MECHANISED SUPPORT FOR RETRENCHMENT IN THE B-TOOLKIT

March 2005

By
Simon Fraser
Department of Computer Science

Abstract

Refinement is a long-established technique used in the formal development of software. It can be argued, however, that the situations in which refinement can be used effectively are limited, and these claims led to the introduction of a more flexible technique, retrenchment. As a relatively new technique, however, the specification and proof of retrenchment steps must be performed manually. This thesis describes the creation of an extension to the B-Toolkit that aims to provide mechanical assistance to this process.

The notions of refinement and retrenchment are reviewed, and their differences shown through examples. The B-Method is introduced, and the notation and processes required to support retrenchment described, before a formal extension to the B-Method is proposed. An overview of the B-Toolkit, and its components is provided, and the impact of supporting retrenchment detailed. Finally, the construction of a specification for a phone system using retrenchment and the extended B-Toolkit is documented, and the results analysed.