

N/A

**Auteur** : Leruth, Guillaume

**Promoteur(s)** : Fontaine, Pascal

**Faculté** : Faculté des Sciences appliquées

**Diplôme** : Master : ingénieur civil en informatique, à finalité spécialisée en "computer systems security"

**Année académique** : 2023-2024

**URI/URL** : <http://hdl.handle.net/2268.2/20979>

---

*Avertissement à l'attention des usagers :*

*Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.*

*Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.*

---

# Specifying and Verifying Safety Properties of Parallel Programming Algorithms Using the TLA<sup>+</sup> Toolbox

Guillaume Leruth

Section: Computer Science and Engineering

Supervisor: Pascal Fontaine - Professor, ULiège

Co-Supervisor: Stephan Merz - Senior Researcher, INRIA Nancy

Academic year 2023 - 2024

The goal of this Master's thesis is to specify and verify safety properties of a few classical algorithms taken from the Parallel Programming lectures taught by Prof. Pascal Fontaine by using the TLA<sup>+</sup> Toolbox.

The first chapter of this work lays out the minimal concepts of concurrent programming required to motivate the distinctive significance of software verification in the world of parallel and distributed algorithms. The second one presents all the tools of the TLA<sup>+</sup> environment used in the following chapters. A rough methodology is then established to turn the pseudo-code descriptions of algorithms presented in the lecture material into unambiguous TLA<sup>+</sup> specifications and to consequently identify and express safety properties of interest before checking and proving them.

The next chapters consist in applying the previously described tools and methods to Barz's algorithm and the Readers-writers algorithms taken from the lecture material. The resulting TLA<sup>+</sup> specifications, adjoining definitions and properties as well as TLAPS proofs constitute the original contribution of this Master's thesis. Regarding Barz's algorithm, the main achievement is the refinement proof which states that Barz's algorithm is a valid implementation of the abstract general semaphore. When it comes to the readers-writers, the proof associated to the main inductive invariant required significant manual tuning using the TLAPS theory of finite sets.