Integrating and opening research infrastructures of European interest

H2020-INFRAIA-2018-2020

Logipedia

Coordinator: Gilles Dowek (gilles.dowek@inria.fr)

Section 4

Members of the consortium

4.1 Individual Participants

4.1.1 Inria: Institut National de Recherche en Informatique et Automatique (FR)

Established in 1967, Inria is the only French public research body fully dedicated to computational sciences. It is a national operator in research in digital sciences and is a primary contact point for the French Government on digital matters. Under its founding decree as a public science and technology institution, jointly supervised by the French ministries for research and industry, Inria's missions are to produce outstanding research in the computing and mathematical fields of digital sciences and to ensure the impact of this research on the economy and society in particular. Inria covers the entire spectrum of research at the heart of these activity fields and works on digitally-related issues raised by other sciences and by actors in the economy and society at large. Beyond its structures, Inria's identity and strength are forged by its ability to develop a culture of scientific innovation, to stimulate creativity in digital research. Throughout its 8 research centres and its 220 project teams, Inria has a workforce of 2 400 employees (including 1600 researchers) with an annual budget of 231 million euros, 25% of which coming from its own resources. Inria's mission is to pursue excellent research in computer science and applied mathematics in order to play a major role in resolving scientific, societal and industrial challenges. Therefore, Inria actively collaborates with public and private bodies including strategic partnerships with large firms, SME's technology platforms and industrial clusters. Technology transfer is further enhanced by helping to launch new companies (since 1984, about 160 companies have stemmed from Inria) and by forming partnerships with innovative SMEs.

The institute is strongly involved in European programmes aimed at fostering scientific excellence, such as the European Research Council (58 Grants) or the Marie S. Curie Actions (24 projects in Horizon 2020).

Inria makes a firm commitment to Horizon 2020, with which the institute's strategic plan is aligned. The objective is to combine scientific excellence with a more focused consideration of major European and global societal challenges to which Inria can bring a key contribution. Inria is currently involved in more than 140 H2020 funded projects.

Inria is also playing a lead role in the development of the Knowledge and Innovation Community (KIC) EIT Digital as host of the French node. EIT Digital's ambition is to create for Europe a structure dedicated to technology transfer and innovation in the digital field. Besides EIT Digital, Inria is also a core partner of the KIC EIT Health.

Main tasks:

- Gilles Dowek is the coordinator of the project and leads WP9. He developed the Dedukti proof format and coordinated tools for translating other proof format to/from Dedukti.
- Frédéric Blanqui leads the WP8. He is a member of the steering committees of the Logic in Computer Science (LICS) and TYPES conferences, and of the International School on Rewriting (ISR).
- Stephan Merz leads the task **T6.7**. He is one of the designers and developers of the TLA$^+$ Proof System.
- Bruno Barras leads task **T6.1**.
- Enrico Tassi participates to **T1.6** and **T7.5**. He is a core developer of the Coq system and of the ELPI programming language (used in **T7.5**).

Publications, products or services:

- "Dedukti: a logical framework based on the $\lambda\Pi$-calculus modulo theory", by A. Assaf, G. Burel, R. Cauderlier, D. Delahaye, G. Dowek, C. Dubois, F. Gilbert, P. Halmagrand, O. Hermant and R. Saillard, Technical report, 2019.
- "A generalization of the Takeuti–Gandy interpretation", by B. Barras, T. Coquand and S. Huber. In Mathematical Structures in Computer Science, vol 25(5), pp 1071-1099, 2015.
- "TLA$^+$ Proofs", by D. Cousineau, D. Doligez, L. Lamport, S. Merz, D. Ricketts, H. Vanzetto. 18th Intl. Symp. Formal Methods (FM 2012).
- "ELPI: fast, Embeddable, λProlog Interpreter", by Cvetan Dunchev, Ferruccio Guidi, Claudio Sacerdoti Coen, Enrico Tassi. Proceedings of LPAR, Nov 2015.

Previous projects or activities:

- Stephan Merz is a core member of the team designing and developing the TLA$^+$ Proof System at the Joint Microsoft Research-Inria Centre. He also is a senior collaborator in the project *Matryoshka* (Principal investigator: Jasmin Blanchette, Vrije Universiteit Amsterdam, ERC Starting Grant 2016, Grant agreement no. 713999) on reducing the gap between efficient automated reasoning systems and more expressive interactive proof assistants.
- Bruno Barras has been a member of the ANR project Paral-ITP, led by Burkhart Wolff (University Paris-Saclay), which was targeting of advanced parallelisation techniques for Coq and Isabelle.

Infrastructures or technical equipments:

- Inria develops tools around the Dedukti proof format since 2009.
- Since 1984, Inria develops the Coq proof assistant which received in 2013 the ACM SIGPLAN Programming Languages Sofware and the ACM Software System awards.
- Since 2006 Inria has supported the development of the Mathematical Components library. Initially created to support the computer proof of the Odd Order Theorem, since 2012 the library is publicly distributed and has been used in many third party verification projects.
- Since 2008 Inria has supported the development of the TLA$^+$ Proof System.
- Inria hosts the Grid5K infrastructure for running large-scale computing experiments.

Persons primarily responsible for carrying out the proposed activities:

- **Bruno Barras** is a research scientist at Inria since 2000. His research focuses on the formal study of the metatheoretical properties of Type Theory and on designing efficient algorithms for type-checking and conversion modulo rewriting. He obtained his PhD in 1999 at the University Denis Diderot (Paris 7). In 2012, he participated to the IAS Special Year on Univalent Foundations in Princeton, which has been an important stepstone in the dissemination of Homotopy Type Theory. He received with other colleagues the ACM Software System Award 2013 for his contribution to the implementation of Coq.
- **Frédéric Blanqui** leads the WP8. He is a research scientist at Inria since 2003. His research interests are centred on the termination of programmes and the use of rewriting techniques in logics and proof assistants. He is the coordinator of the developments of the Dedukti interface and tactic language. He obtained his PhD (2001) at the University Paris-Sud and his habilitation (2012) at the University Denis-Diderot. He actively contributed to the development of the CPF language for termination certificates used in the international termination competition. He published about 35 papers in peer-reviewed international conferences and journals, and has been PC member of international conferences such as PPDP, RTA, FOSSACS, FSCD, ICTAC and CICM. He is now member of the steering committees of ISR, TYPES and LICS, and organised the 11th International School on Rewriting in Paris in 2019.
- **Valentin Blot** is a research scientist at Inria since 2019. His research focuses on the semantic interpretation of proofs and programs, in particular through realisability. He obtained his PhD in 2014 at École Normale Supérieure de Lyon. He published papers in the most recognised international conferences in the field, served on the program committee of national and international conferences and published papers in international journals.
- **Pierre Boutry** is a postdoctoral researcher in the STAMP Inria team at the research centre in Sophia Antipolis - Méditerranée since 2019. He obtained his PhD (2018) at the University of Strasbourg. His main research interest is in the formalisation of foundation of geometry. He published 9 papers in peer-reviewed international conferences and journals. He has been an invited speaker at the Logic Colloquium in 2019.
- **Arthur Charguéraud** is a research scientist at Inria since 2013. His research interests range from interactive programme verification and mechanised semantics of programming languages, to multicore programming.

He obtained his PhD (2010) at the University Paris Diderot. He published 27 papers in peer-reviewed international conferences and journals, and has been PC member of international conferences such as PPOPP, OOPSLA, ITP, and ESOP. He is the main developer of the TLC Coq library and of the CFML programme verification tool. He was recently funded by Inria for an "Exploratory Action" to develop a framework for user-guided interactive source-to-source optimisations, with formal correctness guarantees. He co-organises and designs tasks for the french version of the Bebras Contest, attended each year by 700.000+ pupils aged 8 to 18.

- **Gilles Dowek** is the coordinator of the project. He is a researcher at Inria and professor at the École normale supérieure de Paris-Saclay. He has previously been a professor at the École polytechnique and a consultant for the NASA Langley research centre. He has been active in several types of outreach activities, especialy by writinb books, articles in several magazines, a column in *Pour la Science*, and different types of live activities. He has published several textbooks, popular science books, and philosophy of science books. Some of them have been translated to Chinese, English, German, Greek, Italian, Korean, Romanian, and Spanish. He has been a member of two ethics committees: the CERNA, and then the CNPEN. He has been active in the promotion of Computer science education in K-12 in France. He has been the President of the Scientific Board of the French informatics society.
  His work addresses the formalisation of mathematics, the proof processing systems, the physics of computation, the safety of aerospace systems, and the epistemology and ethics of informatics. Together with Denis Cousineau, he is at the origin of the $\lambda\Pi$-calculus modulo theory. He is the head of the Deducteam group, where the logical framework Dedukti has been developed.
- **Hugo Herbelin** is a member of the πr^2 Inria team located in Paris. Former coordinator of the Coq development team, his research mixes contributions to proof theory and logical foundations and contributions to the development of the Coq proof assistant. His interests are moving towards the design and development of proof assistant features targeting mathematics the way mathematicians think about them.
- **Dominique Méry** is a professor of computer science at the University of Lorraine (Telecom Nancy) and head of the MOSEL team at LORIA in Nancy. He is a member of the Veridis project. His research interests are centred on the correct-by-construction design of software-based systems using refinement and on the verification of distributed algorithms, in particular proofs of safety and liveness properties. Among other contributions, he implemented an interactive proof assistant using Isabelle for deriving safety and liveness properties of SDL programs (CAV 1992) and the closed-loop model of a pacemaker with a heart model. He obtained his PhD (1983) and Thèse d'État (1993) degrees at the University of Nancy and joined University of Lorraine in 1993. He published papers in peer-reviewed international conferences and journals and has been a PC co-chair of conferences such as FM, iFM, TASE, and ABZ. He is member of the IFIP Working Group 1.3 on Foundations of System Specification and has been a junior member of IUF from 1995 till 2000.
- **Stephan Merz** is a senior research scientist and head of the VeriDis research group, as well as the deputy for science, at Inria Nancy – Grand Est. His research interests are centred on the formal specification and verification of distributed algorithms, in particular proofs of safety and liveness properties, as well as refinement relations between specifications expressed at different levels of abstraction. He is a main contributor to TLAPS, the TLA$^+$ Proof System. He obtained his PhD (1992) and habilitation (2002) degrees at LMU München and joined Inria in 2002. He has published more than 100 papers in peer-reviewed international conferences and journals and has been a PC chair of conferences such as iFM, ICFEM, and ITP. He co-founded the FRiDA (Formal Reasoning in Distributed Algorithms) series of workshops as well as the VTSA (Verification Technology, Systems, and Applications) summer school. He has been a member of the scientific directorate of Schloss Dagstuhl, as well as a member of the Inria Evaluation Committee and of the National Committee of Scientific Research in France.
- **Pierre Senellart** is head of the Inria team Valda at the Inria research centre in Paris. He received his PhD in 2007 from Université Paris-Sud. He has been a Professor in the Computer Science Department at the École normale supérieure (ENS, PSL University) in Paris, France since 2016, when he founded the Inria Valda team focusing on extracting *Value from data*. Before joining ENS, he was an Associate Professor (2008–2013) then a Professor (2013–2016) at Télécom Paris. He also held secondary appointments as Lecturer at the University of Hong Kong in 2012–2013, and as Senior Research Fellow at the National University of Singapore from 2014 to 2016. Pierre Senellart is currently holding a Chair within the Paris Artificial Intelligence Research Institute (PRAIRIE), and is a Research Fellow at the Centre on Regulation

in Europe (CERRE). His research interests focus around practical and theoretical aspects of Web data management, including Web crawling and archiving, Web information extraction, uncertainty management, Web mining, and intensional data management.

- **Enrico Tassi** is a member of the STAMP Inria team at the research centre in Sophia-Antipolis. He obtained his PhD (2008) at the University of Bologna and he joined Inria as research scientist in 2012. He is interested in the design and implementation of interactive provers and in high level languages for extending their functionalities. He is a core developer of the Coq system, the Mathematical Components library and the Elpi programming language. He regularly serves as PC member of international conferences such as ITP, CPP, PADL, MKM. He regularly organises schools on Coq and the Mathematical Components library.
- **Pierre-Yves Strub** is Teaching Assistant in Computer Sciences at École Polytechnique, France since 2016. During that time, and during time spent as a post-doctoral researcher at the IMDEA software institute (Madrid, Spain) and Microsoft/Inria Joint Lab (Paris, France), he has been contributing to the development and application of formal methods to security in general, and cryptography in particular. Starting with his PhD, Dr. Pierre-Yves Strub also works on the theory and practice of proof assistants with applications to security and mathematics formalisation. He has a strong and consistent track record of strong academic publications on this topic, and has applied the formal techniques and tools whose development he contributes to various aspects of cryptography, formally verifying security proofs for standard primitives and constructions. He has also contributed to the development of new techniques and tools for formally reasoning about differential privacy and side-channel countermeasures. He is one of the two main developers of the EasyCrypt tool (an interactive framework for verifying the security of cryptographic constructions in the computational model) and is strongly involved in the development of Jasmin (a framework for developing high-speed and high-assurance cryptographic software).

4.1.2 Unistra: Université de Strasbourg (FR)

Université de Strasbourg

Located in the heart of Europe, the University of Strasbourg is heir to a great tradition born of the humanism of the 16 th century.

On 1 January 2009 the University of Strasbourg was born - a unique and pioneering example of merging universities in France: Louis Pasteur, Marc Bloch and Robert Schuman. European by nature and international by design, the University's fundamental training and research goals include forging partnerships with European and international universities. Located on 4 campuses spread all over the city, the University of Strasbourg is one of the largest universities in France, with nearly 51 000 students (including 20 % of international students).

Certified Excellence Initiative (IdEx) - obtained in 2012 and definitively confirmed in 2016 by the national programme "Investissements d'Avenir - the University of Strasbourg strengthens its position as an internationally attractive university. Implementing innovative projects that foster excellence, the University of Strasbourg is involved in supporting its researchers and students. As a leading European centre for training and research, the University of Strasbourg has developed a strong French-German cooperation and is now a privileged partner among the Upper-Rhine universities.

The University is involved in national and European research projects within various programmes. Since 2009, the University of Strasbourg obtained 74 FP7 projects, 76 H2020 projects, 30 INTERREG IV projects, 29 INTERREG V projects and 375 projects under the French National Research Programme (ANR). Presently 107 ANR projects, 50 H2020 projects, 23 INTERREG V projects and 19 Erasmus+ projects (1 European University, 2 Erasmus Mundus master degrees, 5 Erasmus + strategic partnerships, 1 knowledge alliance, 1 capacity building project, 1 Erasmus + Sport project and 6 Jean Monnet actions - including 1 Centre of excellence) are active. It currently coordinates 42 EU projects and is preparing and awaiting the evaluation of approximately 40 proposals.

ICube: Created in 2013, the laboratory brings together researchers of the University of Strasbourg, the CNRS(Centre National de la Recherche Scientifique), in the fields of engineering science and computer science. In this context the IGG team focuses on geometric modelling, visualisation, constraint solving and formalisation of geometry. The member of the project focus on the formal definition of the geometric universe, proof of properties, automatic generation of geometric objects defined by a specification and deriving certified geometric algorithms. We work on computer science methods allowing to assist proofs, guarantee the correctness and the feasibility and, when possible, to insure automatically some task using Coq tactics or, geometric constraint solving. The results of

these researches can be exploited in geometric modelling, computational geometry, pure geometry, mathematics teaching.

Main tasks:

- Integration of the GeoCoq library in Logipedia: WP3, task **T3.3**. As maintainers of the GeoCoq library, the group can adapt the library for easier integration into Logipedia.
- Concept alignment for geometry: WP7, task **T7.2**.
- Animation of the club of users in education: WP8, task **T8.7**
- User interface for interactive theorem proving: WP4, task **T4.2**

Publications, products or services:

- "Changing Data Representation within the Coq System", by Nicolas Magaud. In TPHOLs'2003, volume 2758 of LNCS. Springer-Verlag, 2003.
- "Formalization of the Arithmetization of Euclidean Plane Geometry and Applications", by Pierre Boutry, Gabriel Braun, Julien Narboux. Journal of Symbolic Computation, Elsevier, 2019, Special Issue on Symbolic Computation in Software Science, 90, pp.149-168.
- "Proof-checking Euclid", by Michael Beeson, Julien Narboux, Freek Wiedijk. Annals of Mathematics and Artificial Intelligence, Springer Verlag, 2019, pp.53.
- "Towards A Certified Version of the Encyclopedia of Triangle Centers", Julien Narboux, David Braun. Mathematics in Computer Science, Springer, 2016.
- "Two Cryptomorphic Formalizations of Projective Incidence Geometry", by David Braun, Nicolas Magaud, Pascal Schreck. Annals of Mathematics and Artificial Intelligence, Springer Verlag.

Previous projects or activities:

- The French ANR project Galapagos ANR-07-BLAN-0329, focused on the formalisation of geometry, the formalisation of computational geometry algorithms and automatic theorem proving in geometry.
- Serbian-French Co-Operation grant EGIDE/Pavle Savic 680-00-132. This project deals with formalisation and automation of geometric reasoning.

Infrastructures or technical equipments:

- GeoCoq, by Michael Beeson, Pierre Boutry, Gabriel Braun, Charly Gries, Julien Narboux, 2018. swh:1:dir:97ce53176b7d5e89d069bc60f49c3fa186831307. GeoCoq is a library of formal proofs about foundations of geometry. It includes formalisations of Euclid's, Hilbert's and Tarski's geometry.

Persons primarily responsible for carrying out the proposed activities:

- **Julien Narboux** Julien Narboux is an associate professor at the Department of Computer Science, University of Strasbourg, France since 2007. He received a doctorate from University of Orsay in 2006 about "Formalization and automation of geometric reasoning". After that he held a postdoc positions at TUM. He published about 30 papers in peer-reviewed international conferences and journals, and has been PC member of international conferences and workshops such as ADG, AISC, SCSS, FVPS, ThEdu. He is the head of the steering committee of the Automatic Deduction in Geometry conference. Julien Narboux is the leader of the GeoCoq project.
- **Nicolas Magaud** is an associate professor at the Department of Computer Science, University of Strasbourg, France since 2005. He received a PhD from the University of Nice Sophia-Antipolis, France in 2003. His thesis subject was "changing data representation in the calculus of constructions". Before being hired by University of Strasbourg, he was a senior research associate at the University of New South Wales, Sydney, Australia. In Strasbourg, Nicolas Magaud has been working on formalising various aspects of geometry using Coq, spanning from computational geometry algorithms to exact real computations applied to discrete geometry. He published about 15 papers in peer-reviewed international conferences and journals.
- **Pascal Schreck** is full professor in computer science since 2002. He is interested in the formalisation of various geometries from the rule and compass constructions to finite incidence geometry including geometric algebras, Tarski and Wu's geometries *etc.* He studied some applications of theses formal geometries mainly in mechanical CAD and computer aided education.

4.1.3 INPT: Institut National Polytechnique de Toulouse (FR)

Institut National Polytechnique de Toulouse (INPT) is a French federation of 7 Higher Schools ("Grandes Ecoles") based in Toulouse. About 7 000 students are present on the 12 INPT sites, and the Engineering Schools awards about 1 300 Engineers diploma and INPT 150 PhD per year. A thousand researchers and research students work within 18 research units, most of which are associated with the CNRS or with the INRA organisations.

Research conducted in Computer Science and Information Technology at INPT takes place at IRIT (Institut de Recherche en Informatique de Toulouse), the imposing mixed research unit UMR 5505 at the national level (CNRS, INPT, Toulouse universities 1, 2 and 3). IRIT is composed of 270 researchers and research professors, on a global workforce of 700 people. It holds ERC grants and is involved in the 3IA (French Artificial Intelligence programme) with the Aniti project. The 20 research teams, are structured in 7 scientific topics (Information Analysis and Synthesis, Indexing and Information Search, Interaction, Autonomy, Dialogue and Cooperation, Reasoning and Decision, Modelisation Algorithms and High Performance Calculus, Architecture, Systems and Networks, Reliability of Systems and Software).

IRIT Safe software and/or system development group, named ACADIE belonging to the Reliability of Systems and Software group, aims at improving the costs and delays of software and more generally of system validation. This purpose is achieved by using, formal approaches (type theory and proof assistants, design of proof certified development methods, distributed systems modelling, refinement and proof, domain specific languages, static analysis for distributed object-oriented technologies). It has recognised competencies in the area of formal methods and refinement with expertise in the Event-B and Coq methods. Among the application domains of the conducted work are: first stepwise formal modelling, validation using animation and model checking and its application to substantial case studies related to avionic, robotic and medical domains. Several research projects have supported this work either locally or at the national or European level both with academic and industrial partners. Moreover, the team has also been reinforced by competencies issued from domain modelling, particularly in the engineering area.

All the researchers involved in LOGIPEDIA proposal are members of the ACADIE research team. They bring their expertise in 1) Type theory based formalisation of development processes and decision procedures; 2) Proof and refinement based formal methods: Event-B; 3) Type theory, type systems as formal proof systems; 4) Formal development and verification of distributed, real-time, hybrid, interactive systems; 5) Ontology based formal system engineering.

Main tasks:

- **T1.4** Instrument Atelier-B/Rodin. Design an import/export to/from Dedukti of Event-B machines, proof obligations and proofs. Experiments will be defined for validation purposes. The team has a long experience in meta-level reasoning within proof assistants, formal model transformation and verification.
- **T5.3** Reference ontology. Import/export to/from Dedukti of specific domain theories encoding knowledge domains in system engineering with a specific focus on transportation systems. Part of the team as a long experience in formal modelling based on ontologies and event-based modelling languages.

Publications, products or services:

- “Using Event-B for Critical Device Software Systems”, by Neeraj Kumar Singh. 2013, Springer Book ISBN 978-1-4471-5260-6, published by Springer-Verlag GmbH.
- “Making explicit domain knowledge in formal system development”, by Yamine Ait-Ameur and Dominique Méry. Science of Computer Programming SCP. Elsevier. Vol 121. 2O16.
- “Event algebra for transition systems composition Application to timed automata”, by Elie Fares, Jean-Paul Bodeveix, Mamoun Filali. In : Acta Informatica, Springer, Vol. 1, p. 1-38, 2017.
- “Proof-Based Approach to Hybrid Systems Development: Dynamic Logic and Event-B”, by Guillaume Dupont, Yamine Aït Ameur, Marc Pantel, Neeraj Kumar Singh. 6th International conference on state based formal method ABZ 2018. LNCS 10817. pp: 155-170

- "Mechanically Verifying the Fundamental Liveness Property of the Chord Protocol", by Jean-Paul Bodeveix, Julien Brunel, David Chemouil, Mamoun Filali. In : Formal Methods (FM 2019), LNCS 11800, pp. 45-63, 2019.

Previous projects or activities:

- **EBRP [2019-2023]** is a French ANR funded project, coordinated by IRIT, whose purpose is to enhance Event-B and the corresponding RODIN tool set by engaging in some basic research dealing with various mathematical theories that are not currently available in Event-B and RODIN. In order to validate this research a number of new case studies, issued from various engineering domains, will be performed.
- **DISCONT [2018-2022]** is a French ANR funded project dealing with the verification of the correctness of such hybrid systems formal models including both discrete and continuous behaviours. Correctness should arise from a design process based on sound abstractions and models of the relevant physical laws. In this project, the IRIT partner has developed a generic Event-B model together with Event-B theories for continuity and control theory. It has been applied to several hybrid systems.
- **MOISE [2015-2019]** (MOdels and Information sharing for System engineering in Extended enterprise) is a French IRT St Exupéry funded project. It targets the upstream part of the design cycle: after capturing user needs from the product definition phase and before the detailed design of system components. In this project, the IRIT partner has formalised architectural patterns with variability and their application to component-based models. Event-B has been used as the underlying semantic framework.
- **Comet IntegR [2015-2018]** In this Franco-Austrian project, the IRIT partner has developed a correct-by-construction Event-B model for characterising realisable choreographies. A formal Event-B development based on refinement and proof has been designed to synthesise asynchronous distributed systems communicating through FIFO channels whose behaviour is equivalent to a defined choreography.
- **FORMEDICIS [2017-2020]** is a French ANR funded project dealing with the design of critical human-computer interactive systems. The target application domain is aerospace interactive systems. A formal modelling language, named Fluid, has been designed to fill the gap between high level requirements and concrete interactive systems. Many formal verification techniques, among them Event-B (contribution of IRIT), have been applied on Fluid Models.
- **IMPEX [2013-2016]** Implicit and Explicit Semantics Integration in Proof Based Developments of Discrete Systems. The objective of IMPEX is to build formal models that explicitly take into account the context of the system under development. The correct system behaviour is then represented as a ternary relation between the requirements, the system, and its context. The project started in December 2013 and is funded by the French ANR. INPT-IRIT participates to this project coordinated by LORIA-VeriDis.

Infrastructures or technical equipments:

- Neeraj SINGH has developed the EB2ALL toolchain (downloaded more than 1500 times since 2011) for code generation from Event-B formal specification to in multiple programming languages.

Persons primarily responsible for carrying out the proposed activities:

- **Yamine Ait-Ameur** is full professor at INPT in Toulouse and member of the ACADIE research group at IRIT. His research addresses model heterogeneity reduction. Two main important aspects characterise his work. On the one hand the fundamental aspects are studied through the use of formal modelling techniques based on refinement and proof (in particular using Event-B), explicit formalisation of semantics using formal ontology models. On the other hand, practical aspects are addressed through the development of operational applications, allowing validating the proposed approaches. Embedded systems in avionics, engineering, interactive systems, CO2 capture, cyber physical systems are some of the application domains targeted by this work. Yamine Ait-Ameur has participated to several national and European research and industrial projects. He has published several research papers, edited special issues of international journals and he is the member the program committee of well established conferences in formal methods and ontology based modelling.
- **Jean-Paul Bodeveix** is full professor of Computer Science at Université Toulouse III - Paul Sabatier and member of the ACADIE research team. His research interests concern formal development methods, semantics of programming or modelling languages and formal verification of real-time systems and combine the use of model checking, theorem proving and refinement-based development. His Coq-based developments are related to the meta-modelisation of synchronous or real-time models for verifying semantic properties (determinism, timed-bisimulation). His work on refinement-based development are supported by the B

method and are about the verified development of protocols such as Chord. Work around real-time model checking was based on model transformations.

- **Mamoun Filali-Amine** is a CNRS researcher at IRIT (Toulouse Institute for Research in Computer Science) within the ACADIE team (Assistance to the Certification of Distributed and Embedded Applications). His research focuses mainly on specification, development by refinement and validation of distributed and real-time algorithms using assisted theorem provers and/or automatic provers. In the recent years, he has been more particularly interested in critical real-time embedded systems and more particularly in the study of architecture languages and the application of formal methods in this area.
- **Neeraj Kumar Singh** is an Associate Professor at INPT and member of ACADIE research since September 2015. He leads his research in the area of theory and practice of rigorous software engineering and formal methods to design and implementation of safe, secure and dependable critical systems related to automotive, medical, avionic and nuclear domains. He is an active participant to the Pacemaker Grand Challenge. He holds PhD in computer science from University of Lorraine, France (2011), entitled *"Using Event-B for Critical Device Software Systems"*. From 2012 to 2013, he was a research associate in the Computer Science Department of University of York, UK, working on the EPSRC funded project: High-integrity Java Applications using Circus (HiJaC). From 2013 to August 2015, he was a research fellow and team leader in the Centre for Software Certification (McSCert) at McMaster University, Canada, working on Ontario Research Fund - Research Excellence (ORF-RE) funded project: Certification of Safety Critical Software-Intensive Systems, and Automotive Partnership Canada (APC) funded project: Centre is the Network for the Engineering of Complex Software-Intensive Systems (NECSIS) for Automotive Systems. The results of his research works are published in more than 45 refereed articles in well known journals, books and international conferences.

4.1.4 UIBK: Universität Innsbruck (AT)

universität
innsbruck

The University of Innsbruck is a global Top-200 university and the second largest university in Austria. UIBK has been involved in a number of FWF projects related to formal proof, and a large number of national and international projects including dozens of projects as part of FP5, FP6, FP7, and H2020. The research of the Computational Logic group is concerned with the logical foundations of computer science and their application to the analysis and verification of complex systems. The group has developed the IsaFoR library, the largest formalisation of rewriting with more than 5000 theorems. Various hammer systems developed in the group are today strongest automation techniques for various formalisations including the Flyspeck project.

Main tasks:

- Specification of the Mizar logical foundations and type system, WP6, **T6.4**.
- Internal proof automation using direct proof term construction, WP2, **T2.4**.
- Contributions to automatic search for alignments using neural methods, WP7, **T7.3**.

Publications, products or services:

- "Semantics of Mizar as an Isabelle Object Logic", C. Kaliszyk and Karol Pąk, Journal of Automated Reasoning, 63(3): 557–595, 2019.
- "Aligning Concepts across Proof Assistant Libraries", T. Gauthier and C. Kaliszyk, Journal of Symbolic Computation, 90:89–123, 2019.
- "Hammer for Coq: Automation for Dependent Type Theory", Ł. Czajka and C. Kaliszyk, Journal of Automated Reasoning, 2018.

Previous projects or activities:

- 2017–2022, ERC starting grant, "Strong Modular proof Assistance: Reasoning across Theories".
- 2013–2017, FWF grant, "Interactive Proof: Proof Translation, Premise Selection, Rewriting"

Persons primarily responsible for carrying out the proposed activities:

- **Cezary Kaliszyk** has been working on making proof assistants more accessible by developing proof automation, proof advice, and other packages for formal proofs. He has worked on the Isabelle/Mizar object logic, where features of Mizar were expressed in a logical framework. Kaliszyk has also worked on machine learning for interactive proofs and has co-organised the AITP conference on the topic in the last

few years (AITP). He has developed multiple hammer systems for higher-order logic and intuitionistic type theory. Kaliszyk has also worked on alignments between formal systems and between informal and formal mathematics. These exactly correspond to the three tasks that Innsbruck will be involved in.

4.1.5 ULiege: Université de Liège (BE)

The University of Liège (ULiege) is located in the Fédération Wallonie-Bruxelles of Belgium in the Euregio region. ULiege is the only public and complete university institution of the French-speaking region of Belgium. The ULiege counts 2977 lecturers-researchers and 24688 students (incl. 2095 PhD students). 23% of the students at ULiege are foreign students from 127 different countries. A wide variety of fundamental and applied research projects have emerged from about 43 Faculty and 11 interfaculty Research Units. On the international level, the University of Liege is actively involved in research projects with more than seventy countries worldwide. ULiege has been involved in 191 European FP7 and H2020 projects and is active in 8 H2020 INFRA projects. At the end of 2018, 2093 research agreements were in progress, of which 1458 involved an international partner. In parallel, ULiege has developed an active policy in terms of technology transfer, resulting in the creation of more than 144 spin-off companies and in the ownership of 834 patents.

The Montefiore Institute is the electricity, electronics and computer science department of the Faculty of Applied Sciences of the University of Liège. It was founded in 1883. Research in the Software Reliability and Security group of the Montefiore Institute focuses on symbolic techniques for verification of systems. One objective is to study the theoretical properties of symbolic data structures based on finite-state automata and logical formulas. Another line of research, connected to the first, relates to automated reasoning, and more specifically, the satisfiability checking problem for large logical formulas, in particular those expressed in a combination of theories. Its main goal consists in engineering tools known as Satisfiability Modulo Theories (SMT) solvers, whose application field spans several areas of computer science, including verification. Automated reasoning is strongly linked to this project.

Main tasks:

- Pascal Fontaine is main leader of the WP8, co-leader of the WP2 and leader of task **T2.1**, and he will also be significantly involved in task **T2.2** and **T2.3**. He has been developing SMT solvers for two decades and has been a leader in the production of proofs for SMT solvers. He has been very active in several areas related to proof exchange for theorem proving (e.g. he is one initiator of the successful PxTP series on this topic). In this project, he will instrument ATPs to output proofs at the appropriate level of detail.
- Bernard Boigelot is an expert in arithmetic decision procedures, one subtle decision procedure w.r.t. proof output. In this project, he will help for the proof production for arithmetic.

Publications, products or services:

- "Scalable Fine-Grained Proofs for Formula Processing", by Haniel Barbosa, Jasmin Christian Blanchette, Pascal Fontaine. CADE 2017.
- "The SMT-LIB Standard: Version 2.6", by Clark Barrett, Pascal Fontaine, Cesare Tinelli, 2017.
- "Efficient Symbolic Representation of Convex Polyhedra in High-Dimensional Spaces", by Bernard Boigelot, Isabelle Mainz. ATVA 2018.
- "Theory Combination: Beyond Equality Sharing. Description Logic, Theory Combination, and All That", by Maria Paola Bonacina, Pascal Fontaine, Christophe Ringeissen, Cesare Tinelli, 2019.
- "Expressiveness + Automation + Soundness: Towards Combining SMT Solvers and Interactive Proof Assistants", by Pascal Fontaine, Jean-Yves Marion, Stephan Merz, Leonor Prensa Nieto, Alwen Fernanto Tiu. TACAS 2006.

Previous projects or activities: Members of the group have expertise in the field of automated theorem proving, notably SMT solving, and automata based symbolic techniques for arithmetic. They have been part of several national and international projects, including

- ANR-DFG SMArT (Programmes blancs 2013): 800k French-German project on Satisfiability Modulo Arithmetic Theories (2013-2017). Pascal Fontaine was leader.
- H2020-FETOPEN-2015-CSA SC-SQUARE: 350k Coordination and Support Action on Satisfiability Checking and Symbolic Computation (2016-2018). Pascal Fontaine was a principal investigator.

- European Research Council (ERC) Starting Grant 2016 Matryoshka (Grant agreement No. 713999): Fast Interactive Verification through Strong Higher-Order Automation (2017-2022). Pascal Fontaine is a senior collaborator.

Infrastructures or technical equipments:

- David Déharbe, Pascal Fontaine, Haniel Barbosa. The SMT solver veriT.
- Clark Barrett, Pascal Fontaine, Cesare Tinelli. The SMT-LIB language reference and library.

Persons primarily responsible for carrying out the proposed activities:

- **Bernard Boigelot** is professor at the University of Liège since 1999. His research interests mainly focus on computer-aided verification, particularly reachability analysis of infinite-state systems, and symbolic data structures and automata-based procedures for mixed integer and real arithmetic reasoning. He has designed the LASH toolset for representing infinite sets and exploring infinite state spaces. He has been PC member of international conferences such as TACAS, ATVA, IJCAR and RP, and workshops such as SPIN and INFINITY. He is a regular co-organiser of the annual VTSA Summer School on Verification Technology, Systems & Applications.
- **Pascal Fontaine** (co-leader of work package WP2) is a professor at the University of Liège since 2019. He obtained his PhD in 2004 in Liège and was maître de conférence at the University of Loraine in the Inria team VeriDis between 2004 and 2019. He obtained is habilitation (2019) at the University of Lorraine. His research interests focus on automated reasoning, and particularly on satisfiability modulo theories. He was PC member of international conferences such as CADE, FroCoS, IJCAI, IJCAR, SAT and Tableaux. He has been PC chair of the international conferences CADE and FroCoS, and the workshops PAAR, SC-square and SMT. Fontaine was co-founder of the PxTP (Proof eXchange for Theorem Proving) series of workshops. He is a member of the steering committees of CADE and SMT. He was co-organiser of the international Summer School on SAT and SMT, in Vienna 2014. He is one of the main developers of the veriT SMT solver, which, among its strong features, provides detailed unsatisfiability proofs. He is one of the three coordinators of the SMT-LIB initiative.

4.1.6 Unibo: Alma Mater Studiorum – Università di Bologna (IT)

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Founded in 1088, the Alma Mater Studiorum – Università di Bologna (UNIBO) is known as the oldest University of the western world. Nowadays, UNIBO still remains one of the most important institutions of higher education across Europe and the second largest university in Italy. UNIBO is organised in a multicampus structure with 5 operating sites and, since 1998, also a permanent headquarters in Buenos Aires: 11 Schools, 33 Departments, 12 Research and Innovation Centers and more than 84.000 students. The Alma Mater has already been partner or coordinator of more than 244 EU projects in the Horizon 2020 program, for a grand total of more than 100,000,000 euros.

The activity of the University of Bologna are conducted within the Department of Computer Science and Engineering (DISI), which is one of the top Computer Science and Engineering departments in Italy, offering a broad spectrum of expertise ranging from theoretical computer science to software, hardware and application design and development. DISI is currently member or coordinator of 12 on-going EU projects.

The research group that will be in charge of Logipedia at UNIBO is leaded by Dr. Claudio Sacerdoti Coen. The group is active in the areas of formal methods, interactive theorem proving and mathematical knowledge management, which are all relevant to the project.

Main tasks:

- WP1, task **T1.5**: Integrate the Matita translator in Matita itself. The participants to the project are the head developers of Matita.
- WP1, task **T1.6**: Instrument Coq. Sacerdoti Coen developed a Coq plug-in to export Coq libraries to XML. The plug-in was at the base of the MoWGLI project and it has been recently ported to the latest versions of Coq.
- WP5, task **T5.4**: Ontological Representation of Formal Libraries. Asperti and Sacerdoti Coen are experts in the Mathematical Knowledge Management field.

- WP7, task **T7.5**: Alignment-Based Proof-Rewriting. Sacerdoti Coen is a developer of ELPI, an high level language that allows to concisely express proof transformations. He also published papers on translations between procedural and declarative representations of proofs.

Publications, products or services:

- "Implementing type theory in higher order constraint logic programming", by F. Guidi, C. Sacerdoti Coen, E. Tassi. Mathematical Structures in Computer Science 29(8): 1125-1150 (2019).
- "Relational Data Across Mathematical Libraries", by A. Condoluci, M. Kohlhase, D. Müller, F. Rabe, C. Sacerdoti Coen, M. Wenzel. CICM 2019: 61-76.
- "ELPI: Fast, Embeddable, λProlog Interpreter", by C. Dunchev, F. Guidi, C. Sacerdoti Coen, E. Tassi. LPAR 2015: 460-468
- "User Interaction with the Matita Proof Assistant", by A. Asperti, C. Sacerdoti Coen, E. Tassi, S. Zacchiroli. J. Autom. Reasoning 39(2): 109-139 (2007)
- "A Content Based Mathematical Search Engine: Whelp", by A. Asperti, F. Guidi, C. Sacerdoti Coen, E. Tassi, S. Zacchiroli. TYPES 2004: 17-32

Previous projects or activities: Members of the group have expertise in the fields of Mathematical Knowledge Management and Interactive Theorem Proving, notably designing and implementing of theorem provers and building (web-)services for mathematical libraries. They have been part of several national and international projects, including

- FET-Open EU Project MoWGLI (Math on the Web: Get it by Logic and Interfaces). The project was focused on making the library of the Coq prover easily accessible outside the system and on the Web. MoWGLI explored independent verification, indexing, search and retrieval and transformation of proofs coming from Coq. All the previous services were implemented as web services using W3C technologies. Logipedia is more ambitious in aiming at providing the same services but for every system at once. They by-product of MoWGLI was the creation of the interactive theorem prover Matita.
- FET-Open EU Project CerCo (Certified Complexity). The project focused on formal proofs applied to formal methods in the domain of real time systems and complexity preserving compilation. The main technical tool employed was Matita.
- IST-2001-37057 MKMNET, the COST Action EUTypes and a number of previous successful European projects on Mathematical Knowledge Management and on Type Theory.

Infrastructures or technical equipments:

- The ELPI Higher Order Constraint Logic Programming language, co-developed with INRIA, a general purpose programming language that doubles as a domain specific language for the manipulation of logical and mathematical expressions and for the implementation of proof transformations.
- The interactive theorem prover Matita
- Web services developed in the MoWGLI EU project to provide access on the Web to Coq proofs, with indexing and searching capabilities.

Persons primarily responsible for carrying out the proposed activities:

- **Claudio Sacerdoti Coen Leader** is associate professor of computer science since 2015. He published more than 15 journal papers and 50 conference papers on Mathematical Knowledge Management, Interactive Theorem Proving and the theory of lambda-calculus. The most recent project he coordinated was the EU FET Open Project CerCo (Certified Complexity). He was also work-package leader for the EU FET Open Project MoWGLI (Math on the Web, Get it by Logic and Interfaces). He is one of the main developers of Matita and co-developer of the ELPI language.
- **Andrea Asperti** is full professor of computer science at the University of Bologna, one of the founders of the Mathematical Knowledge Management discipline and the previous coordinator of the HELM project that lead to the development of Matita. Before becoming an expert in interactive theorem proving he worked on category theory, lambda-calculus and linear logic. His current research interests also cover machine learning.

4.1.7 UBel: Matematički fakultet, Univerzitet u Beogradu (RS)

Founded in 1808, the University of Belgrade (Univerzitet u Beogradu) is the oldest and the largest higher educational institution in Serbia and one of the leading educational institutions in Central and Eastern Europe. The Faculty of Mathematics has a history of almost 150 years, with a number of well recognised researchers during this period. The Department of Computer Science at the Faculty of Mathematics builds upon the tradition going back to 1961. Today, the Department has around 50 academic staff, working in a range of computer science subfields, primarily artificial intelligence, automated reasoning, data mining, machine learning, optimisation, etc.

Automated Reasoning Group (ARGO) at Faculty of Mathematics, University of Belgrade (Mamematički fakultet, Univerzitet u Beogradu) is interested in automated reasoning, especially in SAT and SMT (satisfiability modulo theories), interactive theorem proving, automated theorem proving in coherent logic, automated reasoning in geometry, software verification and other applications of automated and interactive theorem proving. This research group is internationally visible and well recognised: over the last 10 years its eight members published around 50 articles at leading international conferences and in leading scientific journals, its members served on programme committees of several conferences, gave invited lectures, hosted more than 60 distinguished researchers from 20 countries, and organised a number of seminars and international workshops. The group members participated in several national and international projects and their results and tools are widely cited and used by users at academia, IT industry, and educational institutions.

Main tasks:

- Predrag Janičić participates at WP2, task **T2.1** and WP2, task **T2.2**. He coauthored three automated theorem provers for coherent logic, and worked on their applications and their links with other reasoning tools.
- Vesna Marinković participates in WP2, task **T2.3**. She is a coauthor of an automated theorem prover for coherent logic.
- Filip Marić and Danijela Simić participate at WP7, task **T7.2**. They are coauthors of several formalisations of geometry (Euclidean and hyperbolic) in Isabelle/HOL.
- Sana Stojanović Đurđević participates in WP7, task **T7.2**. She is a coauthor of an automated theorem prover for coherent logic, and the coautor of several interactive and automated formalisations of Euclidean geometry.

Publications, products or services:

- "Computer-Assisted Theorem Proving in Synthetic Geometry" by Julien Narboux, Predrag Janičić, Jacques Fleuriot. Handbook of Geometric Constraint Systems Principles (editors Meera Sitharam, Audrey St. John, Jessica Sidman), pp. 21–60, Chapman and Hall/CRC, Taylor & Francis Group, 2018. ISBN-13: 978-1-4987-3891-0
- "Proof Simplification in the Framework of Coherent Logic" by Vesna Marinković. Computing and Informatics, vol. 34, no. 2, pp. 337–366, 2015.
- "Formalizing Complex Plane Geometry" by Filip Marić, Danijela Petrović. Annals of Mathematics and Artificial Intelligence, November 2014, ISSN: 1012-2443, DOI: 10.1007/s10472-041-9436-4
- "Formalization and Implementation of Algebraic Methods in Geometry" by Filip Marić, Ivan Petrović, Danijela Petrović, Predrag Janičić. Electronic Proceedings in Theoretical Computer Science 79, pp. 63–81. ISSN: 2075-2180. DOI: 10.4204/EPTCS.79.4
- "A Coherent Logic Based Geometry Theorem Prover Capable of Producing Formal and Readable Proofs" by Sana Stojanović, Vesna Pavlović, Predrag Janičić. Automated Deduction in Geometry, ADG 2010, volume 6877 of Lecture Notes in Artificial Inteligence, pp. 200–219. Springer, 2011. DOI 10.1007/978-3-642-25070-5_12

Previous projects or activities:

- National grant (Ministry of science of Serbia) 174021 "Automated Reasoning and Data Mining" (2011-2019). Janičić was the grant holder.

- COST (EU) projekat IC0901 “Rich-Model Toolkit - An Infrastructure for Reliable Computer Systems” (2009-2013)
- Swiss fund SNF’s SCOPES grant IZ73Z0_127979 “Decision Procedures: from Formalizations to Applications” (2010-2013). Janičić was grant co-holder.
- Serbian-French Technology Co-Operation grant EGIDE/“Pavle Savic” 680-00-132/2012-09/12 “Formalization and automation of geometry” (2012-2013). Janičić was grant co-holder.
- COST project EUTypes CA15123 “The European research network on types for programming and verification” (2016–2020)

Infrastructures or technical equipments:

- Argo group has at its disposal a cluster computer with 32 dual core 2GHz Intel Xeon processors with 2GB RAM per processor. This computer can be used for carrying out computationally more demanding experiments needed within a project.

Persons primarily responsible for carrying out the proposed activities:

- **Predrag Janičić** received his PhD in computer science from the Faculty of Mathematics, University of Belgrade in 2001, where he now holds a position of a full professor. His main research interests are in the area of automated reasoning (automated theorem proving in coherent logic, automated and interactive proving of geometrical theorems, SAT/SMT) and mathematical software (dynamic geometry software, symbolic computation). He has published seven books, one book chapter and more than fifty research article in international journals and conferences. He gave six invited lectures, and served as a PC chair or a PC member at a number of international conferences, such as ADG, CICM, CADE, CADGME. He worked as a visiting researcher at the University of Edinburgh and visited a number of other universities. He is the author of the intelligent dynamic geometry tool GCLC and of the system URSA used for uniform reduction to SAT. He is also actively working on provers for coherent logic.
- **Filip Marić** received his PhD in computer science from the Faculty of Mathematics, University of Belgrade in 2009, where he now holds a position of an associate professor. His main research interests are in the area of interactive and automated theorem proving, and applications in formalising mathematics and verifying algorithm and software correctness. He authored and co-authored several university and high-school textbooks in informatics and programming, and more than 20 research articles in international journals and conferences. He had an internship at Google Inc., and had research visits at a number of universities. He is the author of the library ArgoLib of decision procedures and of the formally verified SAT solver called ArgoSAT. He is also the author of a language Stereos used for formulating 3d geometry constructions. He is one of the founders of Petlja Foundation with the aim of promoting and improving algorithmic literacy in Serbia, and is actively involved in organising programming competitions within Mathematical Society of Serbia.
- **Vesna Marinković** is an assistant professor at the Department of Computer Science, Faculty of Mathematics, University of Belgrade. She finished her PhD studies at the same faculty in 2015. Her main areas of research include automated reasoning in geometry and automated and formal theorem proving in coherent logic. She has more than 10 research articles in international journals and conferences. During 2009 she worked for three months as a visiting researcher at the Polytechnical University of Valencia, Spain. She is an author of a tool ArgoTriCS used for solving triangle construction problems in geometry and a co-author of a coherent logic prover ArgoCLP.
- **Danijela Simić** is a teaching assistant at the Computer Science Department, Faculty of Mathematics, University of Belgrade. She finished her PhD studies at the same faculty in 2017. Her main areas of research include interactive theorem proving and automated reasoning in geometry. Together with Filip Marić she is a co-author of many formalisations like formalisation of Poincaré disc model and formalization of complex geometry. She received the reward for excellency for her PhD thesis – Award from Mathematical Institute of Serbian Academy of Art and Science for PhD in computer science.
- **Sana Stojanović Đurđević** is a teaching assistant at the Department of Computer Science, Faculty of Mathematics, University of Belgrade. She finished her PhD studies at the same faculty in 2016. Her main areas of research include axiomatic systems, automated reasoning in geometry and automated and formal theorem proving in coherent logic. She is one of the authors of the coherent logic prover ArgoCLP and an author of programme ArgoChecker used for automated verification of semi-formal proofs.

4.1.8 TUM: Technische Universität München (DE)

The Technische Universität München (TUM) is characterised by a unique profile with its core domains natural sciences, engineering, life sciences and medicine. The institutional strategy is focused on strengthening the excellence of disciplinary core competences in research, teaching and learning, but is also targeted towards the promotion of ground-breaking, interdisciplinary research. TUM is committed toward the major challenges facing society in the 21st century in areas such as energy, climate, and environment, natural resources, health and nutrition, communication and information, mobility and infrastructure. The student body of TUM is currently more than 41 000 students and is constantly rising. TUM is regularly among the best national performers in international rankings. For the fifth time in a row, TUM took the first place among the German universities in the renowned QS World University Ranking (rank 55 worldwide). Looking at the contributions published in the particularly renowned academic journals of the "Nature" Group and the "Science" Group, TUM is positioning itself as number 42 and 1st in Germany. TUM was ranked 6th in the Global University Employability Ranking in which companies worldwide evaluate the quality of university graduates. The World University Ranking has rated the Technische Universität München (TUM) as one of the four best technical universities in Europe. TUM placed second in comparison to all other universities in Germany and was ranked number 43 worldwide. In 2012 and 2019, TUM has again secured the title “University of Excellence”.

Research and Training Programmes Previous Involvement in Research and Training Programmes: During the last two Framework Programmes for Research and Technological Development of the EC (FP7 and Horizon2020), TUM was and is involved in more than 500 EU research projects and has participated in over 100 ERC grants in total. Current involvement in Research and Training Programmes: Currently, TUM is involved in more than 200 Horizon 2020 projects, for more than 75 of which TUM has a coordinating role. That includes 28 ERC Starting Grants, 28 ERC Consolidator Grants, 14 ERC Advanced Grants, 5 ERC Proof of Concept Grants and 1 ERC Synergy Grant.

Main tasks:

- Nipkow leads WP3 and task **T3.2**. He heads the Isabelle project at TUM where the Analysis and Probability Theory library is being developed and he is one of the founding editors of the AFP.
- Wenzel is a subcontractor for WP1, task **T1.2** and WP3, task **T3.1**. He has been the chief technologist for Isabelle since 2008.

Publications, products or services:

- “Isabelle/HOL — A Proof Assistant for Higher-Order Logic”, by T. Nipkow, L. Paulson and M. Wenzel. Springer LNCS 2283, 2002.
- “Mining the Archive of Formal Proofs”, by J. Blanchette, M. Haslbeck, D. Matichuk and T. Nipkow. Springer LNCS 9150, pp. 3-17, 2015.
- “Interactive Theorem Proving — from the perspective of Isabelle/Isar”, by M. Wenzel. In: *All about Proofs, Proofs for All.* Ed. by B. Woltzenlogel Paleo and D. Delahaye. Vol. 55. Studies in Logic. College Publications, 2015.
- “From LCF to Isabelle/HOL”, by T. Nipkow, L. Paulson and M. Wenzel. *Formal Aspects of Computing* 31, pp. 675-698, 2019.

Previous projects or activities:

- A string of national and European projects to develop and use the Isabelle system. Most recently the EUR 1.25 million DFG Koselleck grant Verified Algorithm Analysis.

Infrastructures or technical equipments:

- The open-source theorem prover Isabelle jointly developed by Nipkow, Paulson and Wenzel.
- The Archive of Formal Proofs, an online open-access collection of proof libraries and larger scientific developments for the theorem prover Isabelle. It is organised in the way of a scientific journal. Nipkow is a co-founder, editor and maintainer.

Persons primarily responsible for carrying out the proposed activities:

- **Tobias Nipkow** (leader of work package WP3) is a full professor for Logic and Verification at TUM. He received his Ph.D. in Computer Science from the University of Manchester in 1987. He has been a lecturer at the University of Manchester (1984–1987), post-doctoral associate at MIT (1988–1989) and at Cambridge

University (1989-1992). He was appointed associate professor for Theory of Programming at TUM in 1992 and promoted to his current position in 2011. Since 2008 he has been Editor-in-Chief of the Journal of Automated Reasoning and is currently serving on the editorial board of Logical Methods in Computer Science. He founded the steering committee for the conference Interactive Theorem Proving in 2007 and served as its chair until 2017. He has served as a programme committee chair on a number of conferences in the general area of computational logic. Nipkow's main research interests are in computational logic, in particular, the design of interactive theorem provers (he is one of the designers of the Isabelle theorem prover), the design and semantics of programming languages and in particular the verification of functional and imperative programmes.

- **Makarius Wenzel** participates as a subcontractor. He is an independent provider of Isabelle prover technology located in Augsburg (since Sep-2014). Before, he has spent 4.5 years (2010–2014) at LRI / Univ. Paris-Sud to work on the Paral-ITP project, with Pr. Burkhart Wolff and further colleagues from the Coq development team. Earlier, he has worked many years at TU München with Prof. Tobias Nipkow in the Isabelle development team (1994–2010, exluding a few intermediate years). He received the title of Dr. rer. nat. in Feb-2002 from the Institut für Informatik, TU München. He served as the chief technologist, coordinator and release manager for Isabelle since 2008.

4.1.9 TUDelft: Technische Universiteit Delft (NL)

TU Delft

The Programming Languages Research Group at TU Delft is an internationally leading research group in programming languages, and active in areas such as language engineering, language design, domain-specific languages, software verification, and programme logics. Specifically, Dr. Jesper Cockx is an expert on the Agda system.

Main tasks:

- Jesper Cockx is the leader of WP1 and task **T1.1**. He is one of the main implementors of the Agda system and worked with Guillaume Genestier on a prototype of Agda2Dedukti.
- WP1, task **T1.1**: Encoding of features that rely on type-directed conversion – such as eta-equality and definitional irrelevance – in Dedukti (which does not have type-directed conversion).
- WP1, task **T1.1**: Investigating possible designs for a core language for Agda, in order to facilitate the exporting of Agda developments to Logipedia.
- WP1, task **T1.1**: Improving the current state-of-the-art on dependently typed languages with user-defined rewrite rules on areas such as confluence and termination checking.

Publications, products or services:

- "Pattern matching without K", by Jesper Cockx, Dominique Devriese, Frank Piessens. Proceedings of the 19th ACM SIGPLAN International Conference on Functional programming, ACM, 2014.
- "Unifiers as equivalences: proof-relevant unification of dependently typed data", by Jesper Cockx, Dominique Devriese, Frank Piessens. Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming, ACM, 2016.
- "Elaborating dependent (co)pattern matching", by Jesper Cockx, Andreas Abel. Proceedings of the ACM on Programming Languages, 2(ICFP), 2018.
- "Definitional proof-irrelevance without K", by Gaëtan Gilbert, Jesper Cockx, Matthieu Sozeau, Nicolas Tabareau. Proceedings of the ACM on Programming Languages, 3, 2019.

Previous projects or activities:

- Jesper Cockx has implemented a new version of the unification engine used by Agda for checking definitions by dependently typed pattern matching.
- He has also worked on extending Agda with user-defined rewrite rules similar to the ones found in Dedukti.
- In addition, he has extended Agda with a new universe `Prop` of definitionally proof-irrelevant propositions.

Infrastructures or technical equipments:

- The dependently typed programming language and proof assistant Agda (N.B. that although Agda was originally implemented in Göteborg, the continued development is now spread over several places across Europe, including Delft).

Persons primarily responsible for carrying out the proposed activities:

- **Jesper Cockx** (leader of work package WP1 and task **T1.1**) is an expert on the theory and implementation of Agda, a dependently typed programming language and proof assistant that is widely used within the programming languages community and beyond. He has worked on both foundational parts of Agda such as elaboration of dependent (co)pattern matching and new extensions such as rewrite rules and definitional proof irrelevance. He is also one of the main contributors to the implementation of Agda.

4.1.10 USaclay: Université Paris-Saclay (FR)

Université Paris-Saclay is a newly created university since the 1st of January 2020. Created from the merger of Université Paris-Sud and the community of universities and institutions "Université Paris-Saclay", it is recognised for its top level in fundamental science. Since 2006, scientists from the University were awarded two Fields medals, one Nobel Prize and a number of other international and national prizes. University Paris Saclay has a complete array of competences, ranging from the purest of exact sciences to clinical practices in medicine, covering life and health sciences, legal sciences and economics. Research at the University of Paris-Saclay, an essential part of academic understanding, is completed by research activities with a high valorisation potential. Located on the Paris-Saclay site, at the heart of the most influential private financial and research areas in Europe, Université Paris-Saclay is a significant driving force in the development of industries, particularly in high-tech and technology fields. 300 laboratories constitute the research potential of the Université Paris-Saclay. They cover all scientific disciplines that mobilise over 15,000 researchers, and PhD students.

Inside Université Paris-Saclay, the Laboratory for Computer Science (LRI) covers a wide spectrum of computer science. Its VALS team works in the Area of Verification and Validation of Algorithms, Languages and Systems, right in the heart of the scientific field of Formal Methods. Its group working on Logipedia will include Chantal Keller and Burkhart Wolff.

Main tasks:

- Chantal Keller is one of the two coordinators of WP2. She has strong expertise in interoperability between interactive and automatic theorem provers (ATPs). She is the leader of the SMTCoq project that links the Coq proof assistant with external ATPs. In this EU project, she will contribute to make automatic theorem provers interact with Logipedia: proofs will be exchange to and fro, ATPs will be used to check proofs from other systems and increase interaction between them, and to detect, organise and discharge theory alignments (**T7.3** of WP7).
- Burkhart Wolff is one of the two coordinators of WP5. He pioneered an Ontological Framework, which is currently mostly used for document ontologies and ontologies imposing a particular theory structure and typed meta-data. He implemented this framework in Isabelle/HOL, together with Prof. A.D. Brucker. In this EU project, his role is to supervise the conception and implementation of a Dedukti-oriented ontological framework. He will contribute to the conception of ontologies used for prover interoperability as well as domain-specific ontologies supporting advanced search and access mechanisms. As such, he has the role of a mediator between the technical needs for (efficient) alignments on the one hand and end-users of the Logipedia libraries needing advanced search mechanisms in order to access its mathematical knowledge.

Publications, products or services:

- “Importing HOL Light into Coq”, by Chantal Keller and Benjamin Werner, First International Conference on Interactive Theorem Proving, 2010.
- “A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses”, by Michaël Armand, Germain Faure, Benjamin Grégoire, Chantal Keller, Laurent Théry and Benjamin Werner, First International Conference on Certified Programs and Proofs, 2011.
- “SMTCoq: A Plug-In for Integrating SMT Solvers into Coq”, by Burak Ekici, Alain Mebsout, Cesare Tinelli, Chantal Keller, Guy Katz, Andrew Reynolds and Clark W. Barrett, 29th International Conference on Computer Aided Verification, 2017.
- “Using The Isabelle Ontology Framework: Linking the Formal with the Informal”, by Achim D. Brucker, Idir Ait-Sadoune, Paolo Crisafulli and Burkhart Wolff, 11th Conference on Intelligent Computer Mathematics, 2018.

- "Using Ontologies in Formal Developments Targeting Certification", by Achim D. Brucker and Burkhart Wolff, 15th International Conference on Integrated Formal Methods, 2019.

Previous projects or activities:

- Burkhart Wolff was a member of the ANR project Paral-ITP with the partners INRIA Roquencourt, INRIA Saclay (Bruno Barras) and U-PSud/LRI (B.Wolff, Project Leader), which was targeting of advanced parallelisation techniques for Coq and Isabelle.
- Burkhart Wolff was a member of the EU-Project EUROMILS (Oct. 2012 - Sept. 2015) and the ANR project PST, which were both targeting at applying Formal Methods in an industrial effort aiming at a high-level certification (Common Criteria EAL6, CENELEC SIL4). The latter project incited the development of Isabelle/DOF[1].

Infrastructures or technical equipments:

- Université Paris-Saclay participates in the development of the Coq and Isabelle interactive theorem provers.
- Université Paris-Saclay is the leader of the SMTCoq project since 2015.
- Université Paris-Saclay participates in the development of the Isabelle/DOF implementation of the Ontological Framework.

Persons primarily responsible for carrying out the proposed activities:

- **Chantal Keller** is Associate Professor at Université Paris-Saclay since 2015. She obtained her PhD (2013) at École polytechnique. Her research focus on the development, democratisation, use and interoperability of formal methods. She is a pioneer of interoperability between proof systems as the developer of one of the first tools to import proofs between two interactive theorem provers with very different underlying logics: HOL Light and Coq.
- **Burkhart Wolff** is Full Professor at Université Paris-Saclay since 2008. He has a strong background in interactive theorem proving for the modelling of languages semantics as well as applications to model-based testing. He recently proposed an ontological framework for document consistency and meta-data, which is implemented on top of Isabelle/HOL.

4.1.11 FAU: Friedrich-Alexander Universität Erlangen-Nürnberg (DE)

FAU is the second largest state university in the state Bavaria. It has 5 faculties, 23 departments/schools, 30 clinical departments, 19 autonomous departments, 656 professors, and about 40 000 students.

FAU has a strong departments of Computer Science and Mathematics (both 25 Professors) with strong groups in scientific computing, mathematical modelling, and simulation, data management, data visualisation, and Pattern recognition. All of these deal with mathematical data in some way and thus constitute a conducive and supportive environment for Logipedia. Importantly the collaborating departments constitute a reservoir of know-how and potential user expertise the Logipedia project can draw upon for evaluation and testing.

The site leader is Prof. Dr. Michael Kohlhase. PD Dr. Florian Rabe will be co-PI for the site.

Main tasks:

- The site co-leads WP5: Structure of the encyclopedia.
- The site leads task **T7.4**: Alignment-Based Search.

Publications, products or services: The site developed

- the OMDoc (Open Mathematical Document) format for representing mathematical knowledge[2], which anticipated much of the research proposed here,
- the MMT logical framework[3] (which uses OMDoc as its representation format), a close relative of Dedukti,
- the notion of alignments[4], which will be critical in WP7,
- the comprehensive representation of many major proof assistant libraries (albeit often proof objects) in OMDoc/MMT[5],

[1] Brucker and Wolff, "Isabelle/DOF: Design and Implementation", see n. 73.

[2] M. Kohlhase. *OMDoc – An open markup format for mathematical documents [Version 1.2]*. LNAI 4180. Springer Verlag, 2006.

[3] F. Rabe and M. Kohlhase. "A Scalable Module System". In: *Information & Computation* 0.230 (2013), pp. 1–54.

[4] Müller et al., see n. 94.

[5] M. Kohlhase and F. Rabe. "Experiences from Exporting Major Proof Assistant Libraries". under review. 2020.

- the MathWebSearch search engine for symbolic formulas knowledge[6].

Previous projects or activities:

- Prof. Kohlhase and Dr. Rabe were co-PIs of the OpenDreamKit H2020 infrastructure project (2015–2019) on virtual research environments that integrate mathematical computation systems.
- Prof. Kohlhase and Dr. Rabe are the PIs of the German-funded OAF project (2014–2020) about representing proof assistant libraries in logical frameworks, specifically the MMT framework.
- Prof. Kohlhase co-initiated and organised the three NTCIR community challenges for mathematics information retrieval in 2014/16/17.
- Prof. Kohlhase initiated and led the CALCULEMUS! IHP-Research and Training Network.
- Prof. Kohlhase participated in the FP6 IST MoWGLI (Mathematics on the Web: Get it by Logic and Interfaces) project.

Infrastructures or technical equipments:

- The site hosts http://mathhub.info, a portal for formalised mathematics, mathematical databases, and active mathematical documents. It hosts about 10GB of data (Theorem Prover Libraries, OEIS, semantic course materials and a multilingual mathematical glossary), serves it via the MMT system and a lightweight browser-based front-end, and includes services like 2D/3D theory graph visualisation of the modular structure.

Persons primarily responsible for carrying out the proposed activities:

- **Michael Kohlhase** holds the *Professorship for Knowledge Representation and Management* in the Computer Science Department. The KWARC (KnoWledge Adaptation and Reasoning for Content) Group headed by him specialises in knowledge management for Science, Technology, Engineering, and Mathematics (STEM), focusing on the last as a test subject. Formal logic, natural language semantics, and semantic web technology provide the foundations for the research of the group. Its group working on Logipedia will be composed of the following non-exhaustive list: Prof. Dr. Michael Kohlhase, Dr. Florian Rabe, Tom Wiesing, Dennis Müller, Jonas Betzendahl and Jan Frederik Schaefer.
- **Florian Rabe** obtained his PhD in 2008 and his habilitation in 2014 and is now Akad. Oberrat and Privatdozent in the KWARC group. Within the group, Kohlhase and Rabe co-advise most students and have shared the administration of research projects for 10 years. He is an expert in the design, implementation, and evaluation of representation languages for mathematical knowledge and meta-logical frameworks. He currently chairs the steering committee of *Logical Frameworks and Meta-Languages: Theory and Practice*. He is the main developer of the MMT language and system and the LATIN logic atlas and has designed and overseen the representation of proof assistant libraries in the OAF project.

4.1.12 ULeeds: University of Leeds (UK)

UNIVERSITY OF LEEDS

The University of Leeds is acclaimed world-wide for the quality of its teaching and research, and is ranked 93rd in the QS World University Rankings 2019. Leeds is in the top 10 universities in the UK (Times/Sunday Times, 2018). The results of the most recent Research Excellence Framework exercise (REF) identified that 82.76% of its research activity has a top quality rating of either 'world leading' or 'internationally excellent' which makes it a constant member of the UK's prestigious Russell Group of research intensive universities.

In 2017/18 it had an annual income of £715m and its annual research income exceeded £175m, of which 15.2% was derived from EU awards. The University includes the School of Mathematics, which hosts the Logic group, one of the strongest internationally, with expertise across the whole spectrum of logic and good links with the School of Computing.

Main tasks:

- Nicola Gambino leads **T7.1** and participates in **T6.1**. He is an expert on type theory, including Homotopy Type Theory, and categorical logic, with experience in computer-assisted proof-checking.
- Michael Rathjen participates in **T7.1**. He is a leading figure at international level on proof theory.
- Paul Shafer participates to **T7.1**. He is an expert in reverse mathematics and computability theory.

[6] M. Kohlhase, B. A. Matican, and C. C. Prodescu. "MathWebSearch 0.5 – Scaling an Open Formula Search Engine". In: *Intelligent Computer Mathematics*. LNAI 7362. 2012, pp. 342–357.

The combination of expertise available at Leeds makes the team uniquely placed to develop **T7.1**, as the task will require relating type theories, investigating their proof-theoretic properties and analyse the strength of some statements via reverse mathematics. Dr Gambino's experience in HoTT makes him ideally suited to help in **T6.1**.

Publications, products or services:

- "Homotopy-initial algebras in type theory", by S. Awodey, N. Gambino and K. Sojakova, *Journal of the Association for Computing Machinery*, 63 (6), 2017, 45pp.
- "The identity type weak factorisation system" by N. Gambino and R. Garner, *Theoretical Computer Science* 409 (1), 2008, pp. 94-109.
- "Relativized ordinal analysis: The case of Power Kripke-Platek set theory", by M. Rathjen, *Ann. Pure Appl. Logic*, 165(1), 2014, pp. 316-339
- "Constructive Zermelo-Fraenkel Set Theory, Power Set, and the Calculus of Constructions", by M. Rathjen, *Epistemology versus Ontology*, 2012, pp. 313-349.
- "The reverse mathematics of the Tietze extension theorem" by P. Shafer, *Proceedings of the American Mathematical Society*, 144, 2016, pp. 5359-5370.

Previous projects or activities:

- From Mathematical Logic To Applications (MALOA), EU ITN Network (FP7-PEOPLE), October 2009 – September 2013, Value: EUR 4.3M.
- EPSRC Standard Grant, "Homotopy Type Theory: Programming and Verification", joint project with the University of Nottingham and the University of Strathclyde, March 2015 – September 2019, Value: GBP 1.2M
- EPSRC Standard Grant, "Homotopical inductive types", May 2013 – June 2016, Value: GBP 283K.

Persons primarily responsible for carrying out the proposed activities:

- **Nicola Gambino** is Associate Professor in Pure Mathematics at the University of Leeds. His publication record includes papers leading journals in both mathematics (e.g. Memoirs of the AMS, Journal of the LMS) and computer science (e.g. Journal of the ACM, Theoretical Computer Science). He was a plenary invited speaker at the International Conference in Category Theory in 2016 and Logic Colloquium in 2000. His research has been consistently funded by EPSRC and the US Air Force for Scientific Research. He successfully supervised 4 PhD students and 1 PDRA. He serves on the editorial boards of Mathematical Structure in Computer Science and Applied Categorical Structures. Nicola Gambino's research focuses on type theory, categorical logic and category theory. He is one of the leading experts in Homotopy Type Theory, a subject to which he made fundamental contributions.
- **Michael Rathjen** is Professor of Pure Mathematics at the University of Leeds. His publication record includes about 100 papers. He has been an invited speaker at the International Congress of Mathematicians in 2006 and Logic Colloquium (6 times, most recently in 2019), as well as many other conferences in mathematical logic. His research has been consistently funded by the German Science Foundation, NSF, EPSRC, Leverhulme Trust and the Templeton Foundation. He successfully supervised 17 PhD students and 5 PDRAs. He serves on the editorial boards of Notre Dame Journal of Formal Logic, Oxford University Press Logic Guides, and Documenta Mathematica.
- **Paul Shafer** is Lecturer in Mathematical Logic at the University of Leeds. His publication record includes papers some of the top journals in mathematics (e.g., Transactions of the AMS, Proceedings of the AMS, Transactions of the LMS) and mathematical logic (e.g., Journal of Symbolic Logic, Annals of Pure and Applied Logic). He is frequently invited to speak at major meetings in mathematical logic (e.g., Logic Colloquium, ASL North American Annual Meeting). He has received prestigious fellowships from the Fondation Sciences Mathématiques de Paris (France) and the Fonds Wetenschappelijk Onderzoek (Belgium) as well as travel and exchange grants from EPSRC and the Royal Society. He has successfully supervised 1 PhD student.

4.1.13 UGot: Göteborgs Universitet (SE)

UNIVERSITY OF
GOTHENBURG

Founded in 1891, the University of Gothenburg is located in the city centre of Gothenburg and is home to 47,500 students and 6,000 employees across 39 departments. Strong research and attractive study programmes attract scientists and students from all around the world. The University of Gothenburg is environmentally certified and works actively for sustainable development.

The Logic and Types group at Gothenburg University has been a leading group in the research on dependent type theory and interactive theorem proving since the 1980's and has implemented several well known proof systems. Most recently the widely used Agda system, designed and implemented by Dr. Ulf Norell as part of his PhD thesis, and still actively developed by the group. The group also has a strong presence in formalised mathematics, led by professor Thierry Coquand and has received several European grants in this area.

Main tasks:

- Task **T1.1**: Instrumenting the Agda system to produce Dedukti proofs.
- Task **T1.1**: Investigating possible designs for a core language for Agda, in order to facilitate the exporting of Agda developments to Logipedia.

As an expert on the implementation of proof systems, and the Agda system in particular, Dr. Ulf Norell is exceptionally qualified to carry out these tasks.

Publications, products or services:

- "Towards a practical programming language based on depedent types", by Ulf Norell. PhD thesis, Chalmers University of Technology, 2007.
- "Interactive programming with dependent types", by Ulf Norell. Proceedings of the 18th ACM SIGPLAN international conference on Functional programming. 2013.

Previous projects or activities:

- Formalisation of Mathematics, an EU FP7 STREP FET-open project led by Thierry Coquand at University of Gothenburg. March 2010–July 2013, Grant nr. 243847.
- Formalization of Constructive Mathematics, an EU FP7 ERC Advanced Grant led by Thierry Coquand at University of Gothenburg. April 2010–March 2015, Grant nr. 247219.
- Types for Proofs and Programs, a Swedish Research Council project led by Thierry Coquand at University of Gothenburg. Jan 2013–Dec 2016. Grant nr. 2012-05294.
- Termination Certificates for Dependently-Typed Programs and Proofs via Refinement Types, a Swedish Research Council project led by Andreas Abel at University of Gotheburg. Jan 2015–Dec 2018. Grant nr. 2014-04864.

Infrastructures or technical equipments:

- The Agda proof system is developed by the Logic and Types group at Gothenburg University.

Persons primarily responsible for carrying out the proposed activities:

- **Ulf Norell** got his PhD from Chalmers University of Technology in 2007 on the design and implementation of dependently typed programming languages. After his PhD he continued as a PostDoc at Chalmers, and since 2011 he has been working as a research engineer at Gothenburg University. He is the main developer and maintainer of the Agda proof assistant, which is widely used in both research and teaching. He gave the keynote at ICFP 2013, and is a member of IFIP Working Group 2.8 on functional programming.

4.1.14 Chalmers: Chalmers Tekniska Högskola (SE)

CHALMERS UNIVERSITY OF TECHNOLOGY

Chalmers University of Technology conducts research and education in technology, science, shipping and architecture with an emphasis on sustainability at a global scale. Chalmers has 10 300 full-time students and 3 100 employees. Its Computer Science and Engineering Department is joint with Gothenburg University.

Chalmers' previous involvement in research and training programmes: During the last two Framework Programmes for Research and Technological Development of the EC (FP7 and Horizon2020), Chalmers was and is involved in 146 EU research projects and has participated in over 100 ERC grants in total. Current involvement in Research and Training Programmes: Currently, Chalmers is involved in more than 100 Horizon 2020 projects. To date, researchers at Chalmers have been granted 26 ERC Grants.

Main tasks:

- Myreen leads task **T1.3**. Myreen is a developer and expert user of HOL4. At Chalmers, he leads a research group of six people where everyone uses HOL4 as the primary tool for their work.
- Myreen leads task **T3.5**. He is a founding member of the team behind the verified CakeML compiler and proof tools built around CakeML.

Publications, products or services:

- "The verified CakeML compiler backend", by Tan, Myreen, Kumar, Fox, Owens, Norrish. Journal of Functional Programming, Cambridge University Press, 2019.
- "Self-Formalisation of Higher-Order Logic; Semantics, Soundness, and a Verified Implementation", by Kumar, Arthan, Myreen, Owens. Journal Automated Reasoning, Springer, 2016.
- "CakeML: A Verified Implementation of ML", by Kumar, Myreen, Norrish, Owens. In Principles of Programming Languages, ACM, 2014

Previous projects or activities:

- Myreen is PI on "Trustworthy software by programming and compiling in logic" (2017-2021) from the Swedish Foundation for Strategic Research. The grant is worth 12 million SEK (approx. 1.12 million EUR)

Infrastructures or technical equipments:

- The open-source verified CakeML compiler jointly developed by a group including Myreen.

Persons primarily responsible for carrying out the proposed activities:

- **Magnus O. Myreen** is an associate professor at Chalmers University of Technology. Myreen completed his PhD on programme verification at the University of Cambridge in 2009. His PhD dissertation was selected as the winner of the BCS Distinguished Dissertation Competition 2010. In 2012, Myreen became a Royal Society University Research Fellow. In 2014, Myreen moved to Chalmers where he became associate professor in 2015. He is a member of the steering committee for the conference on Interactive Theorem Proving and the streering committee for Certified Programmes and Proofs. Myreen regularly serves on programme committees for top conferences on the topic of mechanised reasoning and programming languages.

4.1.15 LMU: Ludwig-Maximilians-Universität München (DE)

Ludwig-Maximilians-Universität (LMU) is a public research university located in München, Germany. LMU consists of 18 faculties which accommodate various departments and institutes including the Mathematisches Institut, where the research group of mathematical logic is headed by Prof. Dr. Helmut Schwichtenberg. The research areas of the group are such as proof theory, realisability interpretation, programme extraction, constructive analysis, constructive algebra, and proof assistant. In particular in the research area of proof assistant, the logic group has been actively developing the Minlog system since early 1990's.

Main tasks:

- Encoding the underlying theory of Minlog in Dedukti. WP6: Theories **T6.3**
- Implementing the encoder, so that Minlog's libraries and formal proofs of constructive analysis is available in Dedukti with proof checking. The Logipedia integration level of Minlog is increased to 3 from 0. WP6: Theories **T6.3**
- Making Minlog's classical extraction available within Dedukti. Alignment for concepts in constructive analysis, in particular (co)induction/(co)recursion and predicativity. WP7: Proof engineering **T7.1**.

Publications, products or services:

- "Refined program extraction from classical proofs", by U. Berger, W. Buchholz, and H. Schwichtenberg. Annals of Pure and Applied Logic, 114:3–25, 2002.
- "Dialectica interpretation of well-founded induction", by H. Schwichtenberg. Math. Logic. Quarterly, 54(3):229–239, 2008.
- "Realizability interpretation of proofs in constructive analysis", by H. Schwichtenberg. Theory of Computing Systems, 43(3):583–602, 2008.
- "Basic Proof Theory", by A. S. Troelstra and H. Schwichtenberg. Cambridge University Press, second edition, 2000.

- "Proofs and Computations", by H. Schwichtenberg and S. S. Wainer. Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, 2012.

Previous projects or activities:

- 1997-2006, Speaker of the DFG-Graduiertenkolleg 301 "Logik in der Informatik"
- 2004-2008, LMU Coordinator of the EST (Early Stage Training) Programme "MathLogAps" (MEST-CT-2004-504029) of the EU, together with the universities of Leeds, Manchester, Lyon and ENS Lyon
- 2009-2013, LMU Coordinator of the ITN (Network for Initial Training) Programme PITN-GA-2009-238381 "MALOA" of the EU, together with the universities of Leeds, Manchester, Oxford, CNRS, Paris 7, Münster, Prague
- 2017-2021, LMU Coordinator of the 731143-CID project of LMU
- 05/2018-08/2018, Co-organiser (with D. Bridges, M. Rathjen and P. Schuster) of a Trimester on "Types, Sets, Constructions" at the Hausdorff Institute for Mathematics, Bonn

Infrastructures or technical equipments:

- The logic group at LMU has developed the Minlog proof assistant since 1990.
- The Minlog library for constructive analysis has been developed since 2004 and corecursion and coinduction have been involved since 2010.
- The Minlog feature for classical extraction has been developed since 2002.

Persons primarily responsible for carrying out the proposed activities:

- **Josef Berger** is a Privatdozent at LMU. He earned his Doctoral degree in 2002 from LMU, in Nonstandard stochastics, supervised by Horst Osswald, and his Habilitation in 2014 at LMU with a thesis on "Perspectives in Constructive Reverse Mathematics".
- **Nils Köpp** is a teaching assistant and a PhD student at LMU. Master thesis 2017 on "Automatically verified programme extraction from proofs with applications to constructive analysis".
- **Franz Merkl** is a professor and the chair of stochastics at LMU. He has supervised some Diploma theses on subjects in probability theory, which were formalised in Mizar. He himself has also worked with Mizar and published in the "Journal of Automated Reasoning", where only papers checked by Mizar are accepted.
- **Kenji Miyamoto** is a teaching assistant and a postdoc researcher at LMU. Doctorate 2013 at LMU with a thesis "Programme extraction from coinductive proofs and its application to exact real arithmetic". Worked as Postdoc and teaching assistant at LMU and in Innsbruck (with Georg Moser).
- **Iosif Petrakis** is a lecturer and a postdoc researcher at LMU. Doctorate 2015 at LMU with a thesis "Constructive Topology of Bishop Spaces". Presently preparing his Habilitation in Mathematics.
- **Helmut Schwichtenberg** is a professor (emeritus) of Mathematics at LMU. Book (with Stanley Wainer) on Proofs and Computations, Cambridge University Press, 2012. Book (with Anne Troelstra) "Basic Proof Theory", Cambridge University Press, 2nd ed. 2000. Coorganiser (with Douglas Bridges, Michael Rathjen and Peter Schuster) of the Hausdorff Trimester on Sets, Types and Constructions at the Hausdorff Institute, Universität Bonn, May-August 2018. Coorganiser (with Klaus Mainzer and Peter Schuster) of the annual Autumn School on Proofs and Computations.
- **Franziskus Wiesnet** is a PhD student co-supervised by Peter Schuster (Verona) and Helmut Schwichtenberg (LMU). Master thesis "Konstruktive Analysis mit exakten reellen Zahlen" 2017 at LMU. He is supported by a Marie Skłodowska-Curie fellowship of the Istituto Nazionale di Alta Matematica
- **Chuangjie Xu** is a postdoc researcher at LMU, holding a Humboldt grant. PhD 2015 in Birmingham under the supervision of Martin Escardo. Half of the theses consisted of an Agda implementation of the theoretical results achieved.

4.1.16 IMT: Institut Mines-Télécom (FR)

IMT (Institut Mines-Télécom) is a French institute that groups together 13 engineering and management graduate schools, around 12,300 students from Bachelor to PhD degrees. ENSIIE is an engineering school centred on applied mathematics and computer science; this school is associated to the IMT group. SAMOVAR is a research unit under the IMT umbrella that gathers researchers from Télécom SudParis (which is part of IMT) and ENSIIE. Its key domains are Applied Mathematics, Computer Science, Networks, IT applications and uses, Signal and

image processing. EUProofInfra participants are members of the METHODES team, whose research activities are devoted to optimisation, verification and performance evaluation.

Main tasks:

- Translate ATP traces into Dedukti WP2. Guillaume Burel leads Task **T2.2**; he is one of the experts on the translation of SAT-solver traces into Dedukti and on the reconstruction of TSTP traces.
- Automatic detection of alignments WP7. Stefania Dumbrava leads Task **T7.3**; she will be in charge of investigating approaches to aligning theories based on ontology reasoning methods. She is one of the experts on automated reasoning and databases.
- Export B models to Dedukti WP1. Catherine Dubois leads the Task **T1.4**. She developed the translator of FoCaLiZe into Dedukti and participated in the Bware project, concerning Dedukti-based proofs and B proof obligations.
- Expand the use of Logipedia within certification authorities WP8. Catherine Dubois also leads the Task **T8.6**. She has already worked with the French security agency, ANSII, to study the security of functional languages.

Publications, products or services:

- "CoqInE: Translating the Calculus of Inductive Constructions into the $\lambda\Pi$-calculus Modulo", by M. Boespflug and G. Burel. 2nd Intl. Workshop on Proof Exchange for Theorem Proving, 2012.
- "Translating HOL to Dedukti", by A. Assaf and G.Burel. 4th Intl. Workshop on Proof eXchange for Theorem Proving, 2015.
- "ML Pattern-Matching, Recursion, and Rewriting: From FoCaLiZe to Dedukti", by R. Cauderlier and C. Dubois. Proceedings of ICTAC, 2016.
- "FoCaLiZe and Dedukti to the Rescue for Proof Interoperability", by R. Cauderlier and C. Dubois. Proceedings of ITP, 2017.
- "Certifying Standard and Stratified Datalog Inference Engines in SSReflect", by V. Benzaken, E. Contejean, and S. Dumbrava. Proceedings of ITP, 2017.

Previous projects or activities:

- "BWare, A Proof-Based Mechanized Plate-Forme for the Verification of B Proof Obligations", funded by French National Research Agency, project manager: David Delahaye, 08/2012 – 12/2016

Infrastructures or technical equipments:

- Production of Dedukti proofs by automated theorem provers (iProverModulo)
- Reconstruction of proof traces (lrat2dk and Ekstrakto)
- Translation of proofs into Dedukti. (Coq proofs, HOL proofs, FoCaLiZe proofs)
- Interoperability of HOL and Coq through FoCaLiZe and Dedukti (proof of concept)

Persons primarily responsible for carrying out the proposed activities:

- **Guillaume Burel** is assistant professor at the ENSIIE since 2010. He defended his PhD, entitled "Good Proofs in Deduction Modulo", in March 2009. From September 2009 to August 2010, he was postdoctoral fellow at the Max Planck Institute for Informatics in Saarbrücken, Germany, in the research group on Automation of Logic. From September 2010 to December 2015, he was a member of the CEDRIC laboratory of the Cnam. Since January 2016, he is member of the SAMOVAR laboratory (UMR 5157 CNRS Télécom Sud Paris), where he belongs to the METHODES team. He was temporarily assigned to Inria-team Deducteam from September 2017 to August 2019. He has 4 publications in peer-reviewed international journals and 12 in international conferences ; he co-supervised 2 PhD theses, and he is co-supervising 1 PhD student and 1 postdoctoral fellow. He is the main developer of iProverModulo.
- **Catherine Dubois** is a professor at ENSIIE since 2000. She defended her PhD, entitled "Static determination of types for the SetL language", in 1989 and her Habilitation in 2000 entitled a *A journey from programming to proof*. She is a member of the Samovar laboratory (Télécom SudParis), in the METHODES team. Before, she was the leader of a research team at the CEDRIC laboratory (CNAM). Her research activities concern the application of formal methods (in particular with Coq, FoCaLiZe and B) and their combination with testing techniques. She supervised 10 Phd thesis and is currently supervising one PhD student. She participated to the translation of FoCaLiZe into Dedukti and the interoperability of Coq and HOL proofs through Dedukti. She is one of the task leaders of WP8.
- **Stefania Dumbrava** is an assistant professor at ENSIIE since 2019. She is also a permanent researcher in the SAMOVAR laboratory (UMR 5157 CNRS Télécom Sud Paris), where she belongs to the METHODES team. She obtained her PhD at Université Paris-Saclay in 2016 with a thesis on the formalisation of

relational and deductive databases. Her fields of expertise are theorem proving, in particular with the Coq proof assistant, and databases. This expertise is relevant for the research concerning automated alignment detection using reasoning engines. She is one of the task leaders of WP7.

4.1.17 UBia: Uniwersytet w Białymstoku (PL)

The University of Bialystok (UwB) was established in 1997 from a branch of Warsaw University after 29 years of its existence. Today UwB is one of the largest and strongest academic centres in North-Eastern Poland. It consists of nine faculties (including one located in Vilnius, Lithuania) and five institutes. Classes and lectures are delivered by approx. 850 academic teachers (nearly 200 are independent research scholars). At present UwB educates over 8000 students in almost 30 fields of study.

The Mizar research group at UwB has several decades of experience in designing formal languages for efficient encoding of mathematical data and implementing formal proof-checking software. The group coordinates the development of the Mizar Mathematical Library (MML) – a large centralised collection of formalised mathematical definitions, theorems and their proofs authored by over 260 contributors from 20 countries. The library is maintained and distributed in a variety of data formats, including interactive web-based documents and automatically generated natural language journal articles. The members of the group have participated in a number of EU funded research and collaboration projects, as well as the EUTYPES Cost Action. The Mizar group has also organised the MKM 2004 and CICM 2016 conferences.

Main tasks:

- Expressing the foundations of the Mizar logic in Dedukti. WP6: Theories **T6.4**
- Extracting in-depth knowledge from the Mizar proofs. WP6: Theories **T6.4**
- Developing Dedukti techniques corresponding to Mizar proof checking. WP6: Theories **T6.4**

Publications, products or services:

- "The role of the Mizar Mathematical Library for interactive proof development in Mizar", by G. Bancerek and C. Byliński and A. Grabowski and A. Korniłowicz and R. Matuszewski and A. Naumowicz and K. Pąk, Journal of Automated Reasoning **61**(1), pp. 9–32, 2018.
- "Mizar: State-of-the-art and Beyond", by G. Bancerek and C. Byliński and A. Grabowski and A. Korniłowicz and R. Matuszewski and A. Naumowicz and K. Pąk and J. Urban, Intelligent Computer Mathematics, International Conference, CICM 2015, Washington, DC, USA, July 13–17, 2015, Proceedings., (M. Kerber, J. Carette, C. Kaliszyk, F. Rabe, V. Sorge Ed(s).), Lecture Notes in Comput. Sci. vol. 9150, pp. 261–279, Springer, Berlin, 2015.
- "Semantics of Mizar as an Isabelle Object Logic", by C. Kaliszyk and K. Pąk, Journal of Automated Reasoning **63**(3), pp. 557–595, 2019.
- "Scalable Declarative Proof Translation", by C. Kaliszyk and K. Pąk, Tenth International Conference, Interactive Theorem Proving, ITP 2019, Portland, OR, USA. Proceedings, LIPIcs, Vol. 141, 35:1–35:7, 2019.
- "Higher-order Tarski Grothendieck as a Foundation for Formal Proof", by C.E. Brown and C. Kaliszyk and K. Pąk, Tenth International Conference, Interactive Theorem Proving, ITP 2019, Portland, OR, USA. Proceedings, LIPIcs, Vol. 141, 9:1–9:16, 2019.

Previous projects or activities: The Mizar research group has carried out several grants within European Union Framework Projects and also funded by Polish National Science Center and Office of Naval Research, US. The most related to the project are:

- "Isabelle Emulator for Mizar: Environment for Mizar Mathematical Library Re-verification", funded by Polish National Science Center, project manager: Karol Pąk, 7/2016–7/2019
- "Independent Verification of Mizar Logic", funded by the OeAD Scientific & Technological Cooperation with Poland, project coordinator at the Polish side: Karol Pąk, 5/2016–4/2018

- "Algorithms Concerning the Legibility of Natural Deduction Proofs", funded by Polish National Science Center, project manager: Karol Pąk, 7/2013–1/2017
- "Management of a Large Repository of Computer Verified Mathematical Knowledge", funded by Polish Ministry of Science and Higher Education, project manager: Andrzej Trybulec, 5/2009–5/2012
- "Types for Proofs and Programs", TYPES II EU FP6 510996, site of the project coordinated by Chalmers, 9/2004–8/2007

Infrastructures or technical equipments:

- Mizar proof-assistant – one of the pioneering systems for mathematics formalisation (since 1973).
- Mizar Mathematical Library – a centrally-managed mathematical knowledge base (established in 1989).

Persons primarily responsible for carrying out the proposed activities:

- **Czesław Byliński** is head of the Computer Networks Section at the University of Bialystok. He received his PhD in computer science from Shinshu University, Japan in 1998. Since 1978 he has been a member of the Mizar Project. He participates in the implementation of the Mizar language and the developing the Mizar system tools. Since 2014, he has been in charge of the Mizar implementation team.
- **Adam Grabowski** is an adjunct at UwB since 2006, with a focus on the formalisation of mathematics and computer science. He received his PhD in mathematics from the University of Silesia in Katowice, Poland in 2005 and PhD in computer science from Shinshu University, Nagano, Japan in 2005. Currently, he works on the application of automated proof assistants in the modelling of the reasoning under uncertainty: fuzzy and rough sets. He has authored over 120 papers in refereed journals and international conference proceedings, including over 70 formalisations in Mizar. He received twice the Śleszyński Prize (1998, 2000) granted by the Association of Mizar Users. Since 1999 he has been the head of the Library Committee of Association of Mizar Users, taking care of the management and development of the Mizar Mathematical Library.
- **Artur Korniłowicz** is the deputy director for science and head of the Department of Programming and Formal Methods at the Institute of Informatics at the University of Bialystok. Korniłowicz received his PhD in computer science from Shinshu University, Nagano, Japan in 2001. In 2017 he received habilitation from the University of Warsaw, Poland. Korniłowicz's main research interests are in formal verification of mathematics and verification of algorithms. He is one of the key developers of the Mizar proof-assistant and the author of over 100 Mizar formalisations. In 2005 he was awarded Śleszyński Prize for Formalisation of the Jordan Curve Theorem. In the period 7/2001–6/2002 Korniłowicz was a CALCULEMUS postdoctoral fellow at the Istituto per la Ricerca Scientifica e Tecnologica, Trento, Italy under the CALCULEMUS project within EU FP5; and in the period 7/2003–3/2005 he was a Japan Society for the Promotion of Science postdoctoral fellow at the Shinshu University, Nagano, Japan.
- **Adam Naumowicz** is a member of the core Mizar development team. With his background in mathematics and linguistics, he received his PhD in computer science in 2005 for research on formalising recent mathematical results. His recent works focus on extending Mizar checker's computational power, interacting with external tools and developing web-based services. He's been elected twice to serve as Mathematical Knowledge Management representative to the Steering Committee of Conference on Intelligent Computer Mathematics (CICM). He was also the main organiser of CICM 2016 held at the University of Bialystok. He acts as Poland's representative in the Management Committee of the European research network on types for programming and verification (Cost Action EUTypes).
- **Karol Pąk** has developed the Isabelle/Mizar system where he specified Mizar in the Isabelle logical framework giving the complete semantics of the system, including the underlying first-order logic variant, soft type system, and definitional mechanisms. Additionally, he proposed a semi-automatic translation of several MML articles to the resulting object logic to cross-verify them. Furthermore he has been developing methods that automatically improve readability of natural deduction proofs by the step order manipulation as well as lemma extraction.

4.1.18 ClearSy: ClearSy (FR)

CLEARSY
SAFETY SYSTEMS AND SOFTWARE

CLEARSY is an SME specialised in the development of safety critical software and systems in the fields of railways (main focus), microelectronics, information systems, defence, and automotive. Engineering activities include:

- The realisation of worldwide projects committed to achieving results in the design and/or validation of systems and software.
- A technical support activity in the fields of formal methods and operational safety..

CLEARSY engineers are skilled in various engineering domains (systems, mechanics, electronics, software, operational safety) and apply IT tools and an electronic laboratory to create prototypes and conduct trials. Collaborations with laboratories and industrial partnerships ensure the production of the various systems components (sensors and interfaces).

CLEARSY developed and has been maintaining for the past 20 years proof systems addressing the logic of B and Event-B. These systems are packaged in the Atelier B and Rodin platforms. They are used routinely by large European players in the railways domain to assist the development of safety-critical software such as automatic train control. CLEARSY also provides these actors technical assistance for the formal development of software and system, including proof-centric activities.

Specific expertise:

- Formal methods for the development of software and systems.
- Automatic theorem proving.
- Development of proof rule libraries and their validation.

Main tasks:

- WP1: task B-method.
- WP4: task *pp* theorem prover and connections to Zenon, ProB, SMT-Lib.
- WP8: dissemination to industrial and certification actors.

Publications, products or services:

- "Applying a Formal Method in Industry: A 25-Year Trajectory" by Thierry Lecomte, David Déharbe, Étienne Prun and Erwan Mottin. SBMF 2017: 70-87.
- "Web Service Compensation at Runtime: Formal Modeling and Verification Using the Event-B Refinement and Proof Based Formal Method", by Guillaume Babin, Yamine Aït Ameur and and Marc Pantel, IEEE Trans. Services Computing, Vol. 10, Num 1, p. 107–120, 2017.
- "Teaching an Old Dog New Tricks - The Drudges of the Interactive Prover in Atelier B" by Lilian Burdy and David Déharbe, ABZ 2018 Proceedings, p. 415-419, 2018.
- "Interfacing Automatic Proof Agents in Atelier B: Introducing "iapa"" Lilian Burdy, David Déharbe and Étienne Prun, F-IDE@FM 2016 Proceedings, p. 82-90, 2016.
- "Typechecking in the lambda-Pi-Calculus Modulo : Theory and Practice", by Ronan Saillard. Mines ParisTech, France, 2015.

Previous projects or activities: CLEARSY has been involved in several collaborative research projects:

- EU R&D projects: Reaims (1994-1995), FMERail (1998-2001), Matisse (2000-2003), Pussee (2001-2004), Rodin (2004-2007), and Deploy (2008-2012).
- French R&D projects: Forcoment (2001-2006), Equast (2002-2004), Verbatim (2003-2007), Rimel (2007-2010), Cercles-2 (2011-2014), DEPARTS (2012-2016)and BWare (2012-2015).

These projects are dedicated to the introduction of a formal method (B or Event-B) in the industry and through the development of dedicated tools and methods are addressing software and electronic based system development.

Infrastructures or technical equipments:

- CLEARSY maintains and develops Atelier B, an integrated development environment for software development with the B method and system modelling with Event-B.
- As part of Atelier B, CLEARSY maintains the theorem provers **pr**, based on conditional rewriting, and **pp**, based on tableaux calculus.
- The **pr** theorem prover is extensible with proof rules, it is being distributed with more than 3000 such rules, targetting primarily the expression language of the B method.
- Also as part of Atelier B, CLEARSY has developed proof obligation generators for different third-party proof systems, i.e. Why3, SMT-Lib, ProB.

Persons primarily responsible for carrying out the proposed activities:

- **David Déharbe** will be the site leader for CLEARSY. He obtained his PhD degree in Computer Science from Université Grenoble Alpes (France). He has held a software engineer position at CLEARSY since 2015, following an 18 year long academic career in UFRN (Brazil), where he was a key actor in the creation of the graduate studies in Computer Science, and a 2-year visiting research position at CMU (USA), where he developed a model checker for VHDL. He has published 40 conference papers and 18 journal papers, and has

been involved in several national- and international-level research projects. He has been in the programme committees of many scientific events. His research interests include formal methods and automatic proof techniques, and their application in industrial contexts. Gender: male.

- **Guillaume Babin** is a formal methods engineer at CLEARSY. After obtaining a PhD in Computer Science from Université de Toulouse (France), Guillaume joined CLEARSY to apply formal methods to safety-critical software systems in the transportation industry. He is interested in tooling, automation and the application of formal methods in industrial systems.
- **Lilian Burdy** is an expert in safety critical software. He has been participating to several safety critical software development since 1996, mainly in railway domain, but also in smart card domain. He has notably been working for Siemens, Gemplus, Alstom, Thales, RATP as employee or sub-contractor, being architect or developing safety critical parts of automatic train controllers, side-way equipments, etc. He has participated to several formal tools development, notably AtelierB for Clearsy or Jack for INRIA. He has published 12 conference papers and 3 journal papers, and has been involved in several national- and international-level research projects.
- **Maximilien Colange** holds a PhD in Computer Science from Université Pierre et Marie Curie (France). He followed an academic career in Switzerland and France during 5 years, during which he published a dozen conference papers. His research interests include formal methods, especially model-checking of both discrete and timed systems, and synthesis of reactive programmes. He now holds a software engineer position at CLEARSY, with a focus on formal methods tools.
- **Thierry Lecomte** is R&D Project Director. He has been involved in several formal methods oriented, R&D projects at European and French levels. His current subjects of interest include formal methods with proof, safety critical applications, safety computers. Gender: male.
- **Etienne Prun** is Activity Manager for CLEARSY. He was project manager in several industrial projects in property-driven software analysis and property-Driven systems analysis. He has managed several European and French R&D projects. He has been AtelierB development coordinator for 8 years. He was involved in teaching B methods in engineering school and for corporate training. His current research interests include safety system, safety software, with use of formal method with proof (automatic or not) in industrial context.
- **Ronan Saillard** holds a PhD in Computer Science from Mines ParisTech (France) where he worked on both theoretical and praticable aspects of the implementation of Dedukti, a typechecker for the $\lambda\Pi$-calculus modulo. He has held a software engineer position at CLEARSY since 2015. His research interests include programming languages, formal methods and their application in industrial contexts.

4.1.19 OcamlPro: OCamlPro (FR)

OCaml PRO

The software company OCamlPro was created in 2011. They harness their OCaml expertise and formal methods know-how to design, prototype, and build high quality software in demanding projects. Their team of PhD-level engineers also contributes open source development tools for the programming language OCaml, helping to improve the efficiency and usability of the OCaml compiler and tools (the free and open-source OCaml package manager OPAM, the optimising compiler flambda, the SMT Solver Alt-Ergo, etc.).

Main tasks:

- **T2.1**: Implement a proof trace output for the SMT solver Alt-Ergo. As the maintainers and main developers of Alt-Ergo, OCamlPro is uniquely competent in modifying the source code of Alt-Ergo for such a purpose. Additionally, Guillaume Bury already has experience generating formal proofs from an SMT solver as described in his PhD thesis[7].
- **T2.3**: Task leader on the translation of Dedukti statements into input format for automatic tools. As the developer of the Dolmen library for parsing input format for automatic tools, Guillaume Bury already has experience manipulating such formats, and is thus suited to leading this task aimed at translating Dedukti statements into such formats.
- **T4.3**: provide access to proofs using the open source opam package manager, now used as the official package manager of the OCaml community. As the author, developer and maintainer of opam, OCamlPro is again uniquely suited to leading this task given its unparalleled expertise on the opam package manager.

[7] G. Bury. "Integrating Rewriting, Tableau and Superposition into SMT". PhD thesis. Univ. Sorbonne Paris Cité, 2019.

Publications, products or services:

- Guillaume Bury's PhD thesis presented a new automated theorem prover, named Archsat, capable of generating formal Dedukti proofs. To date, Archsat and the tableaux-based theorem prover Zenon are the only two automated theorem provers able to produce Dedukti proofs.
- Dolmen is an OCaml library developed by Guillaume Bury, that deals with parsing and type-checking most input languages used in the automated theorem prover community.
- Opam is a source-based package manager developed by OCamlPro, which has been successfully used by the OCaml community since 2012, where it manages 2585 versioned packages for a total of 13196 combinations of package and version, guaranteeing its ability to connect people across large communities. Furthermore, opam is meant to provide management capabilities not only to OCaml, but to any language, which is why it is already used as a proof manager by the Coq community where it has been proven to be reliable and suited to managing formal proofs.

Previous projects or activities: French R&D projects:

- FUI LCHIP (2017-2020)
- ANR Vocal (2015-2020)
- ANR BWare (2013-2016)
- FUI HILITE (2010-2013)

Infrastructures or technical equipments:

- The Alt-Ergo solver[8] is an SMT solver developed and maintained by OCamlPro. It is used behind software verification tools such as Frama-C, SPARK, Why3, Atelier-B and Caveat.

Persons primarily responsible for carrying out the proposed activities:

- **Raja Boujbel** Raja holds a PhD in software deployment and multi-agent systems from University of Toulouse. Previously, she had studied functional programming and compiler design at Université Pierre et Marie Curie, then worked on the Opa language among MLstate's distribution team. She joined OCamlPro in March 2018 as a lead maintainer for opam, an open-source package manager for OCaml.
- **Guillaume Bury** Guillaume holds a research Master in computer science from Ecole Normale Supérieure in Paris, France, and has studied the integration of rewriting techniques inside SMT solvers during his PhD obtained under the direction of Gilles Dowek and David Delahaye in Deducteam at ENS Cachan. He joined OCamlPro in October 2018 and works in the Flambda team, on optimisations passes for the OCaml compiler.
- **Sylvain Conchon** Sylvain is a Professor of Computer Science at Université Paris-Saclay and currently on a sabbatical leave at OCamlPro. His research interests are at the crossroads of Model Checking, SMT solving, functional programming, and compilation techniques. He currently focuses on the design and development of the SMT solver Alt-Ergo and the SMT-based model checker Cubicle.
- **Albin Coquereau** Albin has a PhD in computer science, which he obtained for his work on improving the performance of the SMT solver Alt-Ergo. He also helped adding a support for the SMT-LIB standard in Alt-Ergo allowing it to participate to the SMTCOMP 2018.
- **Mattias Roux** Mattias Roux holds a PhD in computer science for his work on the model checker Cubicle, with an extension of the backward reachability algorithm. He now works at OCamlPro on the Alt-ergo theorem prover.

4.1.20 UoB: University of Birmingham (UK)

[8] S. Conchon et al. "Alt-Ergo 2.2". In: *Proceedings of the 16th International Workshop on Satisfiability Modulo Theories, SMT 2018*. 2018.

The University of Birmingham is one of the leading research-based universities in the United Kingdom. A distinctive characteristic of UoB is the wide breadth of research expertise. The last UK research assessment in 2014 confirmed that 87% of the University's research has global reach, meaning it is recognised internationally in terms of its originality, significance and rigor. The University is 79th in the 2019 QS World University Rankings, cementing its position in the top 100 universities globally and placing it 14th out of the 24 Russell Group universities to feature in the ranking. The School of Computer Science (CS) at UoB is world leading for its research. The School of Computer Science is home to one of world's leading theoretical computer science groups.

Main tasks:

- Ahrens will contribute to the import of the UniMath library of univalent mathematics into Dedukti, and to the specification of 2LTT and Cubical Type Theory in Dedukti, cf. **T6.1**. He is one of the main developers of UniMath, and has authored several papers on the syntax and semantics of type theories.
- Ahrens will provide training on Logipedia for students, researchers, and teachers, cf. **T8.3** and **T8.4**. He has taught type theory at the Midlands Graduate School, and has designed, organised, and run two one-week training events on univalent type theory. He has also been organising the HoTT/UF workshop 2017-present.

Publications, products or services:

- "UniMath — a computer-checked library of univalent mathematics", by V. Voevodsky, B. Ahrens, D. Grayson, and others
- "Univalent categories and the Rezk completion", by B. Ahrens, K. Kapulkin, and M. Shulman, Mathematical Structures in Computer Science 25 (2015), pp. 1010–1039
- Organisation of the School and Workshop on Univalent Mathematics, previously in 2017 and 2019, next planned for 2020
- Coorganisation of the Midlands Graduate School in the Foundations of Computing, yearly one-week school for participants from academia and industry, 1999-present

Previous projects or activities:

- EPSRC New Investigator Award "A theory of type theories", PI Benedikt Ahrens, ongoing

Infrastructures or technical equipments:

- UniMath — a computer-checked library of univalent mathematics
- Introduction to Univalent Foundations of Mathematics with Agda: textbook with accompanying computer-checked proofs in Agda, by Martín Hötzel Escardó

Persons primarily responsible for carrying out the proposed activities:

- **Benedikt Ahrens** is an expert in the development of mathematics in univalent foundations, and has written several works on category theory in univalent mathematics. In another strand of work, he develops syntax and categorical semantics for programming languages with features such as typing and operational semantics. He has recently received an EPSRC New Investigator Award for the development of a theory of type theories. Ahrens has designed and organised two schools on univalent foundations, with 60 participants and 10 mentors each. He has furthermore chaired the Workshop on Homotopy Type Theory and Univalent Foundations (HoTT/UF) in 2017, 2018, and 2020. He is currently a guest editor for Mathematical Structures in Computer Science, editing a special volume on HoTT/UF.

4.1.21 CEA: Commissariat à l'Energie Atomique et aux Energies Alternatives (FR)

CEA is a public multidisciplinary research organization whose research fields range from nuclear industry to biosciences and fundamental physics. It is made of several research centres located in France. CEA repre- sents: 15024 employees, 2.7 B Euros budget, 1689 patents registered or active, 1300 contracts signed with industry, 83 new companies created since 1984 in high technologies sectors, 9 research centres. In HORIZON 2020, CEA is already involved in more than 100 projects. The CEA LIST ("Laboratoire d'Intégration de Systèmes et des technologies") department is part of CEA TECH, the CEA Technological Research Division. CEA LIST combines

basic research and industrial R&D and is primarily concerned with the development of technologies that combine software and hardware to form highly integrated complex systems. The research activities are structured into three major themes: em- bedded systems, interactive systems and sensors and signal processing. CEA LIST focuses on methods and tools for the design of embedded systems with appropriate architectures, software, and an optimal level of safety. Within CEA LIST, the LSL ("Laboratoire de Sureté et de Sécurité des Logiciels", Software Safety and Secu- rity Lab) is focused on the verification & validation of software and hardware components. The LSL devel- ops methods and tools for the static analysis and test case generation of safety-critical applications. CEA LIST has participated to several international and national research projects in the above mentioned fields, within the FP6, FP7, RNTL, ANR and ITEA Programmes. In particular, LSL develops Frama-C since 2005. Since the initial release of the platform in 2008, LSL actively maintains and extends the kernel and a growing set of analysis plugins. An important part of Frama- C's development is done through close interaction with users during collaborative projects. In particular, one can cite ANR projects CAT and U3CAT, and FP7 project STANCE. Generally, when successful mature technologies emerge, they are transferred from CEA to its partners by means of the following mechanisms: 1) Joint Laboratories, consisting of specific contracts aiming at transfer- ring some well-defined intellectual property from CEA to industry, possibly using a team of dedicated per- sonnel, 2) patents and intellectual properties sale, and 3) the creation of start-up companies. Concerning the methods and tools developed by LSL , once validated on representative industrial applications, they are disseminated through 1) an open source distribution platform (such as OPEES1), 2) by direct industrial contracts or 3) transferred to companies commercialising such tools.

Main tasks:

- François Bobot leads the task **T2.5**. He is one of the designers and developers of the Why3 Tool.
- Allan Blanchard participates to task **T2.5**. He is a core developer of the Frama-C Platform.

Publications, products or services:

- "Why3: Shepherd Your Herd of Provers", by F. Bobot and J-C. Filliâtre and C. Marché and A. Paskevich, Boogie 2011, First International Workshop on Intermediate Verification Languages.
- "Qed. Computing What Remains to Be Proved", by L.Correnson, NASA Formal Methods - 6th International Symposium (NFM 2014).
- "Towards Full Proof Automation in Frama-C Using Auto-active Verification", A. Blanchard and F. Loulergue and N. Kosmatov, NASA Formal Methods, May 2019, (NFM 2019).

Previous projects or activities:

- The H2020 DECODER project aims at providing a unified interface for storing and querying any kind of information related to a given software project, from initial requirements to code to formal specifications and analysis results, including proof artifacts. It would of course be very beneficial for both projects to agree on a common exchange format for such objects, and coordination with the DECODER consortium (in which CEA acts as technical leader) will seek to achieve that.

Infrastructures or technical equipments:

- CEA members are the main developers of the Frama-C platform for C verification since 2005.
- CEA members participate in the development of Why3, since 2009, and CVC4, since 2012.
- CEA has access to industrial use-cases (e.g. Aeronautic, energy) which could be improved by Logipedia new certification methods and sharing of model.

Persons primarily responsible for carrying out the proposed activities:

- **Allan Blanchard** is an engineer-researcher at CEA since 2019. He is interested in the analysis of concurrent code using formal methods and more precisely using deductive verification.
  He obtained his PhD in Computer Science from the University of Orléans in 2016. He prepared his PhD at the Software Reliability Laboratory of the CEA LIST. His most recent research work focused on applying formal verification to an operating system for internet of things, using the Frama-C analysis platform.
- **François Bobot** is an engineer-researcher at CEA since 2012. He work at different steps of formal methods using deductive verification techniques: from helping industrial partners to use formal tools, designing and extending verification tools (Why3, Frama-C) to improving automatic solvers (Alt-Ergo, CVC4, COLIBRI).

4.1.22 DHBW: Duale Hochschule Baden-Württemberg (DE)

DHBW

Baden-Wuerttemberg Cooperative State University (*Duale Hochschule Baden-Württemberg/DHBW*) was founded in 2009, combining nine previously independent cooperative teaching academies. The university's official seat is in Stuttgart. Based on the US State University System, the organizational structure of DHBW is unique in Germany, comprising a central level and a local level. The central level consists of the DHBW Headquarter and the Center for Advaced Studies. At the local level are nine DHBW academies with three additional subordinate campuses. Through its acedemies, the university offers a broad range of undergraduate study programmes in the field of business, engineering, and social work. Graduate courses are provided centrally via the Center for Advances Studies.

With around 34,000 enrolled students, over 9,000 partner companies and more than 145,000 graduates, DHBW is one of the largest institutions of higher education in the German Federal State of Baden-Wuerttemberg, and by number of yearly graduates, one of the largest in Germany. Since its 2009 integration as a *Hochschule* proper, DHBW has been building its research portfolio, in particular performing cooperative reseach with its partner companies.

Main tasks:

- Stephan Schulz will support the efficient production of detailed proofs for first-order reasoners (WP2,**T2.1**), the use of Logipedia to improve automatisation of ATP guidance (WP2, **T2.3**), and the training of students (WP8, **T8.3**). He is the main developer of **E** and has pioneered the extraction and use of proof traces from automated theorem provers since 1993, including proof structuring, presentation, extraction from distributed ATPs, low-overhead proof generation, and learning from previous proof experience. He is one of the main contributors to the TPTP language for problems, proofs and models, which is in wide use in the ATP community. Schulz has supervised a large number of bachelor and master students, and has co-supervised several Ph.D. candidates. He has taught at several summer schools.

Publications, products or services:

- "Faster, Higher, Stronger: E 2.3", by Schulz, S., S. Cruanes, and P. Vukmirović. In: Proc. of the 27th CADE, Natal, Brasil. Ed. by P. Fontaine. LNAI 11716. Springer, 2019, pp. 495–507.
- "Proof Generation for Saturating First-Order Theorem Provers", by Schulz, S. and G. Sutcliffe. In: All about Proofs, Proofs for All. Ed. by D. Delahaye and B. Woltzenlogel Paleo. Vol. 55. Mathematical Logic and Foundations. London, UK: College Publications, Jan. 2015, pp. 45–61. isbn: 978-1-84890-166-7.
- "The TPTP Typed First-order Form with Arithmetic", by Sutcliffe, G., S. Schulz, K. Claessen, and P. Baumgartner. In: Proc. of the 18th LPAR, Merida. Ed. by N. Bjørner and A. Voronkov. Vol. 7180. LNAI. Springer, 2012, pp. 406–419.
- "Using the TPTP Language for Writing Derivations and Finite Interpretations", by Sutcliffe, G., S. Schulz, K. Claessen, and A. V. Gelder. In: Proc. of the 3rd IJCAR, Seattle. Ed. by U. Fuhrbach and N. Shankar. Vol. 4130. LNAI. Springer, 2006, pp. 67–81.
- "Extending a brainiac prover to lambda-free higher-order logic", by Vukmirović, P., J. C. Blanchette, S. Cruanes, and S. Schulz. In: Proc. 25th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'19). Ed. by T. Vojnar and L. Zhang. LNCS 11427. Springer, 2019, pp. 192–210.

Previous projects or activities:

- Stephan Schulz is the creator and a core developer of the theorem prover E. He has participated in a number of research projects at TUM. He currently is a senior collaborator in the project *Matryoshka* (Principal investigator: Jasmin Blanchette, Vrije Universiteit Amsterdam, ERC Starting Grant 2016 Grant agreement No. 713999), which is working towards reducing the gap between efficient automated reasoning systems and more expressive interactive proof assistants.

Infrastructures or technical equipment:

- Schulz, Stephan (et al.): The high-performance automated theorem prover E
- DHBW provides reasonable computing resources for medium-scale experiments.

Persons primarily responsible for carrying out the proposed activities:

- **Stephan Schulz** is a tenured Professor at DHBW, with a focus on foundations of computer science. He received his Ph.D. (*Dr. rer.nat*) in Computer Science from the Technische Universität München in 2000, and has taught at the University of Miami, the University of the West Indies, and the University of Hildesheim. From 2005 to 2014 he worked as technical project leader and project manager in the field of air traffic control systems. He joined DHBW in Mai 2014. Dr. Schulz has co-created the biannual *Workshop on Practical Aspects of Automated Reasoning* in 2008 and the yearly *Conference on Artificial Intelligence and Theorem*

Proving in 2016. He has served in a number of organisational roles, including as programme chair of the *International Joint Conference on Automated Reasoning* in 2018 and a trustee of CADE Inc. (ex-officio since 2017, elected 2018). His research contributions include work in high-performance deduction systems, AI-based search heuristics, and practical languages for proof problems and proof objects. He has published more than 50 peer-reviewed papers and edited several proceedings and journal issues.

4.1.23 Edukera: Edukera (FR)

The Edukera software company, created in 2013, develops the eponym application, an interactive prover dedicated to education.

Edukera is an online application for students to solve mathematical exercises that require to formulate a mathematical proof. The proof is automatically and instantly verified by the application. Professors have access to detailed activity reports of the class. They can select exercises in the exercises database for training and scheduled homeworks.

Since its commercial launch in 2016, the Edukera interactive prover has enabled more than 8000 students (117 classes) from L1 to M2 to solve more than 250 000 exercises (half a million attempts). It currently provides 911 exercises free of charge for students, dispatched in various domains:

- 193 formalisation exercises
- 148 Logic exercises (Connectors/Quantifiers)
- 226 Set Theory exercises (level L1)
- 344 Algebra exercises (level High School)

Main tasks:

- **T8.10** : Web interface for doing proofs at school
  Edukera has 8 years of experience in designing a web application for education built on top of a formal proof engine (the current edukera application is built on top of the Coq proof assistant). We consider the edukera application to be currently the most advanced user interface in terms of ease of use and ergonomic design.

Publications, products or services:

- Edukera: an interactive web prover for education

Previous projects or activities:

- Edukera is the mathematical platform of the SONATE project, the e-learning platform for students to pass the DAEU (Diplôme d'Accès aux Etudes Universitaires - Diploma to enter University), developed by the UNIT foundation.

Persons primarily responsible for carrying out the proposed activities:

- **M. Benoit Rognier** is the co-founder and CEO at Edukera. Before Edukera, he worked in the software industry in the domain of Artifical Intelligence as a software engineer (2000-20005 at KXEN inc.), presales engineer (2005-2010 at KXEN inc. and SmartFocus inc.) and director of innovation (2010-2012 at Probance inc.). He specialised in applying Artifial Intelligence techniques in marketing automation solutions. He graduated (2000) from the Institut Supérieur de la Matière et du Rayonnement with a major in Computer Science.
- **Guillaume Duhamel** is the co-founder and CTO at Edukera. Before Edukera, he worked in the software industry in the domain of Artificial Intelligence as a software engineer (2010-2012 at Probance inc.). He specialised in developing full-stack web applications. He graduated (2008) from EPITA with a major in Artificial Intelligence.

4.1.24 MED-EL: MED-EL Elektromedizinische Geraete GmbH (AT)

MED-EL is the leading European Cochlear Implant (CI) company with worldwide operations. Since its founders developed one of the world's first cochlear implants in 1975, MED-EL has set new standards, developing and manufacturing technologically advanced hearing implant solutions. With over 1,500 employees across more than 100 countries, MED-EL is the global leader in ground-breaking advances and superior clinical outcomes.

MED-EL has continually driven progress through research initiatives at our state-of-the-art R&D campus and through partnerships with research institutes, universities, and clinics worldwide.

Main tasks:

- Case study of the application of formal verification in the industrial setting in WP6.

Publications, products or services:

- "A Semantic Web Services Architecture", by Mark H. Burstein, Christoph Bussler, Michal Zaremba, Timothy W. Finin, Michael N. Huhns, Massimo Paolucci, Amit P. Sheth, Stuart K. Williams. IEEE Internet Computing 9(5): 72-81 (2005)
- "Enabling execution of Semantic Web Services - WSMX core platform", by Michal Zaremba, Matthew Moran. WIW 2004
- "Integration of business modelling methods for enterprise information system analysis and user requirements gathering", by Hui Shen, Brian Wall, Michal Zaremba, Yuliu Chen, Jim Browne. Computers in Industry 54(3): 307-323 (2004)
- "SWS Challenge - First Year Overview", by Charles J. Petrie, Holger Lausen, Michal Zaremba. ICEIS (4) 2007: 407-412
- "Semantically-enabled service oriented architecture : concepts, technology and application", by Tomas Vitvar, Adrian Mocan, Mick Kerrigan, Michal Zaremba, Maciej Zaremba, Matthew Moran, Emilia Cimpian, Thomas Haselwanter, Dieter Fensel. Service Oriented Computing and Applications 1(2): 129-154 (2007)

Previous projects or activities:

- MED-EL has previously participated in several EU-funded as NeuEar, HEAR-EU, NANOCI and NANOEAR. Michal Zaremba and Daniel Winkler as employees of other organizations participated in SWS, SUPER, SOA4ALL, COIN, DIP, LarKC, SEALS Knowledge Web and several other EU-funded projects.

Persons primarily responsible for carrying out the proposed activities:

- **Michal Zaremba** is Head of Applied Artificial Intelligence Group and is responsible for the innovation of AI based solutions.
- **Daniel Winkler** is Research Scientist at Applied AI Gros up. He is responsible for the development of frontend systems for speech and hearing rehabilitation.

4.1.25 P&R: Prove & Run (FR)

PROVE & RUN

Prove & Run's mission is to help its customers resolve the security challenges linked to the large-scale deployment of connected devices and of the Internet of Things. Thanks to an innovative software development toolchain (called ProvenTools) based on state of the art proof techniques, Prove & Run can deal with the development of the most sensitive software components (microkernels, hypervisors, OSes, secure bootloaders, etc) and meet the highest security requirements (such as CC EAL7) in a cost effective manner, taking also into account time-to-market and required skill levels constraints.

Using ProvenTools, Prove & Run has developed two unique critical off-the-shelf software bricks:

- ProvenCore: a next generation ultra-secure OS (TEE) available for ARM® Cortex®-A, Cortex®-M and RISC-V processors, certified at the EAL7 level according to the Common Criteria evaluation scheme.
- ProvenVisor: an ultra-secure hypervisor available for ARM Cortex-A processors.

Prove & Run was founded in 2009 and today employs 40 engineers. It is independent and privately owned.

Main tasks:

- WP6, task **T6.6**: Translate models and proofs from ProvenTools to Dedukti. Stéphane Lescuyer will be in charge of this task. He is the main architect and developer of ProvenTools' internal verification condition generator and automated prover.

Publications, products or services:

- "Security Filters for IoT Domain Isolation", by Dominique Bolignano, Embedded Conference, 2018
- "Formally Proven and Certified Off-The-Shelf Software Components", by D. Bolignano, C&SAR, 2016
- "Proven Security for the Internet of Things", by Dominique Bolignano, Embedded Conference, 2016
- "ProvenCore: Towards a Verified Isolation Micro-Kernel", by S. Lescuyer, 10th HiPEAC Conference, 2015

Previous projects or activities:

- EPI: The European Processor Initiative (EPI) is a project financed by the European Commission, whose aim is to design and implement a roadmap for a new family of low-power European processors for extreme scale computing, high-performance Big-Data and a range of emerging applications. Prove & Run is the Security Leader of this project.
- CPS4EU: The CPS4EU project aims to arm Europe with an extensive value chain across key sectors by: 1. Strengthening Cyber-Physical Systems (CPS) technology providers, mainly European SMEs, to increase their market share and their competitiveness to become world leaders, 2. Improve design efficiency and productivity and enable secure certification, 3. Enabling the creation of innovative European CPS products that will strengthen the leadership and competitiveness of Europe by both large groups and SMEs, 4. Large dissemination of CPS technologies.
- SECREDAS: European collaborative project aimed at developing an innovative solution for the safety, security, and privacy of automated systems, including a reference architecture, powerful components, and common approaches to integration and verification in the automotive, health and rail sectors, led by NXP.
- MuSiC: European collaborative research project aimed at providing a scalable and certifiable security solution for the mid to high data-rate cost-effective devices in order to secure against application, OS, web, and network based threats and protect critical services on shared networks, led by STMicroelectronics.

Persons primarily responsible for carrying out the proposed activities:

- **Dominique Bolignano** led the formal methods' group of Bull until 1996, prior to taking charge of all the technology transfer initiatives of the Dyade GIE (created by INRIA and Bull) within the formal methods and security areas. In 1999 he created Trusted Logic, a start-up of INRIA, which he led for eleven years, until its sale to Gemalto in 2009. With more than one hundred experts, researchers and engineers, Trusted Logic became the world leader in its field: operating systems and middleware security for smart cards and mobile terminals. In 2009 he founded Prove & Run and is currently its CEO. In parallel with these activities, he has maintained many academic positions. In particular he was Associate Professor at the Paris Dauphine University for nine years and then a member of the Scientific Council of CNRS in the field of engineering and computer science for four years, until September 2010. Most recently he chaired the AERES evaluation committee for the INRIA Rennes Bretagne and led the quadrennial assessment of its research laboratories.
- **Guillaume Dufay** (PhD, CISSP) has more than 15 years of experience in security architecture and security evaluation for connected and embedded devices. This experience was acquired from academic research and security consulting missions in various vertical domains (Mobile, Financial services, IoT, Transport, DRM, Enterprise). He is the author of ARM PSA Certified security certification scheme and ARM IoT Protection Profiles; co-author of the GlobalPlatform TEE, Java Card and (U)SIM Protection Profiles; and the author of security targets based on Java Card, secure signature, payment, TPM, car-to-car and e-passport Protection Profiles. He managed several Common Criteria evaluations of smartcards and similar devices products including the interactions with ITSEFs and certification bodies.
- **David Garnier** holds a Master's Degree in Engineering from the Ecole des Mines de Nantes and a Master's Degree in Computer Science from the University of Nantes. He worked for four years at Trusted Logic, leading studies in the field of secure embedded computing for customers such as Orange and SFR. He then created the Integration Group within Trusted Labs and led the implementation of prototypes of secure embedded system in collaboration with the DGA and RATP, among others. Prior to joining Prove & Run, he obtained an MBA from the Rotterdam School of Management.
- **Stéphane Lescuyer** graduated from the Ecole Polytechnique and is a State Engineer of the Mines, a technical corps of the French state. He earned a PhD degree from University Paris-Sud in the field of automation of formal proofs in the Coq proof assistant, as part of the INRIA Saclay - Ile-de-France. He has ten years of experience of working on formal methods and program verification at Prove & Run, and is the lead architect in charge of ProvenCore's design and proofs.

4.1.26 ZIB: Konrad-Zuse-Zentrum für Informationstechnik Berlin (DE)

The Zuse Institut Berlin (ZIB) is an interdisciplinary research institute for applied mathematics and data-intensive high-performance computing. Its research focuses on modeling, simulation and optimization with scientific cooperation partners from academia and industry. The institute is located at the interface between mathematical method development and the analysis and management of large data sets. It is a link and a communication amplifier between the applied sciences and mathematics. Together with FIZ Karlsruhe we develop and maintain swMATH, a freely accessible information platform for mathematical software.

Main tasks:

- **T8.8**: Expanding the use of Logipedia in publishing
- **T8.9**: Linking scientific publications to Logipedia

Publications, products or services:

- "alsoMATH - A Database for Mathematical Algorithms and Software" by Wolfgang Dalitz, Wolfram Sperber, Moritz Schubotz, Hagen Chrapary, Workshop Papers at 12th Conference on Intelligent Computer Mathematics CICM 2019, 12th Conference on Intelligent Computer Mathematics (CICM 2019), Prague (CZ), July 8-12, 2019
- "Software Products, Software Versions, Archiving of Software, and swMATH", by Hagen Chrapary, Wolfgang Dalitz, in Mathematical Software - ICMS 2018 6th International Conference, South Bend, IN, USA, July 24-27, 2018, Proceedings

Previous projects or activities:

- swMATH (www.swmath.org) is a freely accessible, innovative information service for mathematical software. swMATH not only provides access to an extensive database of information on mathematical software, but also includes a systematic linking of software packages with relevant mathematical publications.

Persons primarily responsible for carrying out the proposed activities:

- **Wolfgang Dalitz** is a researcher at ZIB working in the field of Scientific Information Services. He leads the working group 'Web Technology and Multimedia' in the division 'Scientific Information System' at ZIB.

4.1.27 UAIC: Universitatea Alexandru Ioan Cuza din Iasi (RO)

Alexandru Ioan Cuza University of Iaşi (UAIC) is the oldest higher education institution in Romania. Since 1860, the university has been carrying on a tradition of excellence and innovation in the fields of education and research. With over 24.000 students and 700 academic staff, the university enjoys high prestige at national and international level and cooperates with over 500 universities world-wide.

Faculty of Computer Science (FII) was established in 1992 as a natural development of the computer science chair of the Faculty of Mathematics. FII has active research groups in the area of Data Engineering for Optimization, Evolutionary Computing and Machine Learning, Cryptography, Natural Language Processing, Applied Distributed Systems, and Formal Methods in Software Engineering (FMSE).

The main goal of the FMSE research group, which project members belong to, is to develop methods and tools helping software engineers in applying mathematical-based proof techniques during software development. The use of the formal methods helps in revealing the inconsistencies, incompleteness, ambiguities in a system's or language's design. The group's ambitious is to apply the formal methods in a mechanical way. The primary strength of the group is the use of the algebraic specification theory, logics and rewriting techniques. The main achievements include the development of the CIRC coinductive prover and a major contribution in the design and the implementation of the K framework.

Main tasks: UAIC will be fully involved in the task Instrument K Prover **T6.2**. Its main responsibilities in this include the translation of matching logic proofs expressed in Kore into Dedukti, and the integration of these proofs with those generated by the automated provers. Main achievements obtained up to now and strong related to the project topics include:

- a coinduction-based formalization of the symbolic execution, which is language independent, and its implementation in K Framework 3.4.

- contributions to the development of the K Framework, an independent rewrite-based language framework in which programming languages, type systems and formal analysis tools can be defined and executed.
- a proof system for the circular coinduction and its implementation in CIRC, a prover for equations behavioural equivalence. The method was extended to prove the equivalence of the non-deterministic coalgebras.

All these achievements match very well with the goals of the task, which will be accomplished by the following two main activities:

- Translating Kore into Dedukti;
- Assembling the Kore translation with those produced by automated provers in a single proof.

Publications, products or services:

- "Unification in Matching Logic", by Andrei Arusoaie, Dorel Lucanu. FM 2019: 502-518
- "A generic framework for symbolic execution: A coinductive approach", by Dorel Lucanu, Vlad Rusu, Andrei Arusoaie. J. Symb. Comput. 80: 125-163 (2017)
- "A language-independent proof system for full program equivalence", by Stefan Ciobaca, Dorel Lucanu, Vlad Rusu, Grigore Rosu. Formal Asp. Comput. 28(3): 469-497 (2016)
- "Language definitions as rewrite theories", by Vlad Rusu, Dorel Lucanu, Traian-Florin Serbanuta, Andrei Arusoaie, Andrei Stefanescu, Grigore Rosu. J. Log. Algebraic Methods Program. 85(1): 98-120 (2016)
- "Circular Coinduction: A Proof Theoretical Foundation", by Grigore Rosu, Dorel Lucanu. CALCO 2009: 127-144

Previous projects or activities:

- DAK: An Executable Semantic Framework for Rigorous Design, Analysis and Testing of Systems. The first version of the K framework were developed within this project.
- CIRC: Automated Verification by Circularities. The main outcome of this project is Circ prover, a Maude-based implementation of the circular coinduction proof system. The idea of circular reasoning promoted by Circ was used in reachability logic and K prover.

Infrastructures or technical equipments:

- The needed research infrastructure is provided by the laboratory of the Formal Methods in Software Engineering (FMSE) research group. Since this infrastructure was used to develop the first versions of K, it can support to integrate the proofs generated by the K prover into the Logipedia infrastructure. We will use the FMSE server (fmse.info.uaic.ro) for the webpage of the project.

Persons primarily responsible for carrying out the proposed activities:

- **Andrei Arusoaie** Andrei is currently an associate professor at Alexandru Ioan Cuza University. He has received his PhD in 2014 from Alexandru Ioan Cuza University with a thesis on symbolic execution, applied to program verification. He had a postdoctoral research stay at INRIA Lille, France. He has extensive experience with formal verification, including with formal proof systems such as the Coq proof assistant. Andrei also has experience in developing tools for formal methods. He started working on the K framework during his master studies and continued to develop K for 3.5 years. During this period he worked on the K compiler for language definitions, an engine for symbolic execution, and a prover based on symbolic execution. Andrei is now part of the FMSE group led by Dorel Lucanu, and he was one of the key members in the DAK research project. Recently, Andrei coordinates a university research project where his goal is to generate proof certificates for programs that run on the blockchain.
  Main achievements related to the project topics:
  - Co-author of a coinduction-based formalization of the symbolic execution, which is language independent, and its implementation in K Framework 3.4.
  - Contributions to the development of the K Framework, an independent rewrite-based language framework in which programming languages, type systems and formal analysis tools can be defined and executed.
  - Certification of a procedure for program verification based on symbolic execution.
  - Generation of proof certification for unification in Matching Logic.
- **Rodica Condurache** Rodica is currently a lecturer at Alexandru Ioan Cuza University. She has received her PhD in 2016 from Universite Paris-Est Paris and Universite Libre de Bruxelles with the thesis Synthesis of interactive reactive systems(Synthese des systemes reactifs interactifs) [C2016]. Both the work during the thesis and the further collaborations provided Rodica good experience in verification and synthesis of reactive systems. The main contribution of the thesis consists of procedures to solve (rational) synthesis problems from temporal logic specifications that may lead to efficient implementations. To illustrate the

feasibility of some procedures, she also developed a prototype tool. Some of this contribution was part of the project EQUINOCS from the LACL laboratory in Paris Creteil University. Rodica has also experience in working with temporal logic as ATL to express and verify voting protocols as Three-Ballot. Moreover, more recently she is involved in a project studying the verification of dynamic systems against specifications that may also be given as temporal logic formulas.
After Rodica moved to UAIC, she started to study Matching Logic with focus on deductive proving in of temporal formulas.

- **Dorel Lucanu** Dorel Lucanu is currently professor at Alexandru Ioan Cuza University of Iași. His main research interests include rewriting logic, matching logic, coinductive techniques, and their application to supply formal semantics for programming languages, and to develop tools for program verification and analysis. He is the head of Formal Methods in Software Engineering (FMSE) group at the Faculty of Computer Science and he has experience in applying formal methods, with a focus on the formal semantics of programming languages and program verification and analysis. Dorel Lucanu coordinated two large related research projects: DAK (together with Grigore Roșu, from UIUC) and CIRC. Within the DAK project the first versions of the K Framework (1.0 - 3.4) were defined, and the main contribution of CIRC is the development of a prover for coinductive properties. He was a Management Committee (MC) member of the ICT COST Action IC0701 - Formal Verification of Object-Oriented Software (2008-2012) and currently is a MC member of the CA COST Action CA15123 - The European research network on types for programming and verification (EUTYPES), in both actions representing Romania.

4.1.28 RV: Runtime Verification SRL (RO)

runtime verification

Runtime Verification Inc. is a startup company aimed at using runtime verification-based techniques to improve the safety, reliability, and correctness of software systems.

Runtime Verification SRL is a research and development branch of RV Inc. based in Bucharest Romania. Its main activities include the design and development of the symbolic execution and program verification backend of the K framework, as well as offering consultance with modelling and proving properties about consensus protocols (in the presence of Byzantine faults), with a focus on those used in Blockchains.

Main tasks:

- **T6.2**: RV SRL will lead the task of instrumenting the K Prover to emit enough information about the proving process, in order to allow extracting matching logic (ML) proofs from program verification problems
- **T6.2**: RV SRL will assist the UAIC team with translating Kore (the language of ML) into Dedukti

Publications, products or services:

- "A rigorously designed language and tool ecosystem for the blockchain", by Kasampalis, T., Guth, D., Moore, B., Șerbănuță, T. F., Zhang, Y., Filaretti, D., ... & Roşu, G. (2019, October). In International Symposium on Formal Methods (pp. 593-610). Springer, Cham.
- "All-Path Reachability Logic", by Rosu, G., Serbanuta, T. F., Moore, B., Mereuta, R., Ciobaca, S., & Stefanescu, A. (2019). Logical Methods in Computer Science, 15.
- "Matching μ-Logic", by Chen, X., & Roşu, G. (2019, June). In 2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) (pp. 1-13).
- "From Hybrid Modal Logic to Matching Logic and back", by Leustean, I., Moanga, N., & Serbanuta, T. F. (2019). In Working Formal Methods Symposium (FROM), EPTCS 303, 16-31. arXiv:1907.05029.
- "An overview of the K semantic framework", by Roșu, G., & Șerbănuță, T. F. (2010). Journal of Logic and Algebraic Programming, 79(6), 397-434.

Previous projects or activities: RV SRL is young company and therefore it was not yet involved in EU/national funded projects. However, besides contributing to the development of the infrastructure described below, here are some activities in which RV SRL played an important role:

- The formal modelling (using Coq) of the full and light nodes of Casper-CBC, as well as the partial modelling of a new VLSM model proposed by Vlad Zamfir, as part of a project funded by Casper Labs.
- The design and development of a gas model for IELE, a new virtual machine language for the blockchain aimed at improving security and verification-readiness. IELE was developed as part of a project funded by Input Output Hong Kong.

Infrastructures or technical equipments:

- K Framework is an open source rewrite-based executable semantic framework in which programming languages, type systems and formal analysis tools can be defined using configurations, computations and rules. Originally designed and prototyped by Grigore Roșu and Traian Șerbănuță, it is currently maintained by a team spread between the US and Romanian branches of RV.
- Kore provides a language for expressing matching logic, as well as a rewriting-based engine for performing matching-logic deduction. Kore currently serves as a symbolic execution and program verification backend for the K framework. Most of the team developing Kore is part of RV SRL.

Persons primarily responsible for carrying out the proposed activities:

- **Ana Pantilie** is a software engineer at RV SRL, involved with the research and development of the symbolic execution and program verification backend of the K framework. She enjoys learning about functional programming languages and formal methods. In addition to her duties at RV, Ana is pursuing a Master's degree in Software Engineering at the University of Bucharest. She completed her Bachelor's degree project in Clojure, developing a music composition application.
- **Grigore Roșu** is a full professor of computer science at the University of Illinois and the founder of Runtime Verification, Inc., and of Runtime Verification SRL. He is interested in programming languages, formal methods and software engineering, and especially in how to combine these to increase the safety, security and dependability of computing systems. He was offered the NSF CAREER award, the UIUC outstanding junior award, the Dean's award for excellence in research, and several best paper awards. Grigore got his Ph.D. from the University of California at San Diego.
- **Traian Florin Șerbănuță** is an associate professor of computer science at the University of Bucharest and a research consultant for RV, where he serves as the K Technical Lead. Traian completed his Ph.D. at UIUC, working with Grigore Rosu on the first prototype of K, which serves as a basis for the semantics-based execution and semantics-based program verification tools developed by RV. Additionally, Traian designed a maximal causal model for sequential consistency which serves as a basis for runtime verification of concurrent programs in tools such as RV-Predict.

4.2 Third parties involved in the project (including use of third party resources)

Inria: Institut National de Recherche en Informatique et Automatique (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	Y
École polytechnique, Université de Lorraine, and Mines ParisTech. Three researchers from École polytechnique, Université de Lorraine, and Mines ParisTech have had long term cooperation with the Inria group.	
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	Yes.
École polytechnique: 6 person-months, Université de Lorraine: 8 person-months, and Mines ParisTech: 6 person-months	

Unistra: Université de Strasbourg (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N

Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

INPT: Institut National Polytechnique de Toulouse (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UIBK: Universität Innsbruck (AT)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

ULiege: Université de Liège (BE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

Unibo: Alma Mater Studiorum – Università di Bologna (IT)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UBel: Matematički fakultet, Univerzitet u Beogradu (RS)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

TUM: Technische Universität München (DE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	Y
The subcontractor has spent the last ten years building the technological prerequisites for the required work.	
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

TUDelft: Technische Universiteit Delft (NL)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

USaclay: Université Paris-Saclay (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

FAU: Friedrich-Alexander Universität Erlangen-Nürnberg (DE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	Y
The subcontractor has spent the last ten years building the technological prerequisites for the required work.	
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

ULeeds: University of Leeds (UK)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UGot: Göteborgs Universitet (SE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

Chalmers: Chalmers Tekniska Högskola (SE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

LMU: Ludwig-Maximilians-Universität München (DE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

IMT: Institut Mines-Télécom (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UBia: Uniwersytet w Białymstoku (PL)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

ClearSy: ClearSy (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

OcamlPro: OCamlPro (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UoB: University of Birmingham (UK)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

CEA: Commissariat à l'Energie Atomique et aux Energies Alternatives

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

DHBW: Duale Hochschule Baden-Württemberg (DE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

Edukera: Edukera (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N

Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

MED-EL: MED-EL Elektromedizinische Geraete GmbH (AT)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

P&R: Prove & Run (FR)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

ZIB: Konrad-Zuse-Zentrum für Informationstechnik Berlin (DE)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

UAIC: Universitatea Alexandru Ioan Cuza din Iasi (RO)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N
Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

RV: Runtime Verification SRL (RO)

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)?	N
Does the participant envisage that part of its work is performed by linked third parties?	N

Does the participant envisage the use of contributions in-kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)?	N

Section 5

Ethics and Security

5.1 Ethics

Regarding the section 4 “Ethics” of the proposal submission form, Logipedia is not concerned by any ethical issues mentioned in this form. The Logipedia consortium will pay attention to any ethical issue that might arise during the project. If at some point during the course of the project, the consortium or any scientist is unsure about how to handle a particular situation or requires advice on ethical issues, the partners or the individuals, supported by the EPM, will refer to the operational ethical committee of Inria (the COERLE) before proceeding.

5.2 Security

The LOGIPEDIA project does not involve any activities or results raising security issues nor contain any “EU-classified information” as background or results.

Section 6

Letters of intent of the members of the club of industrial users

ALSTOM

ALSTOM DIGITAL MOBILITY / SAFETY

48 rue Albert Dhalenne
93400 Saint-Ouen-sur-Seine (France)
Tél. : +33 (0)1 57 06 90 00
Fax : +33 (0)1 57 06 96 66
www.alstom.com

Monsieur Frédéric BLANQUI
INRIA - LSV
61 avenue du Président Wilson,
94235 Cachan Cedex, France

Saint-Ouen-sur-Seine, March, 5th 2020

Dear Professor,

Alstom is a major rolling stock and railway signalling systems supplier with more than 35000 employees all over the world. It provides its customers in more than 25 countries with safety-critical systems that prevent hazardous situations for passengers, staff and equipment while ensuring fluent and cost-effective operation.

For more than 30 years Alstom has been developing or verifying with formal methods some of its safety-critical signalling systems. He is therefore an intensive end-user of proof systems (AtelierB, S3, Why3, Isabelle) and highly concerned and interested in all projects that can improve the quality and efficiency of its proof activity.
This is the reason why Alstom, represented by Michel Macheboeuf, Signalling Safety Director, confirms that it is highly interested in the Logipedia project and willing to be an active member of its Industrial User-Group.

Best regards,

Michel MACHEBOEUF
ADM / Signalling Safety Director
Alstom Digital Mobility

ALSTOM Transport SA
Société Anonyme au capital de 343 600 000 euros
Siège social : 48 rue Albert Dhalenne - 93400 Saint-Ouen-sur-Seine (France)
389 191 982 RCS Bobigny - TVA Intra : FR 53 389 191 982

Arm Ltd
110 Fulbourn Road
Cambridge
GB-CB1 9NJ

Tel: +44 (1223) 400 400
Fax: +44 (1223) 400 410

28/02/2020

Dr Frédéric Blanqui
INRIA
Office C1-09
61 avenue du Président Wilson
94235 Cachan Cedex
France

Ref: Logipedia

Dear Frédéric,

I am pleased to write this letter of support for the *Logipedia* project on behalf of Arm.

Arm is the world's largest provider of semiconductor IP and is the architecture of choice for more than 90% of the smart electronic products being designed today: Arm designs have found their way into more than 20,000,000,000 devices in 2018, for instance. Increasingly, the Arm architecture is also being deployed in supercomputers and servers, with Amazon's AWS recently announcing its *Graviton* line of Arm-based high-performance servers.

As well as our 32- and 64-bit CPU cores, our hardware products extend to GPUs, DSP cores, cell libraries, memory compilers and system components. Arm also produces a wide array of software products, many of which are extremely security-sensitive: low-level firmware, privileged security monitors, operating system kernel patches, cryptography libraries, and transport layer security protocol implementations are all developed and actively maintained by Arm engineers on behalf of our wider ecosystem, for example. Arm engineers also play an active role in developing and standardising novel cryptographic protocols and ciphers through various international bodies.

Given the ubiquity of the Arm architecture we have an obvious interest in ensuring that various functional and security properties hold, and also that our microprocessor designs are indeed correct instantiations of this architecture. As a result, semi-automated formal techniques have long been used within the company to ensure the correctness of our architecture and of our microprocessor designs.

Whilst many of our verification flows have been built around commercial tools that we license "off-the-shelf", we also develop our own formal tools using SAT and SMT technology, and many of these tools are in active use by our product engineering groups. Moreover, we are increasingly experimenting with:

- The deployment of formal techniques as an enhanced bug-finding mechanism for especially sensitive software products, using bounded-model checking technology and SMT-based pre/postcondition checking, using tools such as the C-bounded model checker (CBMC) and Frama-C.
- Model checking novel locking mechanisms for highly concurrent code, to spot potential deadlocks, using the TLA model checker.
- Formally documenting and semi-automatically finding security flaws in cryptographic protocols using dedicated model checking tools, such as Tamarin.

However, often we would like to establish deeper properties of the architecture and of our software implementations than can reasonably be obtained using the semi-automated formal approaches described above. For this reason, we have ongoing experiments with the use of *interactive theorem proving,* using both Coq and Isabelle/HOL, two popular tools that have shown promise in academia on a range of software and hardware verification projects.

From Arm's perspective, ideally there would be some way of transferring definitions and proofs between some of these tools so that we can maximise reuse, avoid wasted engineering effort, and also potentially share the models that we develop and associated proofs with the many communities surrounding these tools for use in academic projects. Unfortunately, to our knowledge no robust mechanism exists at present that can achieve this and therefore writing a formal model in Coq almost certainly precludes the Isabelle/HOL community from using that model without significant duplication of engineering effort, for example, and *vice versa*.

In light of the above, we are especially excited by the *Logipedia* project which aims to facilitate the sharing of definitions and proofs between many different interactive theorem proving systems, considering the problem a long-standing issue that is holding back commercial adoption of interactive theorem proving technology. Moreover, we wish to keep track of the project as it progresses, and potentially provide insight from our industrial use of formal methods technology. For this reason, we are committing to joining the *Logipedia* industrial users "club". Our nominated representative will be Dominic Mulligan, Staff Research Engineer in the Arm Research Security Group, who has highly relevant expertise, and aligned research interests. He is also well-placed to share project outcomes and gather contributions from colleagues across Arm.

We wish you every success, and look forwards to a successful outcome in due course.

Yours sincerely,

Andrea Kells
Director Research Ecosystem, UK and Europe

edukera SAS
793 014 333 R.C.S. Nanterre
84 rue Perronet,
92200 Neuilly-Sur-Seine

Neuilly-sur-Seine, the 6th of Mars 2020

Dear Sir or Madam,

Edukera has developed an online educational application to teach mathematics which relies on the use of the formal proof assistant coq (developed by INRIA).

One of the key features is the ergonomic design of the numerical mathematical paper which allows students to build the proof with point and click interactions. This numerical paper has been developed and improved over several years of experiment with students' and teachers' feedback. So much so that we consider the edukera application to be currently the most advanced user interface to do mathematical proofs in education.

Since its commercial launch in 2016, the Edukera application has been successfully used in many universities by 8000 students to solve 250 000 exercises.

Over the years we have experienced an increasing need for formal methods in education. This is due to the emergence of new industrial activities (cryptocurrency and the verification of smart contracts, software dependant autonomous vehicles, ...). This is why we consider the existence of a solid open-source education-dedicated interface for formal proofs, to be critical to the upcoming industrial ecosystem.

However, several issues in the design of the current edukera application prevent a larger user base and need to be solved: developers in formal methods need to create their own theories and teachers must be able to develop their exercises; plus the core edukera solution should be open-sourced for anyone to use, fix and improve when necessary.

The use of Logipedia as the mathematical foundation of the edukera application can solve these critical issues: indeed Logipedia federates a large scientific community around a unique language, and a large developer community around a unique open-source mathematical framework, which is beyond the financial means and traction of the edukera company on its own.

Students may already access the edukera application and exercises. Hence the existence of an open-source version of the edukera application will not affect the business model which is based on the billing of class administration features (activity reports, homework schedule, connection to the LMS, ...)

For these reasons, Edukera is willing to join the club of industrial users of Logipedia.

Benoît Rognier, CEO of edukera

facebook Artificial Intelligence

Paris, February 20th, 2020

To whom it may concern.

Facebook AI Research (FAIR) is the fundamental research lab in Artificial Intelligence of Facebook. Its largest research center in Europe is in Paris and has been employing over 70 people, mixing researchers, engineers and students for over four years now. FAIR is recognized as one of the top leading AI labs in the world and is proud of doing fundamental research. FAIR actively engages with the research community through publications, open source software, participation in technical conferences and workshops, and collaborations with colleagues in academia. FAIR has hundreds of academic partners across the world, such as Inria.

FAIR Paris has a team working on deep learning for theorem proving, a long-term effort in academic research. We use existing formal proofs as our learning datasets and are interested by the Logipedia project as a possible source of training data. We also have a strong interest in automatic language translation and would be keen to apply this to formal proof languages.

As authorized representative of Facebook, I hereby acknowledge our strong interest in joining the club of industrial users that the Logipedia project is willing to create.

We are looking forward receiving confirmation of this creation and knowing more about the actual membership procedure.

Sincerely,

Antoine Bordes,
Managing Director
Facebook Artificial Intelligence Research

Yorktown Heights, NY, Friday 6 March 2020

To whom it may concern,

The Thomas J. Watson Research Center serves as the headquarters of IBM Research – one of the largest industrial research organizations in the world – with 12 labs on six continents. Scientists at T.J. Watson, and at IBM labs around the globe, are pioneering scientific breakthroughs across today's most promising and disruptive technologies including the future of artificial intelligence, blockchain and quantum computing. In all of these areas, formal proofs can bring benefits ranging from reducing bugs to having a deep and fundamental understanding of the studied objects.

The Logipedia project is of strong interest for us. Developing proofs requires a huge effort. Being able to reuse formally proved properties could reduce the development time and thus allows to tackle larger problems. Moreover, each proof assistant requires its own expertise. The ability to reuse proofs coming from any system in the proof assistant of our choice is therefore a great benefit.

We would like to join the club of industrial users of Logipedia. We will also be happy to contribute to the project with Q*cert, a data base query compiler developed in Coq.

Finally, we think that Logipedia is proposed by an excellent team of researchers that could will lead the project to success.

Louis Mandel
IBM Research USA

MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC R&D CENTRE EUROPE

1, ALLEE DE BEAULIEU, CS 10806
35708 RENNES CEDEX 7, FRANCE
TEL. (+33) 02.23.45.58.58 – FAX (+33) 02.23.45.58.59

for a greener tomorrow

Rennes, 5th March 2020

Letter of intent for Logipedia club of industrials

Mitsubishi Electric is one of the world's leading names in the manufacture and sales of electrical and electronic products and systems used in a broad range of fields and applications, in particular Energy and Electric Systems, Industrial Automation, Information and Communication Systems, Electronic Devices, and Home Appliances. One of Mitsubishi Electric's objectives consist in creating new value through innovation and promoting R&D that pursues sustainable growth. For that purpose, Mitsubishi Electric devotes 5% of its revenue to its Research and Development budget, contributing to realizing Society 5.0 and achieving the goals of the United Nation's Sustainable Development goals.

At Mitsubishi Electric R&D Centre Europe, we believe that for achieving those sustainable development goals, one of the key factors is the confidence one can have in software, that drives more and more people's life, industry, etc. That's why we have studied for more than ten years different formal methods theories and tools that can help designing, specifying, implementing and maintaining software. Our objective is to fill the gap between state of the art academic work and industrial objectives and processes, to bring the power of formal methods to regular engineers. Among those formal methods, formal proofs allow to reach the highest level of confidence in software, but they are also the hardest to manipulate for non-specialists. We see the Logipedia project as an important milestone for widening access to formal proofs, and helping their dissemination in Industry for two reasons. First, by giving access to an encyclopedia of off-the-shelf and ready-to-use formal proofs, avoiding to prove many times the same properties. Second, by also strengthening the European formal proofs community and helping them to provide a kind of unified interface to industry problems.

For those reasons, we strongly support the Logipedia project proposal and we intent to participate to its club of industrials if it is accepted.

David Mottier
General Manager

To whom it may concern

Subject: Support to the Logipedia project

February 28th, 2020

Nomadic Labs (hereinafter NL) is a R&D company that contributes to the development of the Tezos protocol. NL gathers experts in formal methods, distributed systems, and programming language theory and practice. NL puts a particular emphasis on formal verification, and uses and develops related tools, applying them to the Tezos codebase, algorithms, and smart contracts. NL uses mostly the Coq and F* proof assistants, and supports the development of Coq and other tools dedicated to formal verification through its partnerships with premier research institutes.

The Logipedia project aims to create a library of formal proofs in a common pivot language called Dedukti. The existence of such a populated library, and the possibility of bringing proofs from one proof system to another one, will favor the general use of formal verification by avoiding the duplication of efforts, and encouraging proof reuse.

Nomadic Labs is of course very interested by such a project and is willing to be a member of the club of its industrial users.

Oana Ladret Piciorus
Directeur Général

DocuSigned by:
Oana Ladret Piciorus
34DCEA76D85F435...

Michel Mauny
Directeur Scientifique

DocuSigned by:
Michel Mauny
EC40E4BC254E4BB...

Nomadic Labs SAS 6 rue Germaine Richier, 75013 Paris
RCS Paris 813 239 118 TVA FR41813239118
contact@nomadic-labs.com www.nomadic-labs.com

Logipedia

H2020-INFRAIA-2018-2020

Statement of Support

ONERA has research activities in the development and application of formal methods for critical systems and software for aerospace applications. We believe formal techniques are useful for risk analyses, safety and security assessment of critical systems, development and verification of critical software. We apply formal techniques for aerospace applications (aircrafts, UAVs, robotics). We have also been part of the international group that defined DO-333 (Formal methods technical supplement to DO-178, software certification standard for aeronautics).

We agree on the significance of the problems addressed by the Logipedia infrastructure (H2020 INFRAIA-2018-2020). We have a serious interest in the approach of the Logipedia project to tackle these problems.

We want to be involved in the project by becoming a member of the Industrial Follower Group. As a member of this group we will follow the progress of the project and provide feedback and advice. We also would like to contribute in formulating challenges that are important to us, especially in relationship with certification constraints.

Toulouse, 02/03/20

Virginie Wiels
ONERA/DTIS Director

ONERA
THE FRENCH AEROSPACE LAB

Origin Labs S.A.S.
Éditeur de logiciels

21, rue de Chatillon,
75014, Paris
http://www.origin-labs.com/

E-Mail : fabrice.le_fessant@origin-labs.com

Paris, March 6, 2020

Logipedia Project

Object : Support letter for the Logipedia project

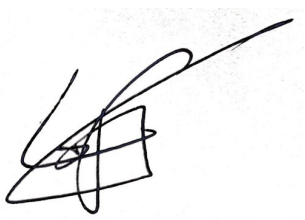
To whom it may concern,

Our company, Origin Labs, develops blockchain applications and tooling for blockchains. We are currently developing the Dune Network blockchain, a public blockchain that has been running since June 2019. One of our main concerns is security and safety, because our developments are often used to store and manage sensitive information and assets. Formal methods are a corner stone of our strategy around security and safety, and we plan to start developing soon a framework for formal verification of smart contracts for Dune Network.

The Logipedia project looks very interesting for us. Formal verification is often a difficult task, even for what looks like simple programs. Being able to reuse existing work, and translating such works for different provers and tools, are important challenges, to ease the development of industrial tooling for formal verification. For these reasons, we would like to give our support to the Logipedia project, and be part of its club of industrial users.

Paris, March 6, 2020

Fabrice Le Fessant
président



RATP INFRASTRUCTURES

Paris, Friday 13th March 2020

Julien Ordioni
RATP Infrastructures
Direction Projets & Ingénierie / Systèmes du Transport Ferroviaire
11 avenue Louison Bobet
94120 Fontenay-sous-Bois
France

Object: RATP interest in joining the Club of the Industrial Users of LOGIPEDIA

RATP is well known for more than 30 years in the railway industry to use formal methods in industrial applications. We participated at the end of the 90's to the birth of the B method with the Atelier B. Since then, we still promote formal methods both for our suppliers and our safety software assessment studies.

Mutualizing the proof concepts and axioms of different languages is kind of a logic path from our point of view to ensure sustainability, share and improve fundamental knowledge which be applied in our future applications.

Thus, RATP is interested to support LOGIPEDIA by joining the Club of the Industrial Users.

Best regards,

Julien Ordioni

Julien ORDIONI
Responsable AQL

SIEMENS

Reference : SMO_RI_MT_FR_ADC_DC/MB/133.0020.20/DIL/DIL 0001 00 EN

Name	**Fabrice LASSIA**	**To the attention of :**
Entity	**SMO RI MT FR ADC**	**Gilles Dowek** **ENS Paris-Saclay**
E-mail	**fabrice.lassia@siemens.com**	

Memo	1106091
Diffusion	Diffusion non restreinte
Date	**11/03/2020**

Subject : <u>Letter of intent – Participation in the H2020 research project - Logipedia</u>

Dear Sir,

We are writing this letter in support of the H2020 research proposal Logipedia.

Being one of the World's leading suppliers of control systems for automatic urban transport, we at Siemens Mobility in Chatillon, France, rely on formal methods in order to guarantee the safety of the systems we provide.

Participating in the research project Logipedia is interesting for us because it would help us remain up to date with the latest research developments in the subject of formal proof, more precisely, the possibility of exchange of proof certificates among different proof assistant software that is the subject of the research proposal. Formal mathematical proof is an important part of the formal methods that we use.

This is precisely what is offered by Logipedia's industrial users' club, which plans for periodic meetings between researchers and the industry where industrials would be kept up to date with the latest developments in the area.

Looking forward to participating in the research project,

Sincerely,

LASSIA Fabrice
SMO RI MT FR ADC
Head of Department

Lassia Fabrice

Signé numériquement par Lassia Fabrice
DN : cn=Lassia Fabrice, o=Siemens, email=fabrice.lassia@siemens.com
Date : 2020.03.11 18:16:14 +01'00'

Our Reference: DT_LT_20200226_A
Contact:

Laurent Voisin

Tél : +33 4 42 90 65 50

laurent.voisin@systerel.fr

LSV, CNRS & ENS Paris-Saclay

Gilles Dowek

61, avenue du Président Wilson

94235 CACHAN Cedex

Aix en Provence, 26 February 2020

Object : Letter of support for the Logipedia project

Systerel is an SME specialized in the specification, design, development, verification & validation, and assessment of real-time and safety-critical systems. Systerel's main achievements thus concern: on-board systems with hard real time or safety requirements; safety related tools (data preparation, data validation, system maintenance, …); formal specification of complex industrial systems; evaluation of the RAMS (Reliability / Availability / Maintainability / Safety) level of dependable systems.

Systerel applies formal methods to industrial systems everyday (mainly using Systerel Smart Solver, B and Event-B). Systerel had also been in charge of the maintenance of the Rodin platform for more than 10 years. It is thus quite naturally that we got interested in the Logipedia project. The purpose of the project is very relevant to our business for several reasons: Firstly, the usage of Dedukti would allow us to put better trust in automated theorem provers and SMT solvers, by allowing an external verification of their proofs. Secondly, we are sometimes in the need to prove some general well-known theorem (in order to apply it to a specific case), and the library approach of the Logipedia project would prove very useful by permitting proof reuse, rather than having to carry one again a manual proof (which can be quite costly).

This explains that Systerel wants to join the Club of industrial users and participate to the advisory board of the Logipedia project.

Yours sincerely,

Laurent Voisin

R&D Manager

Trusted Labs
Creating trust in a connected world

6, rue de la Verrerie – CS 20001
92197 Meudon Cedex – France

Tel : + 33 (0)1 30 97 26 20
Fax : +33 (0)1 30 97 26 19
www.trusted-labs.com

Meudon, March 6, 2020

Our references: Tla-L2003.005/BDH

Subject: Logipedia Industrial users club

Dear Madam, Sir,

Trusted Labs is a global expert in security consulting and evaluation within the connected ecosystem, and is the world leader in security certification scheme definition.
Trusted Labs is also an accredited ITSEF Lab in France, and conducts Common criteria evaluations.

Since more than 15 years, we've acquired a great experience in formal methods and support customers to get high level certifications for their products. We also conduct or support industrials on evaluations for common criteria certifications.

We provide our expertise to a large variety of customers, in sectors such as healthcare, automotive, energy and connected devices, and we are convinced this will bring value to the Logipedia club.

Hence, Trusted Labs is very interested to be part of the Logipedia Industrial users club and bring its expertise in formal proofs.

This is why it would be an honor for Trusted labs to be part of the Logipedia Industrial users club and bring its contribution on formal proofs.

Yours faithfully,

TRUSTED LABS S.A.S
6, rue de la Verrerie - CS 20001
92197 MEUDON Cedex - FRANCE
Tél. 01 30 97 26 20 - Fax 01 30 97 26 19
RCS NANTERRE 483 191 227

Brigitte D'HEYGERE

VP Security Consulting & Services
Trusted labs SAS

TRUST IN SOFT

Paris, le 6 mars 2020

Objet : Participation au club des utilisateurs industriels de Logipedia

Je soussigné, Benjamin Monate, Directeur général de TrustInSoft, société par actions simplifiée au capital de 136 841 €, dont le siège social est sis 222 cour avenue du Maine – 75014 Paris, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 793 371 907 RCS Paris, déclare par la présente que TrustInSoft souhaite participer au futur club des utilisateurs industriels du projet Logipedia.

Pour servir et faire valoir ce que de droit