The Rodin Platform: Latest and Future Additions

Michael Butler

DEPLOY Tool-Building Team

www.deploy-project.eu

www.event-b.org

Rodin Tool for Event-B

- Extension of Eclipse IDE (Java based)
- Proof manager use a range of
- Rodin Eclipse *Builder* coordinates:
  - Well-formedness + type checker
  - Proof obligation generator
  - Proof manager
  - Propagation of changes

Rodin Proof Manager (PM)

- PM constructs proof tree for each PO
- Automatic and interactive modes
- PM manages used hypotheses
- PM calls *reasoners* to
  - discharge goal, or
  - split goal into subgoals
- Collection of reasoners:
  - simplifier, rule-based, decision procedures, …
- Basic tactic language to define PM and reasoners

Rodin Plug-ins

- AtelierB provers
- Linking UML and Event-B
- ProB: animation, consistency and refinement checking
- AnimB
- Brama
- Camille (texteditor)

Recent Additions

- Event extension
- Undo/redo
- Text editor
- Name completion
- Renaming
- Theorems everywhere
- Small changes to mathematical language

  partition(S, T1, T2, …, Tn)

Rodin Release Policy

- Every 3 months with 2 week code freeze
- Announce release on developer mailing list then 2 days later on announce+user mailing list
- Plug-ins announced on announce+user mailing list + wiki page for plug-in status
- Plug-ins should strive to meet release date but release will not be held back
- Adopt Eclipse versioning policy

Theory component and rule-based prover

- Supports mathematical extension and rule-based prover
  - Data types including inductive types
  - Polymorphic operators
  - Polymorphic basic predicates
  - Proof: theories, rewrites and inference rules
    - Soundness POs
    - Rule-based provers
  - Link to ProB model-checking

- Dates:
  - April 2010: theories, rules
  - June 2010: datatypes, operators, basic predicates

Other Verification Plans

- Prover extensions
  - FO prover bridge (Early 2010)
  - SMT bridge (Early 2010)
- Model based testing (mid 2010)
- Graphical tactic language (open)

Scaling

- Team-based development
  - Parallel development: viewing conflicts / merge (October 2009)
  - Impact on proof (open)

- Composition + decomposition (early 2010)
  - Shared variables style
  - Shared evetnstyle (composition plug-in available)
  - Plug-in for decomposing models and independent refinement

Code Generation

- Introduce *algorithmic* structures
  - introduced through refinement
  - sequential and concurrent
  - data types defined in theory components
  - Back-end to Ada/C
- Dates
  - Jan 2010: algorithmic language definition V1
  - June 2010: demonstrator tool for V1
  - Jan 2011: algorithmic language definition V2
  - June 2011: prototype tool for V2
- Event-B importer for AtelierB (Early 2010)

Draft syntax for tasks (V0.1)

- *Task* :=

  task *Name*

  tasktype periodic(p) | triggered | repeating | oneshot

  variables *Variables*

  invariants *Invariants*

  begin *TaskBody* **end**

- *TaskBody* ::=

  Event

  | *TaskBody* ; *TaskBody*

  | **if** *Event* **[]** *Event* **[]** … **[]** *Event* **fi**

  | **do** *Event* **endwith** *Event* **od**

Other Deploy commitments

- Requirements tracing
  - Prototype plug-in exists
  - concepts still evolving
- Reuse:
  - Instantiation of generic developments (early 2010)
  - Refinement patterns (evolving)
- Tighter integration of UML-B and Event-B (early 2010)
  - state machines and class diagrams within Event-B models

Wish list

- Enabledness POs
- Automatic refinement
- Support for probability
- Automated provers/SMT for set theory
    - common context
    - used hypothesis
    - extensible operator
- Reasoned modelling support
- Flexible document management

Keep up to date / contribute

- www.event-b.org
- wiki.event-b.org
  - share your Event-B models
  - share your plug-in plans
  - suggest plug-in ideas