Proof automation for Event-B theories

Peter Riviere, Yamine Aït-Ameur, Neeraj Kumar Singh, Guillaume Dupont

Proof automation for Event-B theories

P. Rivière[1], N. K. Singh[1], Y. Aït-Ameur[1], and G. Dupont[1] *

INPT-ENSEEIHT/IRIT, University of Toulouse, France
{peter.riviere, nsingh, yamine, guillaume.dupont}@enseeiht.fr

In order to enrich its expressiveness, Butler et al. [2] proposed a mathematical extension to Event-B. This extension enables the description of algebraic definitions for data-types and operators in a reusable component, *theories*. Theories may also present new theorems and proof rules to handle the new user-defined constructs, which may be used seamlessly when proving models.

Currently, the elements introduced by theories are not always properly handled by automatic provers, especially SMT solvers and Atelier-B provers. If users want to use these tools, they need to manually unfold and rewrite each operator to classical Event-B expressions, which can be cumbersome.

In this presentation, we propose to encode new proof principles as well as to introduce new strategies to automatically unfold theory operator, hence improving proof automation. This solution is adopted in the development of the reflexive EB4EB framework [3,4].

The main objective of the EB4EB reflexive framework [3,4] is to provide explicit manipulation of Event-B components as first-class objects, making it possible to reason on these objects and define new Event-B analyses. For this purpose, the concept of Event-B machine is formalised as a data-type in a theory (a meta-theory), together with a set of operators that guarantee the correctness, relative to Event-B semantics, of instances of this data-type. The meta-theory formalises the semantics of Event-B, as described in the Event-B Book [1], i.e. a set of states and guarded events defined as a relation between states. In addition, the EB4EB framework is extended to support new analyses, possibly non-intrusive, mechanisms associated to different properties not expressed in core Event-B [6]. In this work, we present three properties, *deadlock freeness*, *invariant weakness analysis* and *reachability*, to demonstrate extension of reasoning mechanism using the reflexive Event-B. Furthermore, this reflexive framework EB4EB has been extended to formalise and operationalise the automatic generation of proof obligations associated to *temporal properties* expressed in LTL [5].

THEORY EvtBTheo
TYPE PARAMETERS $STATE, EVENT$
DATATYPES
$Machine(STATE, EVENT)$
CONSTRUCTORS
$Cons\_machine($
$Event : \mathbb{P}(EVENT)$,
$State : \mathbb{P}(STATE)$,
$Init : EVENT$,
$Progress : \mathbb{P}(EVENT)$
$AP : \mathbb{P}(STATE)$,
$Grd : \mathbb{P}(EVENT \times STATE)$,
$BAP : \mathbb{P}(EVENT \times (STATE \times STATE))$,
$Inv : \mathbb{P}(STATE)$
$Thm : \mathbb{P}(STATE)$,
$Variant : \mathbb{P}(STATE \times \mathbb{Z})$,
$Ordinary : \mathbb{P}(EVENT)$,
$Convergent : \mathbb{P}(EVENT))$

* The authors thank the ANR-19-CE25-0010 *EBRP:EventB-Rodin-Plus* project.

These theories are extended with automatic rewriting rules that substitute operators by their given definition in order to automate proof processes. These rules are written to extract relevant information from machine objects, add them to the hypotheses, and produce multiple simpler goals. For example, Listing `rew2` shows rewriting rule for simplifying proof process related to deadlock freeness. Similarly, several rules are encoded in the theories. These rules are defined to be applied automatically and chained together, greatly improving proof automation. Indeed, these rewrite rules are included in Rodin's user-defined proof tactics, once and for all, increasing automation when proving the theorems formalising the newly defined POs. Note that these rules follows a pattern that can be applied systematically.

PROOF RULES
extension_def:
Metavariables
$m : Machine(STATE, EVENT)$
Rewrite Rules
...
$rew2:\ DeadlockFreeness\_Definition(m)$
rhs1: $\top \Rightarrow \forall g, i, p \cdot Progress(m) = p \land Grd(m) = g \land Inv(m) = i \Rightarrow i \subseteq g[p]$

Proof automation using rewriting rules is demonstrated on Clock examples in particular analysis of different POs. Table 1 presents the proof statistics for each analysis. The important number of nodes (representing atomic steps) in the proof trees is due to the extensive use of theory operators which the prover cannot handle directly, and thus their definitions must be unfolded. The introduction of the rewrite rules in a proof tactic perform automatically these unfold and reductions, making almost all steps fully automatic despite the introduction of the meta level (An entry of 0 in the interactive nodes column of Table 1). The rightmost column provides the number of tactic applications (iterations) during the proof. Indeed, a single tactic application may not be sufficient to fully discharge the proof goals.

Model	PO	Max Depth	Nodes	Interactive Nodes	Number of Tactic application
DeadlockFree clock	thmDeadlock (THM)	169	221	1	2
Reachability clock	thmReach (WD)	112	577	0	1
	thmReach (THM)	191	731	4	5
Inspect Inv clock	thmInspectInvEVTM5 (THM)	111	167	0	1
	thmInspectInvEVTH5 (THM)	112	169	0	1
	thmInspectInvEVTMH1 (THM)	113	171	0	1
Strong Inv clock	thmInspectInvEVTM5 (THM)	105	158	0	1
	thmInspectInvEVTH5 (THM)	118	171	0	1
	thmInspectInvEVTHM1 (THM)	128	181	0	1

Table 1: Proof statistic for the Clock model and its analyses

References

1. Abrial, J.R.: Modeling in Event-B: System and software engineering. Cambridge University Press (2010)
2. Butler, M.J., Maamria, I.: Practical theory extension in Event-B. In: Theories of Programming and Formal Methods - Essays Dedicated to Jifeng He on the Occasion of His 70th Birthday. pp. 67–81 (2013)
3. Riviere, P., Singh, N.K., Aït Ameur, Y.: EB4EB: A Framework for Reflexive Event-B. In: International Conference on Engineering of Complex Computer Systems, ICECCS 2022. pp. 71–80. IEEE (2022)
4. Riviere, P., Singh, N.K., Aït Ameur, Y.: Reflexive Event-B: Semantics and Correctness the EB4EB Framework. IEEE Transactions on Reliability pp. 1–16 (2022)
5. Riviere, P., Singh, N.K., Aït Ameur, Y., Dupont, G.: Formalising liveness properties in Event-B. In: NASA Formal Methods 2023. LNCS (2023)
6. Riviere, P., Singh, N.K., Aït Ameur, Y., Dupont, G.: Standalone Event-B models analysis relying on the EB4EB meta-theory. In: International Conference on Rigorous State Based Methods, ABZ 2023. LNCS, Springer Verlag (2023)