

What good are Formal Methods for Model-Based Design?

Formal Methods can not replace the human creativity

They can point out some of our blunders

Formal Methods: The Zoo

- specification formalisms with formal semantics
- model-checking, stochastic and not . . .
- specification-based testing (a.k.a automatic test-case generation)
- correctness proofs of spec refinement
- performance/dependability/performability evaluation
- theorem proving: proving properties of model-classes
(more general than model-checking)

Formal Methods: Gains

- **unambiguous** specifications
- MC: proof of timeliness properties, deadlock-freeness, probability to run in deadlock, etc.
- testing: automated falsification of implementation conformance to specification
- correct refinements
- a good idea of the expected performance, reliability, dependability, indication of dimensioning problems . . .
- correctness proofs

Formal Methods: Restrictions

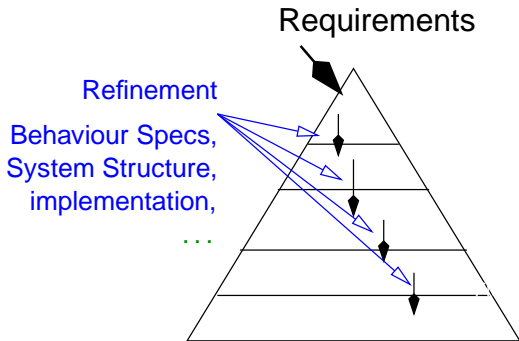
- restricted model classes to which methods applicable
- No **one-size-fits-all** model class
 - ⇒ Different models: consistency problems
- Complexity often unfavourable
 - ⇒ treatable models often very abstract
- inherent **incompleteness** (testing, model-checking)

Formal Methods: Prerequisite

formal, **unambiguous** model of system to be analysed:

- 1 mathematical reasoning about model must be possible
- 2 prerequisite to produce correct algorithms

Model-Based Design

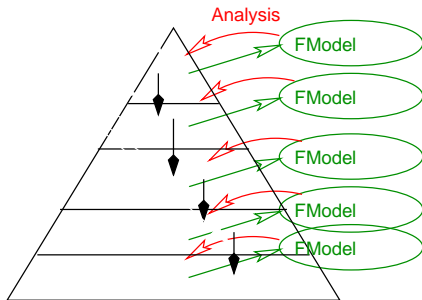


- Specs modeled in UML (sequence diagrams, state charts)
- Each refinement step more or less informal

MBD, UML, and FM

- UML more designed to be a notation, rather than a rigorous formalism
- Popular are sequence diagrams, which show only certain aspects of system behaviour, not overall picture.
(Interference)
- UML state diagrams the closest to a formal model
- However, quantitative

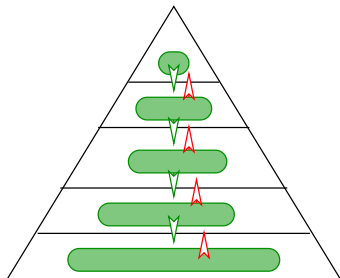
Model-Based Design and Formal Methods



Employing Formal Methods

- Creating FModels creative and tedious process itself
- Has merits in itself: inconsistencies can be discovered in informal system description

Model-Based Design



- Desirable: formal spec formalism in the design process :
 - easier extraction of specialized models
 - ideal: proof of soundness of refinements wrt. upper layers