Holistic Neural Network Verification with Imandra

Remi Desmartin

March 15, 2022

Abstract

The increased complexity of critical software systems has made it harder to reason about them and to predict edge failure cases. A contributing factor to the complexification of critical systems is the introduction of artificial intelligence (AI) components, often relying on machine learning (ML) techniques.

This reason, among others, has led to an increased demand for automated verification tools. Imandra is one such tool, initially designed for the verification of FinTech systems like trading algorithms and blockchain smart contract infrastructure. Imandra is both a language, in which programs can be modeled and executed, and a reasoning engine. The reasoning engine offers capabilities common to theorem provers such as SMT solving and induction reasoning, and original features (e.g. input space region decomposition); these allow to verify and describe programs' properties.

The integration of ML components adds a layer of complexity to the already nontrivial verification task for which Imandra was designed. Currently, verification of ML algorithms such as neural networks requires separate dedicated tools.

Thus the main goals of this thesis are:

1. to investigate the role of ML components in complex systems
2. to investigate the methods of verification of these components
3. to investigate the integration of ML components' verification in larger verification projects
4. to produce a fully functional ML library in Imandra, which will include domain-specific proof heuristics.