Tool Support for Production Use of Formal Techniques

John C. Knight, P. Thomas Fletcher, and Brian R. Hicks

Department of Computer Science
University of Virginia, Charlottesville, VA 22903, USA

Abstract. Despite their popularity in academia and many claimed benefits, formal techniques are still not widely used in commercial software development. We claim that lack of effective tools is a major factor limiting the adoption of formal techniques.

Tools supporting formal techniques must integrate smoothly into the overall software development process. To be accepted for regular use in engineering development, innovative tool ideas must be combined with a multitude of essential though routine facilities. Formal specifications using notations like Z include both formal and informal content, and developers of such specifications appreciate the value of innovative analysis but must be able to perform routine manipulations conveniently. However, implementing these routine facilities requires very extensive resources. This has led to valuable tools being developed with very restricted routine facilities thereby limiting the exploitation of their innovation in commercial software development.

To test the idea that high performance tools will promote the use of formal techniques, we have developed a toolset (named Zeus) for the manipulation of Z specifications. Recent experience has shown that large package programs can be reused to provide convenient access to routine facilities. Zeus is based on FrameMaker, a commercial desktop publishing system, and as a result it provides all the document-processing features that FrameMaker provides including WYSIWYG editing using the Z character set and a wealth of formatting features, such as controlling page layouts. It also provides the standard look and feel of Microsoft Windows applications and access to all operating-system services and supported applications. Supplementing these basic features, Zeus provides many Z-specific facilities. Graphic structures are inserted automatically using a menu selection, move with the text to which they are anchored, are resized as their contents change, and can be cut, copied and pasted as desired. Zeus also provides convenient access to Z/EVES, a widely-used, high-performance system for the analysis of Z specifications. Formal text from a FrameMaker document can be selected and sent to Z/EVES for analysis, and the document is annotated to show which text has been checked. The interface seen by a Zeus user is a desktop publishing system that permits convenient manipulation of Z text together with a relatively seamless connection to a powerful analysis capability and access to all the other services supporting software development that are present on the development platform, such as configuration management tools. Whether such a system will promote the wider use of formal techniques in industry is the subject of ongoing experimentation.

Information about Zeus is available at `http://www.cs.virginia.edu/zeus`. This work was supported in part by the National Science Foundation under grant number CCR-9213427, and in part by NASA under grant number NAG1-1123-FDP.