

Title: Verification of Cost Bounds in Coq

Description: The goal of the project is to develop a checker that can formally prove, by using the Coq proof assistant, the correctness of the cost bounds inferred by an existing cost analysis tool (whose implementation has not been proven correct). We will follow a translation validation approach in which rather than verifying the cost analyzer, we verify the correctness of the bounds generated by it. Both proof assistants and static analysis tools will be studied in the courses of the Master.

Supervisors: Elvira Albert (elvira@sip.ucm.es) and Samir Genaim (sgenaim@ucm.es)

Title: Plugin for automatic testcase generation in Python

Description: Testing is an important activity of software developers. It improves code quality and detects bugs before releasing your program. Additionally, Python is one of the most popular programming languages. In this master thesis, you will implement a plugin for a popular IDE (Eclipse or IntelliJ). It will automatically generate a set of testcases for a Python program such that they fulfill a specific type of branch coverage.

Supervisors: Manuel Nuñez (mn@sip.ucm.es), José Ignacio Requeno (jrequeno@ucm.es)

Title: Study of Computability and/or Complexity

Description: the project will consist in developing some original research in Computability or Complexity areas in some topic to be agreed with the student. For instance, the following choices are possible: (a) considering a problem from the Computer Science area or out of it (e.g. Economics, Biology, Physics, Political Science, social sciences in general, etc.) whose Complexity or Computability properties have not been studied yet, and proving properties such as NP-hardness, approximability hardness, hardness beyond NP, Turing-completeness, etc.; (b) developing some new knowledge around the P vs NP problem, such as identifying properties of problems which cannot be solved with polynomial-size circuits (approaching $P \neq NP$ via P/poly); (c) identifying new properties around central theorems of Complexity theory, such as the PCP theorem; etc.

Supervisor: Ismael Rodríguez Laguna (isrodrig@ucm.es).

Title: Formal testing of quantum programs

Description: The goal of this master's thesis is to review the state-of-the-art on formal approaches to test quantum programs and present a new proposal building on top of current work. Specifically, metamorphic testing, a testing technique used to validate systems where an oracle is not available, seems to be a very suitable candidate to work well with quantum programs. In order to carry out this thesis, the student does not need to have previous knowledge on quantum programming or formal testing.

Supervisors: Luis Llana (llana@ucm.es) and Manuel Núñez (mn@sip.ucm.es)

Title: Metamorphic testing and machine learning models

This thesis will consist of two main parts. The first part will provide a comprehensive survey of the state of the art in *metamorphic testing* applied to machine learning systems. This survey will review existing approaches, types of metamorphic relations, application domains, and evaluation methodologies, identifying current limitations and open research challenges in testing machine learning models without reliable test oracles.

The second part of the thesis will focus on original research, in which new metamorphic relations will be defined and validated for a machine learning application domain that has not been previously addressed in the literature. The student will design and implement these novel relations, apply them to appropriate models and datasets, and experimentally assess their effectiveness in revealing faults or improving confidence in model behavior, thereby contributing new insights to the field.

Supervisor: Manuel Núñez

Title: Computer-aided verification of abstract interpretation-based analyses

Description: Abstract interpretation is a fundamental static analysis framework that enables sound and automatic reasoning about program behavior without executing programs. Its core idea is to approximate the concrete semantics of programs using abstract domains by defining a correspondence between an abstract domain of properties and a concrete domain of values.

The objective of this Master's Thesis is to study computer-aided verification of abstract interpretation-based analyses. First, the thesis aims to formalize and verify some simple concrete analyses in a verification platform, with particular emphasis on the relationship between concrete and abstract semantics. Second, it seeks to specify a generic framework for abstract interpretation-based analyses within a verification platform, capturing general properties such as soundness and monotonicity. No prior knowledge of a specific verification tool (e.g., Dafny, Lean) is required, although enrollment in the course Computer-aided program verification is recommended.

Supervisor: Manuel Montenegro (montenegro@fdi.ucm.es)

Title: Fully Formal Design of Concurrent Systems

Description: We have observed that the use of Formal Models is nearly unavoidable when defining Concurrent Systems, as far as we aim to ensure their correct behaviour with respect to a given specification. However, even when strictly adhering to this methodology, we still have to undertake the development of formal proofs to guarantee the expected properties of our systems. Indeed, there are specific tools to support the use of Process Algebras and Petri Nets as Formal Models; yet, in practice, it is possible to become less rigorous, presenting only partial or overly informal proofs of the desired properties.

For this reason, we advocate for the use of Theorem Provers, such as Lean, to support the development and certification of our systems, ensuring fully verified results. To this end, we propose familiarizing oneself with Lean and the components available in its library, mathlib, to tackle the development of concurrent systems based on Process Algebras or Petri Nets.

Supervisors: Ignacio Fábregas, Fernando Rosa y David de Frutos