A small experiment in Event-B rippling

Gudmund Grov, Alan Bundy & Lucas Dixon

Although many POs in Rodin are discharged automatically, a large number still require user input – and in many cases, an expert can easily see how to complete a proof. Moreover, in many cases the same “idea” applies to several of the POs, thus creating families of POs (with a similar proof strategy).

In our newly started AI4FM project the goal is to achieve a higher degree of automation by relying on expert intervention to carry out one proof, where this would enable a prover to discharge the others in the same family. Specifically, we hope to build a tool that will learn enough from one proof attempt to improve the chances of proving “similar” results automatically.

Central to our goal is that we find high-level strategies capable of cutting down the search space in proofs. Our hypothesis is:

We believe that it is possible (to devise a high-level strategy language for proofs and) to extract strategies from successful hand proofs that will facilitate automatic proofs of related POs.

Designing a strategy language capable of capturing such properties (in an abstract form) is key to the success of AI4FM. Rippling [1] provides evidence for the possibility of such strategy language. Although it was originally developed to automate step-cases in inductive proofs, it has been used in many domains – including verification of functional, logical and imperative programs; synthesis of theorems, programs and witnesses; correction of faulty specifications and hardware verification.

Our talk is twofold. First we give a general overview of the AI4FM project. Then, we report on a minor experiment in the use of rippling to automate Event-B POs – generated using Rodin. The experiment is conducted in the IsaPlanner system [2].

Acknowledgements

This work is supported by EPSRC grant EP/H024204/1 (AI4FM: using AI to aid automation of proof search in Formal Methods).

References
