An Approach to Combining the Institutions for Event-B and Temporal Logic*

Marie Farrell[1], Rosemary Monahan[2], James F. Power[2], and Michael Fisher[1]

[1] Department of Computer Science, University of Liverpool, UK
[2] Department of Computer Science, Maynooth University, Ireland

The Event-B formal specification language has been used at an industrial scale for proving safety properties of a system's specification [1]. Event-B is a state-based language that supports the process of formal refinement, it uses a set-theoretic modelling notation and is based on first-order logic. Our previous work on the development of the institution for Event-B, $\mathcal{EVT}$, involved decomposing the syntax of the Event-B language into three layers [3]. These are the superstructure layer, the infrastructure layer and a base layer where the latter contains the mathematical language used by Event-B, as shown in Figure 1. We used the institution for first-order predicate logic with equality, $\mathcal{FOPEQ}$, to specify this mathematical layer.

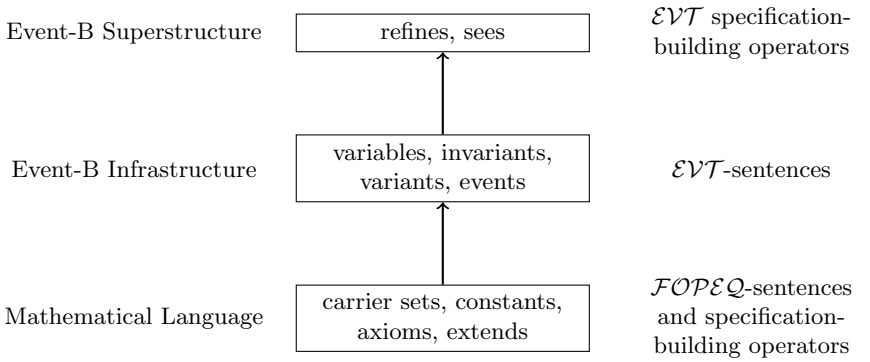

Fig. 1: The Event-B syntax is split into three layers: superstructure, infrastructure and a mathematical language.

The relationship between the mathematical layer, $\mathcal{FOPEQ}$, and the other layers, $\mathcal{EVT}$, is that of a comorphism from $\mathcal{FOPEQ}$ to $\mathcal{EVT}$. This comorphism allows us to define the satisfaction condition in $\mathcal{EVT}$ by transforming $\mathcal{EVT}$-models into $\mathcal{FOPEQ}$-models and evaluating the satisfaction relation in $\mathcal{FOPEQ}$ [3]. It also facilitates the use of $\mathcal{FOPEQ}$-sentences in $\mathcal{EVT}$-sentences. In our current work, we seek to exploit the modular, plug and play nature of $\mathcal{EVT}$ and outline a mechanism for replacing this base mathematical layer, $\mathcal{FOPEQ}$, with the institution for temporal logic, $\mathcal{TL}$ [2].

* This work is partially supported through EPSRC Hubs for Robotics and AI in Hazardous Environments: EP/R026092 (FAIR-SPACE), EP/R026173 (ORCA), and EP/R026084 (RAIN).

There are many variants of temporal logic, for example, linear-time temporal logic [4]. The institution for linear-time temporal logic, $\mathcal{LTL}$, bears similarities to both $\mathcal{EVT}$ (in its models) and $\mathcal{FOPEQ}$ (in its signatures) [7]. The core component of evaluating the satisfaction relation in $\mathcal{EVT}$ involves transforming $\mathcal{EVT}$-models into $\mathcal{FOPEQ}$-models. Therefore, if we replace $\mathcal{FOPEQ}$ with the institution for linear-time temporal logic, then we can either (1) define a comorphism from $\mathcal{LTL}$ to $\mathcal{EVT}$ that transforms $\mathcal{EVT}$-models into $\mathcal{LTL}$-models, or (2) show how $\mathcal{LTL}$-models can be reduced to $\mathcal{FOPEQ}$-models. The former of these approaches is more favourable as it provides a direct link between $\mathcal{EVT}$ and $\mathcal{LTL}$ rather than using $\mathcal{FOPEQ}$ as a bridge between them. As $\mathcal{LTL}$ signatures are the same as those of $\mathcal{FOPEQ}$, the principal effort in constructing this comorphism is to extract $\mathcal{LTL}$-models from $\mathcal{EVT}$-models. Intuitively, this involves extracting sequences of data states from the initialising set, L, and the relations, R, in an $\mathcal{EVT}$-model. These sequences can then be interpreted as $\mathcal{LTL}$-models. We have discussed linear-time temporal logic as a small example here but our work examines how the institution for temporal logic in general, $\mathcal{TL}$, can be combined with $\mathcal{EVT}$.

By combining $\mathcal{EVT}$ and $\mathcal{TL}$ in this way, we provide a basis for the verification of both safety and liveness properties. Recently, work has been done on incorporating linear-time temporal logic into the Event-B specification language, particularly during refinement steps [5]. However, this is not at the level of institutions and future work includes comparing this work with our institutional approach. Furthermore, our work provides a basis for the development of an institution for the TLA+ state-based specification language that uses temporal logic [6], and for relating the institutions for Event-B and TLA+.

References

1. J.-R. Abrial. *Modeling in Event-B: System and Software Engineering.* Cambridge University Press, 2010.
2. M. V. Cengarle. The temporal logic institution. Technical report, Bericht 9805, Ludwig-Maximilians-Universität München, Insitut für informatik, 1998.
3. M. Farrell, R. Monahan, and J. F. Power. An institution for Event-B. In *International Workshop on Algebraic Development Techniques*, volume 10644 of *Lecture Notes in Computer Science*, pages 104–119, 2016.
4. M. Fisher. *An Introduction to Practical Formal Methods Using Temporal Logic.* Wiley, 2011.
5. T. S. Hoang, S. Schneider, H. Treharne, and D. M. Williams. Foundations for using linear temporal logic in Event-B refinement. *Formal Aspects of Computing*, 28(6):909–935, 2016.
6. L. Lamport. *Specifying systems: the TLA+ language and tools for hardware and software engineers.* Addison-Wesley, 2002.
7. D. Sanella and A. Tarlecki. *Foundations of Algebraic Specification and Formal Software Development.* Springer, 2012.