THE UNIVERSITY of EDINBURGH
informatics

Productive use of failure in formal methods

Yuhui Lin, Gudmund Grov & Alan Bundy

ARW
Glasgow, 11 April 2011

FMs and POs

- Top down formal methods (FMs) stepwise develops a system from the high-level design to the end product
  - ensures consistency between layers
  - correctness-by-construction
- Posit-and-prove FMs ensures consistency by proof of generated proof obligations (POs).
- Nature of POs in FMs:
  - the number of POs is huge.

  e.g. the Paris Metro line 14, 2250 / 27800 POs
  - 5 - 10% POs require human interaction, which are are expensive to discharge
  - POs tends to exhibit a notion of “similarity”.

  e.g. an industrial case-study using Event-B” 300 POs/200 auto/100 interactive with 5 familes.

THE UNIVERSITY of EDINBURGH
informatics

AI4FM

Outline of proposed work

- Our research hypothesis:
  - *It is possible to classify FM POs/proofs into families by analysing the context of failures.*
  - *In each family there exist patterns of proof strategies.*
  - *The strategy can be used to guide the proof search of the blocked proofs from the same family.*
- Our approach
  - Analyse POs from (mainly existing) models
    - Event-B, VDM, B, Z etc.
    - preferable industrial/GC6

    e.g. Tokeneer, FreeRTOS, ...
  - Derive strategies & patterns of failures from them
  - Develop (strategy) language to capture them

THE UNIVERSITY of EDINBURGH
informatics

AI4FM

Some motivation & initial results

- Rippling is a rewriting technique for the automation of mathematical reasoning which works when the goal is embedded in one of the givens.
  - not exhaustive rewriting - skeleton preserving and measure decreasing
  - guarantees termination whilst allowing rewriting in both directions
- Productive use of failure: rippling critics
  - type of rippling failure can e.g. suggest a missing lemma, generalisation or a different induction rule...
- Rippling is applicable for certain invariant type of POs
  - new rippling critics is our starting point - early experiment indicates
    - Secondary measure on the symbols.
    - Many non-rippling conditionals which requires new strategies/critics.

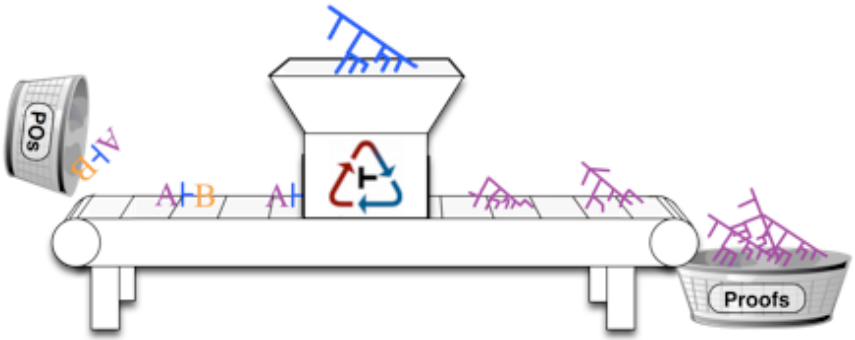
THE UNIVERSITY of EDINBURGH
informatics

AI4FM

The bigger picture: AI4FM

- Proof obligations grouped into families
  - e.g. by shape, data-structures, POG, ...
- Expert user provides one (or more) exemplar proof of each family

- Strategy extracted from proof and used to discharge remaining POs in the family



- Need to understand the strategies before addressing learning
- Critics ensures robustness - many POs will be at the fringe of strategy