Activity Report 2018

Section Software

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

6. New Software and Platforms

6.1. APOLLO

Automatic speculative POLyhedral Loop Optimizer

KEYWORD: Automatic parallelization

FUNCTIONAL DESCRIPTION: APOLLO is dedicated to automatic, dynamic and speculative parallelization of loop nests that cannot be handled efficiently at compile-time. It is composed of a static part consisting of specific passes in the LLVM compiler suite, plus a modified Clang frontend, and a dynamic part consisting of a runtime system. It can apply on-the-fly any kind of polyhedral transformations, including tiling, and can handle nonlinear loops, as while-loops referencing memory through pointers and indirections.

- Participants: Aravind Sukumaran-Rajam, Juan Manuel Martinez Caamaño, Manuel Selva and Philippe Clauss
- Contact: Philippe Clauss
- URL: http://apollo.gforge.inria.fr

6.2. Clan

A Polyhedral Representation Extraction Tool for C-Based High Level Languages

KEYWORD: Polyhedral compilation

FUNCTIONAL DESCRIPTION: Clan is a free software and library which translates some particular parts of high level programs written in C, C++ or Java into a polyhedral representation called OpenScop. This representation may be manipulated by other tools to, e.g., achieve complex analyses or program restructurations (for optimization, parallelization or any other kind of manipulation). It has been created to avoid tedious and error-prone input file writing for polyhedral tools (such as CLooG, LeTSeE, Candl etc.). Using Clan, the user has to deal with source codes based on C grammar only (as C, C++ or Java). Clan is notably the frontend of the two major high-level compilers Pluto and PoCC.

- Participants: Cédric Bastoul and Imèn Fassi
- Contact: Cédric Bastoul
- URL: http://icps.u-strasbg.fr/people/bastoul/public_html/development/clan/

6.3. Clay

Chunky Loop Alteration wizardrY

FUNCTIONAL DESCRIPTION: Clay is a free software and library devoted to semi-automatic optimization using the polyhedral model. It can input a high-level program or its polyhedral representation and transform it according to a transformation script. Classic loop transformations primitives are provided. Clay is able to check for the legality of the complete sequence of transformation and to suggest corrections to the user if the original semantics is not preserved.

- Participant: Cédric Bastoul
- Contact: Cédric Bastoul
- URL: http://icps.u-strasbg.fr/people/bastoul/public_html/development/clay/

6.4. CLooG

Code Generator in the Polyhedral Model

FUNCTIONAL DESCRIPTION: CLooG is a free software and library to generate code (or an abstract syntax tree of a code) for scanning Z-polyhedra. That is, it finds a code (e.g. in C, FORTRAN...) that reaches each integral point of one or more parameterized polyhedra. CLooG has been originally written to solve the code generation problem for optimizing compilers based on the polyhedral model. Nevertheless it is used now in various area e.g. to build control automata for high-level synthesis or to find the best polynomial approximation of a function. CLooG may help in any situation where scanning polyhedra matters. While the user has full control on generated code quality, CLooG is designed to avoid control overhead and to produce a very effective code. CLooG is widely used (including by GCC and LLVM compilers), disseminated (it is installed by default by the main Linux distributions) and considered as the state of the art in polyhedral code generation.

RELEASE FUNCTIONAL DESCRIPTION: It mostly solves building and offers a better OpenScop support.

- Participant: Cédric Bastoul
- Contact: Cédric Bastoul
- URL: http://www.cloog.org

6.5. OpenScop

A Specification and a Library for Data Exchange in Polyhedral Compilation Tools
FUNCTIONAL DESCRIPTION: OpenScop is an open specification that defines a file format and a set of data structures to represent a static control part (SCoP for short), i.e., a program part that can be represented in the polyhedral model. The goal of OpenScop is to provide a common interface to the different polyhedral compilation tools in order to simplify their interaction. To help the tool developers to adopt this specification, OpenScop comes with an example library (under 3-clause BSD license) that provides an implementation of the most important functionalities necessary to work with OpenScop.

- Participant: Cédric Bastoul
- Contact: Cédric Bastoul
- URL: http://icps.u-strasbg.fr/people/bastoul/public_html/development/openscop/

6.6. ORWL

Ordered Read-Write Lock
KEYWORDS: Task scheduling - Deadlock detection
FUNCTIONAL DESCRIPTION: ORWL is a reference implementation of the Ordered Read-Write Lock tools. The macro definitions and tools for programming in C99 that have been implemented for ORWL have been separated out into a toolbox called P99.

- Participants: Jens Gustedt, Mariem Saied and Stéphane Vialle
- Contact: Jens Gustedt
- Publications: Iterative Computations with Ordered Read-Write Locks - Automatic, Abstracted and Portable Topology-Aware Thread Placement - Resource-Centered Distributed Processing of Large Histopathology Images - Automatic Code Generation for Iterative Multi-dimensional Stencil Computations

6.7. musl

KEYWORDS: Standards - Library
SCIENTIFIC DESCRIPTION: musl provides consistent quality and implementation behavior from tiny embedded systems to full-fledged servers. Minimal machine-specific code means less chance of breakage on minority architectures and better success with "write once run everywhere" C development.

musl's efficiency is unparalleled in Linux libc implementations. Designed from the ground up for static linking, musl carefully avoids pulling in large amounts of code or data that the application will not use. Dynamic linking is also efficient, by integrating the entire standard library implementation, including threads, math, and even the dynamic linker itself into a single shared object, most of the startup time and memory overhead of dynamic linking have been eliminated.

FUNCTIONAL DESCRIPTION: We participate in the development of musl, a re-implementation of the C library as it is described by the C and POSIX standards. It is lightweight, fast, simple, free, and strives to be correct in the sense of standards-conformance and safety. Musl is production quality code that is mainly used in the area of embedded devices. It gains more market share also in other areas, e.g. there are now Linux distributions that are based on musl instead of Gnu LibC.

- Participant: Jens Gustedt
- Contact: Jens Gustedt
- URL: http://www.musl-libc.org/

6.8. Modular C

KEYWORDS: Programming language - Modularity

FUNCTIONAL DESCRIPTION: The change to the C language is minimal since we only add one feature, composed identifiers, to the core language. Our modules can import other modules as long as the import relation remains acyclic and a module can refer to its own identifiers and those of the imported modules through freely chosen abbreviations. Other than traditional C include, our import directive ensures complete encapsulation between modules. The abbreviation scheme allows to seamlessly replace an imported module by another one with an equivalent interface. In addition to the export of symbols, we provide parameterized code injection through the import of "snippets". This implements a mechanism that allows for code reuse, similar to X macros or templates. Additional features of our proposal are a simple dynamic module initialization scheme, a structured approach to the C library and a migration path for existing software projects.

- Author: Jens Gustedt
- Contact: Jens Gustedt
- Publications: Modular C - Arbogast: Higher order automatic differentiation for special functions with Modular C - Futex based locks for C11's generic atomics
- URL: http://cmod.gforge.inria.fr/

6.9. arbogast

KEYWORD: Automatic differentiation

SCIENTIFIC DESCRIPTION: This high-level toolbox for the calculus with Taylor polynomials is named after L.F.A. Arbogast (1759-1803), a French mathematician from Strasbourg (Alsace), for his pioneering work in derivation calculus. Its modular structure ensures unmatched efficiency for computing higher order Taylor polynomials. In particular it permits compilers to apply sophisticated vector parallelization to the derivation of nearly unmodified application code.

FUNCTIONAL DESCRIPTION: Arbogast is based on a well-defined extension of the C programming language, Modular C, and places itself between tools that proceed by operator overloading on one side and by rewriting, on the other. The approach is best described as contextualization of C code because it permits the programmer to place his code in different contexts – usual math or AD – to reinterpret it as a usual C function or as a differential operator. Because of the type generic features of modern C, all specializations can be delegated to the compiler.

- Author: Jens Gustedt
- Contact: Jens Gustedt
- Publications: Arbogast: Higher order automatic differentiation for special functions with Modular C - Arbogast – Origine d'un outil de dérivation automatique
- URL: https://gforge.inria.fr/projects/arbo

6.10. CFML

Interactive program verification using characteristic formulae

KEYWORDS: Coq - Software Verification - Deductive program verification - Separation Logic

FUNCTIONAL DESCRIPTION: The CFML tool supports the verification of OCaml programs through interactive Coq proofs. CFML proofs establish the full functional correctness of the code with respect to a specification. They may also be used to formally establish bounds on the asymptotic complexity of the code. The tool is made of two parts: on the one hand, a characteristic formula generator implemented as an OCaml program that parses OCaml code and produces Coq formulae, and, on the other hand, a Coq library that provides notations and tactics for manipulating characteristic formulae interactively in Coq.

- Participants: Arthur Charguéraud, Armaël Guéneau and François Pottier
- Contact: Arthur Charguéraud
- URL: http://www.chargueraud.org/softs/cfml/

6.11. SPETABARU

SPEculative TAsk-BAsed RUntime system

KEYWORDS: HPC - Parallel computing - Task-based algorithm

FUNCTIONAL DESCRIPTION: SPETABARU is a task-based runtime system for multi-core architectures that includes speculative execution models. It is a pure C++11 product without external dependency. It uses advanced meta-programming and allows for an easy customization of the scheduler. It is also capable to generate execution traces in SVG to better understand the behavior of the applications.

- Contact: Bérenger Bramas
- URL: https://gitlab.inria.fr/bramas/spetabaru

CARAMBA Project-Team

6. New Software and Platforms

6.1. Belenios

Belenios - Verifiable online voting system
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION: Belenios is an open-source online voting system that provides confidentiality and verifiability. End-to-end verifiablity relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Confidentiality relies on the encryption of the votes and the distribution of the decryption key.

Belenios builds upon Helios, a voting protocol used in several elections. The main design enhancement of Belenios vs. Helios is that the ballot box can no longer add (fake) ballots, due to the use of credentials. Moreover, Belenios includes a practical threshold decryption system that allows splitting the decryption key among several authorities.

NEWS OF THE YEAR: Since 2015, it has been used by CNRS for remote election among its councils (more than 30 elections every year) and since 2016, it has been used by Inria to elect representatives in the "comités de centre" of each Inria center. In 2018, it has been used to organize about 250 elections (not counting test elections). Belenios is typically used for elections in universities as well as in associations. This goes from laboratory councils (e.g. Irisa, Cran), scientific societies (e.g. SMAI) to various associations (e.g. FFBS - Fédération Française de Baseball et Softball, or SRFA - Société du Rat Francophone et de ses Amateurs).

In total in 2018, more than 13000 ballots have been cast using the voting platform Belenios.

- Participants: Pierrick Gaudry, Stéphane Glondu and Véronique Cortier
- Partners: CNRS - Inria
- Contact: Stéphane Glondu
- URL: http://belenios.gforge.inria.fr/

6.2. CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve
KEYWORDS: Cryptography - Number theory
FUNCTIONAL DESCRIPTION: CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields. It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers.

NEWS OF THE YEAR: The main program for relation collection now supports composite "special-q", and also parallelizes better. The memory footprint of the central step of linear algebra has been reduced, and the parallelism of this step has been improved.

- Participants: Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann
- Contact: Emmanuel Thomé
- URL: http://cado-nfs.gforge.inria.fr/

6.3. rrspace

RIemann-Roch spaces
KEYWORD: Riemann-Roch spaces

FUNCTIONAL DESCRIPTION: The software rrspace implements an algorithm for computing a basis of the Riemann-Roch space associated to a divisor on a curve defined over a finite field. It also implements an algorithm for computing the group law in the Jacobian of such curves. The main algorithm is a variant of Brill-Noether's approach, designed during Aude Le Gluher's Master thesis.

- Participants: Pierre-Jean Spaenlehauer and Aude Le Gluher
- Contact: Pierre-Jean Spaenlehauer
- URL: https://gitlab.inria.fr/pspaenle/rrspace

6.4. Platforms

6.4.1. Platform: computational resources

The computational resources of Caramba have increased significantly in 2018. On the one hand, the CPER «CyberEntreprises» (French Ministry of Research, Région Grand Est, Inria, CNRS) funded the acquisition of a 64-node, 2,048-core cluster called `grvingt`. This cluster is installed in the Inria facility. Other slightly older hardware (a medium-size cluster called `grcinq` from 2013, funded by ANR, and a special machine funded by the aforementioned CPER grant) was moved in the same location to form a coherent platform with about 3,000 cpu cores, 100 TB of storage, and specific machines for RAM-demanding computation. As a whole, this platform provides an excellent support for the computational part of the work done in Caramba. This platform is also embedded in the larger Grid'5000/Silecs platform (and accessible as a normal resource within this platform). Technical administration is done by the Grid'5000 staff.

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

6. New Software and Platforms

6.1. ISOTOP

Topology and geometry of planar algebraic curves

KEYWORDS: Topology - Curve plotting - Geometric computing

FUNCTIONAL DESCRIPTION: Isotop is a Maple software for computing the topology of an algebraic plane curve, that is, for computing an arrangement of polylines isotopic to the input curve. This problem is a necessary key step for computing arrangements of algebraic curves and has also applications for curve plotting. This software has been developed since 2007 in collaboration with F. Rouillier from Inria Paris - Rocquencourt.

NEWS OF THE YEAR: In 2018, an engineer from Inria Nancy (Benjamin Dexheimer) finished the implementation of the web server to improve the diffusion of our software.

- Participants: Luis Penaranda, Marc Pouget and Sylvain Lazard
- Contact: Marc Pouget
- Publications: Rational Univariate Representations of Bivariate Systems and Applications - Separating Linear Forms for Bivariate Systems - On The Topology of Planar Algebraic Curves - New bivariate system solver and topology of algebraic curves - Improved algorithm for computing separating linear forms for bivariate systems - Solving bivariate systems using Rational Univariate Representations - On the topology of planar algebraic curves - On the topology of real algebraic plane curves - Bivariate triangular decompositions in the presence of asymptotes - Separating linear forms and Rational Univariate Representations of bivariate systems
- URL: https://isotop.gamble.loria.fr/

6.2. SubdivisionSolver

KEYWORDS: Numerical solver - Polynomial or analytical systems

SCIENTIFIC DESCRIPTION: The goal underlying the developpement of RealSolver is the ability to solve large polynomial systems with certified results using adaptive multi-precision arithmetic for efficiency.

The software is based on a classic branch and bound algorithm using interval arithmetic: an initial box is subdivided until its sub-boxes are certified to contain either no solution or a unique solution of the input system. Evaluation is performed with a centered evaluation at order two, and existence and uniqueness of solutions is verified thanks to the Krawczyk operator.

RealSolver uses two implementations of interval arithmetic: the C++ boost library that provides a fast arithmetic when double precision is enough, and otherwise the C mpfi library that allows to work in arbitrary precision. Considering the subdivision process as a breadth first search in a tree, the boost interval arithmetic is used as deeply as possible before a new subdivision process using higher precision arithmetic is performed on the remaining forest.

The software is can be interfaced with sage and the library Fast_Polynomial that allows to solve systems of polynomials that are large in terms of degree, number of monomials and bit-size of coefficients.

FUNCTIONAL DESCRIPTION: The software RealSolver solves square systems of analytic equations on a compact subset of a real space. RealSolver is a subdivision solver using interval arithmetic and multiprecision arithmetic to achieve certified results. If the arithmetic precision required to isolate solutions is known, it can be given as an input parameter of the process, otherwise the precision is increased on-the-fly. In particular, RealSolver can be interfaced with the Fast_Polynomial library (https://bil.inria.fr/en/software/view/2423/tab#lA) to solve polynomial systems that are large in terms of degree, number of monomials and bit-size of coefficients.

NEWS OF THE YEAR: In 2018, Mohamed Eissa was recruited on a FastTrack contract for porting the code to python.

- Contact: Rémi Imbach

6.3. CGAL Package : 2D hyperbolic triangulations

KEYWORDS: Geometry - Delaunay triangulation - Hyperbolic space
FUNCTIONAL DESCRIPTION: This package implements the construction of Delaunay triangulations in the Poincaré disk model.
NEWS OF THE YEAR: This package has been submitted to the CGAL Editorial Board for future integration into the library.

- Participants: Mikhail Bogdanov, Olivier Devillers, Iordan Iordanov and Monique Teillaud
- Contact: Monique Teillaud
- Publication: Hyperbolic Delaunay Complexes and Voronoi Diagrams Made Practical
- URL: https://github.com/CGAL/cgal-public-dev/tree/Periodic_4_hyperbolic_triangulation_2-IIordanov

6.4. CGAL Package : 2D periodic hyperbolic triangulations

KEYWORDS: Geometry - Delaunay triangulation - Hyperbolic space
FUNCTIONAL DESCRIPTION: This module implements the computation of Delaunay triangulations of the Bolza surface.
NEWS OF THE YEAR: This package has been submitted to the CGAL Editorial Board for future integration into the library.

- Authors: Iordan Iordanov and Monique Teillaud
- Contact: Monique Teillaud
- Publication: Implementing Delaunay Triangulations of the Bolza Surface
- URL: https://github.com/CGAL/cgal-public-dev/tree/Periodic_4_hyperbolic_triangulation_2-IIordanov

6.5. CGAL package: 3D periodic mesh generation

KEYWORDS: Flat torus - CGAL - Geometry - Delaunay triangulation - Mesh generation - Tetrahedral mesh - Mesh
FUNCTIONAL DESCRIPTION: This package of CGAL (Computational Geometry Algorithms Library http://www.cgal.org) allows to build and handle volumic meshes of shapes described through implicit functional boundaries over the 3D flat torus whose fundamental domain is a cube.
NEWS OF THE YEAR: This new package has been released in CGAL 4.13

- Participants: Mikhail Bogdanov, Aymeric Pellé, Mael Rouxel-Labbe and Monique Teillaud
- Contact: Monique Teillaud
- Publications: CGAL periodic volume mesh generator - Periodic meshes for the CGAL library
- URL: https://doc.cgal.org/latest/Manual/packages.html#PkgPeriodic_3_mesh_3Summary

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

6. New Software and Platforms

6.1. Software

6.1.1. FiatLux

- Participants: Nazim Fatès, Nicolas Gauville

FiatLux is a simulation program for cellular automata and discrete dynamical systems. It is developed by Nazim Fatès ; the project is currently available at the Inria GForge. The program is published with the CeCILL license. New features have been implemented in 2018, as for example the possibility to define some systems directly in the software by writing the local transition rules in Java. These features were mostly added by Nicolas Gauville, a Master's student who was an intern in the team.

PESTO Project-Team

6. New Software and Platforms

6.1. Akiss

AKISS - Active Knowledge in Security Protocols
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: AKISS (Active Knowledge in Security Protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. AKISS implements a procedure to verify equivalence properties for a bounded number of sessions based on a fully abstract modelling of the traces of a bounded number of sessions of the protocols into first-order Horn clauses and a dedicated resolution procedure. The procedure can handle a large set of cryptographic primitives, namely those that can be modeled by an optimally reducing convergent rewrite system, as well as the exclusive or (xor) operator.

- Contact: Steve Kremer
- URL: https://github.com/akiss

6.2. Belenios

Belenios - Verifiable online voting system
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION: Belenios is an open-source online voting system that provides confidentiality and verifiability. End-to-end verifiablity relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Confidentiality relies on the encryption of the votes and the distribution of the decryption key.

Belenios builds upon Helios, a voting protocol used in several elections. The main design enhancement of Belenios vs. Helios is that the ballot box can no longer add (fake) ballots, due to the use of credentials. Moreover, Belenios includes a practical threshold decryption system that allows splitting the decryption key among several authorities.

NEWS OF THE YEAR: Since 2015, it has been used by CNRS for remote election among its councils (more than 30 elections every year) and since 2016, it has been used by Inria to elect representatives in the "comités de centre" of each Inria center. In 2018, it has been used to organize about 250 elections (not counting test elections). Belenios is typically used for elections in universities as well as in associations. This goes from laboratory councils (e.g. Irisa, Cran), scientific societies (e.g. SMAI) to various associations (e.g. FFBS - Fédération Française de Baseball et Softball, or SRFA - Société du Rat Francophone et de ses Amateurs).

In total in 2018, more than 13000 ballots have been cast using the voting platform Belenios.

- Participants: Pierrick Gaudry, Stéphane Glondu and Véronique Cortier
- Partners: CNRS - Inria
- Contact: Stéphane Glondu
- URL: http://belenios.gforge.inria.fr/

6.3. Deepsec

DEEPSEC - DEciding Equivalence Properties in SECurity protocols
KEYWORDS: Security - Verification

FUNCTIONAL DESCRIPTION: DEEPSEC (DEciding Equivalence Properties in SECurity protocols) is a tool for verifying indistinguishability properties in cryptographic protocols, modelled as trace equivalence in a process calculus. Indistinguishability is used to model a variety of properties including anonymity properties, strong versions of confidentiality and resistance against offline guessing attacks, etc. DEEPSEC implements a decision procedure to verify trace equivalence for a bounded number of sessions and cryptographic primitives modeled by a subterm convergent destructor rewrite system. The procedure is based on constraint solving techniques. The tool also implements state-of-the-art partial order reductions and allows to distribute the computation on multiple cores and multiple machines.

- Contact: Vincent Cheval
- URL: https://deepsec-prover.github.io/

6.4. Tamarin

TAMARIN prover
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: The TAMARIN prover is a security protocol verification tool that supports both falsification and unbounded verification of security protocols specified as multiset rewriting systems with respect to (temporal) first-order properties and a message theory that models Diffie-Hellman exponentiation, bilinear pairing, multisets, and exclusive-or (XOR), combined with a user-defined convergent rewriting theory. Its main advantages are its ability to handle stateful protocols and its interactive proof mode. Moreover, it has been extended to verify equivalence properties. The tool is developed jointly by the PESTO team, the Institute of Information Security at ETH Zurich, and the University of Oxford. In a joint effort, the partners wrote and published a user manual in 2016, available from the Tamarin website.

- Contact: Jannik Dreier
- URL: http://tamarin-prover.github.io/

6.5. SAPIC

SAPIC: Stateful Applied Pi Calculus
KEYWORDS: Security - Verification
FUNCTIONAL DESCRIPTION: SAPIC is a plugin of the TAMARIN tool that translates protocols from a high-level protocol description language akin to the applied pi-calculus into multiset rewrite rules, that can then be analysed by the TAMARIN prover. TAMARIN has also been extended with dedicated heuristics that exploit the form of translated rules and favor termination.

SAPIC offers support for the analysis of protocols that include states, for example Hardware Security Tokens communicating with a possibly malicious user, or protocols that rely on databases. It also allows us to verify liveness properties and a notion of location and reporting used for modelling trusted execution environments. It has been successfully applied on several case studies including the Yubikey authentication protocol, and extensions of the PKCS#11 standard. SAPIC also includes support for verifying liveness properties, which are for instance important in fair exchange and contract signing protocols, as well as support for constructions useful when modelling isolated execution environments.

- Contact: Steve Kremer
- URL: http://sapic.gforge.inria.fr/

6.6. TypeEquiv

A type checker for privacy properties
KEYWORDS: Security - Cryptographic protocol - Privacy

FUNCTIONAL DESCRIPTION: TypeEquiv provides a (sound) type system for proving equivalence of protocols (to anaylse privacy properties such as vote privacy, anonymity, unlinkability), for both a bounded or an unbounded number of sessions and for the standard cryptographic primitives. TypeEquiv takes as input the specification of a pair of security protocols, written in a dialect of the applied-pi calculus, together with some type annotations. It checks whether the two protocols are in equivalence or not. The tool provides a significant speed-up compared with tools that decide equivalence of security protocols for a bounded number of sessions.

- Partner: Technische Universität Wien
- Contact: Véronique Cortier

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

6. New Software and Platforms

6.1. Redlog

Reduce Logic System

KEYWORDS: Computer algebra system (CAS) - First-order logic - Constraint solving

SCIENTIFIC DESCRIPTION: Redlog is an integral part of the interactive computer algebra system Reduce. It supplements Reduce's comprehensive collection of powerful methods from symbolic computation by supplying more than 100 functions on first-order formulas.

Redlog generally works with interpreted first-order logic in contrast to free first-order logic. Each first-order formula in Redlog must exclusively contain atoms from one particular Redlog-supported theory, which corresponds to a choice of admissible functions and relations with fixed semantics. Redlog-supported theories include Nonlinear Real Arithmetic (Real Closed Fields), Presburger Arithmetic, Parametric QSAT, and many more.

NEWS OF THE YEAR: Parts of the Redlog code are 25 years old now. Version 1 of the underlying computer algebra system Reduce has been published even 50 years ago. In 2018 we therefore decided to go for major revisions and improvements of Redlog's software architecture.

Redlog is, as well as the underlying Reduce, implemented in a language called RLISP, which technically parses an Algol-style procedural notation into a quite minimalistic Lisp 1 dialect called Standard Lisp. RLISP and Reduce and, subsequently, Redlog are bootstrapped on the basis of an existing Standard Lisp. Today, there are two independent implementations of Standard Lisp left, which are supported only on the basis of private commitment of essentially one individual per Lisp. With the large code base of Redlog plus the necessary algebraic algorithms from Reduce a migration to a different language or computer algebra system is not feasible. We are therefore experimenting with the realization of a Standard Lisp on the basis of ANSI Common Lisp, which could allow an RLISP-Reduce-Redlog bootstrap. Given that Common Lisp is a Lisp 2, this is feasible but not at all straightforward. Also, it naturally comes with a loss of efficiency, which requires careful programming. We are grateful that Inria supports this project with an engineer's position for limited time (ADT-135 Fast Track).

We are furthermore working on an improved design of Redlog's black-box and service schedulers [Dolzmann and Sturm, ACM SIGSAM Bull. 31, 1997] and a revision of global Boolean switches in favor of named optional arguments. In that course we store related information more explicitly, which will allow automatic consistency checks of the schedulers and automated interface generation with named arguments. In addition, this supports an interactive help system inside Reduce, which is also under construction.

- Participant: Thomas Sturm
- Contact: Thomas Sturm
- URL: http://www.redlog.eu/

6.2. SPASS

KEYWORD: First-order logic

SCIENTIFIC DESCRIPTION: The classic SPASS is an automated theorem prover based on superposition that handles first-order logic with equality and several extensions for particular classes of theories. With version SPASS 3.9 we have stopped the development of the classic prover and have started the bottom-up development of SPASS 4.0 that will actually be a workbench of automated reasoning tools. Furthermore, we use SPASS 3.9 as a test bed for the development of new calculi.

SPASS 3.9 has been used as the basis for SPASS-AR, a new approximation refinement theorem proving approach.

FUNCTIONAL DESCRIPTION: SPASS is an automated theorem prover based on superposition that handles first-order logic with equality and several extensions for particular classes of theories.

NEWS OF THE YEAR: We released the second version of SPASS-IQ, our solver for linear integer arithmetic that we are currently extending to real and mixed real-integer arithmetic.

- Contact: Christoph Weidenbach
- URL: http://www.spass-prover.org/

6.3. SPASS-SATT

KEYWORDS: Automated deduction - Decision

SCIENTIFIC DESCRIPTION: SPASS -SATT is an SMT solver for the theories of linear integer arithmetic, linear rational arithmetic and mixed linear arithmetic. It features new tests for the satisfiability of unbounded systems, as well as new algorithms for the detection of integer solutions.

We further investigated the use of redundancy elimination in SAT solving and underlying implementation techniques. Our aim is a new approach to SAT solving that needs fewer conflicts (on average) *and* is faster than the current state-of-the art solvers. Furthermore, we have developed a new calculus and first prototypical implementation of a SAT solver with mixed OR/XOR clauses.

FUNCTIONAL DESCRIPTION: SPASS-SATT is an SMT solver for linear integer arithmetic, mixed linear arithmetic and rational linear arithmetic.

NEWS OF THE YEAR: The first version of SPASS-SATT was released in June 2018. It participated in SMTCOMP-2018 in the quantifier free integer and rational linear arithmetic categories. In both categories it solved more problems in a shorter period of time than any other SMT solver. With respect to the weighted bucket ranking it scored first in the linear integer category and second in the linear rational category.

- Participants: Martin Bromberger, Mathias Fleury and Christoph Weidenbach
- Contact: Martin Bromberger
- URL: https://www.mpi-inf.mpg.de/departments/automation-of-logic/software/spass-workbench/spass-satt/

6.4. SPIKE

KEYWORDS: Proof - Automated deduction - Automated theorem proving - Term Rewriting Systems - Formal methods

SCIENTIFIC DESCRIPTION: SPIKE, an automatic induction-based theorem prover built to reason on conditional theories with equality, is one of the few formal tools able to perform automatically mutual and lazy induction. Designed in the 1990s, it has been successfully used in many non-trivial applications and served as a prototype for different proof experiments and extensions.

FUNCTIONAL DESCRIPTION: Automated induction-based theorem prover

RELEASE FUNCTIONAL DESCRIPTION: Proof certification with Coq, cyclic induction, decision procedures

- Participant: Sorin Stratulat
- Contact: Sorin Stratulat

6.5. veriT

KEYWORDS: Automated deduction - Formula solving - Verification

SCIENTIFIC DESCRIPTION: veriT comprises a SAT solver, a decision procedure for uninterpreted symbols based on congruence closure, a simplex-based decision procedure for linear arithmetic, and instantiation-based quantifier handling.

FUNCTIONAL DESCRIPTION: VeriT is an open, trustable and efficient SMT (Satisfiability Modulo Theories) solver, featuring efficient decision procedure for uninterpreted symbols and linear arithmetic, and quantifier reasoning.

NEWS OF THE YEAR: Efforts in 2018 have been focused on non-linear arithmetic reasoning, quantifier handling and proof production.

The veriT solver participated in the SMT competition SMT-COMP 2018 with good results.

We target applications where validation of formulas is crucial, such as the validation of TLA$^+$ and B specifications, and work together with the developers of the respective verification platforms to make veriT even more useful in practice. The solver is available as a plugin for the Rodin platform, it is integrated within the Atelier B.

veriT is also a prototype platform for ideas developed within the Matryoshka project, aiming at greater availability of automated reasoning for proof assistants.

- Participants: Haniel Barbosa, Daniel El Ouraoui, Pascal Fontaine and Hans-Jörg Schurr
- Partner: Université de Lorraine
- Contact: Pascal Fontaine
- URL: http://www.veriT-solver.org

6.6. Nunchaku

The Nunchaku Higher-Order Model Finder
KEYWORDS: Proof - Higher-order logic
SCIENTIFIC DESCRIPTION: Nunchaku is a model finder for higher-order logic, with dedicated support for various definitional principles. It is designed to work as a backend for various proof assistants (notably Isabelle/HOL and Coq) and to use state-of-the-art model finders and other solvers as backends.
FUNCTIONAL DESCRIPTION: Nunchaku is a model finder (counterexample generator) for higher-order logic.
NEWS OF THE YEAR: A noteworthy development this year is a preliminary integration of Nunchaku in the Lean proof assistant. This work was performed by Pablo Le Hénaff during an internship at Vrije Universiteit Amsterdam. See his internship report at http://matryoshka.gforge.inria.fr/pubs/lehenaff_report.pdf for details.

- Participants: Jasmin Christian Blanchette and Simon Cruanes
- Partner: Vrije Universiteit Amsterdam
- Contact: Jasmin Christian Blanchette
- Publications: Extending Nunchaku to Dependent Type Theory - Model Finding for Recursive Functions in SMT
- URL: https://github.com/nunchaku-inria

6.7. TLAPS

TLA+ proof system
KEYWORD: Proof assistant
FUNCTIONAL DESCRIPTION: TLAPS is a platform for developing and mechanically verifying proofs about TLA+ specifications. The TLA+ proof language is hierarchical and explicit, allowing a user to decompose the overall proof into proof steps that can be checked independently. TLAPS consists of a proof manager that interprets the proof language and generates a collection of proof obligations that are sent to backend verifiers. The current backends include the tableau-based prover Zenon for first-order logic, Isabelle/TLA+, an encoding of TLA+ set theory as an object logic in the logical framework Isabelle, an SMT backend designed for use with any SMT-lib compatible solver, and an interface to a decision procedure for propositional temporal logic.

NEWS OF THE YEAR: Ioannis Filippidis joined the development team in November 2018 and started designing and implementing support for reasoning about TLA+'s ENABLED construct.

- Participants: Damien Doligez, Stephan Merz and IOANNIS FILIPPIDIS
- Contact: Stephan Merz
- URL: https://tla.msr-inria.inria.fr/tlaps/content/Home.html

6.8. Apalache

Abstraction-based Parameterized TLA+ Checker
KEYWORD: Model Checker
FUNCTIONAL DESCRIPTION: The first version implements a symbolic bounded model checker for TLA$^+$ that runs under the same assumptions as the explicit-state model checker TLC. It checks whether a TLA$^+$ specification satisfies an invariant candidate by checking satisfiability of an SMT formula that encodes: (1) an execution of bounded length, and (2) preservation of the invariant candidate in every state of the execution. Our tool is still in the experimental phase, due to a number of challenges posed by the semantics of TLA$^+$ to SMT solvers.

- Partner: Technische Universität Wien
- Contact: Igor Konnov
- Publications: BmcMT: Bounded Model Checking of TLA + Specifications with SMT - Extracting Symbolic Transitions from $TLA+$ Specifications
- URL: https://forsyte.at/research/apalache/

6.9. ByMC

Byzantine Model Checker
KEYWORDS: Model Checker - Distributed computing - Verification
SCIENTIFIC DESCRIPTION: In recent work, we have introduced a series of techniques for automatic verification of threshold-guarded distributed algorithms that have the following features: (1) up to t of n processes may exhibit crash or Byzantine failures, (2) the correct processes count messages and progress when they receive sufficiently many messages, e.g., at least $t + 1$, (3) the number n of processes in the system is a parameter, as well as t, (4) and the parameters are restricted by a resilience condition, e.g., $n > 3t$.
FUNCTIONAL DESCRIPTION: ByMC implements several techniques for the parameterized verification of threshold-guarded distributed algorithms such as reliable broadcast, one-step Byzantine consensus, non-blocking atomic commit, condition-based consensus, and randomized consensus. The tool accepts two kinds of inputs: (i) threshold automata (the framework of our verification techniques) and (ii) Parametric Promela (which is similar to the way in which the distributed algorithms are presented in the distributed computing literature). Internally, the tool analyzes representative executions by querying an SMT solver. Apart from verification, ByMC also implements a technique for the automatic synthesis of threshold guards.

The tool can run on a single computer as well as in an MPI cluster, e.g., Grid5000 or Vienna Scientific Cluster. NEWS OF THE YEAR: We have introduced a parallel extension of the tool, which allows one to run verification experiments in an MPI cluster. The parallel version of the tool demonstrated a good speed-up on large benchmarks run in Vienna Scientific Cluster and Grid 5000.

- Partner: Technische Universität Wien
- Contact: Igor Konnov
- Publications: ByMC: Byzantine Model Checker - Reachability in Parameterized Systems: All Flavors of Threshold Automata - Model Checking of Fault-Tolerant Distributed Algorithms: from Classics towards Contemporary - Verification of Randomized Distributed Algorithms under Round-Rigid Adversaries
- URL: https://forsyte.at/software/bymc/

SPHINX Project-Team

5. New Software and Platforms

5.1. GetDDM

KEYWORDS: Large scale - 3D - Domain decomposition - Numerical solver
FUNCTIONAL DESCRIPTION: GetDDM combines GetDP and Gmsh to solve large scale finite element problems using optimized Schwarz domain decomposition methods.

- Contact: Xavier Antoine
- URL: http://onelab.info/wiki/GetDDM

5.2. GPELab

Gross-Pitaevskii equations Matlab toolbox
KEYWORDS: 3D - Quantum chemistry - 2D
FUNCTIONAL DESCRIPTION: GPELab is a Matlab toolbox developed to help physicists for computing ground states or dynamics of quantum systems modeled by Gross-Pitaevskii equations. This toolbox allows the user to define a large range of physical problems (1d-2d-3d equations, general nonlinearities, rotation term, multi-components problems...) and proposes numerical methods that are robust and efficient.

- Contact: Xavier Antoine
- URL: http://gpelab.math.cnrs.fr/

TOSCA Project-Team (section vide)

BIGS Project-Team (section vide)

CAPSID Project-Team

6. New Software and Platforms

6.1. Hex

KEYWORDS: 3D rendering - Bioinformatics - 3D interaction - Structural Biology
SCIENTIFIC DESCRIPTION: Hex is an interactive protein docking and molecular superposition program for Linux Mac-OS and Windows-XP. Hex understands protein and DNA structures in PDB format, and it can also read small-molecule SDF files. The recent versions now include CUDA support for Nvidia GPUs. On a modern workstation, docking times range from a few minutes or less when the search is constrained to known binding sites, to about half an hour for a blind global search (or just a few seconds with CUDA).
FUNCTIONAL DESCRIPTION: The underlying algorithm uses a novel polar Fourier correlation technique to accelerate the search for close-fitting orientations of the two molecules.

- Participant: David Ritchie
- Contact: David Ritchie
- URL: http://hex.loria.fr

6.2. Kbdock

KEYWORD: 3D interaction
SCIENTIFIC DESCRIPTION: Kbdock is a database of 3D protein domain-domain interactions with a web interface.
FUNCTIONAL DESCRIPTION: The Kbdock database is built from a snapshot of the Protein Databank (PDB) in which all 3D structures are cut into domains according to the Pfam domain description. A web interface allows 3D domain-domain interactions to be compared by Pfam family.

- Authors: Anisah Ghoorah, David Ritchie and Marie-Dominique Devignes
- Contact: David Ritchie
- URL: http://kbdock.loria.fr

6.3. Kpax

KEYWORDS: Bioinformatics - Structural Biology
SCIENTIFIC DESCRIPTION: Kpax is a program for aligning and superposing the 3D structures of protein molecules.
FUNCTIONAL DESCRIPTION: The algorithm uses a Gaussian representation of the protein backbone in order to construct a similarity score based on the 3D overlap of the Gaussians of the proteins to be superposed. Multiple proteins may be aligned together (multiple structural alignment) and databases of protein structures may be searched rapidly.

- Participant: David Ritchie
- Contact: David Ritchie

6.4. Sam

Protein Symmetry Assembler
KEYWORDS: Proteins - Structural Biology
SCIENTIFIC DESCRIPTION: Sam is a program for making symmetrical protein complexes, starting from a single monomer.

FUNCTIONAL DESCRIPTION: The algorithm searches for good docking solutions between protein monomers using a spherical polar Fast Fourier transform correlation in which symmetry restraints are built into the calculation. Thus every candidate solution is guaranteed to have the desired symmetry.

- Authors: David Ritchie and Sergey Grudinin
- Partner: CNRS
- Contact: David Ritchie
- URL: http://sam.loria.fr

6.5. gEMfitter

KEYWORDS: 3D reconstruction - Cryo-electron microscopy - Fitting
SCIENTIFIC DESCRIPTION: A program for fitting high resolution 3D protein structures into low resolution cryo-EM density maps.
FUNCTIONAL DESCRIPTION: A highly parallel fast Fourier transform (FFT) EM density fitting program which can exploit the special hardware properties of modern graphics processor units (GPUs) to accelerate both the translational and rotational parts of the correlation search.

- Authors: Van-Thai Hoang and David Ritchie
- Contact: David Ritchie
- URL: http://gem.loria.fr/gEMfitter/

6.6. ECDM

ECDomainMiner
KEYWORD: Functional annotation
SCIENTIFIC DESCRIPTION: EC-DomainMiner uses a recommender-based approach for associating EC (Enzyme Commission) numbers with protein Pfam domains from EC-sequence relationships that have been annotated previously in the SIFTS and Uniprot databases.
FUNCTIONAL DESCRIPTION: A program to associate protein Enzyme Commission numbers with Pfam domains

- Contact: David Ritchie
- URL: http://ecdm.loria.fr

6.7. GODM

GO-DomainMiner
KEYWORD: Functional annotation
FUNCTIONAL DESCRIPTION: GO-DomainMiner is is a graph-based approach for associating GO (gene ontology) terms with protein Pfam domains.

- Contact: David Ritchie
- URL: http://godm.loria.fr

6.8. BLADYG

A Block-centric graph processing framework for LArge Dynamic Graphs
KEYWORDS: Distributed computing - Dynamic graph processing

FUNCTIONAL DESCRIPTION: BLADYG is a block-centric framework that addresses the issue of dynamism in large-scale graphs. BLADYG starts its computation by collecting the graph data from various data sources. After collecting the graph data, BLADYG partitions the input graph into multiple partitions. Each BLADYG worker loads its block/partition and performs both local and remote computations, after which the status of the blocks is updated. The BLADYG coordinator orchestrates the execution of the considered graph operation in order to deal with graph updates.

- Partner: University of Trento
- Contact: Sabeur Aridhi

6.9. CGC

Clebsch-Gordan Coefficients
KEYWORDS: Clebsch-Gordan coupling coefficient - 3j symbol
FUNCTIONAL DESCRIPTION: Clebsch-Gordan coupling coefficients appear in many areas of physics and chemistry. CGC is a small library of functions and a demo driver program for calculating Clebsch-Gordan coupling coefficients up to very high principal quantum numbers.

- Contact: David Ritchie
- URL: http://cgc.loria.fr

6.10. GrAPFI

GrAPFI: Graph-based Automatic Protein Function Inference
KEYWORD: Proteins
FUNCTIONAL DESCRIPTION: GrAPFI is a Graph-based Automatic Protein Function Inference tool that aims to annotate protein sequences with EC numbers. The underlying philosophy of GrAPFI assumes that proteins can be linked through the domains, families, and superfamilies that they share. Several domain databases exist such as e.g. Pfam, SMART, CDD, Gene3D, and Prosite. Furthermore, InterPro aims to integrate information from all such databases by assigning them unique InterPro signatures. GrAPFI tool also shares Interpro signatures, as it includes information from several major family and domain databases. Our computational analysis and cross-validation show that GrAPFI achieves state-of-the-art performance in EC number prediction.

- Contact: Sabeur Aridhi
- URL: http://grapfi.loria.fr/

6.11. Platforms

6.11.1. The MBI Platform

The MBI (Modeling Biomolecular Interactions) platform (http://bioinfo.loria.fr) was established to support collaborations between Inria Nancy – Grand Est and other research teams associated with the University of Lorraine. The platform is a research node of the Institut Français de Bioinformatique (IFB), which is the French national network of bioinformatics platforms (http://www.france-bioinformatique.fr). **In 2018, funding for an engineer was awarded to Marie-Dominique Devignes for a project on bioinformatics service integration.**

- Contact: Marie-Dominique Devignes

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

6. New Software and Platforms

6.1. SOFA

Simulation Open Framework Architecture

KEYWORDS: Real time - Multi-physics simulation - Medical applications

FUNCTIONAL DESCRIPTION: SOFA is an Open Source framework primarily targeted at real-time simulation, with an emphasis on medical simulation. It is mostly intended for the research community to help develop new algorithms, but can also be used as an efficient prototyping tool. Based on an advanced software architecture, it allows : the creation of complex and evolving simulations by combining new algorithms with algorithms already included in SOFA, the modification of most parameters of the simulation (deformable behavior, surface representation, solver, constraints, collision algorithm, etc.) by simply editing an XML file, the building of complex models from simpler ones using a scene-graph description, the efficient simulation of the dynamics of interacting objects using abstract equation solvers, the reuse and easy comparison of a variety of available methods.

- Participants: Christian Duriez, François Faure, Hervé Delingette and Stéphane Cotin
- Partner: IGG
- Contact: Stéphane Cotin
- URL: http://www.sofa-framework.org

6.2. SofaCV Plugin

Keywords: Simulation - Visualization - Image processing

Functional Description: SofaCV is a plugin for the simulation framework SOFA. Its purpose is to provide computer vision tools to SOFA. More specifically, its goal is to enable the use of SOFA simulations in augmented reality, and virtual reality applications. The SofaCV plugin is not a standalone plugin by itself. Instead it provides an API for submodules (mainly Sofa's ImageProcessing and DataAcquisition plugin) such as base datatypes, Python bindings, SofaQtQuick widgets etc, along with some utility SOFA Components to read, write or display an image in the scene view.

The ImageProcessing plugin is a plugin for the simulation framework SOFA. Its purpose is to provide general purpose Computer vision features to Sofa. More specifically, its goal is to enable the use of SOFA simulations in augmented reality, and virtual reality applications. The ImageProcessing plugin depends on the SofaCV Base plugin. The ImageProcessing plugin doesn't have the ambition to provide cutting-edge computer vision algorithms, but instead, wraps OpenCV's features while taking advantage of SOFA's Component-based API. This plugin also provides useful Camera components, providing on-the-fly conversions from/to OpenGL & OpenCV's camera calibration parameters. (calibrating cameras, modifying both intrinsic and extrinsic camera parameters in OpenGL)

- Author: Bruno Marques
- Contact bruno.josue.marques@inria.fr

6.3. Needle Insertion Plugin

Keywords: Simulation - Needle insertion - Haptic feedback

Functional Description: This plugin contains needle/tissue interaction models for real time simulations of needle insertion in deformable objects using the open-source sofa framework. This allows for modeling the different forces playing a role during the insertion process (penetration forces, friction along the shaft...) using a constrained-based formulation. This formulation provides a fast and stable solution for the simulation of complex insertions (and reinsertion) of the needle in deformable Finite Element models.

- Authors: Hadrien Courtecuisse
- Contact: hcourtecuisse@unistra.fr

6.4. Optimus Plugin

Keywords: Simulation - Stochastic Filtering - Data Assimilation - State Estimation - Medical applications
Functional Description:

The goal of the plugin is to implement a real integration of Verdandi in SOFA in order to provide a complex and efficient tool for data-assimilation and state-estimation based on filtering prediction-correction scheme.

- Main Author: Igor Peterlik
- Collaborators: Sergei Nikolaev, Nava Schulmann, Raffaella Trivisonne
- Contact:
    - igor.peterlik@inria.fr
    - sergei.nikolaev@inria.fr
    - nava.schulmann@inria.fr
    - raffaella.trivisonne@inria.fr

6.5. RGBDTracking Plugin

Keywords: Simulation - RGBD data Processing - Object tracking - data fusion - Numerical simulations
Functional Description: RGBDTracking is a SOFA plugin to register and track deformable objects in real-time using an RGB-D sensor. This frame-by-frame system relies on a prior visual segmentation of the object in the RGB image. The resulting segmented point cloud is then used to register the object, first in a rigid manner, and then by non-rigidly fitting the known mesh, based on the Finite Element Method to model elasticity, and on vision-based external forces exerted on the mesh.

- Author: Antoine Petit
- Contact: antoine.a.petit@inria.fr

NEUROSYS Project-Team

6. New Software and Platforms

6.1. OpenVIBE

KEYWORDS: Neurosciences - Interaction - Virtual reality - Health - Real time - Neurofeedback - Brain-Computer Interface - EEG - 3D interaction

FUNCTIONAL DESCRIPTION: OpenViBE is a free and open-source software platform devoted to the design, test and use of Brain-Computer Interfaces (BCI). The platform consists of a set of software modules that can be integrated easily and efficiently to design BCI applications. The key features of OpenViBE software are its modularity, its high-performance, its portability, its multiple-users facilities and its connection with high-end/VR displays. The designer of the platform enables to build complete scenarios based on existing software modules using a dedicated graphical language and a simple Graphical User Interface (GUI). This software is available on the Inria Forge under the terms of the AGPL licence, and it was officially released in June 2009. Since then, the OpenViBE software has already been downloaded more than 60000 times, and it is used by numerous laboratories, projects, or individuals worldwide. More information, downloads, tutorials, videos, documentations are available on the OpenViBE website.

- Participants: Cédric Riou, Thierry Gaugry, Anatole Lécuyer, Fabien Lotte, Jussi Tapio Lindgren, Laurent Bougrain, Maureen Clerc and Théodore Papadopoulo
- Partners: INSERM - GIPSA-Lab
- Contact: Anatole Lécuyer
- URL: http://openvibe.inria.fr

6.2. Platforms

6.2.1. EEG experimental room

A room at Inria Nancy - Grand Est is dedicated to electroencephalographic recordings. An umbrella agreement and several additional experiment descriptions have been approved by the Inria Operational Legal and Ethical Risk Assessment Committee (COERLE). A new 64 channels Biosemi EEG amplifier has been added this year to be able to record two experimental campaign in parallel (Regional initiative *Contrat de Projet État Région (CPER) IT2MP* see section 8.1). Specific experimentation have been done in interaction with Pepper, a semi-humanoid robot.

Figure 1. Electroencephalographic Experimental room at Inria Nancy-Grand Est

TONUS Team

6. New Software and Platforms

6.1. CLAC

Conservation Laws Approximation on many Cores

SCIENTIFIC DESCRIPTION: It is clear now that future computers will be made of a collection of thousands of interconnected multicore processors. Globally it appears as a classical distributed memory MIMD machine. But at a lower level, each of the multicore processors is itself made of a shared memory MIMD unit (a few classical CPU cores) and a SIMD unit (a GPU). When designing new algorithms, it is important to adapt them to this kind of architecture. Our philosophy will be to program our algorithms in such a way that they can be run efficiently on this kind of computers. Practically, we will use the MPI library for managing the coarse grain parallelism, while the OpenCL library will efficiently operate the fine grain parallelism.

We have invested for several years until now into scientific computing on GPUs, using the open standard OpenCL (Open Computing Language). We were recently awarded a prize in the international AMD OpenCL innovation challenge thanks to an OpenCL two-dimensional Vlasov-Maxwell solver that fully runs on a GPU. OpenCL is a very interesting tool because it is an open standard now available on almost all brands of multicore processors and GPUs. The same parallel program can run on a GPU or a multicore processor without modification.

Because of the envisaged applications of CLAC, which may be either academic or commercial, it is necessary to conceive a modular framework. The heart of the library is made of generic parallel algorithms for solving conservation laws. The parallelism can be both fine-grained (oriented towards GPUs and multicore processors) and coarse-grained (oriented towards GPU clusters). The separate modules allow managing the meshes and some specific applications. In this way, it is possible to isolate parts that should be protected for trade secret reasons.

FUNCTIONAL DESCRIPTION: CLAC is a generic Discontinuous Galerkin solver, written in C/C++, based on the OpenCL and MPI frameworks.

- Partner: AxesSim
- Contact: Philippe Helluy
- URL: http://clac.gforge.inria.fr/

6.2. Selalib

SEmi-LAgrangian LIBrary

KEYWORDS: Plasma physics - Semilagrangian method - Parallel computing - Plasma turbulence

SCIENTIFIC DESCRIPTION: The objective of the Selalib project (SEmi-LAgrangian LIBrary) is to develop a well-designed, organized and documented library implementing several numerical methods for kinetic models of plasma physics. Its ultimate goal is to produce gyrokinetic simulations.

Another objective of the library is to provide to physicists easy-to-use gyrokinetic solvers, based on the semi-lagrangian techniques developed by Eric Sonnendrücker and his collaborators in the past CALVI project. The new models and schemes from TONUS are also intended to be incorporated into Selalib.

FUNCTIONAL DESCRIPTION: Selalib is a collection of modules conceived to aid in the development of plasma physics simulations, particularly in the study of turbulence in fusion plasmas. Selalib offers basic capabilities from general and mathematical utilities and modules to aid in parallelization, up to pre-packaged simulations.

- Partners: Max Planck Insitute - Garching - Université de Strasbourg
- Contact: Philippe Helluy
- URL: http://selalib.gforge.inria.fr/

6.3. SCHNAPS

Solver for Conservative Hyperbolic Nonlinear Applications for PlasmaS
KEYWORDS: Discontinuous Galerkin - StarPU - Kinetic scheme
FUNCTIONAL DESCRIPTION: Generic systems of conservation laws. Specific models: fluids, Maxwell, Vlasov, acoustics (with kinetic representation). Multitasking with StarPU. Explicit solvers (RK2, RK3, RK4): accelerated with OpenCL Implicit solvers: through kinetic representations and palindromic time integration.

- Contact: Philippe Helluy
- URL: http://schnaps.gforge.inria.fr/

6.4. Slappy

KEYWORDS: Python - Opencl
FUNCTIONAL DESCRIPTION: The code Slappy solves the advection equations on multi-patch and non-conform complex geometries with the Semi-Lagrangian method. Using this we can also treat some hyperbolic/parabolic PDE with the Approximate BGK method which, allows to write a PDE as a transport plus a local relaxation step. The code is written in PyOpcenCL and can be used on CPU/GPU.

- Contact: Emmanuel Franck

6.5. Patapon

Parallel Task in Python
KEYWORDS: Python - Parallel computing - High order time schemes
FUNCTIONAL DESCRIPTION: Patapon is a code in PyOpenCL which allows to solve PDE like MHD using the vectorial Lattice Boltzmann method on Cartesian grids.

- Contact: Philippe Helluy

Coast Project-Team

5. New Software and Platforms

5.1. BeGoood

FUNCTIONAL DESCRIPTION: BeGoood is a generic system for managing non-regression tests on knowledge bases. BeGoood allows to define test plans in order to monitor the evolution of knowledge-bases. Any system answering queries by providing results in the form of set of strings can be tested with BeGoood. BeGoood has been developed following a REST architecture and is independent of any application domain. BeGoood is a part of the Kolflow infrastructure.

- Participant: Gérôme Canals
- Contact: Gérôme Canals
- URL: https://github.com/kolflow/begoood

5.2. MUTE

Multi-User Text Editor

FUNCTIONAL DESCRIPTION: MUTE (Multi-User Text Editor) is a web-based text editing tool that allows to edit documents collaboratively in real-time. It implements our recent work on collaborative editing algorithms and more specifically the LogootSplit+ approach. Compared to existing web-based collaborative text editing tool this editor does not require a powerful central server since the server is not performing any computation and acts as a simple broadcast server. Our editor offers support for working offline while still being able to reconnect at a later time.

- Participants: Claudia-Lavinia Ignat, François Charoy, Gérald Oster and Luc André
- Contact: Gérald Oster
- URL: https://github.com/coast-team/mute-demo/

5.3. Replication Benchmarker

FUNCTIONAL DESCRIPTION: The Replication Benchmarker is a performance evaluation framework for optimistic replication mechanisms used in collaborative applications. It contains a library of implementation of several CRDT (Commutative Replicated Data Type) and OT (Operational Transformation) algorithms for different data types: text, set, trees. The framework is able to evaluate the performance of comparable algorithms on different corpus of events traces. These events traces can be produced randomly according to different parameters, can be extracted from real real-time editing session that have been recorded, or can be automatically extracted from distributed version control repositories such as the one produced with Git. Performances of the algorithms are measured in term of execution time, memory footprint and merge result quality (compared to manual merge history stored in git repositories).

- Participants: Gérald Oster, Mehdi Ahmed-Nacer and Pascal Urso
- Contact: Pascal Urso
- URL: https://github.com/score-team/replication-benchmarker/

5.4. Rivage

Real-tIme Vector grAphic Group Editor

FUNCTIONAL DESCRIPTION: Rivage is a real-time collaborative graphical editor. Several users can edit at the same time and in real-time a graphical document, user changes being immediately seen by the other users. The editor relies on a peer-to-peer architecture where users can join and leave the group at any time. Each user has a copy of the shared document and user changes on the document copies are merged in real-time by using a CRDT (Commutative Replicated Data Type) algorithm.

- Participant: Claudia-Lavinia Ignat
- Contact: Claudia-Lavinia Ignat
- URL: https://github.com/stephanemartin/rivage/

RESIST Team

6. New Software and Platforms

6.1. Distem

KEYWORDS: Large scale - Experimentation - Virtualization - Emulation

FUNCTIONAL DESCRIPTION: Distem is a distributed systems emulator. When conducting research on Cloud, P2P, High Performance Computing or Grid systems, it can be used to transform an homogenenous cluster (composed of identical nodes) into an experimental platform where nodes have different performance, and are linked together through a complex network topology, making it the ideal tool to benchmark applications targetting such environments, or aiming at tolerating performance degradations or variations which are frequent in the Cloud or in other applications distributed at large scale (P2P for example).

RELEASE FUNCTIONAL DESCRIPTION: New features in Distem 1.3 include: (1) New network emulation parameters: loss, duplication, corruption, reordering and jitter, (2) Support for Debian Stretch, (3) Added many tests, (4) Moved project from GForge to GitHub (https://github.com/madynes/distem).

NEWS OF THE YEAR: New version 1.3

- Participants: Luc Sarzyniec, Lucas Nussbaum and Tomasz Buchert
- Partners: CNRS - Université de Lorraine - Loria - Grid'5000 - Inria
- Contact: Lucas Nussbaum
- URL: http://distem.gforge.inria.fr

6.2. Grid'5000

Grid'5000 experimental platform

KEYWORDS: HPC - Cloud - Big data - Testbeds

FUNCTIONAL DESCRIPTION: The Grid'5000 experimental platform is a scientific instrument to support computer science research related to distributed systems, including parallel processing, high performance computing, cloud computing, operating systems, peer-to-peer systems and networks. It is distributed on 10 sites in France and Luxembourg, including Lyon. Grid'5000 is a unique platform as it offers to researchers many and varied hardware resources and a complete software stack to conduct complex experiments, ensure reproducibility and ease understanding of results.

NEWS OF THE YEAR: This year's highlights include the first joint FIT-Grid'5000 school, and various improvements (update to Debian 9, several new clusters, etc.). More information on https://www.grid5000.fr/w/News

- Participants: Christian Pérez, David Loup, Frédéric Desprez, Laurent Lefèvre, Laurent Pouilloux, Marc Pinhède, Simon Delamare, Lucas Nussbaum, Teddy Valette and Alexandre Merlin
- Contact: Frédéric Desprez
- URL: https://www.grid5000.fr/

6.3. HTTP-NDN gateway

A gateway to transport HTTP over NDN

KEYWORDS: Internet protocols - Interoperability - Named Data Networking - Web - Network gateway

FUNCTIONAL DESCRIPTION: In order to creat an NDN island using our HTTP over NDN architecture, we propose two kinds of gateways: (1) an ingress gateway (iGW), which converts HTTP user requests into NDN messages and converts requested NDN messages into HTTP responses sent to the end-users, and (2) an egress gateway (eGW), the counterpart of the first one, which converts requested NDN messages into HTTP requests towards web sites and converts HTTP responses into NDN messages.

The whole thing can be considered as an HTTP proxy for the outsiders of the NDN network because the gateways represent the input(s) and output(s) of the NDN network island which can store the HTTP responses passing through. The gateway also features intelligent naming and cache management of web contents passing through the NDN network to better use the NDN architecture. Native NDN clients and NDN web servers can be present inside this NDN network, and they can communicate with the same mapping protocol used by the gateways to communicate with regular HTTP/IP clients or servers.

NEWS OF THE YEAR: First release

- Partner: Orange Labs

- Contact: Thibault Cholez

- URL: https://github.com/DOCTOR-ANR/NDN-HTTP-Gateway

6.4. micro-NDN

microservices for NDN

KEYWORDS: Named Data Networking - Network Function Virtualization - Microservices

FUNCTIONAL DESCRIPTION: micro-NDN proposes to split the main functions of an NDN (Named-Data Networking) router into multiple microservices and to orchestrate them. Currently, it implements seven microservices: five are usual functions of an NDN router as in the NFD forwarding deamon (http://named-data. net/doc/NFD/current), and two are proposed to improve security: - Name Router (NR): Route Interest packets to producers that have registered a prefix of the name of the packet, it is like the Forwarding Information Base (FIB) in an NDN router, - Backward Router (BR): Route back Data packets to the consumers that have asked for it, it is like the Pending Interest Table (PIT) in an NDN router, - Packet Dispatcher (PD): Select the right pipeline for each kind of packet, - Content Store (CS): Aims to store Data packets to reuse them later when reasked, like the Content Store (CS) in an NDN router, - Strategy Forwarder (SF): A more general way to apply strategy (fail-over, round-robin, etc.), - Signature Verifier (SV): Verify the signature of the NDN packet based on the trusted keys, - Name Filter (NF): Drop packets based on their name.

We also provide a central manager that can monitor and orchestrate all the microservices. It provides a web-based GUI and a REST API to dynamically manipulate the topology (spawn a microservice, link them, etc.). It can also trigger actions based on predefined rules, for example to scale-up a bottleneck component.

NEWS OF THE YEAR: First release

- Contact: Thibault Cholez

- URL: https://github.com/DOCTOR-ANR/NDN-microservices

6.5. ndnperf

tool for server-side evaluation of NDN throughput

KEYWORDS: Named Data Networking - Performance measure

FUNCTIONAL DESCRIPTION: NDNperf is a tool for NDN server-side performance evaluation and sizing purposes, in order to have an idea of the throughput a server can achieve when it has to generate and transmit NDN Data packets. It is very similar to iPerf and also needs a client and a server to perform the measurements while minimizing the number of instructions between Interest reception and Data emission. It exists in two flavors (Java and C++) and has the following features: - Periodic performance report: end-to-end throughput, latency, processing time, - Multi-threaded (one main thread for event lookup and N threads for NDN Data generation), - Able to use all the available signatures implemented in the NDN library, choose the size of the key, and the transmission size of Data packets, - Message broker implementation (Java version only, currently no update is scheduled).

NDNperf features many options regarding the signing process because we identified it as the main bottleneck of application performances.

NEWS OF THE YEAR: First release

- Contact: Thibault Cholez
- URL: https://github.com/DOCTOR-ANR/ndnperf

6.6. SCUBA

A Tool Suite for the automated security assessment of IoT environments

KEYWORDS: Cybersecurity - Internet of things - Machine learning - Artificial intelligence

FUNCTIONAL DESCRIPTION: IoT devices are used in different fields of application, not only for the general public, but also in industrial environments. SCUBA is tool suite for the security assessment of industrial and general public IoT devices. It mainly relies on collected information through passive and active scanning of a running IoT device in its exploitation environment to build its Security Knowledge Base (SKB). The knowledge base contains all relevant information of the device regarding its network communications extracted from PCAP files, the enumeration of its used hardware and software represented in the CPE (Common Platform Enumeration) format, the list of its known vulnerabilities in the CVE (Common Vulnerabilities and Exposures) format associated to their CWE (Common Weakness Enumeration) and CAPEC (Common Attack Pattern Enumeration and Classification) descriptions. The SKB is used by SCUBA to predict the intrusion chains associated to an IoT device and its environment. SCUBA tries to be as automated as possible to face the large scale and the great heterogeneity of IoT networks.

NEWS OF THE YEAR: First release

- Participants: Abdelkader Lahmadi, Frédéric Beck, Thomas Lacour and Jérôme François
- Contact: Abdelkader Lahmadi

6.7. Platforms

6.7.1. CPS Security Assessment Platform

During 2018, we have extended our Cyber-Physical systems security assessment platform with new hardware components including multiple types of Programmable Logic Controllers (PLCs), a small scale distribution and sorting testbed, and an experimental system modelled after a microgrid system. The physical platform is also extended with several IoT devices dedicated to residential networks (heating control, lightning system, home gateways, etc). The platform will be mainly used for building security assessment and evaluation experimentation on the available devices to identify and validate their associated attack patterns and discover new vulnerabilities. This platform is used as a testbed for the development carried on the SCUBA (see 6.6) tool suite to assess the security of IoT and SCADA systems.

ALICE Project-Team

6. New Software and Platforms

6.1. Graphite

Graphite: The Numerical Geometry Workbench

KEYWORDS: 3D modeling - Numerical Geometry - Texturing - Lighting - CAD - Visualization

SCIENTIFIC DESCRIPTION: Graphite is an experimental 3D modeler, built on top of the Geogram programming library. It has data structures and efficient OpenGL visualization for pointsets, surfacic meshes (triangles and polygons), volumetric meshes (tetrahedra and hybrid meshes). It has state-of-the-art mesh repair, remeshing, reconstruction algorithms. It also has an interface to the Tetgen tetrahedral mesh generator (by Hang Si). This year, Graphite3 was released. It is a major rewrite, based on Geogram, with increased software quality standards (zero warnings on all platforms, systematic documentation of all classes / all functions / all parameters, dramatically improved performances). It embeds Geogram (and optionally Vorpaline) with an easy-to-use Graphic User Interface.

FUNCTIONAL DESCRIPTION: Graphite is a dedicated software platform in numerical geometry that enables, among other things, 3D modelling and texture baking.

- Participants: Bruno Lévy, David Lopez, Dobrina Boltcheva, Jeanne Pellerin, Nicolas Ray and Samuel Hornus
- Contact: Bruno Lévy
- URL: http://alice.loria.fr/software/graphite

6.2. GEOGRAM

GEOGRAM : A functions library for geometric programming

KEYWORD: 3D modeling

FUNCTIONAL DESCRIPTION: GEOGRAM is a programming library with a set of basic geometric algorithms, such as search data structures (AABB tree, Kd tree), geometric predicates, triangulations (Delaunay triangulation, Regular triangulation), intersection between a simplicial mesh and a Voronoi diagram (restricted Voronoi diagram). GEOGRAM also includes a code generator for predicates (PCK: Predicate Construction Kit) and an efficient implementation of expansion arithmetics in arbitrary precision. GEOGRAM is shipped with WARP-DRIVE, the first program that computes semi-discrete optimal transport in 3D.

- Participant: Bruno Lévy
- Contact: Bruno Lévy
- URL: http://alice.loria.fr

6.3. OpenNL

Open Numerical Library

KEYWORDS: 3D modeling - Numerical algorithm

FUNCTIONAL DESCRIPTION: Open Numerical Library is a library for solving sparse linear systems, especially designed for the Computer Graphics community. The goal for OpenNL is to be as small as possible, while offering the subset of functionalities required by this application field. The Makefiles of OpenNL can generate a single .c + .h file, very easy to integrate in other projects. The distribution includes an implementation of the Least Squares Conformal Maps parameterization method.

RELEASE FUNCTIONAL DESCRIPTION: Latest version available as part of GEOGRAM:

∗ OpenMP parallel solver

∗ more compact data structures, X2 acceleration

∗ SuperLU weak coupling (dynamically loads SuperLU .so if available)

- Participants: Bruno Lévy, Nicolas Ray and Rhaleb Zayer
- Contact: Bruno Lévy
- URL: http://alice.loria.fr/index.php/software/4-library/23-opennl.html

6.4. IceSL

KEYWORD: Additive manufacturing
FUNCTIONAL DESCRIPTION: IceSL allows to model complex shapes through CSG boolean operations. Objects can be directly prepared and sent to a 3d printer for fabrication, without the need to compute an intermediate 3D mesh.

- Participants: Frédéric Claux, Jean Hergel, Jérémie Dumas, Jonas Martinez-Bayona, Samuel Hornus and Sylvain Lefebvre
- Contact: Sylvain Lefebvre
- URL: http://shapeforge.loria.fr/icesl/

6.5. LibSL

Simple Library For Graphics
KEYWORDS: 3D - Graphics
FUNCTIONAL DESCRIPTION: LibSL is a toolbox for rapid prototyping of computer graphics algorithms, under both OpenGL, DirectX 9 - 10, Windows and Linux.

- Participant: Sylvain Lefebvre
- Contact: Sylvain Lefebvre

6.6. 3DPrintScaffoldings

KEYWORDS: 3D - 3D modeling - Additive manufacturing
FUNCTIONAL DESCRIPTION: Support generation for additive manufacturing. Optimizes scaffolding made of vertical pillars and horizontal bars that are optimized to use minimal material, be easily removed and support the part at all stages of the fabrication process.

- Participants: Jean Hergel, Jérémie Dumas and Sylvain Lefebvre
- Partner: Université de Lorraine
- Contact: Sylvain Lefebvre
- URL: http://shapeforge.loria.fr/icesl/

6.7. VORPALINE

VORPALINE mesh generator
KEYWORDS: 3D modeling - Unstructured heterogeneous meshes
FUNCTIONAL DESCRIPTION: VORPALINE is a surfacic and volumetric mesh generator, for simplicial meshes (triangles and tetrahedra), for quad-dominant and hex-dominant meshes.

- Participant: Bruno Lévy
- Contact: Bruno Lévy
- URL: http://alice.loria.fr/index.php/erc-vorpaline.html

LARSEN Project-Team

6. New Software and Platforms

6.1. Limbo

LIbrary for Model-based Bayesian Optimization

KEYWORDS: Black-box optimization - C++ - Global optimization - Machine learning - Policy Learning - Bayesian optimization - Gaussian processes

FUNCTIONAL DESCRIPTION: Limbo is an open-source C++11 library for Gaussian processes and Bayesian Optimization which is designed to be both highly flexible and very fast. It can be used to optimize functions for which the gradient is unknown, evaluations are expensive, and where runtime cost matters (e.g., on embedded systems or robots). Benchmarks on standard functions show that Limbo is about 2 times faster than BayesOpt (another C++ library) for a similar accuracy.

NEWS OF THE YEAR: - publication of a paper in the Journal of Open Source Software - several bug fixes and performance improvement

- Partners: UPMC - Imperial College London
- Contact: Jean-Baptiste Mouret
- Publication: Limbo: A Flexible High-performance Library for Gaussian Processes modeling and Data-Efficient Optimization
- URL: http://www.resibots.eu/limbo

6.2. sferes2

A lightweight generic C++ framework for evolutionary computation

KEYWORDS: Evolutionary Algorithms - Evolution - Global optimization - Multi-objective optimisation

FUNCTIONAL DESCRIPTION: Sferes2 is a high-performance, multi-core, lightweight, generic C++11 framework for evolutionary computation. It is intently kept small to stay reliable and understandable.

Sferes2 relies heavily on template-based meta-programming in C++ to get both abstraction and execution speed.

NEWS OF THE YEAR: - integration of a new set of classes for quality diversity, based on Antoine Cully's paper (IEEE TEC, 2018) - new documentation in Sphinx - new random generator (more thread safe, C++11) - drop the C++98 support (now C++11 only)

- Partner: UPMC
- Contact: Jean-Baptiste Mouret
- Publication: Sferes_v2: Evolvin' in the Multi-Core World
- URL: http://github.com/sferes2/sferes2/

6.3. xsens_driver

KEYWORD: IMU driver

FUNCTIONAL DESCRIPTION: This is a driver for the third and fourth generation of Xsens IMU devices. The driver is in two parts, a small implementation of most of the MT protocol in Python and a ROS node. It works both on serial and USB interfaces.

These MT* devices can store their configuration and will retrieve it at each boot and then stream data according to this configuration. The node only forwards the data streamed onto ROS topics. In order to configure your device, you can use the mtdevice.py script (or the vendor tool on Windows).

RELEASE FUNCTIONAL DESCRIPTION: bug fixes

NEWS OF THE YEAR: version 2.1.0 (2017-04-14) - several bugfixes and a new option.

- Contact: Francis Colas
- URL: https://github.com/ethz-asl/ethzasl_xsens_driver

6.4. SeekPlans

KEYWORDS: Robotics - Depth map

FUNCTIONAL DESCRIPTION: The SeekPlanes software is a high-performance C99 micro library which seeks planes in a depth image. It provides the height, the pitch and the roll of the camera that takes the image, in order to use the same orthonormal model for multi-camera acquisition. In addition, this library provides all the image planes: walls, ceiling, but also the top of a table or a bed, etc. Ultra fast, written in full portable C99 with optional X86 vectorizations (SSE and/or AVX), it has been tested on Linux and Windows, in 32 and 64 bits, and also on a Raspberry PI model 3.

- Contact: François Charpillet

<div align="center">

MAGRIT Project-Team

</div>

6. New Software and Platforms

6.1. PoLAR

Portable Library for Augmented Reality

FUNCTIONAL DESCRIPTION: PoLAR (Portable Library for Augmented Reality) is a framework which aims to help creating graphical applications for augmented reality, image visualization and medical imaging. PoLAR was designed to offer powerful visualization functionalities without the need to be a specialist in Computer Graphics. The framework provides an API to state-of-the-art libraries: Qt to build GUIs and OpenSceneGraph for high-end visualization, for researchers and engineers with a background in Computer Vision to be able to create beautiful AR applications, with little programming effort. The framework is written in C++ and published under the GNU GPL license

- Contact: Erwan Kerrien
- URL: http://polar.inria.fr

6.2. Fast>VP

KEYWORDS: Vanishing points - Image rectification

FUNCTIONAL DESCRIPTION: Fast>VP is a fast and effective tool to detect vanishing points in uncalibrated images of urban or indoor scenes.

This tool also allows automatic rectification of the vertical planes in the scene, namely generating images where these planes appear as if they were observed from a fronto-parallel view.

It is the Matlab implementation of the algorithm described in [6].

- Contact: Gilles Simon
- URL: https://members.loria.fr/GSimon/fastvp/

6.3. NoLoDuDoCT

A non-local dual-domain cartoon and texture decomposition

KEYWORDS: Image analysis - Cartoon and texture decomposition

FUNCTIONAL DESCRIPTION: This is an algorithm decomposing images into cartoon and texture components. Spectrum components of textures are detected on the basis of a statistical hypothesis test, the null hypothesis modeling a purely cartoon patch. Statistics are estimated in a non-local way.

- Contact: Frédéric Sur
- URL: https://members.loria.fr/FSur/software/NoLoDuDoCT/

6.4. BSpeckleRender

A Boolean model for deformed speckle rendering

KEYWORDS: Boolean model - Monte Carlo estimation - Experimental mechanics - Displacement fields

FUNCTIONAL DESCRIPTION: This library implements a new method for synthesizing speckle images deformed by an arbitrary deformation field set by the user. Such images are very useful for assessing the different methods based on digital image correlation (DIC) for estimating displacement fields in experimental mechanics. Since the deformations are very small, it is necessary to ensure that no additional bias is introduced by the image synthesis algorithm. The proposed method is based on the Monte Carlo evaluation of images generated by a Boolean model.

- Contact: Frédéric Sur
- URL: https://members.loria.fr/FSur/software/BSpeckleRender/

MFX Team (section vide)

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

6. New Software and Platforms

6.1. dnnsep

Multichannel audio source separation with deep neural networks

KEYWORDS: Audio - Source Separation - Deep learning

SCIENTIFIC DESCRIPTION: dnnsep is the only source separation software relying on multichannel Wiener filtering based on deep learning. Deep neural networks are used to initialize and reestimate the power spectrum of the sources at every iteration of an expectation-maximization (EM) algorithm. This results in state-of-the-art separation quality for both speech and music.

FUNCTIONAL DESCRIPTION: Combines deep neural networks and multichannel signal processing for speech enhancement and separation of musical recordings.

RELEASE FUNCTIONAL DESCRIPTION: This version derives from version 1.0 (not 1.9). Differences concerns the use of a bidirectional long short-term memory (BLSTM) neural network, smoothing of the multichannel Wiener filter (MWF) over time and frequency, usage of the principal component of the MWF filter, adding a new generalized eigenvector beamformer with blind analytical normalization (GEVB) filter, and normalizing the training and test signals.

- Participants: Aditya Nugraha, Emmanuel Vincent and Antoine Liutkus
- Contact: Emmanuel Vincent

6.2. Dynalips-Player

High realistic lip synchronization for 3d animated characters

KEYWORDS: 3D animation - Graphics - Speech Synthesis

FUNCTIONAL DESCRIPTION: Dynalips provides a solution to synchronize precisely and automatically the movements of the lips of a 3D character with speech (we address 3D animation movies and video games). We have developed a demonstrator that illustrates the whole process: from audio + text to the generation of the animation trajectory, and controlling the animation of a 3D model (e.g. an avatar). The demonstrator is composed mainly by the player developed in Unity 3D (but can be used with any other system) and plays the animation synchronously with speech in realtime. It is possible to generate an animation for Autodesk Maya 3D.

NEWS OF THE YEAR: The whole lip-sync demonstrator is fully operational. From text and recorded speech, the system allows animating two different 3D models. The player is running on Unity 3D.

- Partners: Université de Lorraine - Sayens (SATT Grand Est)
- Contact: Slim Ouni
- URL: http://www.dynalips.com

6.3. KATS

Kaldi-based Automatic Transcription System

KEYWORD: Speech recognition

FUNCTIONAL DESCRIPTION: KATS is a multipass system for transcribing audio data, and in particular radio or TV shows in French, English or Arabic. It is based on the Kaldi speech recognition tools. It relies on Deep Neural Network (DNN) modeling for speech detection and acoustic modeling of the phones (speech sounds). Higher order statistical language models and recurrent neural network language models can be used for improving performance through rescoring of multiple hypotheses.

NEWS OF THE YEAR: New models have been trained for British English and evaluated on MGB data

- Contact: Dominique Fohr

6.4. VisArtico

Visualization of multimodal speech data

KEYWORDS: Data visualization - 3D movement - Speech processing - Videos

SCIENTIFIC DESCRIPTION: VisArtico is a multimodal data visualization software acquired by several systems: articulograph, motion capture, depth camera. This software makes it possible to visualize the positions of real or virtual sensors and to animate them simultaneously with acoustics. Regarding the articulatory data, the user has the possibility to visualise the contour of the tongue and the lips. It also makes it possible to find the midsagittal plane of the speaker, and to deduce the position of the palate, if this information is absent during the acquisition. The software makes it possible to display the segmentation at the level of sentences, words or phonemes. The goal is to provide an effective multimodal data visualization tool that can be useful to anyone studying speech production, audio-visual synthesis, or animation in a more general way.

FUNCTIONAL DESCRIPTION: VisArtico is a user-friendly software which allows visualizing multimodal data acquired by several systems : an articulograph (AG500, AG501 or NDI Wave), motion capture system, depth camera. This visualization software has been designed so that it can directly use the data provided by the different systems to display the spatial and temporal positions of the sensors (real and virtual), synchronized with the corresponding acoustic recordings. Moreover, for articulatory data, VisArtico not only allows viewing the sensors but also enriches the visual information by indicating clearly and graphically the data for the tongue, lips and jaw. Finally, it is possible to generate a movie for any articulatory-acoustic sequence. This software can be useful for researchers in speech production, audiovisual speech synthesis or articulatory speech analysis.

RELEASE FUNCTIONAL DESCRIPTION: The main improvement in this version is the ability to view a video that was recorded along with the articulatory or motion capture data. The software also allows for automatic speech segmentation.

NEWS OF THE YEAR: This year, we have added the possibility to visualize a video simultaneously with the multimodal data and the acoustic data. Several bugs have been fixed.

- Participants: Ilef Ben Farhat, Loïc Mangeonjean and Slim Ouni
- Partners: CNRS - Université de Lorraine
- Contact: Slim Ouni
- Publication: VisArtico: a visualization tool for articulatory data
- URL: http://visartico.loria.fr

6.5. Xarticulators

KEYWORDS: Medical imaging - Natural language processing

FUNCTIONAL DESCRIPTION: The Xarticulators software is intended to delineate contours of speech articulators in X-ray and MR images, construct articulatory models and synthesize speech from X-ray films. This software provides tools to track contours automatically, semi-automatically or by hand, to make the visibility of contours easier, to add anatomical landmarks to speech articulators and to synchronize images with the sound. In addition we also added the possibility of processing digitized manual delineation results made on sheets of papers when no software is available. Xarticulators also enables the construction of adaptable linear articulatory models from the X-ray or MR images and incorporates acoustic simulation tools to synthesize speech signals from the vocal tract shape. Recent work was on the possibility of synthesizing speech from 2D-MRI films, and on the construction of better articulatory models for the velum, lips and epiglottis.

RELEASE FUNCTIONAL DESCRIPTION: The new version allows MRI films to be processed and, above all, it offers a better transition from the shape of the vocal tract to the area function, which corresponds to an approximation of the vocal tract using a series of elementary tubes from the glottis to the lips.

NEWS OF THE YEAR: Improvements to the articulatory model which now takes into account "small" filiform articulators such as the epiglottis and velum using models using the central line. Improvement of the transition from the medio-sagittal 2D form of the vocal tract to the function of area.

- Contact: Yves Laprie
- Publication: Articulatory model of the epiglottis

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

6. New Software and Platforms

6.1. ARPEnTAge

Analyse de Régularités dans les Paysages : Environnement, Territoires, Agronomie
KEYWORDS: Stochastic process - Hidden Markov Models
FUNCTIONAL DESCRIPTION: ARPEnTAge is a software based on stochastic models (HMM2 and Markov Field) for analyzing spatio-temporal data-bases. ARPEnTAge is built on top of the CarottAge system to fully take into account the spatial dimension of input sequences. It takes as input an array of discrete data in which the columns contain the annual land-uses and the rows are regularly spaced locations of the studied landscape. It performs a Time-Space clustering of a landscape based on its time dynamic Land Uses (LUS). Displaying tools and the generation of Time-dominant shape files have also been defined.

- Partner: INRA
- Contact: Jean-François Mari
- URL: http://carottage.loria.fr/index_in_english.html

6.2. CarottAge

KEYWORDS: Stochastic process - Hidden Markov Models
FUNCTIONAL DESCRIPTION: The system CarottAge is based on Hidden Markov Models of second order and provides a non supervised temporal clustering algorithm for data mining and a synthetic representation of temporal and spatial data. CarottAge is currently used by INRA researchers interested in mining the changes in territories related to the loss of biodiversity (projects ANR BiodivAgrim and ACI Ecoger) and/or water contamination. CarottAge is also used for mining hydromorphological data. Actually a comparison was performed with three other algorithms classically used for the delineation of river continuum and CarottAge proved to give very interesting results for that purpose.

- Participants: Florence Le Ber and Jean-François Mari
- Partner: INRA
- Contact: Jean-François Mari
- URL: http://carottage.loria.fr/index_in_english.html

6.3. CORON

KEYWORDS: Data mining - Closed itemset - Frequent itemset - Generator - Association rule - Rare itemset
FUNCTIONAL DESCRIPTION: The Coron platform is a KDD toolkit organized around three main components: (1) Coron-base, (2) AssRuleX, and (3) pre- and post-processing modules.

The Coron-base component includes a complete collection of data mining algorithms for extracting itemsets such as frequent itemsets, closed itemsets, generators and rare itemsets. In this collection we can find APriori, Close, Pascal, Eclat, Charm, and, as well, original algorithms such as ZART, Snow, Touch, and Talky-G. AssRuleX generates different sets of association rules (from itemsets), such as minimal non-redundant association rules, generic basis, and informative basis. In addition, the Coron system supports the whole life-cycle of a data mining task and proposes modules for cleaning the input dataset, and for reducing its size if necessary.

- Participants: Adrien Coulet, Aleksey Buzmakov, Amedeo Napoli, Florent Marcuola, Jérémie Bourseau, Laszlo Szathmary, Mehdi Kaytoue, Victor Codocedo and Yannick Toussaint
- Contact: Amedeo Napoli
- URL: http://coron.loria.fr/site/index.php

6.4. LatViz: Visualization of Concept Lattices

- Contact: Amedeo Napoli
- URL: http://latviz.loria.fr/
- KEYWORDS: Formal Concept Analysis, Pattern Structures, Concept Lattice, Implications, Visualization

FUNCTIONAL DESCRIPTION.

LatViz is a tool allowing the construction, the display and the exploration of concept lattices. LatViz proposes some noticeable improvements over existing tools and introduces various functionalities focusing on interaction with experts, such as visualization of pattern structures for dealing with complex non-binary data, AOC-poset which is composed of the core elements of the lattice, concept annotations, filtering based on various criteria and a visualization of implications [70]. This way the user can effectively perform interactive exploratory knowledge discovery as often needed in knowledge engineering.

The LatViz platform can be associated with the Coron platform and extends its visualization capabilities (see http://coron.loria.fr). Recall that the Coron platform includes a complete collection of data mining algorithms for extracting itemsets and association rules.

6.5. OrphaMine: Data Mining Platform for Orphan Diseases

- Contact: Chedy Raïssi
- URL: http://orphamine.inria.fr/
- KEYWORDS: Bioinformatics, data mining, biology, health, data visualization, drug development.

FUNCTIONAL DESCRIPTION.

The OrphaMine platform enables visualization, data integration and in-depth analytics in the domain of "orphan diseases", where data is extracted from the OrphaData ontology (http://www.orpha.net/consor/cgi-bin/index.php). At present, we aim at building a true collaborative portal that will serve different actors: (i) a general visualization of OrphaData data for physicians working, maintaining and developing this knowledge database about orphan diseases. (ii) the integration of analytics (data mining) algorithms developed by the different academic actors. (iii) the use of these algorithms to improve our general knowledge of rare diseases.

6.6. Siren: Interactive and Visual Redescription Mining

- Contact: Esther Catherine Galbrun
- URL: http://siren.gforge.inria.fr/main/
- KEYWORDS: Redescription mining, Interactivity, Visualization.

FUNCTIONAL DESCRIPTION.

Siren is a tool for interactive mining and visualization of redescriptions. Redescription mining aims to find distinct common characterizations of the same objects and, vice versa, to identify sets of objects that admit multiple shared descriptions. The goal is to provide domain experts with a tool allowing them to tackle their research questions using redescription mining. Merely being able to find redescriptions is not enough. The expert must also be able to understand the redescriptions found, adjust them to better match his domain knowledge and test alternative hypotheses with them, for instance. Thus, Siren allows mining redescriptions in an anytime fashion through efficient, distributed mining, to examine the results in various linked visualizations, to interact with the results either directly or via the visualizations, and to guide the mining algorithm toward specific redescriptions.

New features, such as a visualization of the contribution of individual literals in the queries and the simplification of queries as a post-processing, have been added to the tool.

<div align="center">

SEMAGRAMME Project-Team

</div>

5. New Software and Platforms

5.1. ACGtk

Abstract Categorial Grammar Development Toolkit

KEYWORDS: Natural language processing - NLP - Syntactic analysis - Semantics

SCIENTIFIC DESCRIPTION: Abstract Categorial Grammars (ACG) are a grammatical formalism in which grammars are based on typed lambda-calculus. A grammar generates languages: the abstract language (the language of parse structures), and the object language (the language of the surface forms, e.g., strings, or higher-order logical formulas), which is the realization of the abstract language.

ACGtk provides two softwares to develop and to use ACGs: acgc, which is a grammar compiler, and acg, which is an interpreter of a command language that allows us, for instance, to parse and realize terms.

FUNCTIONAL DESCRIPTION: ACGtk provides softwares for developing and using Abstract Categorial Grammars (ACG).

NEWS OF THE YEAR: The new version extends the syntax for defining operators that can be used in grammars and removes dependencies to obsolete libraries. It also introduces some light optimizations compared to the previous one.

- Participants: Philippe De Groote, Jiri Marsik, Sylvain Pogodalla and Sylvain Salvati
- Contact: Sylvain Pogodalla
- Publications: A syntax-semantics interface for Tree-Adjoining Grammars through Abstract Categorial Grammars - ACGTK: un outil de développement et de test pour les grammaires catégorielles abstraites - Discourse Modeling with Abstract Categorial Grammars - On the expressive power of Abstract Categorial Grammars: Representing context-free formalisms - Towards abstract categorial grammars
- URL: http://acg.loria.fr/

5.2. Dep2pict

KEYWORDS: Syntactic analysis - Semantics

FUNCTIONAL DESCRIPTION: Dep2pict is a program for drawing graphical representation of dependency structures of natural language sentences. Dep2pict takes into account the modified format mixing surface and deep syntactic information used in deep-sequoia.

NEWS OF THE YEAR: The software was adapted to some extensions of the CoNLL format. A new Graphical User Interface (based on PyQt5) was built to replaced the previous one (https://gitlab.inria.fr/dep2pict/gui). It can be installed through PyPI (https://pypi.org/project/dep2pict-gui/)

- Contact: Bruno Guillaume
- URL: http://dep2pict.loria.fr/

5.3. Grew

Graph Rewriting

KEYWORDS: Semantics - Syntactic analysis - Natural language processing - Graph rewriting

FUNCTIONAL DESCRIPTION: Grew is a Graph Rewriting tool dedicated to applications in NLP. Grew takes into account confluent and non-confluent graph rewriting and it includes several mechanisms that help to use graph rewriting in the context of NLP applications (built-in notion of feature structures, parametrization of rules with lexical information).

NEWS OF THE YEAR: In 2018, the version 1.0 of Grew was released. The major novelties are a new implementation of lexical rules and the introduction of a Python binding (described in the book: Application of Graph Rewriting to Natural Language Processing)

- Participants: Bruno Guillaume, Guy Perrier and Guillaume Bonfante
- Contact: Bruno Guillaume
- Publications: Application de la réécriture de graphes au traitement automatique des langues - Application of Graph Rewriting to Natural Language Processing
- URL: http://grew.fr/

5.4. ZombiLingo

KEYWORDS: Syntactic analysis - Natural language processing - Lexical resource - Collaborative science
FUNCTIONAL DESCRIPTION: ZombiLingo is a prototype of a GWAP (Game With A Purpose) where gamers have to give linguistic information about the syntax of natural language sentence, currently in French, and later to other languages.
NEWS OF THE YEAR: The code was factorized and 3 independant librairies where built (available in the github project: https://github.com/gwaps4nlp/ to facilitate their usage in other projects.

- Authors: Bruno Guillaume, Karën Fort, Nicolas Lefebvre and Valentin Stern
- Contact: Karën Fort
- URL: http://zombilingo.org/