The imagination driving Australia's ICT future

NATIONAL ICT AUSTRALIA LIMITED

Probabilistic Refinement

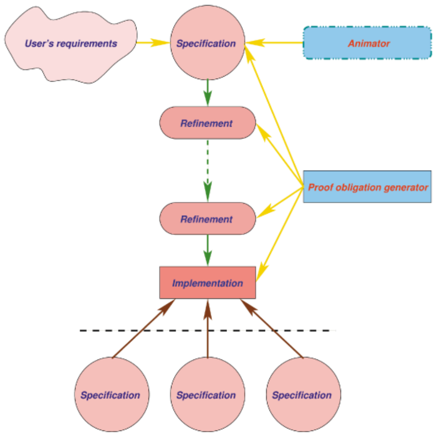
Staff

Thai Son Hoang

B $\Longrightarrow$ pB

Our aim is to produce a theoretical method, and associated tools, that will increase the rigour with which designers can incorporate the probabilistic information necessary to quantify risk and expected cost-of-failure in embedded computer systems.

B Method (B) is a formal development method that facilitates the refinement of specification to code.



Probabilistic B

Our *probabilistic B* (pB) replaces Boolean by real valued probabilities in the range $0..1$. This allows probabilistic uncertainty to be modelled.

Probabilistic choice

$$S \;{}_p\!\oplus\; T$$

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 component?

Example The following illustrates a simple library in which books are lost with probability p.

```
StartLoan ≙
pre  booksInLibrary > 0  then
   booksInLibrary := booksInLibrary − 1  ||
   loansStarted := loansStarted + 1
end


EndLoan ≙
pre  loansEnded < loansStarted  then
   booksLost := booksLost + 1 p⊕ booksInLibrary := booksInLibrary + 1  ||
   loansEnded := loansEnded + 1
end
```

Invariants are replaced by *expectations*. For this specification, the expectation is defined by

$$E \mathrel{\widehat{=}} p * loansEnded - booksLost\ .$$

We can conclude that the expected number of books lost is bounded above by $p * loansEnded$.

Current status

The *extended B (pB)* and modified *B-Toolkit* supports the following:

- ⋆ Probabilistic invariant;
- ⋆ Probabilistic specification substitution;
- ⋆ Termination with probability 1;
- ⋆ Fundamental theorem for refinement;
- ⋆ Probabilistic loops.

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