Formalism: pitfalls and overcoming them (with AI?)

Cliff Jones
Newcastle University

My background

- wrt AI: I've known Alan Bundy for decades
  - that's pretty much it!
- lots of formal methods
  - industry as well as academia
  - built/used several "support" systems
  - reluctant to use TP system until ...

Formal *specifications* (i)

- it is *not* easy to construct real specifications
  - scale, ...
- some ideas
  - Bjørner's *domain models*
  - HJJ
  - Abrial's *horizontal refinement*
- but I plan to ignore this sub-topic

Formal *specifications* (ii)

- scale
  - beyond textbook examples
- errors in specifications!
  - doubts about "transformation"
  - prefer "posit and prove"
    - redundancy is key to dependability

Stepwise design

- "green field"
  - top-down reification
  - IMHO: this is the real payoff for formalism
- "brown field"
  - legacy code
  - establish (partial) properties
- symbiosis (via abstractions)!?

Proof!

- "posit and prove" generates POs
- heuristics are great
  - but cannot discharge 100%
  - remaining POs a real disincentive
  - engineers don't view 50+ POs as fun

Proof (cont)

- some "x% discharged automatically" measurements
  - ... are phoney!
    - measurement at *end* of modifications
  - follow introduction of intermediate steps
  - BTW I do believe in structuring developments
- extra model layers just to reduce TP task?

Where AI *might* help

- "learn from an expert"/proof *process*
- one view (AI4FM project - more from others)
  - properties of spec
  - proof critics: analyse failures
  - talks by AI4FM colleagues
    - possibly including mine?

Some (recent) experience (i)

- EU-funded IP: DEPLOY
  - many "deliverables" on-line (deploy eu project)
- problems of getting specifications
  - Jackson's "Problem Frames" helped
- residual POs
  - greatly influenced by specification "style"
  - do fall into "families"

Some (recent) experience (ii)

- changes are the norm!
- know which version of what design has been shown ...
- fit with existing engineering tools
  - cannot view them as plugins
- use of tools by experts/engineers?

Where AI might help ...

- alternatives
  - over to you :-)
  - pls remember:
    - asking questions might generate good discussions