Multiple-expectation Systems

Thai Son Hoang

Department of Computer Science
Swiss Federal Institute of Technology Zürich (ETH Zürich)

(Joint work with Zhendong Jin, Ken Robinson, Annabelle McIver and Carroll Morgan)

RefineNet Workshop, 31st October 2005, Manchester

Outline

1. Motivation
   - Extension to Probabilistic B
   - Background
2. Our Results/Contribution
   - Multiple Probabilistic Specification Substitutions
   - Fundamental Theorem
   - Case Study: Duelling Cowboys

Outline

1. Motivation
   - Extension to Probabilistic B
   - Background
2. Our Results/Contribution
   - Multiple Probabilistic Specification Substitutions
   - Fundamental Theorem
   - Case Study: Duelling Cowboys

Extending probabilistic B

- To extend the scope of *probabilistic B (pB)* to cover systems with multiple probabilistic properties;
- Need to introduce *multiple probabilistic specification substitution*;
- Investigate the new substitution in the framework of *layered developments*.

Extending probabilistic B

- To extend the scope of *probabilistic B (pB)* to cover systems with multiple probabilistic properties;
- Need to introduce *multiple probabilistic specification substitution*;
- Investigate the new substitution in the framework of *layered developments*.

Extending probabilistic B

- To extend the scope of *probabilistic B (pB)* to cover systems with multiple probabilistic properties;
- Need to introduce *multiple probabilistic specification substitution*;
- Investigate the new substitution in the framework of *layered developments*.

Outline

How *pGSL* extends *GSL*

Expectations replace predicates

Predicates (functions from state to Boolean) are widened to *Expectations* (functions from state to non-negative real).

- For consistency with Boolean logic, we use embedded predicates, $\langle \textit{false} \rangle = 0$, and $\langle \textit{true} \rangle = 1$.
- Notationally, we have kept predicates as much as possible.

How *pGSL* extends *GSL*

Expectations replace predicates

Predicates (functions from state to Boolean) are widened to *Expectations* (functions from state to non-negative real).

- For consistency with Boolean logic, we use embedded predicates, $\langle \mathit{false} \rangle = 0$, and $\langle \mathit{true} \rangle = 1$.
- Notationally, we have kept predicates as much as possible.

How *pGSL* extends *GSL*

Expectations replace predicates

Predicates (functions from state to Boolean) are widened to *Expectations* (functions from state to non-negative real).

- For consistency with Boolean logic, we use embedded predicates, $\langle \mathit{false} \rangle = 0$, and $\langle \mathit{true} \rangle = 1$.
- Notationally, we have kept predicates as much as possible.

Probabilistic generalised substitution language

Summary

$[x := E]exp$	The expectation obtained after replacing all free occurrences of x in exp by E
$[skip]exp$	exp
$[prog_1 \; {}_p\oplus \; prog_2]exp$	$p \times [prog_1]exp + (1-p) \times [prog_2]exp$
$prog_1 \sqsubseteq prog_2$	$[prog_1]exp \Rrightarrow [prog_2]exp$
$[prog_1 \; [] \; prog_2]exp$	$[prog_1]exp \; \min \; [prog_2]exp$
$[@y \cdot pred \Longrightarrow prog]exp$	$\min(y) \cdot (pred \mid [prog]exp)$

Probabilistic generalised substitution language

Summary

$[x := E]exp$	The expectation obtained after replacing all free occurrences of x in exp by E
$[skip]exp$	exp
$[prog_1 \ {}_p\oplus \ prog_2]exp$	$p \times [prog_1]exp$ $+ \ (1-p) \times [prog_2]exp$
$prog_1 \sqsubseteq prog_2$	$[prog_1]exp \Rrightarrow [prog_2]exp$
$[prog_1 \ [] \ prog_2]exp$	$[prog_1]exp \ \min \ [prog_2]exp$
$[@y \cdot pred \Longrightarrow prog]exp$	$\min\ (y) \cdot (pred \mid [prog]exp)$

Probabilistic generalised substitution language

Summary

$[x := E]exp$	The expectation obtained after replacing all free occurrences of x in exp by E
$[skip]exp$	exp
$[prog_1 \,{}_p\!\oplus\, prog_2]exp$	$p \times [prog_1]exp + (1-p) \times [prog_2]exp$
$prog_1 \sqsubseteq prog_2$	$[prog_1]exp \Rrightarrow [prog_2]exp$
$[prog_1 \,[\!]\, prog_2]exp$	$[prog_1]exp \min [prog_2]exp$
$[@y \cdot pred \Longrightarrow prog]exp$	$\min(y) \cdot (pred \mid [prog]exp)$

Probabilistic generalised substitution language

Summary

$[x := E]exp$	The expectation obtained after replacing all free occurrences of x in exp by E
$[skip]exp$	exp
$[prog_1 \; {}_p\oplus \; prog_2]exp$	$p \times [prog_1]exp + (1-p) \times [prog_2]exp$
$prog_1 \sqsubseteq prog_2$	$[prog_1]exp \Rrightarrow [prog_2]exp$
$[prog_1 \; [] \; prog_2]exp$	$[prog_1]exp \; \min \; [prog_2]exp$
$[@y \cdot pred \Longrightarrow prog]exp$	$\min(y) \cdot (pred \mid [prog]exp)$

Probabilistic generalised substitution language

Summary

$[x := E]exp$	The expectation obtained after replacing all free occurrences of x in exp by E
$[skip]exp$	exp
$[prog_1 \;{}_p\oplus\; prog_2]exp$	$p \times [prog_1]exp$ $+ (1-p) \times [prog_2]exp$
$prog_1 \sqsubseteq prog_2$	$[prog_1]exp \Rrightarrow [prog_2]exp$
$[prog_1 \;[\!]\; prog_2]exp$	$[prog_1]exp$ min $[prog_2]exp$
$[@y \cdot pred \Longrightarrow prog]exp$	$\min(y) \cdot (pred \mid [prog]exp)$

(Single) Probabilistic specification substitution

Syntax

$v : \{A\ ,\ B\}$, where A and B are expectations over state x.

- $v \subseteq x$
- B can refer to the original state by using subscripted variables x_0.

The expected value of B over the set of final distributions is at least the expected value of A over the initial distribution.

Semantics

$$[v : \{A\ ,\ B\}]\, C \ \ \hat{=}\ \ A \times [x_0 : = x]\left(\sqcap x \cdot \left(\frac{C}{B \times \langle w = w_0 \rangle}\right)\right)$$

(w is the set of unchanged variables, i.e. $x - v$).
(Similar work can be seen in White[1996] and Ying[2003])

(Single) Probabilistic specification substitution

Syntax

$v : \{A\ ,\ B\}$, where A and B are expectations over state x.

- $v \subseteq x$
- B can refer to the original state by using subscripted variables x_0.

The expected value of B over the set of final distributions is at least the expected value of A over the initial distribution.

Semantics

$$[v : \{A\ ,\ B\}]\,C \quad \widehat{=} \quad A \times [x_0 :\ = x]\left(\sqcap x \cdot \left(\frac{C}{B \times \langle w = w_0 \rangle}\right)\right)$$

(w is the set of unchanged variables, i.e. $x - v$).
(Similar work can be seen in White[1996] and Ying[2003])

Fundamental theorem

Probabilistic Theorem

Assume that $prog_1 \;\widehat{=}\; v : \{A\, ,\; B\}\;.$
For any program $prog_2$,

$$prog_1 \sqsubseteq prog_2$$

if and only if

$$A \;\Rrightarrow\; [x_0 := x]\,[prog_2]\,B^w\;,$$

where $B^w \;\widehat{=}\; B \times \langle w = w_0 \rangle$.

Outline

1. Motivation
   - Extension to Probabilistic B
   - Background
2. Our Results/Contribution
   - Multiple Probabilistic Specification Substitutions
   - Fundamental Theorem
   - Case Study: Duelling Cowboys

Multi-way probabilistic choice

For $i \in (1..n)$, let p_i be a probabilistic expression over the state satisfying

$$\sum_{i=1}^{n} p_i \leq 1 \; ; \qquad (1)$$

Let S_i be a probabilistic substitution. The multi-way probabilistic choice is defined as follows:

$$\left[\begin{array}{|ll} S_1 & @p_1 \\ S_2 & @p_2 \\ \cdots & \\ S_n & @p_n \, , \end{array} \right] E \;\equiv\; \begin{array}{ll} & p_1 \times [S_1]\, E \\ + & p_2 \times [S_2]\, E \\ + & \cdots \\ + & p_n \times [S_n]\, E \, . \end{array} \qquad (2)$$

where E is an arbitrary expectation of the state.

Set of pre- and post-expectations

For $i \in (1..n)$, let p_i be a probabilistic expression over the state x and free from x_0 and satisfying:

$$\sum_{i=1}^{n} p_i \leq 1 \; ; \tag{3}$$

let Q_i be predicates defined over x_0, v (where v is a subset of x) and satisfying, for all Q_i, that we have

$$\forall x_0 \cdot (\exists v \cdot Q_i) \; . \tag{4}$$

Semantics

Let $p_0 = 1 - \sum_{i=1}^{n} p_i$, we define

$$v : \left| \begin{array}{l} \{p_1, \langle Q_1 \rangle\} \\ \{p_2, \langle Q_2 \rangle\} \\ \ldots \\ \{p_n, \langle Q_n \rangle\} \end{array} \right. \quad \widehat{=} \quad \left| \begin{array}{ll} (v : \{1\ ,\ \langle Q_1 \rangle\}) & @p_1 \\ (v : \{1\ ,\ \langle Q_2 \rangle\}) & @p_2 \\ \ldots & \\ (v : \{1\ ,\ \langle Q_n \rangle\}) & @p_n \\ (x : \{1\ ,\ 1\}) & @p_0\ . \end{array} \right. \tag{5}$$

Semantics

Let $p_0 = 1 - \sum_{i=1}^{n} p_i$, we define

$$v : \left| \begin{array}{l} \{p_1, \langle Q_1 \rangle\} \\ \{p_2, \langle Q_2 \rangle\} \\ \ldots \\ \{p_n, \langle Q_n \rangle\} \end{array} \right. \quad \widehat{=} \quad \left| \begin{array}{ll} (v : \{1\ ,\ \langle Q_1 \rangle\}) & @p_1 \\ (v : \{1\ ,\ \langle Q_2 \rangle\}) & @p_2 \\ \ldots & \\ (v : \{1\ ,\ \langle Q_n \rangle\}) & @p_n \\ (x : \{1\ ,\ 1\}) & @p_0\ . \end{array} \right. \tag{5}$$

Examples

A fair coin

$$S_1 \quad \widehat{=} \quad c : \left| \begin{array}{l} \{\tfrac{1}{2}, \langle c = H \rangle\} \\ \\ \{\tfrac{1}{2}, \langle c = T \rangle\} \end{array} \right. \qquad (6)$$

A non-deterministic coin:

A coin which guarantees to return Heads at least $1/3$ of the time and Tails at least $1/3$ of the time.

$$S_2 \quad \widehat{=} \quad c : \left| \begin{array}{l} \{\tfrac{1}{3}, \langle c = H \rangle\} \\ \\ \{\tfrac{1}{3}, \langle c = T \rangle\} \end{array} \right. \qquad (7)$$

Examples

A fair coin

$$S_1 \quad \widehat{=} \quad c : \left| \begin{array}{l} \{\frac{1}{2}, \langle c = H \rangle\} \\ \\ \{\frac{1}{2}, \langle c = T \rangle\} \end{array} \right. \tag{6}$$

A non-deterministic coin:

A coin which guarantees to return Heads at least $1/3$ of the time and Tails at least $1/3$ of the time.

$$S_2 \quad \widehat{=} \quad c : \left| \begin{array}{l} \{\frac{1}{3}, \langle c = H \rangle\} \\ \\ \{\frac{1}{3}, \langle c = T \rangle\} \end{array} \right. \tag{7}$$

Outline

1. Motivation
   - Extension to Probabilistic B
   - Background

2. Our Results/Contribution
   - Multiple Probabilistic Specification Substitutions
   - Fundamental Theorem
   - Case Study: Duelling Cowboys

We consider a special set of multiple probabilistic specification substitutions where for any pair Q_i and Q_j, where $i \neq j$, we have

$$Q_i \wedge Q_j = \mathit{false}\ , \tag{8}$$

Probabilistic Theorem

For all programs T, if

$$(x : \{1\ ,\ 1\}) \quad \sqsubseteq \quad T \quad \mathit{and} \tag{9}$$

$$(v : \{p_i\ ,\ \langle Q_i \rangle\}) \quad \sqsubseteq \quad T, \quad \textit{for all } i \in (1..n), \tag{10}$$

then we have

$$v : \left| \begin{array}{l} \{p_1, \langle Q_1 \rangle\} \\ \{p_2, \langle Q_2 \rangle\} \\ \ldots \\ \{p_n, \langle Q_n \rangle\} \end{array} \right. \quad \sqsubseteq \quad T\ . \tag{11}$$

Outline

1. Motivation
   - Extension to Probabilistic B
   - Background
2. Our Results/Contribution
   - Multiple Probabilistic Specification Substitutions
   - Fundamental Theorem
   - Case Study: Duelling Cowboys

Two cowboys

Conditions

There are two cowboys X and Y fighting a duel. They take turns to shoot at each other.

- The probability for X to hit his opponent is $\frac{2}{3}$.
- The probability for Y to hit his opponent is $\frac{1}{2}$.
- Assuming that X has the advantage of shooting first.

Question?

What are the guaranteed survival probabilities for both cowboys?

Two cowboys

Conditions

There are two cowboys X and Y fighting a duel. They take turns to shoot at each other.

- The probability for X to hit his opponent is $\frac{2}{3}$.
- The probability for Y to hit his opponent is $\frac{1}{2}$.
- Assuming that X has the advantage of shooting first.

Question?

What are the guaranteed survival probabilities for both cowboys?

Formal specification

Let p_X and p_Y be the survival probability for X and Y, respectively. Let s be the cowboy which survives the duelling.

Specification

$$s \longleftarrow \textbf{TwoCowboyXYSpec} \quad \widehat{=} \quad s : \left| \begin{array}{l} \{p_X, \langle s = X \rangle\} \\ \{p_Y, \langle s = Y \rangle\} \end{array} \right.$$

Implementation

$s \longleftarrow$ **TwoCowboyXYImp** $\widehat{=}$
VAR t, n IN
$t := X; s := X; n := 2;$
WHILE $n = 2$ DO
IF $t = X$ THEN
$(s := X; n := 1) \quad {}_{\frac{2}{3}}\oplus \quad t := Y$
ELSE
$(s := Y; n := 1) \quad {}_{\frac{1}{2}}\oplus \quad t := X$
END
EXPECTATIONS $\cdots$
END
END

Implementation

$s \longleftarrow$ **TwoCowboyXYImp** $\widehat{=}$
VAR t, n IN
$t := X; s := X; n := 2;$ // init
WHILE $n = 2$ DO
IF $t = X$ THEN
$(s := X; n := 1) \;_{\frac{2}{3}}\!\oplus\; t := Y$
ELSE
$(s := Y; n := 1) \;_{\frac{1}{2}}\!\oplus\; t := X$
END
EXPECTATIONS $\cdots$
END
END

Implementation

```
s ⟵ TwoCowboyXYImp  ≙
    VAR t, n IN
        t := X ; s := X ; n := 2;
        WHILE n = 2 DO    // Loop
            IF t = X THEN
                (s := X; n := 1)  2/3⊕  t := Y
            ELSE
                (s := Y ; n := 1)  1/2⊕  t := X
            END
        EXPECTATIONS ···
        END
    END
```

Implementation

$s \longleftarrow$ **TwoCowboyXYImp** $\widehat{=}$
  VAR t, n IN
    $t := X; s := X; n := 2;$
    WHILE $n = 2$ DO
      IF $t = X$ THEN // body
        $(s := X; n := 1) \;{}_{\frac{2}{3}}\!\oplus\; t := Y$
      ELSE
        $(s := Y; n := 1) \;{}_{\frac{1}{2}}\!\oplus\; t := X$
      END
    EXPECTATIONS $\cdots$
    END
  END

Proof obligations

In order to prove that **TwoCowboyXYSpec** $\sqsubseteq$ **TwoCowboyXYImp**, we have to prove that

$$(s : \{p_X\ ,\ \langle s = X \rangle\}) \quad \sqsubseteq \quad \textbf{TwoCowboyXYImpl} \tag{12}$$

and

$$(s : \{p_Y\ ,\ \langle s = Y \rangle\}) \quad \sqsubseteq \quad \textbf{TwoCowboyXYImpl}\ . \tag{13}$$

Then we can apply the fundamental theorem for single probabilistic specification substitution for (12) and (13) separately. For (12) we have to prove that

$$p_X \quad \Rrightarrow \quad [init; Loop]\,\langle s = X \rangle\ . \tag{14}$$

Recall proof rules for probabilistic loops

For a probabilistic loop, such as

$$\text{loop} \;\widehat{=}\; \textsc{while}\ G\ \textsc{do}\ S\ \textsc{invariant}\ I\ \textsc{expectation}\ E\ \textsc{end}\ .$$

then $A \Rrightarrow [init; loop]B$ holds if the following satisfies:

$P1$	A	$\Rrightarrow$	$[init]E$
$P2$	$\langle G \wedge I \rangle * E$	$\Rrightarrow$	$[S]\ E$
$P3$	$\langle \neg G \wedge I \rangle * E$	$\Rrightarrow$	B

(Here, I only concentrate on the maintenance of the expectation E)

Tabular method

For proving (14), we try to “guess” the expectation of the loop by tabulating the probabilities of establishing the post-expectation $s = X$ after executing one iteration of the loop.

	$n = 2$	$s = X \wedge n = 1$	$s = Y \wedge n = 1$
$t = X$	$4/5$	1	0
$t = Y$	$2/5$	1	0

We have the expectation of the loop is

$$E \quad \widehat{=} \quad \langle s = X \wedge n = 1 \rangle + \langle n = 2 \wedge t = X \rangle \times \frac{4}{5} + \langle n = 2 \wedge t = Y \rangle \times \frac{2}{5} \,. \quad (15)$$

Apply the proof rule *P1*, we need to prove that

$$p_X \Rrightarrow [t := X; s := X; n := 2]E\ , \tag{16}$$

which is equivalent to

$$p_X \Rrightarrow \frac{4}{5}\ . \tag{17}$$

So we can choose $p_X \equiv \frac{4}{5}$, which will be the guaranteed surviving probability for X. With similar reasoning, we have $p_Y \equiv \frac{1}{5}$.

Development in layers

Three Cowboys

Assume that we have another cowboy, namely Z with the probability of hitting his opponent is $\frac{1}{3}$. With similar setting, what are the surviving probabilities for the cowboys.

Here, we can use the specification of the two cowboys situation when write the implementation, for example, the case when Y has the turn to shoot can be specified as follows:

$$\text{IF } t = Y \text{ THEN}$$
$$(s \longleftarrow \textbf{TwoCowboyXY}; n := 1) \;\; {}_{\frac{1}{2}}\oplus \;\; t := Z$$
$$\text{ELSE} \cdots$$

and the reasoning can be done similarly as in the case for two cowboys.

Summary

- Abstractly specify and refine probabilistic systems with multiple properties.
- Development of these systems can be separated into layers.
- When the state is small, the expectation for loops can be found using the tabular method.

For further reading I

C. Morgan and A. McIver.
Abstraction, Refinement and Proof for Probabilistic Systems.
Springer-Verlag, 2004.

T.S. Hoang, Z. Jin, K. Robinson, C. Morgan and A. McIver.
Development via Refinement in Probabilistic B — Foundation and Case Study.
Proceedings of the 4th International Conference of B and Z Users, volume 3455 of *LNCS*, 2005.

N. White.
Probabilistic Specification and Refinement
Master Thesis, Keble College, 1996.

M.S. Ying.
Reasoning about probabilistic sequential programs in a probabilistic logic.
Acta Informatica, volume 39, 2003.