RESEARCH CENTER
Nancy - Grand Est

FIELD

Activity Report 2013

Section Application Domains

Edition: 2014-03-19

ALGORILLE Project-Team

4. Application Domains

4.1. Promoting parallelism in applications

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

4.2. Experimental methodologies for the evaluation of distributed systems

Our experimental research axis has a *meta* positioning, targeting all large-scale distributed systems. This versatility allows us to factorize the efforts and maximize our efficiency. The resulting findings are typically used by researchers and developers of systems in the following domains:

- High Performance Computing systems (in particular MPI applications on high-end platforms)
- Cloud environments (in particular virtualized environments)
- Grids (in particular high throughput computing systems)
- Peer-to-peer systems

ALICE Project-Team (section vide)

BIGS Project-Team

4. Application Domains

4.1. Data analysis and local regression

Our expertise in data analysis and advanced statistics methods has given raise no a wide number of interdisciplinary collaborations. Among those, here are the most challenging at a scientific level:

(i) Health inequalities: We have recently developed a statistical procedure in order to create a neighborhood socioeconomic index and investigate its influence on health inequalities. The study setting is composed with 3 major French metropolitan areas (Lille, Lyon and Marseille), and we collaborate for this project with a medical team at EHESP (Ecole des Hautes Etudes en Santé Publique) lead by D. Zmirou (see (Lalloue & al, 2012) for further details).

(ii) Fetal pathology: An ongoing work concerning local regression techniques is related to Fetal Biometry, an investigation line suggested by a collaboration between our team and the *Centre de Placentologie et Foetopathologie de la Maternité Régionale de Nancy*, under the direction of Professor Bernard Foliguet. The methods involved in Fetal Biometry are usually based on the comparison of some measured values with the predicted values derived from reference charts or equations in a normal population. However, it happens that maternal and pregnancy characteristics have a significant influence on in-utero Fetal Biometry. We will thus produce some models allowing to construct customized fetal biometric size charts. In order to evaluate them, classical and polynomial regression can be used, but they are not the most appropriate to the kind data we have to handle. Hence, we plan to use local regression estimation in order to perform such an evaluation.

(iii) Cohorts analysis: Some medical teams in Nancy are faced with an overwhelming amount of data, for which a serious statistical assessment is needed. Among those let us mention the INSERM team of Pr. Jean-Louis Guéant. We have thus initiated a common project together with the Inria team Orpailleur (particularly with Marie-Dominique Desvignes and Malika Smail) in this direction. The goal of this collaboration is to extract biological markers for different diseases (cognitive decline; inflammatory intestinal diseases; liver cancer). To this aim, the INSERM team provides us with several data cohorts with a high number of variables and subjects. As in many instances in Biostatistics, one is then faced with a very high dimensional data, from which we hope to extract a reduced number of significant variables allowing to predict the cardiovascular risk accurately. Moreover, these characters should be meaningful to practitioners. The objective for us is thus to design an appropriate variable selection, plus a classification procedure in this demanding context. Let us highlight an original feature of this collaboration: it combines our own data analysis techniques with those developed by the Orpailleur team, based on symbolic tools. We hope that this experience will enrich both points of view and give raise to new methods of data analysis.

4.2. Estimation for complex and biological systems

Our main application for this line of investigation is the photodynamic therapy developed by T. Bastogne. We shall also focus on bacteriophage therapies and subdiffusion within molecules.

(i) Photodynamic therapy. One of the main application we have in mind for our identification problems is to model photodynamic therapy. This promising cancer treatment involves selective uptake and retention of a photosensitive drug in a tumor, followed by irradiation with light at an appropriate wavelength. Photosensitizers are photoactive compounds such as for instance porphyrins and chlorins. The activated photosensitizer is thought to produce singlet oxygen at high doses and thereby to initiate apoptotic and necrotic death of tumor. Due to the lack of response reproducibility, the complexity of interactions between physical, chemical and biological aspects and the high cost of experiments, there is a real demand in good mathematical and physical models which might help to better control and understand PDT responses. We are particularly concerned with modeling the drug uptake into cancer cells, the photoreactions induced by light exposition and tumor growth kinetics.

(ii) Bacteriophage systems. A collaboration between our team, the Mathematics and the Genetics and Microbiology Departments at the *Universitat Autònoma de Barcelona* (UAB) is being set up, focusing on probabilistic aspects of bacteriophage therapies for animal diseases like hemorrhagic septicemia in cattle or atrophic rhinitis in swine. This kind of therapy consists in inoculating a (benign) virus to animals in order to kill the bacteria known to be responsible of the disease. It was in use in the Soviet Union until the 80s, and is now re-emerging, still at an experimental level, due to the progressive slowdown in antibiotic efficiency.

Within this context, our analysis of a noisy predator-prey competition modeling the treatment helps to calibrate and to understand better the behavior of the system in terms of fluctuations around an equilibrium. Note that our preliminary contacts with the Genetics and Microbiology Departments at UAB also open the way to a particle model in order to represent the couple bacteria/virus living on a surface.

CALVI Project-Team

4. Application Domains

4.1. Thermonuclear fusion

Inertial fusion, magnetic fusion, ITER, particle accelerators, laser-matter interaction

Controlled fusion is one of the major prospects for a long term source of energy. Two main research directions are studied: magnetic fusion where the plasma is confined in tokamaks using a large external magnetic field and inertial fusion where the plasma is confined thanks to intense laser or particle beams. The simulation tools we develop can be applied for both approaches.

Controlled fusion is one of the major challenges of the 21st century that can answer the need for a long term source of energy that does not accumulate wastes and is safe. The nuclear fusion reaction is based on the fusion of atoms like Deuterium and Tritium. These can be obtained from the water of the oceans that is widely available and the reaction does not produce long-term radioactive wastes, unlike today's nuclear power plants which are based on nuclear fission.

Two major research approaches are followed towards the objective of fusion based nuclear plants: magnetic fusion and inertial fusion. In order to achieve a sustained fusion reaction, it is necessary to confine sufficiently the plasma for a long enough time. If the confinement density is higher, the confinement time can be shorter but the product needs to be greater than some threshold value.

The idea behind magnetic fusion is to use large toroidal devices called tokamaks in which the plasma can be confined thanks to large applied magnetic field. The international project ITER [1] is based on this idea and aims to build a new tokamak which could demonstrate the feasibility of the concept.

The inertial fusion concept consists in using intense laser beams or particle beams to confine a small target containing the Deuterium and Tritium atoms. The Laser Mégajoule which is being built at CEA in Bordeaux will be used for experiments using this approach.

Nonlinear wave-wave interactions are primary mechanisms by which nonlinear fields evolve in time. Understanding the detailed interactions between nonlinear waves is an area of fundamental physics research in classical field theory, hydrodynamics and statistical physics. A large amplitude coherent wave will tend to couple to the natural modes of the medium it is in and transfer energy to the internal degrees of freedom of that system. This is particularly so in the case of high power lasers which are monochromatic, coherent sources of high intensity radiation. Just as in the other states of matter, a high laser beam in a plasma can give rise to stimulated Raman and Brillouin scattering (respectively SRS and SBS). These are three wave parametric instabilities where two small amplitude daughter waves grow exponentially at the expense of the pump wave, once phase matching conditions between the waves are satisfied and threshold power levels are exceeded. The illumination of the target must be uniform enough to allow symmetric implosion. In addition, parametric instabilities in the underdense coronal plasma must not reflect away or scatter a significant fraction of the incident light (via SRS or SBS), nor should they produce significant levels of hot electrons (via SRS), which can preheat the fuel and make its isentropic compression far less efficient. Understanding how these deleterious parametric processes function, what non uniformities and imperfections can degrade their strength, how they saturate and interdepend, all can benefit the design of new laser and target configuration which would minimize their undesirable features in inertial confinement fusion. Clearly, the physics of parametric instabilities must be well understood in order to rationally avoid their perils in the varied plasma and illumination conditions which will be employed in the National Ignition Facility or LMJ lasers. Despite the thirty-year history of the field, much remains to be investigated.

[1] http://www.iter.org

Our work in modelling and numerical simulation of plasmas and particle beams can be applied to problems like laser-matter interaction, the study of parametric instabilities (Raman, Brillouin), the fast ignitor concept in the laser fusion research as well as for the transport of particle beams in accelerators. Another application is devoted to the development of Vlasov gyrokinetic codes in the framework of the magnetic fusion programme in collaboration with the Department of Research on Controlled Fusion at CEA Cadarache. Finally, we work in collaboration with the American Heavy Ion Fusion Virtual National Laboratory, regrouping teams from laboratories in Berkeley, Livermore and Princeton on the development of simulation tools for the evolution of particle beams in accelerators.

4.2. Nanophysics

Kinetic models like the Vlasov equation can also be applied for the study of large nano-particles as approximate models when ab initio approaches are too costly.

In order to model and interpret experimental results obtained with large nano-particles, ab initio methods cannot be employed as they involve prohibitive computational times. A possible alternative resorts to the use of kinetic methods originally developed both in nuclear and plasma physics, for which the valence electrons are assimilated to an inhomogeneous electron plasma. The LPMIA (Nancy) possesses a long experience on the theoretical and computational methods currently used for the solution of kinetic equation of the Vlasov and Wigner type, particularly in the field of plasma physics.

Using a Vlasov Eulerian code, we have investigated in detail the microscopic electron dynamics in the relevant phase space. Thanks to a numerical scheme recently developed by Filbet et al. [64], the fermionic character of the electron distribution can be preserved at all times. This is a crucial feature that allowed us to obtain numerical results over long times, so that the electron thermalization in confined nano-structures could be studied.

The nano-particle was excited by imparting a small velocity shift to the electron distribution. In the small perturbation regime, we recover the results of linear theory, namely oscillations at the Mie frequency and Landau damping. For larger perturbations nonlinear effects were observed to modify the shape of the electron distribution.

For longer time, electron thermalization is observed: as the oscillations are damped, the center of mass energy is entirely converted into thermal energy (kinetic energy around the Fermi surface). Note that this thermalization process takes place even in the absence of electron-electron collisions, as only the electric mean-field is present.

CAMUS Team

4. Application Domains

4.1. Application Domains

Performance being our main objective, our developments' target applications are characterized by intensive computation phases. Such applications are numerous in the domains of scientific computations, optimization, data mining and multimedia.

Applications involving intensive computations are necessarily high energy consumers. However this consumption can be significantly reduced thanks to optimization and parallelization. Although this issue is not our prior objective, we can expect some positive effects for the following reasons:

- Program parallelization tries to distribute the workload equally among the cores. Thus an equivalent performance, or even a better performance, to a sequential higher frequency execution on one single core, can be obtained.
- Memory and memory accesses are high energy consumers. Lowering the memory consumption, lowering the number of memory accesses and maximizing the number of accesses in the low levels of the memory hierarchy (registers, cache memories) have a positive consequence on execution speed, but also on energy consumption.

CARAMEL Project-Team

4. Application Domains

4.1. Cryptology

The first application domain for our research is cryptology. This includes cryptography (constructive side) and cryptanalysis (breaking systems). For the cryptanalysis part, although it has practical implications, we do not expect any transfer in the classical sense of the term: it is more directed to governmental agencies and the end-users who build their trust, based on the cryptanalysis effort. It is noteworthy that analysis document from governmental agencies (see e.g. [29]) use cryptanalysis results as their key material.

4.1.1. Cryptography

Our cryptographic contributions are related to multiple facets of the large realm of curve-based cryptology. While it is quite clear that enough algorithms exist in order to provide cryptographers with elliptic curves having a suitably hard discrete logarithm (as found in cryptographic standards for instance), one must bear in mind that refinements of the requirements and extensions to curves of higher genus raise several interesting problems. Our work contributes to expanding the cryptographer's capabilities in these areas.

In the context of genus-2 curves, our work aims at two goals. First, improvements on the group law on selected curves yield better speed for the associated cryptosystems. The cryptographic primitives, and then the whole suite of cryptographic protocols built upon such curves would be accelerated. The second goal is the expansion of the set of curves that can be built given a set of desired properties. Using point counting algorithms for arbitrary curves, a curve offering a 128-bit security level, together with nice properties for fast arithmetic, has been computed by CARAMEL [5]. Another natural target for construction of curves for cryptography is also the suitability of curves for pairings. We expect to be able to compute such curves.

Important objects related to the structure of genus 2 curves are the isogenies between their Jacobians. Computing such isogenies is a key point in understanding important underlying objects such as the endomorphism ring, and can be useful in various situations, including for cryptographic or cryptanalytic applications. The team has produced important results in this context [7], [3]

Implementations of curve-based cryptography, both in hardware and software, are a necessary step on the way to assessing cryptographic speed. We plan to provide such implementations. In particular, on the hardware side, one of our goals is the design of a complete cryptographic coprocessor, including all the primitives for curve-based and pairing-based cryptography, providing optimized and configurable efficiency vs area trade-off. Such work has been proposed in [1].

4.1.2. Cryptanalysis

Our research on cryptanalysis is important for the cryptographic industry: by detecting weak instances, and setting new records we contribute to the definition of recommended families of systems together with their key sizes. The user's confidence in a cryptographic primitive is also related to how well the underlying problem is studied by researchers.

In particular, our involvement in computations with "NFS-like" algorithms encompasses of course the task of assessing the computational limits for integer factorization (as was done by the team by factoring RSA-768 [6]) and discrete-logarithm computations (as was done by the team in 2013 for the field $\mathrm{GF}(2^{809})$ [15]). The impact of the former is quite clear as it concerns the RSA algorithm; record-sized computations attract broad interest and determine updates on key-length recommendations. The latter are particularly important for pairing-based cryptography, since, in this context, one naturally encounters discrete-logarithm problems in extension fields of large degree. To this regard the breakthrough provided by the new quasi-polynomial discrete logarithm [22] is of course of utmost importance.

4.2. Computer Algebra Systems

Some of our software libraries are being used by computer algebra systems. Most of those libraries are free software, with a license that allows proprietary systems to link them. This gives us a maximal visibility, with a large number of users.

4.2.1. Magma

Magma is a very large computational algebra package. It provides a mathematically rigorous environment for computing with algebraic, number-theoretic, combinatoric, and geometric objects. It is developed in Sydney, by the team around John Cannon. It is non-commercial (in the sense that its goal is not to make profit), but is not freely distributed and is not open-source.

Several members of the team have visited Sydney — a few years ago — to contribute to the development of Magma, by implementing their algorithms or helping in integrating their software. Our link to Magma exists also via the libraries it uses: it currently links GNU MPFR and GNU MPC for its floating-point calculations, and links GMP-ECM as part of its factorization suite.

4.2.2. Pari-GP

Pari/GP is a computational number theory system that is composed of a C library and an interpreter on top of it. It is developed in Bordeaux, where Karim Belabas from the LFANT project-team is the main maintainer. Its license is GPL. Although we do not directly contribute to this package, we have good contact with the developers.

4.2.3. Sage

Sage is a fairly large scale and open-source computer algebra system written in Python. Sage aggregates a large amount of existing free software, aiming at the goal of selecting the fastest free software package for each given task. The motto of Sage is that instead of "reinventing the wheel" all the time, Sage is "building the car". To date, Sage links GNU MPFR, GMP-ECM, and GNU MPC as standard packages.

4.3. Standardization

4.3.1. Floating-point arithmetic

The IEEE 754 standard for floating-point arithmetic was revised in 2008. The main new features are some new formats for decimal computations, and the recommendation of correctly rounded transcendental functions. The new decimal formats should not have an impact on our work, since we either use integer-only arithmetic, or arbitrary-precision binary floating-point arithmetic through the GNU MPFR library.

A new standard (P1788) is currently under construction for interval arithmetic. We are not officially involved in this standard, but we follow the discussions, to check in particular that the proposed standard will also cover arbitrary precision (interval) arithmetic.

CARTE Project-Team

4. Application Domains

4.1. Computer Virology

4.1.1. The theoretical track.

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

4.1.2. The virus detection track

The crucial question is how to detect viruses or self-replicating malwares. Cohen demonstrated that this question is undecidable. The anti-virus heuristics are based on two methods. The first one consists in searching for virus signatures. A signature is a regular expression, which identifies a family of viruses. There are obvious defects. For example, an unknown virus will not be detected, like ones related to a 0-day exploit. We strongly suggest to have a look at the independent audit [50] in order to understand the limits of this method. The second one consists in analysing the behavior of a program by monitoring it. Following [52], this kind of methods is not yet really implemented. Moreover, the large number of false-positive implies this is barely usable. To end this short survey, intrusion detection encompasses virus detection. However, unlike computer virology, which has a solid scientific foundation as we have seen, the IDS notion of "malwares" with respect to some security policy is not well defined. The interested reader may consult [70].

4.1.3. The virus protection track

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

4.1.4. The experimentation track

This study on computer virology leads us to propose and construct a "high security lab" in which experiments can be done in respect with the French law. This project of "high security lab" in one of the main project of the CPER 2007-2013.

4.2. Computations and Dynamical Systems

4.2.1. Continuous computation theories

Understanding computation theories for continuous systems leads to studying hardness of verification and control of these systems. This has been used to discuss problems in fields as diverse as verification (see e.g. [35]), control theory (see e.g. [43]), neural networks (see e.g. [71]), and so on. We are interested in the formal decidability of properties of dynamical systems, such as reachability [62], the Skolem-Pisot problem [39], the computability of the ω-limit set [61]. Those problems are analogous to verification of safety properties. Contrary to computability theory, complexity theory over continuous spaces is underdeveloped and not well understood. A central issue is the choice of the representation of objects by discrete data and its effects on the induced complexity notions. As for computability, it is well known that a representation is gauged by the topology it induces. However more structure is needed to capture the complexity notions: topologically equivalent representations may induce different classes of polynomial-time computable objects, e.g. Developing a sound complexity theory over continuous structures would enable us to make abstract

computability results more applicable by analysing the corresponding complexity issues. We think that the preliminary step towards such a theory is the development of higher-order complexity, which we are currently carrying out. In contrast with the discrete setting, it is of utmost importance to compare the various models of computation over the reals, as well as their associated complexity theories. In particular, we focus on the General Purpose Analog Computer of Claude Shannon [72], on recursive analysis [77], on the algebraic approach [68] and on computability in a probabilistic context [64]. A crucial point for future investigations is to fill the gap between continuous and discrete computational models. This is one deep motivation of our work on computation theories for continuous systems.

4.2.2. Analysis and verification of adversary systems

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

We are also interested in rewriting techniques, used to describe dynamic systems, in particular in the adversary context. As they were initially developed in the context of automated deduction, the rewriting proof techniques, although now numerous, are not yet adapted to the complex framework of modelization and programming. An important stake in the domain is then to enrich them to provide realistic validation tools, both in providing finer rewriting formalisms and their associated proof techniques, and in developing new validation concepts in the adversary case, i.e. when usual properties of the systems like, for example, termination are not verified. For several years, we have been developing specific procedures for property proofs of rewriting, for the sake of programming, in particular with an inductive technique, already applied with success to termination under strategies [53], [54], [55], to weak termination [56], sufficient completeness [57] and probabilistic termination [59]. The last three results take place in the context of adversary computations, since they allow for proving that even a divergent program, in the sense where it does not terminate, can give the expected results. A common mechanism has been extracted from the above works, providing a generic inductive proof framework for properties of reduction relations, which can be parametrized by the property to be proved [58], [60]. Provided program code can be translated into rule-based specifications, this approach can be applied to correctness proof of software in a larger context. A crucial element of safety and security of software systems is the problem of resources. We are working in the field of Implicit Computational Complexity. Interpretation based methods like Quasi-interpretations (QI) or sup-interpretations, are the approach we have been developing these last years [65], [66], [67]. Implicit complexity is an approach to the analysis of the resources that are used by a program. Its tools come essentially from proof theory. The aim is to compile a program while certifying its complexity.

CASSIS Project-Team

4. Application Domains

4.1. Verification of Security Protocols

Security protocols such as SET, TLS and Kerberos, are designed for establishing the confidence of electronic transactions. They rely on cryptographic primitives, the purpose of which is to ensure integrity of data, authentication or anonymity of participants, confidentiality of transactions, etc.

Experience has shown that the design of those protocols is often erroneous, even when assuming that cryptographic primitives are perfect, i.e., that an encoded message cannot be decrypted without the appropriate key. An intruder can intercept, analyze and modify the exchanged messages with very few computations and therefore, for example, generate important economic damage.

Analyzing cryptographic protocols is complex because the set of configurations to consider is very large, and can even be *infinite*: one has to consider any number of sessions, any size of messages, sessions interleaving, some algebraic properties of encryption or data structures.

Our objective is to automatize as much as possible the analysis of protocols starting from their specification. This consists in designing a tool that is easy to use, enables the specification of a large number of protocols thanks to a standard high-level language, and can either look for flaws in a given protocol or check whether it satisfies a given property. Such a tool is essential for verifying existing protocols, but also for helping in designing new ones. For our tool to be easy to use, it has to provide a graphical interface allowing a user to easily perform push-button verification.

Our tools for verifying security protocols are available as components of the AVISPA platform. As an extension of the AVISPA specification language, we are working on a new environment called *CASRUL* for handling more general protocols like e-business protocols for example.

4.2. Automated Boundary Testing from Formal Specifications

We have introduced a new approach for test generation from set-oriented formal specifications: the BZ-TT method. This method is based on Constraint Logic Programming (CLP) techniques. The goal is to test every operation of the system at every boundary state using all input boundary values of that operation. It has been validated in several industry case studies for smart card OS and application validation (GSM 11-11 standard [69] and Java Card Virtual Machine Transaction mechanism [71]), information system and for embedded software [80].

This test generation method can be summed up as follows: from the formal model, the system computes boundary values to create boundary states; test cases are generated by traversal of the state space with a preamble part (sequences of operations from the initial state to a boundary state), a body part (critical invocations), an identification part (observation and oracle state computation) and a post-amble part (return path to initial or boundary state). Then, an executable test script file is generated using a test pattern and a table of correspondence between abstract operations (from the model) and concrete ones. This approach differs in several main points from previous works (e.g. [76]): first, using boundary goals as test objectives avoids the complete construction of the reachability graph; second, this process is fully automated and the test engineer could just drive it at the boundary value computation level or for the path computation.

The BZ-TT method is fully supported by the BZ-Testing-Tools tool-set. This environment is a set of tools dedicated to animation and test cases generation from B, Z or State-Chart formal specifications. It is based on the CLPS constraint solver, able to simulate the execution of the specification. By execution, we mean that the solver computes a so-called constrained state by applying the pre- and post-condition of operations. A constrained state is a constraint store where state variables and also input and output variables support constraints.

One orientation of the current work is to go beyond the finiteness assumption limitations by using symbolic constraint propagation during the test generation process. Second orientation is to extend the result to object oriented specifications as UML/OCL.Third orientation is to extend the coverage of method for security aspect.

4.3. Program Debugging and Verification

Catching bugs in programs is difficult and time-consuming. The effort of debugging and proving correct even small units of code can surpass the effort of programming. Bugs inserted while "programming in the small" can have dramatic consequences for the consistency of a whole software system as shown, e.g., by viruses which can spread by exploiting buffer overflows, a bug which typically arises while coding a small portion of code. To detect this kind of errors, many verification techniques have been put forward such as static analysis and software model checking.

Recently, in the program verification community, there seems to be a growing demand for more declarative approaches in order to make the results of the analysis readily available to the end user. To meet this requirement, a growing number of program verification tools integrate some form of theorem proving.

The goals of our research are twofold. First, we perform theoretical investigations of various combinations of propositional and first-order satisfiability checking in order to automate the theorem proving activity required to solve a large class of program analysis problems which can be encoded as first-order formulae. Second, we experimentally investigate how our techniques behave on real problems in order to make program analysis more precise and scalable. Building tools capable of providing a good balance between precision and scalability is one of the crucial challenges to transfer theorem proving technology to the industrial domains.

4.4. Verification of Web Services

Driven by rapidly changing requirements and business needs, IT systems and applications are undergoing a paradigm shift: components are replaced by services, distributed over the network, and composed and reconfigured dynamically in a demand-driven way into service-oriented architectures.Exposing services in future network infrastructures means a wide range of trust and security issues need to be adressed. Solving them is extremely hard since making the service components trustworthy is not sufficient: composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality. Thus, one needs validation of both the service components and their composition into secure service architectures. In this context, there is an obvious need of applying formal methods. Our project aims at applying our proof and constraint solving techniques to reason on web services. More precisely, we focus on the composition problem in the presence of security policies.

4.5. Model-Checking of Collaborative Systems

Collaborative systems consitute a class of distributed systems where real human interactions are predominant. In these systems, users at geographically distributed sites interact by simultaneously manipulating shared objects like, text documents, XML trees, filesystems, etc. To improve data availablity, the shared objects are replicated so that the users update their local replicas and exchange their updates between them. One of the main challenges here is how to ensure the data consistency when the updates are executed in arbitrary orders at different replicas. Operational Transformation (OT) is an optimistic technique which has been proposed to overcome the consistency problem. This technique consists of an application-dependent protocol to enforce the out-of-order execution of updates even though these updates do not naturally commute. The data consistency relies crucially on the correctness of OT protocols whose proof is extremely hard. Indeed, possibly infinitely many cases should be tested. Our research work aims at applying symbolic model-checking techniques to automatically verify OT protocols. Most importantly, we are interested in finding under which conditions the model-checking problem can be reduced to a finite-state model.

CORIDA Project-Team (section vide)

CORTEX Team

4. Application Domains

4.1. Overview

Our application domain is twofold:

We design embedded systems such as in-silico implementations of bio-inspired processes, focusing on spatial and distributed computing.

We develop embodied systems such as robotic implementation of sensori-motor loops, the bio-inspiration yielding such interesting properties as adaptivity and robustness.

MADYNES Project-Team

4. Application Domains

4.1. Mobile, ad-hoc and constrained networks

The results coming out from MADYNES can be applied to any dynamic infrastructure that contributes to the delivery of value added services. While this is a potentially huge application domain, we focus on the following environments at the network level:

1. multicast services,
2. ad-hoc networks,
3. mobile devices and IPv6 networks,
4. voice over IP infrastructure.

All these selected application areas exhibit different dynamicity features. In the context of multicast services, we focus on distribution, monitoring and accounting of key distribution protocols. On *ad-hoc* and dynamic networks we are investigating the provisioning, monitoring, configuration and performance management issues.

Concerning mobile devices, we are interested in their configuration, provisioning and monitoring. IPv6 work goes on in Information Models and on self-configuration of the agents.

4.2. Dynamic services infrastructures

At the service level, dynamics is also increasing very fast. We apply the results of our work on autonomous management on infrastructures which support dynamic composition and for which self-instrumentation and management automation is required.

The target service environments are:

- sensor networks,
- peer-to-peer infrastructures,
- information centric networks,
- ambiant environments.

MAGRIT Project-Team

4. Application Domains

4.1. Augmented Reality

We have a significant experience in the AR field especially through the European project ARIS (2001–2004) which aimed at developing effective and realistic AR systems for e-commerce and especially for interior design. Beyond this restrictive application field, this project allowed us to develop nearly real time camera tracking methods for multi-planar environments. Since then, we have amplified our research on multi-planar environments in order to obtain effective and robust AR systems in such environments. We currently investigate both automatic and interactive techniques for scene reconstruction/structure from motion methods in order to be able to consider large and unknown environments. For some time, we are investigating AR for deformable objects in the context of medical applications.

4.2. Medical Imaging

For 15 years, we have been working in close collaboration with University Hospital of Nancy and GE Healthcare in interventional neuroradiology. Our common aim is to develop a multimodality framework to help therapeutic decisions and interventional gestures. In particular, we aim at developing methods and tools allowing the physicians to take advantage of the various existing imaging modalities on the brain in their clinical practice: 2D subtracted angiography (2DSA), 3D rotational angiography (3DRA), fluoroscopy, MRI,.... Recent works concern the use of AR tools for neuronavigation and laparoscopy as well as the development of simulation tools of the interventional act for training or planning. Some of these projects are developed in collaboration with the EPI Shacra.

MAIA Project-Team

4. Application Domains

4.1. Decision Making

Our group is involved in several applications of its more fundamental work on autonomous decision making and complex systems. Applications addressed include:

- Robotics, where the decision maker or agent is supported by a physical entity moving in the real world;
- Medicine or Personally Assisted Living, where the agent can be an analytic device recommending tests and/or treatments, or able to gather different sources of information (sensors for example) in order to help a final user, detecting for example anormal situation needing the rescue of a person (fall detection of elderly people, risk of hospitalization of a person suffering from chronic disease;
- Active Sensing, where decisions have to be taken in order to gather information on a system. This can be applied to many fields, like for example monitoring the integrity of airplanes wings or the behavior of people in public areas.

4.2. Ambient intelligence

As the Nancy – Grand Est Research Center scientific strategy pushes the development of plateforms on Robotics and Smart Living Apartments, some members of the team have recentered their research toward “ambient intelligence and AI” . This choice is backed up by the Inria Large-scale initiative project termed PAL (Personal assistant Living) in which we are strongly involved. The regional council of Lorraine also supports this new research line through the CPER, (project "situated computing" or "INFOSITU" infositu.loria.fr) whose coordinator is a member of MAIA Team. Within this new domain of research in MAIA, we explore how intelligent decentralized complex systems can help designing intelligent environments dedicated to elderly people with loss of autonomy. This domain of research is currently very active, taking up a societal challenge that developed countries have to address.

MASAIE Project-Team

4. Application Domains

4.1. Metapopulation models

Heterogeneity plays an important role in many infectious disease processes. For instance, spatial heterogeneity is a strong determinant of host-parasite relationships. In modeling spatial or geographic effects on the spread of a disease, a distinction is usually made between diffusion and dispersal models. In diffusion models, spread is to immediately adjacent zones, hence the phenomenon of traveling waves can appear. These models traditionally use partial differential equations. However, there are some important situations that cannot be modeled by PDE. This is the case when the space considered is discrete. For example, when we have to consider sparsely populated regions, the human population is located in patches. The organization of human-hosts into well-defined social units such as families, villages or cities, are good examples of patches. Another example arises in the study of the human African Trypanosomiasis. The vector is the tse-tse fly, and it is known that flies take fewer blood meals in villages than in coffee plantations where the villagers work during the day. For such situations where human or vectors can travel a long distance in a short period of time, dispersal models are more appropriate. These models consider migration of individuals between patches. The infection does not take place during the migration process. The situation is that of a directed graph, where the vertices represent the patches and the arcs represent the links between patches. Recently, there has been increased interest in these deterministic metapopulation disease models. We have generalized to n patches the Ross-Macdonald model which describes the dynamics of malaria. We incorporate in our model the fact that some patches can be vector free. We assume that the hosts can migrate between patches, but not the vectors. The susceptible and infectious individuals have the same dispersal rate. We compute the basic reproduction ratio $\mathcal{R}_0$. We prove that if $\mathcal{R}_0 \leq 1$, then the disease-free equilibrium is globally asymptotically stable. When $\mathcal{R}_0 > 1$, we prove that there exists a unique endemic equilibrium, which is globally asymptotically stable on the biological domain minus the disease-free equilibrium.

MASAIE is developing, in the framework of the CAPES-COFECUB project (see international program), a metapopulation model for dengue. This model is for the state of Rio and is using the data of foundation FIOCRUZ.

4.2. Intra-host models for malaria: analysis and estimation problems

We give a brief review of the biological features of malaria. Malaria in a human begins with an inoculum of *Plasmodium* parasites (sporozoites) from a female *Anopheles* mosquito. The sporozoites enter the liver within minutes. After a period of asexual reproduction in the liver, the parasites (merozoites) are released in the bloodstream where the asexual erythrocyte cycle begins. The merozoites enter red blood cells (RBC), grow and reproduce over a period of approximately 48 hours after which the erythrocyte ruptures releasing daughter parasites that quickly invade a fresh erythrocyte to renew the cycle. This blood cycle can be repeated many times, in the course of which some of the merozoites instead develop in the sexual form of the parasites : gametocytes. Gametocytes are benign for the host and are waiting for the mosquitoes. An important characteristic of *Plasmodium falciparum*, the most virulent malaria parasite, is sequestration. At the half-way point of parasite development, the infected erythrocyte leaves the circulating peripheral blood and binds to the endothelium in the microvasculature of various organs where the cycle is completed. A measurement of *Plasmodium falciparum* parasitaemia taken from a blood smear therefore samples young parasites only. Physician treating malaria use the number of parasites in peripheral blood smears as a measure of infection, this does not give the total parasite burden of the patient. Moreover antimalarial drugs are known to act preferentially on different stages of parasite development. Our work consists in developing tools for estimating the sequestered parasites and hence the total parasite burden of the patient.

NEUROSYS Team

4. Application Domains

4.1. General anaesthesia

During general anaesthesia, the EEG on the scalp changes characteristically: increasing the anaesthetic drug concentration the amplitudes of fast EEG-oscillations in the α-band ($\sim 8-12$Hz) in frontal electrodes decrease and the amplitudes of slow oscillations in the $\delta-$band ($2-8$Hz) increase. This characteristic change in the power is the basis of today's EEG-monitors that assist the anaesthesist in the control of the anaesthesia depths of patients during surgery. However, the conventional monitors detect a large variability between the patients and are not able to detect the real depth of anaesthesia. Moreover, a certain number of patients re-gain consciousness during surgery (about $1-2$ out of 1000) and suffer from diverse after-effects, such as nausea or long-lasting cognitive impairments (from days to weeks). Since surgery under general anaesthesia is part of a hospital's everyday practice, a large number of patients suffer from these events everyday. One reason for the occurrence of these disadvantageous effects in hospital practice is the dramatic lack of understanding on what is going on in the brain during general anaesthesia leading to sometimes poorly controllable situations of patients. Consequently, to improve the situation of patients and to develop improved anaesthetic procedures or drugs, it is necessary to perform research in order to learn more about the neural processes in the brain.
The EEG originates from coherent neural activity of populations in the cortex. Hence to understand better the characteristic power changes in EEG during anaesthesia, it is necessary to study neural population dynamics subject to the concentration of anaesthetic drugs and their action on receptors on the single neuron level. We develop computational models which are constrained by the signal features extracted from experimental EEG and behavior. This methodology will reveal new knowledge on the neural origin of behavioral features, such as the loss of consciousness or the un-controlled gain of consciousness during surgery.

4.2. Motor behavior

An improved understanding of the link between single neuron activity and neural population data allows to understand the planning and action of motor behavior. To this end we extract signal features in experimental neural population data obtained in the motor cortex in animals. Synchronously theoretical population models based on single neuron activity aim to understand the typical decoding of motor action by neural populations. Experimental single neuron data assists this model approach.
In addition, we employ and integrate numerically a neural population model whose activity features are compared to the signal features observed in experiments. In addition, we link the signal features to experimental behavioral data.

ORPAILLEUR Project-Team

4. Application Domains

4.1. Life Sciences

Participants: Yasmine Assess, Emmanuel Bresso, Adrien Coulet, Marie-Dominique Devignes, Elias Egho, Anisah Ghoorah, Nicolas Jay, Bernard Maigret, Amedeo Napoli, Nicolas Pépin-Hermann, Gabin Personeni, David Ritchie, Mohsen Sayed, Malika Smaïl-Tabbone, Yannick Toussaint.

Keywords: knowledge discovery in life sciences, bioinformatics, biology, chemistry, genomics

One major application domain which is currently investigated by the Orpailleur team is related to life sciences, with particular emphasis on biology, medicine, and chemistry. The understanding of biological systems provides complex problems for computer scientists, and, when they exist, solutions bring new research ideas for biologists and for computer scientists as well. Accordingly, the Orpailleur team includes biologists, chemists, and a physician, making Orpailleur a very original EPI at Inria.

Knowledge discovery is gaining more and more interest and importance in life sciences for mining either homogeneous databases such as protein sequences and structures, or heterogeneous databases for discovering interactions between genes and environment, or between genetic and phenotypic data, especially for public health and pharmacogenomics domains. The latter case appears to be one main challenge in knowledge discovery in biology and involves knowledge discovery from complex data depending on domain knowledge. The interactions between researchers in biology and researchers in computer science improve not only knowledge about systems in biology, chemistry, and medicine, but knowledge about computer science as well.

4.2. Knowledge Management in Medicine

Participants: Nicolas Jay, Jean Lieber, Thomas Meilender, Amedeo Napoli.

Keywords: knowledge representation, description logics, classification-based reasoning, case-based reasoning, formal concept analysis, semantic web

The Kasimir research project holds on decision support and knowledge management for the treatment of cancer [103]. This is a multidisciplinary research project in which participate researchers in computer science (Orpailleur), experts in oncology ("Institut de Cancérologie de Lorraine Alexis Vautrin" in Vandœuvre-lès-Nancy), Oncolor (a healthcare network in Lorraine involved in oncology), and A2Zi (a company working in Web technologies and involved in several projects in the medical informatics domain, http://www.a2zi.fr/). For a given cancer localization, a treatment is based on a protocol similar to a medical guideline, and is built according to evidence-based medicine principles. For most of the cases (about 70%), a straightforward application of the protocol is sufficient and provides a solution, i.e. a treatment, that can be directly reused. A case out of the 30% remaining cases is "out of the protocol", meaning that either the protocol does not provide a treatment for this case, or the proposed solution raises difficulties, e.g. contraindication, treatment impossibility, etc. For a case "out of the protocol", oncologists try to *adapt* the protocol. Actually, considering the complex case of breast cancer, oncologists discuss such a case during the so-called "breast cancer therapeutic decision meetings", including experts of all specialties in breast oncology, e.g. chemotherapy, radiotherapy, and surgery.

The semantic Web technologies are used and adapted in the Kasimir project since several years [12]. A semantic wiki allowing the management of decision protocols was deployed as an operational system (http://www.oncologik.fr). More precisely, the migration from the static HTML site of Oncolor to a semantic wiki (with limited editing rights and unlimited reading rights) was performed. As a consequence, the editorial chain of the published protocols is more collaborative. A decision tree editor was developed and integrated into this semantic wiki with an export facility to formalized protocols in OWL DL.

4.3. Cooking

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

Keywords: cooking, knowledge representation, knowledge discovery, case-based reasoning, semantic wiki

The origin of the Taaable project is the Computer Cooking Contest (CCC). A contestant to CCC is a system that answers queries about recipes, using a recipe base; if no recipe exactly matches the query, then the system adapts another recipe. Taaable is a case-based reasoning system based on various technologies from semantic web, knowledge discovery, knowledge representation and reasoning. From a research viewpoint the system enables to test scientific results and to study the complementarity of various research trends in an application domain which is simple to understand and which raises complex issues at the same time. Taaable has been at the origin of the ANR CONTINT project Kolflow, whose application domain is WikiTaaable, the semantic wiki of Taaable.

4.4. Agronomy

Participants: Sébastien Da Silva, Florence Le Ber [contact person], Jean-François Mari.

Keywords: simulation, Markov model, Formal Concept Analysis, graph

Sébastien da Silva is working for his PhD thesis in the framework of an Inria-INRA collaboration, which takes place in the INRA research network PAYOTE about landscape modeling. The thesis, supervised both by Claire Lavigne (DR in ecology, INRA Avignon) and Florence Le Ber, is concerned with the characterization and the simulation of hedgerows structures in agricultural landscapes, based on Hilbert-Peano curves and Markov models.

An on-going research work about the representation of peasant knowledge is involved within a collaboration with IRD in Madagascar. Sketches drawn by peasants were transformed into graphs and compared thanks to Formal Concept Analysis [32].

PAREO Project-Team

4. Application Domains

4.1. Application Domains

Beside the theoretical transfer that can be performed via the cooperations or the scientific publications, an important part of the research done in the *Pareo* group team is published within software. *Tom* is our flagship implementation. It is available via the Inria Gforge (http://gforge.inria.fr) and is one of the most visited and downloaded projects. The integration of high-level constructs in a widely used programming language such as Java may have an impact in the following areas:

- Teaching: when (for good or bad reasons) functional programming is not taught nor used, *Tom* is an interesting alternative to exemplify the notions of abstract data type and pattern-matching in a Java object oriented course.
- Software quality: it is now well established that functional languages such as Caml are very successful to produce high-assurance software as well as tools used for software certification. In the same vein, *Tom* is very well suited to develop, in Java, tools such as provers, model checkers, or static analyzers.
- Symbolic transformation: the use of formal anchors makes possible the transformation of low-level data structures such as C structures or arrays, using a high-level formalism, namely pattern matching, including associative matching. *Tom* is therefore a natural choice each time a symbolic transformation has to be implemented in C or Java for instance. *Tom* has been successfully used to implement the Rodin simplifier, for the B formal method.
- Prototyping: by providing abstract data types, private types, pattern matching, rules and strategies, *Tom* allows the development of quite complex prototypes in a short time. When using Java as the host-language, the full runtime library can be used. Combined with the constructs provided by *Tom*, such as strategies, this procures a tremendous advantage.

One of the most successful transfer is certainly the use of *Tom* made by Business Objects/SAP. Indeed, after benchmarking several other rule based languages, they decided to choose *Tom* to implement a part of their software. *Tom* is used in Paris, Toulouse and Vancouver. The standard representation provided by *Tom* is used as an exchange format by the teams of these sites.

PAROLE Project-Team

4. Application Domains

4.1. Application Domains

Our research is applied in a variety of fields from ASR to paramedical domains. Speech analysis methods will contribute to the development of new technologies for language learning (for hearing-impaired persons and for the teaching of foreign languages) as well as for hearing aids. In the past, we developed a set of teaching tools based on speech analysis and recognition algorithms of the group (cf. the ISAEUS [88] project of the EU that ended in 2000). We are continuing this effort towards the diffusion of a course on Internet.

Speech is likely to play an increasing role in man-machine communication. Actually, speech is a natural mean of communication, particularly for non-specialist persons. In a multimodal environment, the association of speech and designation gestures on touch screens can, for instance, simplify the interpretation of spatial reference expressions. Besides, the use of speech is mandatory in many situations where a keyboard is not available: mobile and on-board applications (for instance in the framework of the HIWIRE European project for the use of speech recognition in a cockpit plane), interactive vocal servers, telephone and domestic applications, etc. Most of these applications will necessitate to integrate the type of speech understanding process that our group is presently studying. Furthermore, speech to speech translation concerns all multilingual applications (vocal services, audio indexing of international documents). The automatic indexing of audio and video documents is a very active field that will have an increasing importance in our group in the forthcoming years, with applications such as economic intelligence, keyword spotting and automatic categorization of mails.

SCORE Team (section vide)

SÉMAGRAMME Project-Team

4. Application Domains

4.1. Introduction

Our applicative domains concern natural language processing applications that rely on a deep semantic analysis. For instance, one may cite the following ones:

- textual entailment and inference,
- dialogue systems,
- semantic-oriented query systems,
- content analysis of unstructured documents,
- text transformation and automatic summarization,
- (semi) automatic knowledge acquisition.

However, if the need for semantics seems to be ubiquitous, there is a challenge in finding applications for which a deep semantic analysis results in a real improvement over non semantic-based techniques.

4.2. Text Transformation

Text transformation is an application domain featuring two important sub-fields of computational linguistics:

- parsing, from surface form to abstract representation,
- generation, from abstract representation to surface form.

Text simplification or automatic summarization belong to that domain.

We aim at using the framework of Abstract Categorial Grammars we develop to this end. It is indeed a *reversible* framework that allows both parsing and generation. Its underlying mathematical structure of λ-calculus makes it fit with our type-theoretic approach to discourse dynamics modeling. The ANR project POLYMNIE(see section 7.2.1.1) is especially dedicated to this aim.

SHACRA Project-Team

4. Application Domains

4.1. Medical Simulation

Some of the scientific challenges described previously can be seen in a general context (such as solving constraints between different types of objects, parallel computing for interactive simulations, etc.) but often it is necessary to define a clinical context for the problem. This is required in particular for defining the appropriate assumptions in various stages of the biophysical modeling. It is also necessary to validate the results. This clinical context is a combination of two elements: the procedure we attempt to simulate and the objective of the simulation: training, planning or per-operative guidance. Several simulators applications are being developped in the team for instance Interventional Cerebro- and Cardio- vascular Radiology, Minimally-invasive ear surgery, Deep-Brain Stimulation planning...

It is important also to note that developing these applications raises many challenges and as such this step should be seen as an integral part of our research. It is also through the development of these applications that we can communicate with physicians, and validate our results. SOFA will be used as a backbone for the integration of our research into clinical applications.

4.2. Robotics

Contrary to rigid robots, the number of degrees of freedom (dof) of soft robots is infinite. On the one hand, a great advantage is to multiply the actuators and actuating shapes in the structure to expand the size of the workspace. In the other hand, these actuators are coupled together by the deformation of the robot which makes the control very tricky. Moreover, if colliding their direct environment, the robots may deform and also deform the environment, which complicates even more the control.

This project would build on our recent results, that use a real-time implementation of the finite element method to compute adequately the control of the structure. The present results allow to compute, in real-time, an inverse model of the robot (i.e. provide the displacements of the actuator that creates a desired motion of the end effector of the robot) for a few number of actuators and with simple interactions with its environment. However, the design of the robots, as well as the type of actuator used are far from optimal. The goal of this work is to improve the control methods especially when the robot is in interaction with its environment (by investigating feedback control strategies and by increasing the number of actuators that can be piloted) and to investigate new applications of these devices in medicine (especially for surgical robotics but not only...) and HCI (game, entertainment, art...).

TOSCA Project-Team

4. Application Domains

4.1. Application Domains

TOSCA is interested in developing stochastic models and probabilistic numerical methods. Our present motivations come from Finance, Neuroscience and Biology, Fluid Mechanics and Meteorology, Chemical Kinetics, Diffusions in random media, Transverse problems, Software and Numerical experiments.

Finance For a long time now TOSCA has collaborated with researchers and practitioners in various financial institutions and insurance companies. We are particularly interested in calibration problems, risk analysis (especially model risk analysis), optimal portfolio management, Monte Carlo methods for option pricing and risk analysis, asset and liabilities management. We also work on the partial differential equations related to financial issues, for example the stochastic control Hamilton–Jacobi–Bellman equations. We study existence, uniqueness, qualitative properties and appropriate deterministic or probabilistic numerical methods. At the moment we pay special attention to the financial consequences induced by modelling errors and calibration errors on hedging strategies and portfolio management strategies.

Neuroscience and Biology The interest of TOSCA in biology is developing in three main directions: neuroscience, molecular dynamics and population dynamics. In neuroscience, stochastic methods are developed to analyze stochastic resonance effects, to solve inverse problems and to investigate mean-field/McKean-Vlasov equations. For example, we are studying probabilistic interpretations and Monte Carlo methods for divergence form second-order differential operators with discontinuous coefficients, motivated by the 3D MEG inverse problem. Our research in molecular dynamics focuses on the development of Monte Carlo methods for the Poisson-Boltzmann equation which also involves a divergence form operator, and of original algorithms to construct improved simulation techniques for protein folding or interaction. Finally, our interest in population dynamics comes from ecology, evolution and genetics. For example, we are studying the emergence of diversity through the phenomenon of evolutionary branching in adaptive dynamics. Some collaborations in biostatistics on cancer problems are also being initiated.

Fluid Mechanics and Meteorology In Fluid Mechanics we develop probabilistic methods to solve vanishing viscosity problems and to study the behavior of complex flows at the boundary, and their interaction with the boundary. We elaborate and analyze stochastic particle algorithms. Our studies concern the convergence analysis of these methods on theoretical test cases and the design of original schemes for applicative cases. A first example concerns the micro-macro model of polymeric fluids (the FENE model). A second example concerns stochastic Lagrangian modelling of turbulent flows. We are particularly motivated by the meteorological downscaling, and by the computation of characteristic properties of the local wind activity in areas where windmills are built. Our goal is to estimate local potential resources which are subject to meteorological variability (randomness) by developing a stochastic downscaling methodology, that is able to refine wind prevision at large scale, and to compute management strategies of wind resources.

Chemical Kinetics The TOSCA team is studying coagulation and fragmentation models, that have numerous areas of applications (polymerization, aerosols, cement industry, copper industry, population dynamics...). Our current motivation comes from the industrial copper crushers in Chile. We aim to model and calibrate the process of fragmentation of brass particles of copper in industrial crushers, in order to improve their efficiency at a low cost.

Diffusions in random media A *random medium* is a material with a lot of heterogeneity which can be described only statistically. Typical examples are fissured porous media within rocks of different types, turbulent fluids or unknown or deficient materials in which polymers evolve or waves

propagate. For the last few years, the TOSCA team has been collaborating with the Geophysics community on problems related to underground diffusions, especially those which concern waste transport or oil extraction. We are extending our previous results on the simulation of diffusion processes generated by divergence form operators with discontinuous coefficients. Such an operator appears for example in the Darcy law for the behavior of a fluid in a porous media. We are also developing another class of Monte Carlo methods to simulate diffusion phenomena in discontinuous media.

Transverse problems Several of the topics of interest of TOSCA do not only concern a single area of application. This is the case in particular for long time simulation methds of nonlinear McKean-Vlasov PDEs, the problem of simulation of multivalued models, variance reduction techniques or stochastic partial differential equations. For example, multivalued processes have applications in random mechanics or neuroscience, and variance reduction techniques have applications in any situation where Monte Carlo methods are applicable.

Software, numerical experiments TOSCA is interested in designing algorithms of resolution of specific equations in accordance with the needs of practitioners. We benefit from our strong experience of the programming of probabilistic algorithms of various architectures including intensive computation architectures. In particular, our activity will concern the development of grid computing techniques to solve large dimensional problems in Finance. We are also interested in intensively comparing various Monte Carlo methods for PDEs and in the development of open source libraries for our numerical methods in Fluid Mechanics, MEG or Chemical Kinetics.

TRIO Team

4. Application Domains

4.1. TRIO application domains

Three main application domains can be underlined.

- In-vehicle embedded systems. The work developed in TRIO is oriented towards transportation systems (cars, airplanes, trains etc.). They mainly cover two points. The first one is the specification of what must be modeled in such a system and how to reach a good accuracy of a model. The second point concerns the verification of dependability properties and temporal properties required by these applications.
- Compilation, memory management and low-power issues for real time embedded systems. It becomes mandatory to design embedded systems that respect performances and reliability constraints while minimizing the energy consumption. Hence, TRIO is involved, on the one hand, in the definition of ad-hoc memory management at compilation time and on the other hand, in joint study of memory management strategies and tasks scheduling for real time critical systems.
- Code analyses and software visualization for embedded systems. Despite important advances, it is still impossible to develop and optimize automatically all the programs with all their variety, especially when deployment constraints are considered. Software design and implementation thus remain highly ad-hoc, poorly automated activities, with a human being in the loop. TRIO is thus involved in the design of better tools for software engineering focusing on helping the human developer understand and develop the system, thanks to powerful automated program analyses and advanced visualizations techniques.

VEGAS Project-Team

3. Application Domains

3.1. Computer graphics

We are interested in the application of our work to virtual prototyping, which refers to the many steps required for the creation of a realistic virtual representation from a CAD/CAM model.

When designing an automobile, detailed physical mockups of the interior are built to study the design and evaluate human factors and ergonomic issues. These hand-made prototypes are costly, time consuming, and difficult to modify. To shorten the design cycle and improve interactivity and reliability, realistic rendering and immersive virtual reality provide an effective alternative. A virtual prototype can replace a physical mockup for the analysis of such design aspects as visibility of instruments and mirrors, reachability and accessibility, and aesthetics and appeal.

Virtual prototyping encompasses most of our work on effective geometric computing. In particular, our work on 3D visibility should have fruitful applications in this domain. As already explained, meshing objects of the scene along the main discontinuities of the visibility function can have a dramatic impact on the realism of the simulations.

3.2. Solid modeling

Solid modeling, i.e., the computer representation and manipulation of 3D shapes, has historically developed somewhat in parallel to computational geometry. Both communities are concerned with geometric algorithms and deal with many of the same issues. But while the computational geometry community has been mathematically inclined and essentially concerned with linear objects, solid modeling has traditionally had closer ties to industry and has been more concerned with curved surfaces.

Clearly, there is considerable potential for interaction between the two fields. Standing somewhere in the middle, our project has a lot to offer. Among the geometric questions related to solid modeling that are of interest to us, let us mention: the description of geometric shapes, the representation of solids, the conversion between different representations, data structures for graphical rendering of models and robustness of geometric computations.

3.3. Fast prototyping

We work in collaboration with CIRTES on rapid prototyping. CIRTES, a company based in Saint-Dié-des-Vosges, has designed a technique called Stratoconception® where a prototype of a 3D computer model is constructed by first decomposing the model into layers and then manufacturing separately each layer, typically out of wood of standard thickness (e.g. 1 cm), with a three-axis CNC (Computer Numerical Controls) milling machine. The layers are then assembled together to form the object. The Stratoconception® technique is cheap and allows fast prototyping of large models.

When the model is complex, for example an art sculpture, some parts of the models may be inaccessible to the milling machine. These inaccessible regions are sanded out by hand in a post-processing phase. This phase is very consuming in time and resources. We work on minimizing the amount of work to be done in this last phase by improving the algorithmic techniques for decomposing the model into layers, that is, finding a direction of slicing and a position of the first layer.

VERIDIS Project-Team

4. Application Domains

4.1. Application Domains

Our work focuses on the formal modeling and verification of distributed algorithms and protocols. These are or will be found at all levels of computing infrastructure, from many-core processors and systems-on-chip to wide-area networks. We are particularly interested in novel paradigms, for example ad-hoc networks that underly mobile and low-power computing or overlay networks and peer-to-peer networking that provide services for telecommunication or cloud computing services. Distributed protocols underly computing infrastructure that must be highly available and mostly invisible to the end user, therefore correctness is important. One should note that standard problems of distributed computing such as consensus, group membership or leader election have to be reformulated for the dynamic context of these modern systems. We are not ourselves experts in the design of distributed algorithms, but work together with domain experts on the modeling and verification of these protocols. These cooperations help us focus on concrete algorithms and ensure that our work is relevant to the distributed algorithm community.

Formal verification techniques that we study can contribute to certify the correctness of systems. In particular, they help assert under which assumptions an algorithm or system functions as required. For example, the highest levels of the Common Criteria for Information Technology Security Evaluation require code analysis, based on mathematically precise foundations. While initially the requirements of certified development have mostly been restricted to safety-critical systems, they are becoming more and more common due to the cost associated with malfunctioning system components and software. For example, we are working on modeling and verifying medical devices that require closed-loop models of both the system and its environment.