Specifying and Verifying Safety Properties of Parallel Programming Algorithms Using the TLA+ Toolbox

Auteur : Differdange, Jarod
Promoteur(s) : Fontaine, Pascal
Faculté : Faculté des Sciences appliquées
Diplôme : Master : ingénieur civil en informatique, à finalité spécialisée en "computer systems security"
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/23374

Specifying and Verifying Safety Properties of Parallel Programming Algorithms Using the TLA+ Toolbox

Supervisor : Pascal Fontaine, Professor - ULiège
Co-Supervisor : Stephan Merz, Director of Research - INRIA Nancy

Master's thesis completed in order to obtain the degree of
Master of Science in Computer Science and Engineering

by Jarod Differdange

University of Liège
-
School of Engineering and Computer Science
Academic year 2024-2025

In order to build a formal companion to the Parallel Programming course given by Professor Pascal Fontaine, the algorithms presented therein have to be specified in a formal description language. Using TLA^+, two algorithms presented were formalized and proofs of correctness have been written and verified. First, the barrier synchronization facility presented in the course, which uses a turnstile-like construction. has been shown to behave like an abstract barrier which moves processes synchronously, using invariants that describe the behavior of the barrier. Second, the equivalence of two lock implementations has been verified using the mechanism of refinement. Refinement proves that any execution of an algorithm is a valid execution of another. To prove equivalence a two-way refinement is needed. Using auxiliary variables, this has been achieved between Peterson's algorithm and an abstract lock.

Spécification et vérification de propriétés de sûreté d'algorithmes parallèles avec la TLA+ Toolbox

Promoteur : Pascal Fontaine, professeur - ULiège
Co-promoteur : Stephan Merz, directeur de recherche - INRIA Nancy

Travail de fin d'études présenté en vue de l'obtention du grade de :
Master Ingénieur civil en informatique

par Jarod Differdange

Université de Liège
-
Faculté des Sciences Appliquées
Année académique 2024-2025

Afin de construire un compagnon formel au cours de programmation parallèle donné par le professeur Pascal Fontaine, les algorithmes présentés doivent être spécifiés dans un langage de description formel. En utilisant TLA$^+$, deux algorithmes présentés ont été formalisés et des preuves ont été écrites et vérifiées. Premièrement, le dispositif de synchronisation de barrière présenté dans le cours, qui utilise une construction de type tourniquet, a été montré se comportant comme une barrière abstraite qui déplace les processus de manière synchrone, en utilisant des invariants qui décrivent le comportement de la barrière. Deuxièmement, l'équivalence de deux implémentations de verrous a été vérifiée à l'aide du mécanisme de raffinement. Le raffinement prouve que toute exécution d'un algorithme est une exécution valide d'un autre algorithme. Pour prouver l'équivalence, un raffinement bidirectionnel est nécessaire. En utilisant des variables auxiliaires, cela a été réalisé entre l'algorithme de Peterson et un verrou abstrait.