Model Checking Event-B by Encoding into Alloy — Extended Abstract —

Paulo J. Matos and João Marques-Silva

Electronics and Computer Science, University of Southampton
{pocm,jpms}@ecs.soton.ac.uk

Current day systems are ever more detailed and complex leading to the necessity of developing models that abstract unimportant implementation details while emphasizing their structure. These models are developed in order to be easily verified either by theorem provers or model checkers. Until recently it was only possible to perform temporal model checking in an Event-B model by converting the model to B-method and then using ProB [1]. More recently, a prototype ProB plugin [2] for the RODIN tool has been developed. Nevertheles, encoding Event-B to Alloy allows building on top of the Alloy model finding engine therefore benefiting from all of its optimizations. An extended version of this work can be found elsewhere [3].

There are three aspects to the encoding: encoding of model structures, expressions, and predicates (which are straightforward). The execution model needs to be emulated by the final Alloy model. A signature "State" keeps track of all the state variables that are ordered in time using the ordering module. Events are predicates and facts define not only the initial state but also that one event is triggered per state. Expressions are the hardest part to encode. There is not only a myriad of complex expressions in Event-B but given that Alloy uses only flat relations, some Event-B expressions that introduce relations with nested sets generate many (potentially large) Alloy expressions. Some expressions are straightforward as they have Alloy counterparts, others need to be defined by small functions. Function expressions are encoded as relations and then facts can be added to the model as to assure the semantics is preserved.

The motivation for our work is to allow users of the Event-B language to exploit the accumulated experience from the development of the Alloy tools. The resulting Alloy model can serve to find counterexamples to false invariants and translate them back to Event-B. Future work entails the automatic generation of the encoding and its integration with the RODIN platform. The tool to be developed can then be extended to use other backends besides Alloy.

References

1. Leuschel, M., Butler, M.J.: ProB: A model checker for B. In Araki, K., Gnesi, S., Mandrioli, D., eds.: FME. Volume 2805 of LNCS., Springer (2003) 855–874
2. Ligot, O., Bendisposto, J., Leuschel, M.: Debugging Event-B Models using the ProB Disprover Plug-in. Proceedings of AFADL'07 (June 2007)
3. Matos, P.J., Marques-Silva, J.: Model checking Event-B by encoding into Alloy. Computing Research Repository **abs/0805.3256** (May 2008) http://arxiv.org/abs/0805.3256.