Integrating SMT-solvers in Z and B Tools

A. C. Gurgel*, V. G. Medeiros Jr., M. V. M. Oliveira and D. B. P. Déharbe

Departamento de Informática e Matemática Aplicada, UFRN, Brazil

An important frequent task in both Z [6] and B [1] is the proof of verification conditions (VCs). In Z and B, VCs can be predicates to be discharged as a result of refinement steps, some proof about initialization properties or domain checking. Ideally, a tool that supports any Z and B technique should automatically discharge as many VCs as possible. Here, we present ZB2SMT [1], a `Java` package designed to clearly and directly integrate both Z and B tools to the satisfiability module theory (SMT) solvers such as veriT [2], a first-order logic (FOL) theorem prover that accepts the SMT syntax [5] as input. By having the SMT syntax as target we are able to easily integrate with further eleven automatic theorem provers that are also compatible like: Z3, CVC3 and AltErgo. ZB2SMT is currently used by Batcave [3], an open source tool that generates VCs for the B method and CRefine [4], a tool that supports the *Circus* refinement calculus. Much of the VCs generated to validate the refinement law applications, are based on FOL predicates. Hence, CRefine uses the ZB2SMT package to automatically prove such predicates. The package integrates elements of Z and B predicates in a common language and transforms these predicates into SMT syntax. In this process, a SMT file is generated containing the predicate and some definitions. It is sent to a chosen SMT solver which yields a Boolean value for the predicate or it can be sent to several SMT solvers in a parallel approach. In order to improve the performance of the proof system, ZB2SMT has a module that can call different instances of solvers at different computers, according to a configuration file. It improves the proof process by allowing different strategies to be performed in parallel, reducing the verification time.

Acknowledgments. This work was partially supported by the National Institute of Science and Technology for Software Engineering (INES, www.ines.org.br), funded by CNPq grant 573964/2008-4 and by CNPq grant 553597/2008-6.

References

1. J. R. Abrial. *The B Book: Assigning Programs to Meanings.*, volume 1 of *1*. Cambridge University Press, United States of America, 1 edition, 1996.
2. Thomas Bouton, Diego Caminha B. de Oliveira, David Déharbe, and Pascal Fontaine. veriT: An open, trustable and efficient SMT-solver. In *CADE-22*, pages 151–156, 2009.
3. E. S. Marinho, V. G. Medeiros Jr, Cláudia Tavares, and David Déharbe. Um ambiente de verificação automática para o método B. In *SBMF 2007*, 2007.

* The ANP supports the work of the author through the prh22 project.

[1] Freely available at `http://www.consiste.dimap.ufrn.br/projetos/zb2smt`.

4. M. V. M. Oliveira, A. C. Gurgel, and C. G. de Castro. CRefine: Support for the *Circus* Refinement Calculus. In *6th IEEE on SEFM*, pages 281–290. IEEE, 2008.
5. Silvio Ranise and Cesare Tinelli. The SMT-LIB Standard: Version 1.2, 2006.
6. J. C. P. Woodcock and J. Davies. *Using Z—Specification, Refinement, and Proof*. Prentice-Hall, 1996.