Intégration d'outils de preuves automatiques à Coq : applications à la géométrie

Laboratoire d'accueil : ICube UMR 7357 CNRS - Université de Strasbourg

Directeur de thèse : Nicolas Magaud (MCF HDR) – magaud@unistra.fr

Mots-clés : Coq, tactiques, outils d'aide à la preuve, preuves automatiques

Sujet : Les assistants de preuve comme Coq permettent, dans un même outil, non seulement d'implanter sous forme fonctionnelle des objets mathématiques et des opérations sur ces objets, mais aussi de démontrer formellement leurs propriétés. Ce travail de spécification et de preuve est confié à l'utilisateur, le système se contentant de vérifier, au fur et à mesure, que le raisonnement construit est bien correct. Cette approche permet de s'affranchir des limitations des outils automatiques et de tirer profit, à plein, de l'intelligence et de l'inventivité humaines. Néanmoins, plus les preuves sont complexes, et plus il est nécessaire de fournir des outils pratiques pour aider le développeur. Il existe bien sûr quelques procédures de décision pour des fragments décidables des théories considérées. Très utilisés en pratique, ces outils sont cependant bien moins puissants que certains prouveurs automatiques comme Vampire, CVC4 ou Z3. En plus de ces prouveurs génériques, des prouveurs spécifiques, comme celui dédié à la géométrie projective, ont été développés récemment dans l'équipe IGG.

L'objectif de cette thèse sera d'étudier comment exploiter efficacement en Coq ces outils automatiques pour aider l'utilisateur dans son travail de preuve. Deux directions seront privilégiées. Il s'agira dans un premier temps de faciliter la communication et l'interaction entre les prouveurs automatiques et Coq (en transformant les traces de preuves générées par les prouveurs automatiques en certificats vérifiables automatiquement par Coq). Dans un second temps, on cherchera à intégrer directement dans Coq certains mécanismes de raisonnement utilisés dans les prouveurs automatiques en les rendant disponibles sous forme de tactiques, utilisables interactivement.

Afin d'évaluer les capacités et les performances des outils mis en oeuvre, nous nous intéresserons, en premier lieu, aux modèles finis de la géométrie projective où la taille des modèles est un obstacle à leur formalisation dans un système interactif comme Coq. D'autres applications pourront être envisagées, notamment en combinatoire des objets géométriques. Il s'agira, par exemple, d'énumérer certaines familles de cartes, d'établir des bijections entre des représentations non trivialement équivalentes des cartes ainsi qu'entre les cartes planaires enracinées et λ-termes planaires.

Compétences souhaitées :

Développement logiciel, preuves assistées par ordinateur, programmation fonctionnelle, logique, géométrie

Expertises qui seront acquises :

Développement de preuves formelles de grande taille, interopérabilité des systèmes de preuves, géométrie et combinatoire

Mots-clés : preuve automatique, preuve interactive, Coq, tactiques, outils d'aide à la preuve

Integrating Automated Reasoning Tools to the Coq Proof Assistant: Applications to Geometry

Research Laboratory: ICube UMR 7357 CNRS - Université de Strasbourg

Thesis supervisor: Nicolas Magaud (MCF HDR) – magaud@unistra.fr

Mots-clés : Coq, tactiques, outils d'aide à la preuve, preuves automatiques

Proofs assistants such as Coq allow, using the same infrastructure, not only to implement mathematical objects and their operations using the functional programming paradigm, but also to formally prove some of their properties. This specification and proof task is devoted to the user whereas the system checks that the reasoning arguments are correct. Thanks to this approach, relying on human intelligence, there are no limitations related to the power of the automatic decision procedures available. However, as proofs grow in size and complexity, it becomes unavoidable to have practical tools to help the user carry out some proof steps automatically. Decision procedures for decidable fragments of the considered theories are sometimes available but they are a lot less powerful than automated first-order provers such as Vampire, CVC4 or Z3. In addition to these generic provers, some more specialized provers, especially one dedicated to projective geometry, have been recently developed in the IGG team.

In this thesis project, we aim at proposing new ways to exploit the capabilities of these automated provers to help the user complete its proof development. Two main directions shall be investigated. First, we shall enhance the communication between the automated provers and Coq (by transforming the proof traces they produce into proof certificates automatically checkable by Coq). In a second phase, we plan to integrate this reasoning mechanisms directly inside the Coq proof assistant and provide them as interactive tactics.

To evaluate the performances of these tools, we propose to study finite models of projective geometry where the size of the models makes the formalization in an interactive system like Coq very challenging. Other applications are envisioned in the combinatorics of geometric objects. Among them, we shall consider enumerating some families of combinatorial maps, and establish some non-trivial equivalences between some families of maps and some families of lambda-terms.

Expected skills :

Software development, Interactive Theorem Proving, Coq Functional Programming, Logic

Skills to be acquired during the PhD programme:

Building large proof developments, interoperability of proof systems, geometry and combinatorics, implementation of proof transformations and translations from one system to another

Keywords: automated theorem proving, interactive theorem proving, Coq, tactics, interoperability of systems