

What's new in Rodin 3.9 and the Theory plug-in

Guillaume Verdier¹, Laurent Voisin², Idir Ait-Sadoune³

¹ UPEC

`guillaume.verdier@irit.fr`

² Systemel

`laurent.voisin@systemel.fr`

³ Paris-Saclay University, CentraleSupélec, LMF laboratory

`idir.aitsadoune@centralesupelec.fr`

June 25th, 2024

11th Rodin User and Developer Workshop

Introduction

- ▶ a new version of Rodin is released each year
- ▶ this year's version: 3.9, released on June 11th
- ▶ overview of new features and bugs fixed
- ▶ we also work on the Theory plug-in
- ▶ development is supported by the French ANR project Event-B Rodin Plus (EBRP, ANR-19-CE25-0010)

New proof rules

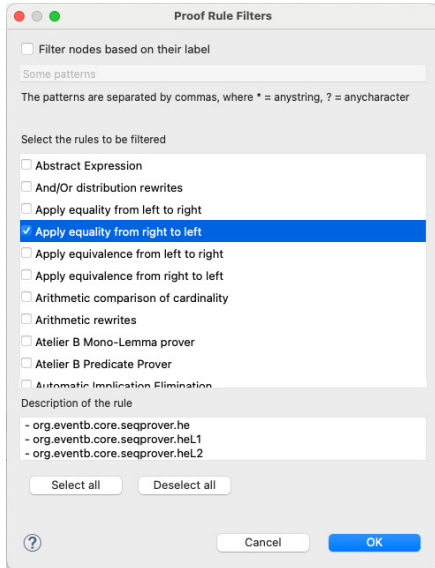
▶ new auto-rewriter rules:

- ▶ $\min(A) \in A \equiv \top$
- ▶ $\max(A) \in A \equiv \top$
- ▶ $\text{bool}(B = \text{TRUE}) \equiv B$
- ▶ $E \mapsto E \in \text{id} \equiv \top$
- ▶ $E \mapsto E \in r \setminus \text{id} \equiv \perp$
- ▶ $E \mapsto E \in S \triangleleft \text{id} \equiv E \in S$
- ▶ $E \mapsto E \in r \setminus (S \triangleleft \text{id}) \equiv E \mapsto E \in S \triangleleft r$

▶ new manual rules:

- ▶ $f(x) = y \equiv x \mapsto y \in f$
- ▶ $F \in \{x, y \cdot P(x, y) \mid E(x, y)\} \equiv \exists x, y \cdot P(x, y) \wedge E(x, y) = F$
- ▶ $E \in \{x \cdot P(x) \mid x\} \equiv P(E)$
- ▶ $a^n \equiv a \times a^{n-1}$ (and new sub-goal $n \neq 0$)
- ▶ infer $\text{finite}(\{i \cdot P(i) \mid F(i)\})$ from $\text{finite}(\{i \mid P(i)\})$

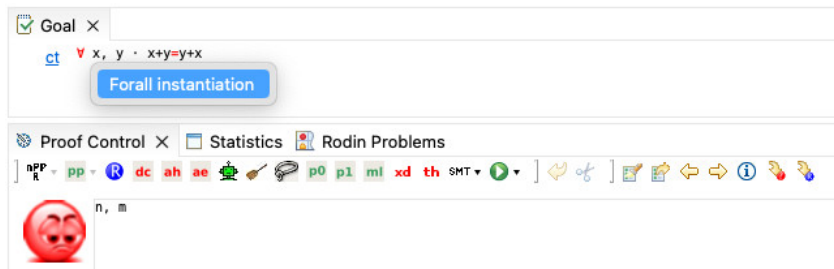
Proof tree rule filtering



User-provided names for new identifiers in proofs

Fresh identifiers in proofs used to be generated automatically; they can now be provided in the proof input:

- ▶ **ae**: input $ident = expr$ instead of $expr$
- ▶ **all**, **exF**, **dt dc**: input a comma-separated list of identifiers

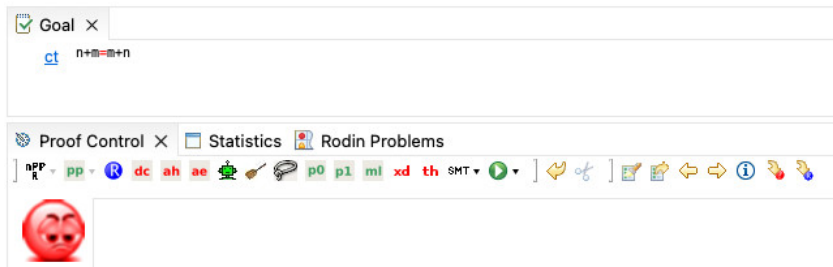


The screenshot shows a proof assistant interface. At the top, there is a "Goal" window with a close button (X) and a checkmark icon. Below the goal, the text "ct $\forall x, y \cdot x+y=y+x$ " is displayed. A blue button labeled "Forall instantiation" is positioned over the goal text. Below the goal window is a toolbar with several icons and labels: "Proof Control" (with a close button), "Statistics", and "Rodin Problems". The toolbar also contains a series of tactic icons: nPP , R , pp , dc , ah , ae , a green robot icon, a paintbrush icon, a speech bubble icon, $p0$, $p1$, ml , xd , th , SMT , a play button, a left arrow, a scissors icon, a right arrow, a left arrow, a right arrow, an information icon, a hand icon, and a blue hand icon. Below the toolbar, the text "n, m" is visible next to a red sad face emoji.

User-provided names for new identifiers in proofs

Fresh identifiers in proofs used to be generated automatically; they can now be provided in the proof input:

- ▶ **ae**: input $ident = expr$ instead of $expr$
- ▶ **all**, **exF**, **dt dc**: input a comma-separated list of identifiers



The screenshot shows a software interface for a proof assistant. At the top, there is a tab labeled "Goal" with a close button. Below it, the goal is displayed as $n + m = m + n$ with a small blue icon labeled "ct" to its left. Below the goal area is a toolbar with several tabs: "Proof Control", "Statistics", and "Rodin Problems". The "Proof Control" tab is active and contains a row of icons for various tactics: nPP , R , pp , R , dc , ah , ae , a green robot icon, a paintbrush icon, a speech bubble icon, $p0$, $p1$, $m1$, xd , th , SMT , a play button, a left arrow, a scissors icon, a right arrow, a left arrow, a right arrow, an information icon, a hand icon, and a blue hand icon. Below the toolbar is a red emoji with a sad face.

Main bugs fixed

- ▶ Rodin 3.8 started hiding rewritten equalities; it now deselects or hides them depending on default hypotheses
- ▶ fixed a breaking bug in an auto-rewrite rule related to nested comprehension sets (found by Yannis Benabbi)
- ▶ the “Prove automatically” setting is now persisted across Rodin restarts
- ▶ various error cases and exceptions have been fixed

Reasoners on inductive types

- ▶ inductive datatypes are implemented in Rodin Core but currently only used by the Theory plug-in
- ▶ note: parameters of datatypes can be arbitrary sets, not just types (e.g., one can write $List(\mathbb{N})$)
- ▶ new reasoners:
 - ▶ $datatype(T1, U1, \dots) = datatype(T2, U2, \dots)$
 $\equiv T1 = T2 \wedge U1 = U2 \wedge \dots$
e.g., $List(\mathbb{Z}) = List(\mathbb{Z}), List(\mathbb{Z}) \neq List(\mathbb{N})$
 - ▶ $cons(a, b, \dots) \in datatype(T, \dots)$
 $\equiv a \in destr1set(T, \dots) \wedge b \in destr2set(T, \dots) \wedge \dots$
e.g., $cons(-1, l) \in List(\mathbb{N}) \equiv -1 \in \mathbb{N} \wedge l \in List(\mathbb{N}) \equiv \perp$

Theory plug-in

- ▶ version 4 released in 2020, three years after the release candidate
- ▶ three more bug-fix releases in 2021 and 2022
- ▶ ongoing work: large refactoring to fix complex underlying issues
 - ▶ handling of formula factories and extensions reworked
 - ▶ static-checker cleaned up and improved
 - ▶ main remaining part: proof obligation generator (and handling of proof rules)

Conclusion

- ▶ Rodin is regularly updated
- ▶ do not hesitate to report bugs or request new features on SourceForge or by email
- ▶ a new major version of the Theory plug-in is coming

Thanks

Questions?