UNIVERSITÉ D'ARTOIS

Avis de Soutenance

Monsieur Daniel CROWLEY

Informatique et applications

Soutiendra publiquement ses travaux de thèse intitulés
A Dual-Approach Framework for Verifying Proof Obligations

Travaux dirigés par Monsieur Daniel LE BERRE et Monsieur Yakoub SALHI

Soutenance prévue le ***vendredi 27 novembre 2026*** à 9h30
Lieu : Faculté des sciences Jean Perrin, Bâtiment B Rue Jean Souvraz S18 62307 Lens Cedex
Salle : des thèses

Composition du jury proposé

M. Daniel LE BERRE	Université d'Artois	Directeur de thèse
M. Yakoub SALHI	Université d'Artois	Co-directeur de thèse
Mme Maroua BOUZID	Université de Caen Normandie	Examinatrice
M. Pascal FONTAINE	Université de Liège	Examinateur
M. Djamal HABET	Aix-Marseille Université	Rapporteur
M. Frédéric LARDEUX	Université Angers	Rapporteur
M. Olivier ROUSSEL	Université d'Artois	Invité

Résumé :
Cette thèse essaye de faire des propositions pour simplifier la vie des ingénieurs qui travaillent avec des obligations de preuve pour vérifier l'exactitude et la sûreté de spécifications de systèmes. Plus spécifiquement, ce travail a été effectué dans le cadre du projet BLaSST visant à enrichir le raisonnement avec la méthode B en bénéficiant de techniques SAT et SMT. Cette thèse se concentre plutôt sur l'approche SAT. Des ingénieurs de sûreté de fonctionnement définissent des machines qui représentent les systèmes étudiés, à partir desquelles sont ensuite générées des obligations de preuve. La validité de chacune de ces obligations de preuve doit être validée afin de garantir la fiabilité de la machine et du système. Une telle obligation de preuve peut être vérifiée et déchargée, soit automatiquement, soit interactivement avec l'aide d'un ingénieur humain. Si la spécification est incorrecte, certaines d'entre les obligations de preuve générées sont invalides. Quand la spécification est fausse, il vaut mieux que l'ingénieur s'en rende compte le plus tôt possible pour éviter de travailler sur un ensemble d'obligations de preuve dont quelques éléments sont forcément invalides et de se mettre à corriger la machine et à prouver des nouvelles obligations de preuve. Munie de techniques basées sur la logique propositionnelle et avec du raisonnement qualitatif, cette thèse cible à automatiser des obligations de preuve générées à partir de machines en langage B qui ne sont pas déjà prouvées automatiquement par des solveurs ateliés à la méthode B. Ce but du travail est la réduction du nombre de preuves interactives nécessaires pour toutes les décharger et pour valider la machine. Un autre but est d'informer les ingénieurs des invalidités d'une manière intuitive en proposant des contre-modèles interprétables qui puissent aiguiller l'ingénieur lors de la redéfinition de la spécification. En lien avec cet aspect serait une proposition d'un moyen de calculer la résistance de contre-modèles à la réparation. Un développement de cette idée pourrait aboutir à un outil qui conseille à l'ingénieur de recommencer la construction d'une spécification ou de manipuler légèrement la machine incorrecte que l'on a déjà définie selon la gravité des erreurs. L'alphabet du langage B offre maintes expressions de la théorie des ensembles : un langage bien plus expressif que celui de la logique propositionnelle. Il existe pourtant des outils très efficaces pour effectuer des tâches en logique propositionnelle quand on arrive à modéliser dans ce langage. Un des plus grands avantages du raisonnement qualitatif est à quel point ses modélisations sont intuitives et visualisables. Cette thèse traduit une partie d'obligations de preuve en langage B en logique propositionnelle et en raisonnement qualitatif mais en plus elle intègre la logique propositionnelle et le raisonnement qualitatif pour permettre à une modélisation qualitative à exprimer des contraintes plus riches, par exemple, avec des implications ou des disjonctions. Outre les spécificités de cette thèse, ce manuscrit présente des résultats expérimentaux pour l'évaluation du projet BLaSST et qui ont été obtenus dans notre unité de recherche.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

anr agence nationale de la recherche