle properties to be verified. However, some characteristics of such systems cannot fall in the field of model checking. The aim is thus not to tell wether a property is satisfied but how well the system performs with respect to a certain measure. Together with researchers from ENS de Cachan and University Paris Est Créteil we have designed a statistical tool made to tackle both performance and verification issues. Following several conference talks, a journal paper is currently written to present both the approach as well as application to a concrete case study: flexible manufacturing systems.