Applying Formal Methods to Railway Control

D. N. Hoover
Odyssey Research Associates, Inc.
301 Dates Dr.
Ithaca NY 14850-1326
Internet: hoove@oracorp.com

Outline of US&S/ORA Collaboration

- ❐ System-level railway control modeling.

- ❐ Verification of translations between different languages in VFRAME++ a railway control CAD system.
  - ❍ Design verification of a translation algorithm.
  - ❍ Automatic translation checker.

Railway Control Safety Modeling

A ``hot'' area.

- Most work is about verifying devices and software (e.g. SACEM--Paris-RER) used in automated control systems.

- Little system level model modeling, none for proof of safety (T.~King, K.M.~Hansen, FME '94 for specification, simulation).

- What we did:
  - Developed railway modeling methods supporting mathematical proof of safety.
  - Applied to classical block control system.
  - Substantial parts formalized and basic properties proved in PVS in order to clarify definitions

DAB-to-GEM Translation

Translation between graphical interface language (DAB) and generic intermediate language (GEM) in VFRAME++.

For exploratory purposes, we formalized the languages, their semantics, and a translation algorithm. We verified that the translation is correct (preserves semantics).

DAB-to-GEM Translation

- DAB (Design Application Builder) representation --- assignment com-plex Boolean expressions to output variables.

  w1 := u1 AND (u2 OR u3)
  w2 := (NOT u2) AND (TRUE OR u3)

  (Full language would also have some arithmetic and control struc-tures.)

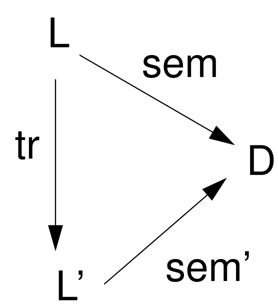
- GEM (Generic Entity Model) representation --- simple assignments only.

DAB-to-GEM Translation

assignments		assertion
v1 := u2	%	v1 = u2
v2 := NOT v1	%	v2 = NOT u2
v3 := TRUE	%	v3 = TRUE
v4 := u3	%	v4 = u3
v5 := v3 OR v4	%	v5 = TRUE OR u3
v6 := v2 AND v5	%	v6 = (NOT u2) AND (TRUE OR u3)
v7 := u1	%	v7 = u1
v8 := v1 OR v4	%	v8 = u2 OR u3
v9 := v7 AND v8	%	v9 = u1 AND (u2 OR u3)
w2 := v6	%	w2 = (NOT u2) AND (TRUE OR u3)
w1 := v9	%	w1 = u1 AND (u2 OR u3)

Results

- Some important basic concepts.
  - How to define the expressions of a language with a grammar.
  - The idea that expressions have a meaning (semantics).
  - That a correct translation is one that preserves semantics.



- FM allows fancier programming without added risk.
  - Our translation algorithm was more sophisticated than US\&S's.
  - They were being cautious, we were trying to show off.

Continuing Work

- Also of concern to US&S: Correct algorithm incorrectly coded.
  - Correct source code incorrectly compiled.
  - Correct object code producing wrong result due to a fault.
  - How do you know the theorem prover/program verifier works correctly? (Tool qualification problem.)
- Therefore US&S prefer also to check a posterior that translation has-been done correctly.
- Advantage: a posteriori check can be done automatically.

A posteriori checking

- A simple checker checks translation and produces a log.
- A really simple checker checks correctness of the log.
- Need to justify only the correctness of the log checker.
- Note: the a posteriori check seems to be simpler than the translation in this case.

Example

```
w1 := u1 AND (u2 OR u3)
w2 := (NOT u2) AND (TRUE OR u3)
```

assignments		assertion
v1 := u2	%	v1 = u2
v2 := NOT v1	%	v2 = NOT u2
v3 := TRUE	%	v3 = TRUE
v4 := u3	%	v4 = u3
v5 := v3 OR v4	%	v5 = TRUE OR u3
v6 := v2 AND v5	%	v6 = (NOT u2) AND (TRUE OR u3)
v7 := u1	%	v7 = u1
v8 := v1 OR v4	%	v8 = u2 OR u3
v9 := v7 AND v8	%	v9 = u1 AND (u2 OR u3)
w2 := v6	%	w2 = (NOT u2) AND (TRUE OR u3)
w1 := v9	%	w1 = u1 AND (u2 OR u3)

Conclusions

Value of FM

- ❒ Concepts from TCS---languages, semantics, abstraction, black-box-specification (precondition/postcondition). Not just algorithms, but-properties and states.
- ❒ Logical methods for manipulation and precise checking of semanticco-ntent of algorithms, code, results. A means of testing specifications.
- ❒ Education: concepts first, formalization later, or else avoid it altogether.
- ❒ In FM applications, often something simple is the most useful.