Caterina Urban
ANTIQUE Research Team
Inria & École Normale Supérieure
caterina.urban@inria.fr

Static Analyses for Robust Reachability and Unreachability

The notion of *robust reachability* [1] refines standard reachability: a bug is robustly reachable if there exists values for the controlled inputs such that the bug is reached independently of the values of the uncontrolled inputs. Robust reachability is better suited than standard reachability in many realistic situations related to security or software engineering.

Goals. The goal of this project is to revisit and build upon an existing static analysis framework proposed for termination, liveness properties, and general CTL properties [2, 3] to design a static analysis-based approach for robust reachability. The analysis will infer an under-approximation of the values of the controlled inputs for which a bug is robustly reachable.

In a first step, the project will consist in collecting relevant C code snippets and examples and identifying cases for which the existing analysis is already suitable and those for which the existing analysis needs to be adapted.

A second step will involve adapting — both in theory and in practice – the existing analysis to find robustly reachable bugs in all the collected cases. An interesting challenge in this step will be to correctly handle C arrays and pointers.

If time permits, a possible extension of the project is to develop a static analysis-based approach to verify *robust unreachability*, i.e., a bug is robustly unreachable if for all values of controlled inputs there exists values for the uncontrolled inputs such that the bug is unreachable.

Useful Prerequisites. The following skills would be helpful, but can also be learned during the project:

- Background in static analysis and abstract interpretation
- Experience with OCaml

Opportunities. The project offers the following opportunities:

- Apply static analysis and abstract interpretation concepts in practice
- Learn to solve challenging programming problems in OCaml

Contacts

- Caterina Urban
  caterina.urban@inria.fr

References

[1] Guillaume Girol, Benjamin Farinier, and Sébastien Bardin. Not all bugs are created equal, but robust reachability can tell the difference. In *CAV, Part I*, pages 669–693, 2021.

[2] Caterina Urban. *Static Analysis by Abstract Interpretation of Functional Temporal Properties of Programs*. PhD thesis, École Normale Supérieure, Paris, France, 2015.

[3] Caterina Urban, Samuel Ueltschi, and Peter Müller. Abstract interpretation of CTL properties. In *SAS*, pages 402–422, 2018.