

Formal Analysis in Model Management: Exploiting the Power of CZT

James R. Williams, Fiona A.C. Polack, and Richard F. Paige*

Department of Computer Science, University of York, UK YO10 5DD
{jw,fiona,paige}@cs.york.ac.uk

Software engineering diagrams are hard to verify and formally analyse, often due to inadequately defined diagram semantics: the semantics often does not enable formal analysis, or may be underspecified to a degree that does not allow useful properties to be checked.

The AUtoZ tools (jamesrobertwilliams.co.uk/autoz.php) provide formalisation in the style of commercially-acceptable model management [3]. AUtoZ is an automated framework based on Amálio's GeFoRME, the generative framework for rigorous model-driven engineering [1]. GeFoRME is designed to give semantically-adaptable support to the construction of formal models from diagrams.

Formal methods tools often produce messages aimed at expert users of the tool and relate to line numbers of the formal specification; mapping these messages back to components in UML diagrams is not trivial. To address this, we are creating an AUtoZ instance that targets the *Community Z Tools* (CZT) project (czt.sourceforge.net). The *ZML* sub-project of CZT [2] supports XML markup for Z. CZT tools annotate the ZML file, for instance with issues raised by formal analysis. Exploiting the fact that, in model engineering, a diagrammatic model must conform to a metamodel (that defines abstract syntax and some semantics), and that ZML has a well-defined metamodel, generic associations can be made at the metamodel level. Therefore we can link elements in the UML and ZML models. Traceability links are thus a side-effect of the Z generation.

By combining AUtoZ with CZT's flexible, open-source formal support mechanisms, a complete tool chain has been designed which can overcome many of the problems of interfacing formal analysis with traditional diagram-based software engineering.

References

1. Amálio, N.: Generative frameworks for rigorous model-driven development. PhD thesis, Computer Science, York, UK (2007)
2. Utting, M., et al.: ZML: XML Support for Standard Z. In: Bert, D., Bowen, J.P., King, S. (eds.) ZB 2003. LNCS, vol. 2651, pp. 437–456. Springer, Heidelberg (2003)
3. Williams, J., Polack, F.: Automated formalisation for verification of diagrammatic models. In: FACS 2009. ENTCS (2009)

* This research was supported by the EPSRC, through the Large-Scale Complex IT Systems project, EP/F001096/1.