Addressing Extensibility Issues in Rodin and Event-B

Issam Maamria and Michael Butler

ECS, University of Southampton, Southampton SO17 1BJ, UK
{im06r, mjb}@ecs.soton.ac.uk

Abstract. Modelling and proof in Event-B are intrinsically linked. Users model discrete transition systems using typed set theory. Reasoning about the developed models is achieved by means of proof obligations. The Rodin [1] philosophy is centred around a reactive environment. In such environment, the user is able to link the changes made to models and proof obligations. As a desired consequence of this philosophy, the user gains a deeper understanding of the model and the system in question by simply inspecting failed automatic proof attempts. To enhance the user modelling capabilities, the provision of an extendible modelling infrastructure is of paramount importance. Indeed, this is achieved through the Rodin database [3]. We argue that offering Event-B language extension facilities will make modelling easier and largely limit the need for duplication. By language extensions we mean polymorphic operators and inductive datatype definitions. The existing (wired/fixed) Event-B mathematical language offers a collection of built-in polymorphic operators (examples include the set union operator and the finite predicate on sets). However, there exists no capability to extend the language with user-defined operators and datatypes. The Records plug-in was a step forward in terms of giving more power to the user, and allows the definition of record structures [2] convenient for many modelling patterns. In this presentation, we describe an approach to deal with wider language extensibility issues. This work is a continuation of an existing work on enhancing Rodin proving infrastructure in the shape of the Rule-based Prover plug-in [4]. We show how the existing theory construct can be extended (thanks to the Rodin database) to enable the definition of polymorphic operators and datatypes. We also show how proof obligations are used to ensure user-defined extensions are logically conservative. Proof rules concerning newly introduced extensions can be defined using the same infrastructure.

References

1. Michael Butler and Stefan Hallerstede. The Rodin Formal Modelling Tool. *BCS-FACS Christmas 2007 Meeting - Formal Methods In Industry, London.*, December 2007.
2. Neil Evans and Michael J. Butler. A Proposal for Records in Event-B. In Jayadev Misra, Tobias Nipkow, and Emil Sekerinski, editors, *FM*, volume 4085 of *Lecture Notes in Computer Science*, pages 221–235. Springer, 2006.

3. Stefan Hallerstede. Justifications for the Event-B Modelling Notation. In Jacques Julliand and Olga Kouchnarenko, editors, *B*, volume 4355 of *Lecture Notes in Computer Science*, pages 49–63. Springer, 2007.
4. Issam Maamria, Michael Butler, Andrew Edmunds, and Abdolbaghi Rezazadeh. On an Extensible Rule-based Prover for Event-B. In *ABZ '10: Proceedings of the 2nd international conference on Abstract State Machines, B and Z*, Berlin, Heidelberg, 2010. Springer-Verlag.