Demonstration of the B-Toolkit

Ib Holm Sørensen

B-Core Limited
Magdalen Centre, Oxford
England
Email: `Ib.Sorensen@comlab.ox.ac.uk`

The B-Toolkit is a suite of integrated programs which implement the B-Method for Software Development. The B-Method is a collection of formal techniques which give a basis to those activities of Software Development that range from technical software specification, through design and integration, to code generation and into maintenance. The B-Method and the specification language AMN (Abstract Machine Notation) are in many respects similar to other "model oriented" formal methods. They employ a conventional "pseudo" programming style. The B-Tool is a language interpreter for the B Theory Language. This language is a special purpose language for writing interactive and automatic proof assistants and other systems where pattern matching, substitution and re-write mechanisms can be used. The B-Toolkit's component tools are implemented in the B Theory Language and is interpreted by the B-Tool.

Description

The B-Toolkit, which supports the B-Method, underwent eight years of research and development at the Programming Research Group in Oxford and British Petroleum Research, and its commercial development is now continuing inside B-Core (UK) Ltd in Oxford. The B-Toolkit is an integrated suite of computer programs, built partly on the B-Tool interpreter, and covers many aspects of software engineering, including:

a) Syntax and type-checking of specification documents as well as low level design documents, with comprehensive error reporting .

b) Verification condition generation (which generates the proof-obligations needed to guarantee specification consistency and correctness of refinement). The refinement rules, which originate from Oxford (Hoare, Sanders, He) and J-R Abrial's formulation in terms of Predicate Transformers, are used within the tool.

c) Automatic & interactive provers for discharging the verification conditions. (Other provers can be used in conjunction with B-Core (UK)'s B-Toolkit). Specification animation, enabling the specification to be "run", validated and tested; pre-conditions, guards for conditional statements, and the values of local and state variables may be inspected during animation.)

d) A translator for translating low level design documents into C.

e) Code generation from declarative descriptions, facilitated by a re-usable library of code modules.

f) A Library of reusable code modules, which are all accessed and used according to their given specification.

g) Rapid prototyping, facilitated by an interface generator, built on the reusable library.

h) Automatic Markup and Indexing of documentation of complete developments (requires LaTeX).

Availability

The B-Toolkit is commercially available in a Trial version or through full release licences. The B-Toolkit is delivered for IBM/RS6000 running AIX and Sun Sparc running SunOS 4.1.x. (5.x is also supported). The Toolkit requires 16Mbytes of RAM and approximately 20Mbytes of Disc. The B-Tookit is highly portable, and will run under most Unix systems implementations. The current B-Toolkit requires as a minimum a Unix Operating System, and for full functionality it further requires LaTeX and a C-Compiler.