Another tale of two proofs

or

what I did in my summer holidays

Jim Woodcock & Steve King

Outline

- The problem
- Motivation
- Progress
- Lessons learnt
- Future plans

The problem: (1) Mondex

- Mondex:
  - smartcard electronic cash system: no central controller
  - formal side developed by Logica, for NatWest (coding by platform 7)
  - highest ITSEC security certification level E6 (1999): first ever product to achieve this
- Z spec and designs published, in sanitised form, as PRG monograph in 2000
- ‘We choose to do rigorous proofs by hand: our experience is that current proof tools are not yet appropriate for a task of this size’ [PRG-126]

The problem (2)

Long-term goal: To mechanise, in ProofPower-Z, the proofs in the published Mondex specification and design, *making as few changes as possible to what has been published.*

Short-term goal (over 2-month study leave at QinetiQ Malvern): to learn as much as possible about ProofPower-Z, and to start on the long-term goal

Motivation

- Personal
  - antidote to increased admin load at York
  - long-standing unfulfilled interest in automated theorem proving
- More general
  - Grand Challenge 6: Dependable Systems Evolution (JCPW and CARH)

Progress (1)

- I now have a reasonable understanding of the basic use of ProofPower (subgoal package, use of tactics etc) for proving Z conjectures. But, much more will be needed …
- I have proved that the 3 abstract operations maintain certain security properties
  - 2.5 pages in PRG-126
  - 15.5 pages of my proof, including lemmas
- I've started on the refinement proofs: A $\sqsubset$B (100 pages) and B $\sqsubset$ C (30 pages)

Progress (2)

Significant changes made to published text:

- missing domain checks

  $f, f' : X \pfun Y$ $\qquad\qquad$ $f'\ x = exp$

  Need: $x \in dom\ f'$, or change to $(x, exp) \in f'$

- schema quantification (in function definitions)

  $\forall x : X; S \bullet pred$

  becomes

  $\forall x : X; s : S \bullet pred'$

  for ease of proof. Easy to prove lemma that 2 forms are equivalent

Progress (3)

- inconsistency between operations

  $f' x = \mu\text{-}exp$ vs $f' x \in \{ \ldots \}$

  these are equivalent, as the set has only one member.

  Caused by sanitisation

Lessons learnt

- easier than expected to learn ProofPower-Z
  - but documentation on basic use could be improved
- sanitisation process is not easy
  - empty schema (caused by hiding all components)
  - allLogs : two similarly named components merged
- for real proof examples, size of screen display is important: don’t use a laptop!
- mechanical theorem-proving is fun

Future plans

- continue work on refinement proofs
  - can the hand proof structure be maintained?
  - can it be improved?
- comparison with Jim's work with Z/Eves
- ? automating the proof

Acknowledgements

- Systems Assurance Group at Malvern:
  - Colin O'Halloran
  - Alf Smith, Mark Adams, Phil Clayton
- Mondex authors, for answering queries

References

- for details of Mondex (& MultOS) publications:

  http://www-users.cs.york.ac.uk/~susan/bib/ss/e6.htm

- for corrections etc to Mondex specs:

  http://www-users.cs.york.ac.uk/~king/papers/mono-err.pdf