Master Internship Proposal

Translation of formal proofs between set theory encodings

Context. The behavior of critical systems, such as programs running automated metros, have to be formally verified to comply with safety guidelines. Several industrial projects use set-based specification formalisms, such as B [BKK+20, Lec24] (or its variant Event-B) and TLA+ [Lam02, NRZ+15], to perform that verification. The ICSPA project (Interoperable and Confident Set-based Proof Assistants) aims at reinforcing the confidence in such formal proofs and allowing interoperability between them. This is done by verifying the proofs developed in B/EventB and TLA+ inside Dedukti[BDG+23], a proof checker simple enough to be audited manually or even re-implemented.

Recently, theory morphisms have been developed for Dedukti [TR25]. Such morphisms can be instantiated to define translations of proofs between different Dedukti encodings.

Purpose. The set theories of B and TLA+ have been encoded in Dedukti [GB25]. The goal of this internship is to translate from the encoding of B/EventB to the encoding of TLA+, and to investigate whether the techniques developed in [TR25] can be applied in order to have interoperability between B/EventB and TLA+. If these two formalisms are based on set theory, they differ in different points. In particular, the set theory of TLA+ is expressed in a logic that does not distinguish terms and formulas. That of B/Event-B is more specific as it is built on top of a typed logic.

Throughout this internship, the candidate is expected to:

- get familiar with the encodings of B/EventB and TLA+ in Dedukti;
- get familiar with theory morphisms in Dedukti [TR25];
- apply theory morphisms to translate from the encoding of B/EventB to the encoding of TLA+;
- implement the translation from the encoding of B/EventB to the encoding of TLA+.

The internship could also explore the translation from TLA+ to B/EventB, even if this one could only be defined partially, exploiting the fact that many proofs do not use the full power of the theory they are expressed in.

Environment. This internship will be supervised by Catherine Dubois (Professor at ENSIIE) and Thomas Traversié (PhD student at CentraleSupélec) in either the Deducteam team at LMF (Laboratoire de méthodes formelles) located at ENS Paris-Saclay or the Samovar laboratory (Paris-Saclay and Evry are two possible locations).

Contact. Catherine Dubois, catherine.dubois@ensiie.fr
Thomas Traversié, thomas.traversie@centralesupelec.fr

References

[BDG+23] Frédéric Blanqui, Gilles Dowek, Émilie Grienenberger, Gabriel Hondet, and François Thiré. A modular construction of type theories. *Log. Methods Comput. Sci.*, 19(1), 2023.

[BKK+20] Michael J. Butler, Philipp Körner, Sebastian Krings, Thierry Lecomte, Michael Leuschel, Luis-Fernando Mejia, and Laurent Voisin. The first twenty-five years of industrial use of the b-method. In Maurice H. ter Beek and Dejan Nickovic, editors, *Formal Methods for Industrial Critical Systems - 25th International Conference, FMICS 2020, Vienna, Austria, September*

2-3, 2020, Proceedings, volume 12327 of *Lecture Notes in Computer Science*, pages 189–209. Springer, 2020.

[GB25] Anne Grieu and Jean-Paul Bodeveix. Encodage du langage mathématique d'Event-B dans Lambdapi. In *36es Journées Francophones des Langages Applicatifs (JFLA 2025)*, Roiffé, France, January 2025.

[Lam02] Leslie Lamport. *Specifying Systems, The TLA+ Language and Tools for Hardware and Software Engineers.* Addison-Wesley, 2002.

[Lec24] Thierry Lecomte. Proving B with atelier B. In Simon Foster and Augusto Sampaio, editors, *The Application of Formal Methods - Essays Dedicated to Jim Woodcock on the Occasion of His Retirement*, volume 14900 of *Lecture Notes in Computer Science*, pages 329–345. Springer, 2024.

[NRZ$^+$15] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. How amazon web services uses formal methods. *Commun. ACM*, 58(4):66–73, 2015.

[TR25] Thomas Traversié and Florian Rabe. Formalizing Representation Theorems for a Logical Framework with Rewriting. working paper or preprint, April 2025.