

# Theory Plug-in for Rodin 3.x

Thai Son Hoang<sup>1</sup>, Asieh Salehi<sup>1</sup>, Michael Butler<sup>1</sup>, and Laurent Voisin<sup>2</sup>

<sup>1</sup> ECS, University of Southampton, U.K.

<sup>2</sup> Systerel, France

In Rodin 3.0, there are major changes within the Rodin Core. In particular, the following changes directly effect the Theory plug-in ([http://wiki.event-b.org/index.php/Rodin\\_Platform\\_3.0\\_Release\\_Notes](http://wiki.event-b.org/index.php/Rodin_Platform_3.0_Release_Notes)).

- **Stronger AST Library:** The API of the AST library has been strengthened to mitigate risks of unsoundness when mixing several formula factories. Now, every AST node carries the formula factory with which it was built, and the AST operations that combine several formulas check that formula factories are compatible.
- **Stronger sequent prover:** In order to improve the reliability of the proof status when working with mathematical extensions, the reasoners can be declared as context-dependent. The proofs that use a context dependent reasoner will not be trusted merely based on their dependencies, but instead they will be replayed in order to update their status. This applies in particular to Theory Plug-in reasoners, that depend on the mathematical language and proof rules defined in theories, which change over time.

Several problems have been reported for the Theory plug-in (with Rodin 3.0)

- Exceptions when opening proof obligation.
- Exceptions when applying rule-based prover reasoners, e.g., **XD** (expand definition).
- Changing the model, e.g., proof rules, theory path has no effects on existing proofs.
- Losing proofs when saving (the problem is in fact in loading previously saved proofs) .

The theory plug-in and its associate rule-based provers need to be upgraded to accommodate the changes in the Rodin Platform core.

We have been working in the last few months on ensuring compatibility of the Theory plug-in with the Rodin Platform core.

- The matching facility has been upgraded to use the *ISpecialization* API (insteads of *Instantiation*) which allows to specialize types consistently. This fixes several exeptions when applying reasoners.
- Improving the matching facitlity for *associative operators*.
- Implement equality between datatype/operator extensions to ensure that the formula factory will assign the same “ID” for datatype/operator with the same definition. This ensures that formula factories coming from different origins can be correctly compared. In particular, this ensures that proofs can be loaded with the correct formula factory.

The upgrades are required some fixed in the Rodin Core hence will be available after the next release of the Rodin Platform (Rodin 3.3?)

We have identified the following future research/improvement for the Theory plug-in.

- Support for *infix predicate operators*.
- Support for *predicate variables* in theory.
- Improve matching facility for *associative commutative operators* (currently does not take into account commutativity).
- *Tactics* for theory
- Theory *instantiation*
- Improving *usability* of the theory plug-in, e.g., performance in interactive proofs.

Some of the improvements are straightforward while the others, e.g. tactics, instantiation, requires further investigation.