

From Graphical Loop Invariants to Formal Verification

Auteur : Grosjean, Antoine

Promoteur(s) : Fontaine, Pascal; Donnet, Benoît

Faculté : Faculté des Sciences appliquées

Diplôme : Master : ingénieur civil en informatique, à finalité spécialisée en "management"

Année académique : 2024-2025

URI/URL : <http://hdl.handle.net/2268.2/23376>

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.

From Graphical Loop Invariants to Formal Verification

Montefiore Institute of Electrical Engineering and Computer Science
Faculty of Applied Sciences
University of Liège

Abstract

Logic and mathematics are essential for understanding and verifying computer programs, yet many first-year computer science students struggle with these subjects.

This Master's thesis represents a first step toward automating the verification of simple C programs without requiring students to master formal logic. It demonstrates the feasibility of developing and implementing a tool that uses Loop Graph Invariants to verify computer programs written in C.

To this end, a comprehensive process was developed and tested on ten programming problems covering the content of the introductory computer programming course taught at the University of Liège. All benchmarks were eventually verified.

The methodology implemented relies on using the Dafny programming and verification language. It also involves a code translator that converts a C program into a program following the Dafny syntax, as well as an Embedding Model for French developed by La Javaness, used to extract the semantics of French sentences.

Although the process is not fully automated, it paves the way for future research on the subject and the eventual realization of a complete system.

Information

Type:	Master's thesis carried out to obtain the degree of Master of Civil Engineering in Computer Science
Author:	Antoine Grosjean
Academic supervisors:	Pr. Pascal Fontaine Pr. Benoît Donnet
Academic year:	2024-2025
Keywords:	Verification, Invariant, Dafny, Loop, C, Graphical Loop Invariant, Predicate, Automation, Logic, Correctness.