Validation of Domain and Meta Models: From Event-B Theories to Practice *

Michael Leuschel[0000−0002−4595−1518],
Yamine Aït-Ameur, Guillaume Dupont, Peter Rivière, Neeraj Kumar Singh

Heinrich-Heine Universität Düsseldorf
leuschel@uni-duesseldorf.de
INP-ENSEEIHT/IRIT, University of Toulouse
{yamine,guillaume.dupont, peter.riviere, neeraj.singh}@enseeiht.fr

The Theory plug-in [5] of Rodin provides the ability to add new data types and operators to Event-B's mathematical toolkit and extend Rodin's proof rules. The theory plug-in plays a major role in a variety of applications: hybrid systems modelling [9, 3], floating point numbers [1], domain modelling [6], and meta modelling (EB4EB) [7]. The EBRP research project aims to improve the support for theories in Rodin. In this article we present how the ProB verification and validation tool [4] was improved to better support Event-B theories and enable validation of the above mentioned case studies.

Meta Models The EB4EB meta modelling framework [7, 2] provides deep and shallow embeddings of Event-B in Event-B itself. We managed to improve ProB so that both embeddings can be validated. This required, e.g., improving symbolic treatment of the relational image operator (used by E4BEB to apply guards, invariants or before-after-predicates to states) and support for inductive data types. Figure 1 shows ProB2-UI for the EB4EB deep embedding of a 24-hour clock. Note that the before-after-predicate of the model is infinite (as it is separate from the guards). Model checking the deep embedding took 1.8 seconds for 1440 states. This is about one order of magnitude slower than the original clock model (0.12 secs), due to the interpretation overhead of EB4EB.

Visualisation of Event-B Models with Theories In the lower middle half of Fig. 1 you can see a visualisation of the current state of the meta model. Here B formulas control the attributes of SVG (sclabale vector graphics) objects, in this case the hour and minute hands of the clock. These attributes are often floating point numbers or strings. As these are not available in Rodin, the VisB formulas are written in classical B with additional access to ProB's external functions. In Fig. 1, an existing SVG image of a clock was used[1] and the hour and minute hands were rotated by setting the transform attributes using floating point calculations. To enable visualisations of Event-B theories in general, we have made the Event-B theory operators available in VisB formulas, as well as in ProB's REPL and other features.

Hybrid Systems and Support for Reals Support for floating point numbers has been added to ProB, in line with Atelier-B's new datatypes FLOAT

* This work was supported by the IVOIRE project funded by DFG/FWF grant # I 4744-N, as well as the EBRP project funded by ANR grant ANR-19-CE25-0010.

[1] https://github.com/tomchen/animated-svg-clock

and REAL. Various B operators now work with floats: +, -, *, /, Σ, Π, min, max. ProB also provides a library (LibraryReals.def) with external functions, e.g., trigonometric functions like RSIN and RCOS. This is useful for visualisations, as seen above, but also for hybrid systems modelled in Event-B. Axiomatic operators in Event-B theories can now be linked to these operators (in .ptm mapping files). This was used to enable animation and visualisation of the floating point theory in [1] as well as floating number approximations of some hybrid models from [9, 3]. In future we want to also support precise reals [8].

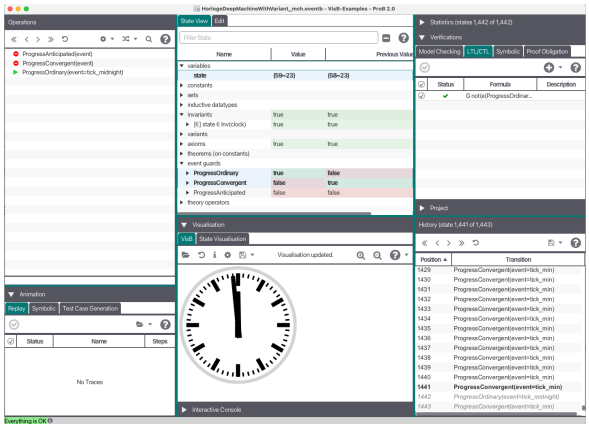

Fig. 1. Screenshot of an animation of deep embedding of clock model

References

1. I. Aït-Sadoune. A floating-point numbers theory for Event-B. In *Proceedings MEDI 2023*, pages 30–43, 2023.
2. Y. A. Ameur, G. Dupont, I. Mendil, D. Méry, M. Pantel, P. Riviere, and N. K. Singh. Empowering the Event-B method using external theories. In *Proceedings IFM 2022*, LNCS 13274, pages 18–35, 2022.
3. G. Dupont, Y. A. Ameur, N. K. Singh, and M. Pantel. Event-B hybridation: A proof and refinement-based framework for modelling hybrid systems. *ACM Trans. Embed. Comput. Syst.*, 20(4):35:1–35:37, 2021.
4. M. Leuschel and M. J. Butler. ProB: an automated analysis toolset for the B method. *STTT*, 10(2):185–203, 2008.
5. I. Maamria, M. Butler, A. Edmunds, and A. Rezazadeh. On an Extensible Rule-based Prover for Event-B. In *ABZ2010*, February 2010.
6. I. Mendil, P. Riviere, Y. A. Ameur, N. K. Singh, D. Méry, and P. A. Palanque. Non-intrusive annotation-based domain-specific analysis to certify Event-B models behaviours. In *Proceedings APSEC 2022*, pages 129–138. IEEE, 2022.
7. P. Riviere, N. K. Singh, and Y. A. Ameur. EB4EB: A framework for reflexive event-b. In *Proceedings ICECCS 2022*, pages 71–80. IEEE, 2022.
8. K. Rutenkolk. Extending modelchecking with ProB to floating-point numbers and hybrid systems. In *Proceedings ABZ'23*, pages 366–370, 2023.
9. W. Su, J. Abrial, and H. Zhu. Formalizing hybrid systems with Event-B and the Rodin platform. *Sci. Comput. Program.*, 94:164–202, 2014.