

# THÈSE DE DOCTORAT DE

NANTES UNIVERSITÉ

ÉCOLE DOCTORALE N° 641  
*Mathématiques et Sciences et Technologies  
de l'Information et de la Communication*  
Spécialité : *Informatique*

Par

**Enzo CRANCE**

## Meta-programming for proof transfer in dependent type theory

Thèse présentée et soutenue à Nantes, le 19 décembre 2023

Unité de recherche : Laboratoire des Sciences du Numérique de Nantes (LS2N)

### Rapporteurs avant soutenance :

Sandrine BLAZY Professeur des universités, Université de Rennes, IRISA  
Anders MÖRTBERG *Associate professor*, Université de Stockholm

### Composition du Jury :

Président :	Prénom NOM	Fonction et établissement d'exercice ( <i>à préciser après la soutenance</i> )
Examineurs :	Sandrine BLAZY Anders MÖRTBERG Enrico TASSI Karl PALMSKOG Guillaume MELQUIOND Nicolas TABAREAU	Professeur des universités, Université de Rennes, IRISA <i>Associate professor</i> , Université de Stockholm Chargé de recherche, Inria Sophia Antipolis Méditerranée, Université Côte d'Azur <i>Senior lecturer</i> , KTH Royal Institute of Technology, Stockholm Directeur de recherche, Inria, Université Paris-Saclay, LMF Directeur de recherche, Inria, Nantes Université
Dir. de thèse :	Assia MAHBOUBI	Directrice de recherche, Inria, LS2N, Nantes
Co-dir. de thèse :	Denis COUSINEAU	Chercheur industriel (docteur), Mitsubishi Electric R&D Centre Europe, Rennes

### Invité(s) :

Mathieu BOESPFLUG Chercheur industriel (docteur), Modus Create

---

**Titre :** Méta-programmation pour le transfert de preuve en théorie des types dépendants

**Mot clés :** preuve formelle, automatisation des preuves, méta-programmation

**Résumé :** En mathématiques comme en informatique, il est d'usage de faire appel à des outils numériques de vérification pour augmenter la confiance dans les preuves et les logiciels. La pratique la plus commune est le test, mais elle est limitée. Les *assistants de preuve interactifs* sont des outils permettant d'effectuer des preuves avec une grande confiance, laissant l'humain trouver les idées des preuves tout en vérifiant méticuleusement que toutes les étapes de la preuve sont valides. Cette thèse s'inscrit dans une lignée de travaux visant à automatiser les preuves, avec l'objectif final de répandre l'usage des assistants de

preuve à la place du test logiciel, partout où cela est possible et pertinent. On s'intéresse ici au partage de théorie formelle entre plusieurs représentations différentes d'un même concept mathématique, ou plusieurs implémentations d'une même spécification. Sur le plan théorique, cette étude s'appuie sur l'analyse de traductions de paramétricité pour le calcul des constructions, et en propose une généralisation. Ces résultats s'incarnent dans la conception de deux outils de transfert de preuve, TRAKT et TROCQ, dont on discute ici l'implémentation, à l'aide du méta-langage COQ-ELPI.

---

**Title:** Meta-programming for proof transfer in dependent type theory

**Keywords:** formal proof, proof automation, meta-programming

**Abstract:** In both mathematics and computer science, it is common practice to use digital verification tools to increase confidence in proofs and software. The most common practice is testing, but it is limited. *Interactive proof assistants* are tools made to perform proofs with high confidence, letting humans come up with proof ideas while meticulously checking that all proof steps are valid. This thesis is part of a line of work aimed at automating proofs, with the ultimate goal of spreading the use of proof assistants in place of software testing, wherever possible and relevant. Here, we are

interested in sharing of formal theory between several different representations of the same mathematical concept, or several implementations of the same specification. From a theoretical point of view, this study is based on the analysis of parametricity translations for the calculus of constructions, and proposes a generalisation of them. These results are made concrete in the design of two proof transfer tools, TRAKT and TROCQ, whose implementation is discussed here, using the COQ-ELPI meta-language.