Formal verification of safety-critical systems using UML

Zamira Daw, Rance Cleaveland

Institute for Systems Research and Computer Science Department

Research goals:
• Verification during model-driven development (MDD) of complex systems
• Integration of model checking and UML modeling
• Extensible formal semantics for UML
• Facilitate the usage of formal methods (FM)

Future work:
• Simulation and verification of UML extensions
• Optimization of state spaces
• Verification of model transformations

Integration of FM into the development process
• Facilitate the verification of safety properties by introducing mathematical formality to MDD models
• Reduce state explosion by leveraging the abstraction of MDD models in the verification

Comparison of model checkers

Goal:
Determine the influence of model checkers and of translation strategies for the generation of formal models on the verification performance (measured in time).

Testbench:
• Model checkers: NuSMV, SPIN, UPPAAL and PES (8 transformations)
• 67 UML activity diagrams

Results:
• Feasibility and advantages of the approach
• UPPAAL presents the best performance due to the variable management
• The big impact of model checkers and transformations drives the need of a model-checker independent formalization of UML-models

Extensible semantics
We are developing a reference semantics based on structural operational semantics, which can be:
• Extended according to domain-specific needs
• Used to verify the consistency of a UML extension/interpretation using simulation
• Used to verify model-transformations using bisimulation

Relevant literature

Research supported by NSF Grant CCF-0926194.