The Development of a Toolkit to Support Probabilistic B-Method

Thai Son Hoang

Introduction

B Method (B) is a formal development method that facilitates the refinement of specification to code. Our probabilistic B (pB) replaces Boolean predicates by real valued probabilities in the range 0–1. This allows probabilistic uncertainty to be modelled.

Probabilistic choice

\[ S \not\Rightarrow \top \]

represents a choice between S and T in which S is taken with probability \( p \) and T is taken with probability \( 1 - p \).

Questions:

* What is the expected running cost of a system?

* What is the reliability for a system given some information about its components?

Probability-one termination

It turns out that we need to specify that the specification does in fact terminate. For any program \( T \subseteq \top \) and only if \( T \Rightarrow [v_0 = x] S B^v \), where \( B^v = B \times (w = u_0) \) (no unmarked variables in the substitution).

Fundamental theorem

Assume that \( S = \nu \{ A, B \} \). For any programs \( T, S \subseteq \top \) if \( T \Rightarrow [v_0 = x] S B^v \), where \( B^v = B \times (w = u_0) \).

Probabilistic specification substitution

Terminating probabilistic specification substitution

It turns out that we need to specify that the specification does in fact terminate.

Fundamental theorem

Assume that \( S = \nu \{ A, B \} \). For any programs \( T, S \subseteq \top \) if \( T \Rightarrow [v_0 = x] S B^v \), where \( B^v = B \times (w = u_0) \).

Conclusion and future work

Work done

The extended B (pB) and modified BBToolkit supports the following:

* Termination with probability-one;

* Probabilistic invariant;

* Probabilistic specification substitution;

* Fundamental theorem for refinement;

* Probabilistic loops.

Future work

More research needs to be done on:

* Specification with multiple expectations;

* Fundamental theorem for multiple expectation specification;

* General data refinement for probabilistic programs.

This project was supported by the Australian Research Council under the large grant A00103115.