Formulaire de soumission (dossier scientifique)

MONTAGE DE RESEAUX SCIENTIFIQUES EUROPEENS OU INTERNATIONAUX (MRSEI)

ÉDITION CONTINUE 2019

I. IDENTIFICATION DE LA PROPOSITION

Acronyme	LOGIPEDIA
Titre de la proposition	LOGIPEDIA: a system-independent encyclopedia of formal proofs
Nom du chercheur coordinateur (France)	Gilles Dowek
Institution de rattachement	Inria
Appel à projets (call) visé	INFRAIA-02-2020: Integrating activities for starting communities
Date de clôture de l'appel visé	March 17th, 2020
2nd appel à projets visé (optionnel)	

II. CONSORTIUM

Univerzitet u Beogradu (Belgrade): Predrag Janičić, Filip Marić, Vesna Marinković, Danijela Simić, Sana Stojanović-Đurđević.

Uniwersytet w Białymstoku (Bialystok): Karol Pąk.

Alma Mater Studiorum – Università di Bologna: Claudio Sacerdoti.

University of Cambridge: Angeliki Koutsoukou-Argyraki, Larry Paulson.

Clearsy: David Deharbe, Thierry Lecomte, Ronan Saillard.

Friedrich-Alexander-Universität Erlangen-Nürnberg: Michael Kohlhase, Dennis Müller, Florian Rabe.

Chalmers Tekniska Högskola (Göteborg): Andreas Abel.

Universität Innsbruck: Joshua Chen, Cezary Kaliszyk, Miroslav Olšák, Stanisław Purgał.

Université de Liège: Pascal Fontaine.

Technische Universität München: Tobias Nipkow, Makarius Wenzel.

Inria Nancy – Grand Est: Stephan Merz.

Inria Paris: Émilio Gallego, Hugo Herbelin, Théo Zimmerman.

České vysoké učení technické v Praze (Prague): Thibault Gauthier, Martin Suda, Josef Urban.

Inria Saclay – Île de France: Bruno Barras, Frédéric Blanqui, Valentin Blot, Guillaume Burel, Gilles Dowek, Catherine Dubois, Georges Gonthier, Olivier Hermant, Jean-Pierre Jouannaud, Chantal Keller, Dale Miller, Pierre-Yves Strub, Burkhart Wolff.

Inria Sophia Antipolis - Méditerranée: Yves Bertot, Pierre Boutry, Cyril Cohen.

Université de Strasbourg: Arthur Charguéraud, Nicolas Magaud, Julien Narboux, Pascal Schreck.

We are discussing with colleagues from other European countries, so a few other sites may be added before the submission in March 2020.

III. RÉSUMÉ

LOGIPEDIA is an on-line system-independent encyclopedia of formal proofs. We plan to submit a proposal to the European call INFRAIA-02-2020: Integrating activities for starting communities on March 17th, 2020 to develop it and transform it into a European e-infrastructure. Our long-term goal is to build in twenty years an encyclopedia that contains all the formal proofs then developed.

Formal proofs and formal methods are now an important part of some advanced industrial projects. For instance, mastering formal methods is key to give Europe a competitive advantage in conquering the market of autonomous vehicles. It is also an important aspect of the evolution of mathematics, as it allows much more complex proofs to be built. But the absence of standard for formal proofs limits this impact, at it limits the interoperability between proof systems and the sustainability of formal proofs. This motivates our project to develop this on-line system-independent encyclopedia of formal proofs.

As a first step in this direction, the LOGIPEDIA kick off meeting, in January 2019, brought together 38 researchers from Austria, Czech Republic, France, Italy, the Netherlands, and Poland. Since then, colleagues from Belgium, Germany, Serbia, Sweden, and United Kingdom have manifested interest. Such an encyclopedia can only have a worldwide ambition. However, as several proof systems developed in the world are European, Europe can take the lead on this project, without excluding our non European colleagues.

The design of such an encyclopedia has several goals: making proof systems interoperable, making formal proofs sustainable, restoring the universality of logical truth, and, more than everything, making formal proofs available to non specialist communities: working mathematicians, engineers, and students.

The development of such an encyclopedia raises scientific questions related to the expression of mathematical theories in a common logical framework, such as DEDUKTI, on which LOGIPEDIA is based, to the analysis of formal proofs in order to decide in which theories they can be expressed, and to the organization of such a large corpus of proofs, in particular concept alignment, that is the identification of isomorphic structures and notions, such as Cauchy and Dedekind real numbers.

Our consortium gathers teams that have experience in the development of proof systems, in interoperability between proof systems, in the development and use of logical frameworks, and in the development of large libraries of proofs.

Our agenda, for the coming years, is focused on

- Defining in DEDUKTI the theories implemented in AGDA, COQ, LEAN, PVS, ISABELLE / HOL, HOL 4, MIZAR, TLA+, and B, besides MATITA, HOL LIGHT, and FOCALIZE that already have been defined.

- Importing libraries in LOGIPEDIA: general libraries, such as the standard libraries of COQ, ISABELLE / HOL, HOL LIGHT, AGDA, etc., advanced mathematical libraries such as the MATHCOMP library, the MIZAR library, the ISABELLE ARCHIVE OF FORMAL PROOFS, the GEOCOQ library, the FLYSPECK library, the NASA PVS library, etc., libraries of proofs of programs, such as the SEL4 library, the COMPCERT library, etc.

- Constructing tools to analyze these proofs and align concepts, that is unify concepts such as connectives and quantifiers, the concept of natural number, etc. and theorems that occur in several libraries.

- Constructing tools to index and browse this encyclopedia, that is find the theorem one needs, either by looking for it with its name, with its statement, or with symbols occurring in it.

The proposal meets several of the objectives of the call INFRAIA-02-2020: Integrating activities for starting communities: synergy, open research data, wider and more efficient access, education, closer interaction between a larger number of researcher, better management of the continuous flow of data, and innovation. It also clearly refers to one of the mentioned cross-cutting activities: open science.

IV. PROPOSITION DE RÉSEAU

1. *a) Pertinence, originalité et innovation du sujet*

We plan to submit a 5 M€ proposal to the European call INFRAIA-02-2020: Integrating activities for starting communities on March 17th, 2020 to make LOGIPEDIA [DowekThiré19, Logipedia] a European e-infrastructure. So far, the project has been funded by Inria through the financing of our research group and the support of two research engineers: Hande Gözükan and Romain Primet.

State of the art

Formal proofs, and software manipulating such proofs, such as COQ [Coq], MATITA [Matita], LEAN [Lean], AGDA [Agda], HOL LIGHT [HOL Light], ISABELLE / HOL [Isabelle], PVS [PVS], MIZAR [Mizar], TLA+ [TLA+], B [Abrial96], etc., have become a central tool both in safety and security and in mathematics, as shown by several major successes: the correctness proof of the Paris metro line 14, the proved operating system SEL4 [Klein09], the proved C compiler COMPCERT [Leroy06], the formalization of the proofs of Feit-Thompson theorem [Gonthier13] and Hales theorem [Hales17], etc. The development of these formal proofs has led to the construction of huge libraries, totalizing millions of hours of work, that are a significant part of mankind's mathematical assets.

Software development has always been accompanied with the definition of standards, that make systems interoperable and data sustainable. For example, web browsers are interoperable and websites are sustainable because they all comply with the HTML standard. The area of formal proofs is however an exception. So,

while we have been talking in the past about (informal) proofs of Pythagoras' theorem or Fermat's little theorem, we are now talking about (formal) proofs in COQ, MATITA, or HOL LIGHT, etc. of these theorems. This lack of standards, is the major weakness of this area, as it jeopardizes the usability and the sustainability of these libraries. Indeed, each library is specific to a proof system, most of the time even to some version of this system. A library developed in one system cannot, in general, be used in another and when the system is no more maintained, the library may disappear. Being a major weakness, standard design is also a major challenge.

On more theoretical grounds, this lack of a standard jeopardizes the universality of logical truth. This problem has already been faced in the past: with non Euclidean geometries in the 19th century, with constructivity in the 20th century, some statements could be true in one geometry or in one logic, but not in others. In these cases, a remediation has been found: the definition of the various geometries in predicate logic permitted to restore the universality of mathematical truth, just like ecumenical logic [Prawitz15, Dowek15, PereiraRodriguez17] later reconciled constructive and classical logic.

This lack of universality of logical truth severely limits the spreading of formal proofs in non specialist communities. For instance, while logic is taught to undergrad students, it is difficult to teach them formal proofs, as this requires the choice of a specific language and system, that looks arbitrary and to explain many idiosyncratic details of this system, that may be seen as a waste of time. The same could be said for the use of formal proofs in industry or by working mathematicians. So another aspect of this challenge is to make formal proofs more accessible, as standards often do.

This idea of building such a standard for proofs has already been investigated in the past, such as in the QED manifesto [Qed94], but, until recently, it has produced no convincing results. Indeed, each system implements a different theory, and a proof developed in one system can not always be translated into another. As already noted, this diversity of theories has already been faced, for instance in the 19th century, with the diversity of geometries. This diversity has however been tamed by the expression of these theories in the same logical framework: predicate logic [HilbertAckermann28]. In predicate logic, each theory is expressed with a finite number of axioms or axiom schemes, making it possible to determine which axioms is used in which proof, for instance if a proof uses the axiom of parallels or not, the axiom choice or not, and thus to determine in which theories it can be expressed. Thus, interoperability of proof systems does not just require the definition of a standard, but also the ability to analyze in which theories a proof can be expressed, a domain traditionally called “reverse mathematics” [Freidman76, Simpson09, Dowek17], this itself requiring the ability to express these theories in a common logical framework.

Predicate logic, the first logical framework in the history of logic, proposed in 1928 by Hilbert and Ackermann, has been a huge success, since three important theories: geometry, arithmetic and set theory have been expressed in it. But it also has limitations. For instance, one of the major theories used at that time: Russell's type theory (*The Principia Mathematica*) has not been expressed in it. Then, several other versions of type theory, Church's type theory [Church40], Martin-Löf's type Theory [Martin-Löf84] and the Calculus of constructions [CoquandHuet88], have also been defined as autonomous theories, and not in predicate logic. This failure has led, in the field of proof processing, to abandon predicate logic, and even the concept of logical framework: the theories implemented in COQ, MATITA, HOL LIGHT, etc. are often defined as autonomous systems, and not in a logical framework.

However, a stream of research has attempted to understand the limitations of predicate logic and to propose other logical frameworks repairing them. The most prominent limitations of predicate logic are the lack of function symbols binding variables, the lack of a syntax for proof terms, the lack of a notion of computation,

the lack of a notion of cut for axiomatic theories, and the impossibility to express constructive proofs. These limitations have led to the development of other logical frameworks: λ-PROLOG [NadathurMiller88,MillerNadathur12], ISABELLE [Paulson90], the λΠ-calculus [HarperHonsellPlotkin91], also called the "Edinburgh logical framework", Deduction modulo theory [DowekHardinKirchner03, DowekWerner03], Pure Type Systems [Berardi88, Terlouw89], and ecumenical logics [Prawitz15, Dowek15, PereiraRodriguez17]. The λΠ-calculus modulo theory [CousineauDowek07], implemented in the system DEDUKTI [ASSAF16], is a synthesis of these frameworks. It not only allows the expression of geometry, arithmetic and set theory, but also that of Russell's type theory, Church's type theory, Martin-Löf's type theory, and the Calculus of constructions.

In the years 2010-2015, it was shown that theories implemented in HOL LIGHT [Assaf12], MATITA [Assaf15], and FOCALIZE [Cauderlier16] could be expressed in DEDUKTI, and that the libraries of these systems could be translated to DEDUKTI, as well as the proofs produced with the automated theorem proving systems IPROVER [Burel10] and ZENON [CauderlierHalmagrand15], in particular on the expression in DEDUKTI of B proofs produced by ZENON and also by the SMT solver ARCHSAT [Bury19]. In the years 2015-2020 we started to focus on the translation of proofs from one library to another [Dowek17, Thiré18]. This led us to propose an on-line system-independent encyclopedia of formal proofs LOGIPEDIA (http://logipedia.science) in which each proof is labeled with the axioms and computation rules it uses, which helps to determine the systems in which it can be used. In particular, we have showed that the arithmetic library of MATITA could be translated into five other, significantly different, systems: HOL LIGHT, ISABELLE / HOL, PVS, COQ, and LEAN.

Thus, since the QED project, the situation has changed radically, because after thirty years of research, we have an empirical evidence that most of the formal proofs developed in one of these systems can also be developed in another, we understand the relationship between the theories implemented in these systems much better, we have developed several logical frameworks, extending predicate logic, in which these theories can be expressed, and we have developed reverse mathematics algorithms to analyze which axioms and rules are used in each proofs and algorithms, such as constructivization algorithms, to translate proofs from one theory to another.

The project

The LOGIPEDIA kick off meeting http://deducteam.gforge.inria.fr/seminars/190121.html, in January 2019, brought together 38 researchers from Austria, Czech Republic, France, Italy, the Netherlands, and Poland. Since then, colleagues from Belgium, Germany, Serbia, Sweden, and United Kingdom have manifested interest. Some of these researchers are ready to contribute to LOGIPEDIA, that currently contains a few hundred lemmas, aiming at having in twenty years all the formal proofs then developed, in a single encyclopedia. Such an encyclopedia can only have a worldwide ambition. However, as several proof systems developed in the world are European, Europe can take the lead on this project, without excluding our non European colleagues working, for instance, on HOL LIGHT, PVS, and LEAN.

Currently, we know how to express the theories of HOL LIGHT, MATITA, and FOCALIZE in DEDUKTI and recheck proofs developed in these systems. In the next five years, we plan to address the theories of AGDA, COQ, LEAN, PVS, ISABELLE / HOL, HOL 4, MIZAR, TLA+, and B. Some systems, for instance NUPRL or ACL2, are kept for later, except if some other groups join the project. Beyond our main focus on interactive systems, we also plan to integrate some proofs coming from automated theorem provers, SMT solvers, and model checkers, when the proofs have a reasonable size. We already have experience with ZENON, IPROVER,

and ARCHSAT, but we also plan to go in this direction, in cooperation with our colleagues working on LFSC [Stump09].

Finally, we must also structure this encyclopedia: some of the libraries we start with already have a structure (modules, qualified names, etc.) that it is important to preserve. But, in addition, each library contains a definition of natural numbers, real numbers, etc. and, most importantly, logical connectors, that must be aligned.

This leads to a first sketch of work packages, that we will define more precisely in the proposal.

1. Define in DEDUKTI the theories implemented in AGDA, COQ, LEAN, PVS, ISABELLE / HOL, HOL 4, MIZAR, TLA+ and B. Some theories, such as those of ISABELLE / HOL, HOL4, LEAN, AGDA and B will require a minimal amount of work, as we have already developed the techniques to deal with the comparable languages. For others, such as those of COQ or PVS, preliminary investigations are been carried out and need to be completed. Others, such as those of MIZAR or TLA+ are newer.

2. Import libraries in LOGIPEDIA: general libraries, such as the standard libraries of COQ, ISABELLE / HOL, HOL LIGHT, AGDA, etc., advanced mathematical libraries such as the MATHCOMP library, the MIZAR library, the ISABELLE ARCHIVE OF FORMAL PROOFS, the GEOCOQ library, the FLYSPECK library, the NASA PVS library, etc., libraries of proofs of programs, such as the SEL4 library, the COMPCERT library, etc.

3. Construct tools and proofs to analyze these proofs and align concepts, that is unify concepts such as connectives and quantifiers, the concept of natural number, etc. and theorems that occur in several libraries.

4. Construct tools to index and browse this encyclopedia, that is find the theorem one needs, either by looking for it with its name, with its statement, or with symbols occurring in it.

The proposal will focus on

1. Hiring doctoral students, post-doctoral researchers, and engineers to solve the above mentioned problems.

2. Organizing a yearly meeting to present the state of the art of the development of the encyclopedia.

3. Organizing smaller meetings where four to eight researchers work on a specific theory or library.

4. Building a permanent advisory board where industrial partners, and international academic partners (including non European ones) will discuss the future of the encyclopedia. This board will include among others June Andronick (Data61, Kensington NSW), Denis Cousineau (Mitsubishi Electric), Natarajan Shankar (SRI), Aaron Stump (Iowa), Laurent Voisin (Systerel).

All these objectives contribute to building a new formal proof community, focused on the values of knowledge exchange and sustainability.

Innovation

Formal methods are now an important part of some advanced industrial projects. For instance, mastering formal methods is key to give Europe a competitive advantage in conquering the market of autonomous cars, trains, planes, and drones. But this penetration of formal methods in industry hits the same obstacle that researchers often promote one method, theory or system, while their industrial partners are in search of

universality. We expect to make formal proofs more accessible to industry by avoiding each project to redevelop elementary proofs, but instead benefit of the formalization work shared with other communities.

b) adéquation de la proposition avec l'appel européen visé H2020

The proposal meets several of the objectives of the call INFRAIA-02-2020: Integrating activities for starting communities (listed on page 56 of the part 4 of *Horizon 2020 Work Programme 2018-2020*). It also clearly refers to one of the mentioned cross-cutting activities: open science.

Synergy – Open research data. Instead of having a scattered community, each group developing a library for its own logic and its own system, researchers will be able to work together on common developments, reusing proofs developed in other systems and in other communities. In terms of networking, we have already organized one LOGIPEDIA meeting and the funding will insure we can continue to organize large-scale international meetings on a regular basis. The first LOGIPEDIA event has proven to be very valuable in terms of exchange of best practices. In terms of joint research activities, a scientific roadmap will be planned during the next months meetings funded by this MRSEI call and the roadmap will insure we can hire scientific personnel whose activities will be dedicated to to improve, in quality, the integrated services provided at European level by LOGIPEDIA.

Wider and more efficient access. In a shared public encyclopedia providing virtual access, each user can find formal proofs in the logic she wants, regardless the logic and system this proof has been developed in. A data management plan will be provided according to Inria's compliance policy with EU regulations. We also engage ourselves to make the evolution of the LOGIPEDIA e-infrastructure compliant with the European charter for access to research infrastructures.

Education – Closer interaction between a larger number of researcher. Education to formal methods in computer science and to formal proofs in mathematics always hits the same obstacle: the need to choose a specific theory or system, which is in contradiction with the universality of logical truth. Education to formal methods and formal proofs will gain in universality once it will be demonstrated that this choice amounts to include, or not, a few axioms and reduction rules. We believe that this renewal of logic education at university level and before is of prime importance in our "post-truth era".

Better management of the continuous flow of data. A shared encyclopedia allows a better sustainability of the formal proofs developed over time. Too many formal proofs developed in the past are not available any more.

Innovation. As said earlier, we expect to make formal proofs more accessible to industry by allowing each project to benefit of the formalization work shared with other communities.

2. ***Qualité et crédibilité du réseau envisagé***

The construction of such a system-independent online encyclopedia of formal proofs requires a cooperation between teams that have experience in

1. the development of proof systems,

2. interoperability between proof systems (point-to-point and larger scale), including concept alignment, that is the identification of isomorphic structures and notions, such as Cauchy and Dedekind real numbers,

3. the development and use of logical frameworks,

4. the development of large libraries of proofs.

We have identified 16 groups in 10 European countries ready to contribute to this effort : Belgrade, Bialystok, Bologna, Cambridge, Clearsy, Erlangen, Göteborg, Innsbruck, Liège, München, Nancy, Paris, Prague, Saclay, Sophia-Antipolis, and Strasbourg.

These include researchers working on the development of proof systems (such as AGDA, COQ, ISABELLE / HOL, and MIZAR) researchers working on interoperability (for instance, between HOL LIGHT and COQ or between proof systems and automated theorem provers: hammers), researchers working on concept alignment (in particular using machine learning to detect similarities), researchers working on databases of theorems (such as the MMT library), researchers working on the development of DEDUKTI and LOGIPEDIA, researchers working on large libraries (such as the ISABELLE ARCHIVE OF FORMAL PROOFS, MATHCOMP, and GEOCOQ).

We also are in contact with non European colleagues at SRI, Nasa Langley Research Center, Amazon WS, the University of Iowa, and Data61 working on HOL LIGHT, PVS, LFSC, and SEL4.

We can already sketch which group is interested in which work packages. Although this will be defined more precisely in the proposal:

+ the Saclay group is interested in the development of DEDUKTI and LOGIPEDIA,

+ the Innsbruck group and the Bialystok group are interested in the expression of the MIZAR library in LOGIPEDIA,

+ the Saclay group, the Paris group and the Sophia-Antipolis group is interested in the expression of the COQ library and of the MATHCOMP library in LOGIPEDIA,

+ the Strasbourg group and the Belgrade group are interested in the expression of geometry in LOGIPEDIA,

+ the Clearsy group is interested in the expression of B in LOGIPEDIA,

+ the Göteborg group is interested in the expression of the AGDA library in LOGIPEDIA,

+ the Cambridge group and the München group are interested in the expression of the ISABELLE / HOL library in LOGIPEDIA,

+ the Bologna group is interested in the expression of the MATITA library in LOGIPEDIA,

+ the Liège group and the Nancy group is interested in exporting proofs from SMT solvers and in TLA+ proofs,

+ the Innsbruck group, the Prague group, the Paris group, the Strasbourg group, and the Belgrade group are interested in concept alignment between theories,

+ the Erlangen group is interested in the architecture of large mathematical libraries.

3. *Qualification du coordinateur scientifique*

CV du coordinateur scientifique

Gilles Dowek is Directeur de Recherche at Inria and Professeur attaché at the École normale supérieure de Paris-Saclay. He has been a professor at the École polytechnique (2002-2010) and deputy scientific director of Inria. He has been a visiting scientist at Nasa Langley Research center, at Carnegie Mellon University, and at Computational Logic Inc., in Austin (Texas). He has been a president of the program committee, member of the program committee, or member of the steering committee of several conferences : RTA, TLCA, LICS, CADE, LPAR, CSL, ISR, TYPES, etc.

He is the head of the Scientific board of the Societé Informatique de France (https://www.societe-informatique-de-france.fr/), a member of the Scientific board of La main à la pâte (https://www.fondation-lamap.org/), of the Institut de Recherche Technologique SystemX (https://www.irt-systemx.fr/). He is a member of the CERNA ethics committee (http://cerna-ethics-allistene.org/) . He has been active for fifteen years in the development of computer science in education, in particular in participating to the elaboration of high school curricula. He has published several popular science and philosophy of science books. He writes a monthly column in Pour la Science. He has received several awards, in particular the Grand prix de philosophie of the Académie française for his book *Les métamorphoses du calcul* (Le Pommier, 2007, *Computation Proof Machines*, Cambridge University Press, 2015, also translated to Greek and to Chinese).

He has coordinated the Deducteam group in the last seven years. He and his colleagues are at the origin of Deduction modulo theory, the λΠ-calculus modulo theory, the system DEDUKTI, and the encyclopedia LOGIPEDIA.

Selected publications

G. Dowek, Models and termination of proof-reduction, *International Colloquium on Automata, Languages, and Programming*, 2017.

G. Dowek, Analyzing individual proofs as the basis of interperability between proof systems, invited talk, *Proof eXchange for Theorem Proving*, 2017.

G. Dowek, A theory independent Curry-De Bruijn-Howard correspondence, invited talk, *International Colloquium on Automata, Languages and Programming*, 2012.

D. Cousineau and G. Dowek, Embedding Pure Type Systems in the lambda-Pi-Calculus modulo, *Typed lambda calculi and applications*, 2007.

G. Dowek, Th. Hardin, and C. Kirchner, Theorem proving modulo, *Journal of Automated Reasoning*, 31, 2003, pp. 33-72.

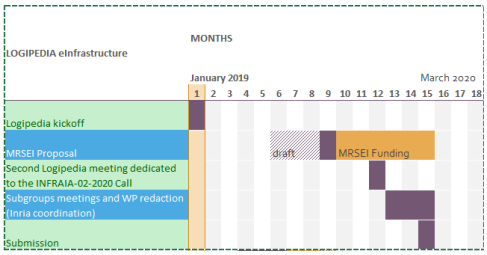
G. Dowek, Third order matching is decidable, *Annals of Pure and Applied Logic*, 1994.

4. *Qualité de la planification de montage du réseau*

The Logipedia kick off meeting took place in January 2019.

We plan to organize a second meeting in December 2019 or January 2020 in order to complete the proposal, in particular to finalize the list of work packages, decide who is going to work on which, and evaluate the number of doctoral students, post-doc, and engineers each group needs to achieve this goals. The project will benefit from Inria Saclay specific support to organise the proposal and the consortium preparation. A part of the requested budget will also be used to optimize the proposal redaction through a consulting agency specialized in the proofreading and coaching of H2020 proposals submissions.

The proposal has to be submitted on March 17th, 2020.



5. *Impact : a) du futur projet b) de l'aide MRSEI*

a) As discussed above, the shift from informal, pencil and paper proofs to formal computerized proof is major improvement on the never ending quest for logical rigor, with a strong impact both on mathematics, where much more complex proofs can be built, and computer science, where safety and security can be dramatically improved with the use of formal methods. But this major step forward also has a negative side effect: we have moved from a time where we had (informal) proofs of Pythagoras' theorem or Fermat's little theorem, to a time where we have (formal) proofs in COQ, in MATITA, in HOL LIGHT, in PVS, etc. of these theorems, jeopardizing the universality of mathematical truth.

We see this loss of universality of mathematical truth as the main obstacle to the diffusion of the notion of formal proof, in the communities of mathematicians and computer scientists, but also engineers and students. Our long-term goal is to resurrect the universality of mathematical truth in order to build a strong formal proof community including specialists and non specialists such as working mathematicians, engineers and students.

This requires to express the theories implemented in these systems in a common logical framework, each with a finite number of axioms and reduction rules, in order to be able to say, not that a proof is expressed in one system or in another, but to say which axioms and reduction rules it uses, as we have been used to since the development of non Euclidean geometries.

Having a standard for expressing theories and proofs and resurrecting this way the universality of mathematical truth will also make proof systems interoperable and will allow the construction of an on-line system-independent encyclopedia. More importantly, this will suppress one of the main obstacles to the diffusion of formal proofs in mathematics, computer science, industry, and education, just like the development of the HTML standard induced a renewal of document sharing in general and the definition of predicate logic induced a renewal of logic in the 1930's.

b) Impact prévisionnel du financement MRSEI pour réussir la coordination du projet européen.

The financing of the Montage de Réseaux Scientifiques Européens ou Internationaux will be used to finance the meeting planed in December or January to finalize the writing of the proposal and several smaller meetings to work on specific aspects of the proposal and also to finance the help of an external agency to help us to finalize the proposal.

This financing is key to the success of this proposal, that gathers almost all the researchers working in Europe (while the community is scattered in sub-communities each focused on a specific theory or systems) and, although the attitude of the community is very positive, its coordination requires some effort.

V. BIBLIOGRAPHIE

1. **Research Papers**

[Abrial96] *The B Book, Assigning Programs to Meanings*, Cambridge University Press (1996).
[Assaf12] A. Assaf, *Traduction de HOL en Dedukti*, Masters thesis (2012).
[Assaf15] A. Assaf, *A framework for defining computational higher-order logics*, Doctoral thesis, École polytechnique (2015).
[Assaf16] A. Assaf *et al.*, "Dedukti : a Logical Framework based on the λΠ-Calculus Modulo Theory", manuscript (2016).
[Avigad18] J. Avigad, The mechanization of Mathematics, Notices of the American Mathematical Society, 65, 6 (2018).
[Berardi88] S. Berardi, "Towards a mathematical analysis of the Coquand-Huet Calculus of Constructions and the other systems in Barendregt's cube", manuscript (1988).
[Burel10] G. Burel, "Embedding deduction modulo into a prover." In A. Dawar and H. Veith, Computer Science Logic, Lecture Notes in Computer Science 6247, Springer-Verlag (2010) pp. 155-169.
[Bury19] G. Bury, *Integrating Rewriting, Tableau, and Superposition into SMT*, Doctoral thesis, Sorbonne Paris Cité (2019).
[Cauderlier16] R. Cauderlier, *Object-Oriented Mechanisms for Interoperability between Proof Systems*, Doctoral thesis, Conservatoire National Des Arts et Métiers (2016).
[CauderlierHalmagrand15] R. Cauderlier, P. Halmagrand, "Checking Zenon Modulo Proofs in Dedukti", Fourth Workshop on Proof eXchange for Theorem Proving (PxTP) (2015).
[Church40] A. Church, "A Formulation of the Simple Theory of Types", *The Journal of Symbolic Logic*, 5(2) (1940), pp. 56–68.
[CoquandHuet88] T. Coquand and G. Huet, "The Calculus of Constructions", *Information and Computation* 76, 2/3 (1988).
[CousineauDowek07] D. Cousineau and G. Dowek, "Embedding Pure Type Systems in the lambda-Pi-calculus modulo", in S. Ronchi Della Rocca, *Typed lambda calculi and applications*, Lecture Notes in Computer Science 4583, Springer-Verlag (2007), pp. 102-117.
[Dowek15] G. Dowek, "On the definition of the classical connectives and quantifiers", E.H. Haeusler, W. de Campos Sanz, and B. Lopes, *Why is this a Proof?, Festschrift for Luiz Carlos Pereira*, College Publications, (2015).
[Dowek17] G. Dowek, "Analyzing individual proofs as the basis of interoperability between proof systems", invited talk, C. Dubois and B. Woltzenlogel Paleo, *Proof eXchange for Theorem Proving*, Electronic Proceedings in Theoretical Computer Science, 262 (2017), pp. 3-12.
[DowekHardinKirchner03] G. Dowek, Th. Hardin, and C. Kirchner, "Theorem proving modulo", *Journal of Automated Reasoning*, 31 (2003) pp. 33-72.
[DowekThiré19] G. Dowek and F. Thiré, "Logipedia: a multi-system encyclopedia of formal proofs", manuscript (2019).
[DowekWerner03] G. Dowek and B. Werner, Proof normalization modulo, *The Journal of Symbolic Logic*, 68, 4 (2003) pp. 1289-1316.
[Friedman76] H. Friedman, "Systems of second-order arithmetic with restricted induction, I, II", *The Journal of Symbolic Logic* 41(2) (1976) pp. 557–559.
[Gonthier13] G. Gonthier *et al.* "A Machine-Checked Proof of the Odd Order Theorem", S. Blazy, Ch. Paulin and D. Pichardie, *4th Conference on Interactive Theorem Proving*, Lecture Notes in Computer Science 7998, Springer-Verlag (2013), pp. 163-179.
[Gowers10] T. Gowers, Rough Structure and Classification, N. Alon, J. Bourgain, A. Connes, M. Gromov, V . Milman, *Visions in Mathematics*, Modern Birkhäuser Classics, Birkhäuser (2010).
[Hales17] T. Hales *et al.*, "A Formal Proof of the Kepler Conjecture". Forum of Mathematics, Pi, 5, E2 (2017).
[HarperHonsellPlotkin91] R, Harper, F, Honsell, and G. Plotkin, "A Framework for Defining Logics", LFCS, Department of Computer Science, University of Edinburgh (1991).
[HilbertAckermann28] D. Hilbert and W. Ackermann, *Grundzüge der theoretischen Logik*, Springer-Verlag (1928).
[Klein09] G. Klein *et al.*, "seL4: Formal verification of an OS kernel", *ACM Symposium on Operating Systems Principles* (2009) pp. 207–220.
[Lamport12] L. Lamport, How to write a 21st century proof, J. Fixed Point Theory Appl. 11: 43 (2012).
[Leroy06] X. Leroy. "Formal certification of a compiler back-end, or: programming a compiler with a proof assistant", *33rd ACM symposium on Principles of Programming Languages (POPL 2006)*, ACM Press (2006), pp. 42-54.
[Martin-Löf84] P. Martin-Löf. *Intuitionistic type theory* (Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980), Bibliopolis (1984).
[MillerNadathur12] D. Miller and G. Nadathur, Programming with Higher-Order Logic, Cambridge University Press", (2012)
[NadathurMiller88]G. Nadathur and D. Miller, An Overview of lambdaProlog, K.A. Bowen and R.A. Kowalski, Fifth International Logic Programming Conference, MIT Press (1988) pp. 810-827.
[Paulson90] L.C. Paulson, "Isabelle: The Next 700 Theorem Provers", P. Odifreddi, *Logic and Computer Science*, Academic Press (1990) pp. 361-386.
[Paulson18] L. Paulson, Formalising mathematics in simple type theory (2018).

[PereiraRodriguez17] L.C. Pereira and R.O. Rodriguez, Normalization, Soundness and Completeness, for the Propositional Fragment of Prawitz' Ecumenical System, Revista Portuguesa de Filosofia 73 (3-4) (2017) pp. 1153-1168.
[Prawitz15] Prawitz, Dag. “Classical versus intuitionistic logic”, E.H. Haeusler, W. de Campos Sanz, and B. Lopes, *Why is this a Proof?, Festschrift for Luiz Carlos Pereira*, College Publications, (2015).
[Qed94] “The QED Manifesto”, A. Bundy, *Proceedings of the 12th International Conference on Automated Deduction (CADE-12)*, Springer-Verlag (1994), pp. 238-251.
[Simpson09] S. G. Simpson, *Subsystems of second-order arithmetic*, Cambridge University Press (2009).
[Stump09] A. Stump, Proof Checking Technology for Satisfiability Modulo Theories, Electronic Notes Theoretical Computer Science 228, (2009), pp. 121–133.
[Terlouw89] J. Terlouw, "Een nadere bewijstheoretische analyse van GSTT’s", manuscript (1989).
[Thiré18] F. Thiré, “Sharing a Library between Proof Assistants: Reaching out to the HOL Family”, Electronic Proceedings in Theoretical Computer Science, EPTCS 274 (2018) pp.57-71.
[Voevodsky14] V. Voevodsky, The Origins and Motivations of Univalent Foundations, The Institute Letter, Institute of Advanced Studies (2014).

2. **System and Library Websites**

[AFP] Archive of Formal Proofs, https://www.isa-afp.org/
[Agda] https://wiki.portal.chalmers.se/agda/pmwiki.php
[CompCert] http://compcert.inria.fr/
[Coq] http://coq.inria.fr
[Dedukti] https://deducteam.github.io/
[GeoCoq] https://geocoq.github.io/GeoCoq/
[HOL4] https://hol-theorem-prover.org/
[HOLLight] https://github.com/jrh13/hol-light
[Isabelle] https://isabelle.in.tum.de/
[Lean] https://leanprover.github.io/
[Logipedia] http://logipedia.inria.fr/
[MathComp] Mathematical Components, https://math-comp.github.io/math-comp/
[Matita] http://matita.cs.unibo.it/
[Mizar] http://mizar.uwb.edu.pl/
[MML] The Mizar Mathematical Library, http://mizar.org/library/
[PVS] http://pvs.csl.sri.com/
[TLA+] https://tla.msr-inria.inria.fr/tlaps/content/Home.html

VI. JUSTIFICATION DU PREVISIONNEL DE DÉPENSES MRSEI

The financing of the Montage de Réseaux Scientifiques Européens ou Internationaux will be used

- to finance the meeting planed in December or January to finalize the writing of the proposal (15 000 €),

- several smaller meetings to work on specific aspects of the proposal (6 777 €),

- to optimize the proposal redaction through a consulting agency specialized in the proofreading and coaching of H2020 proposals submissions (6 000 €),

- frais d'environnement (2 222 €).