Automated Reasoning for Probabilistic Sequential Programs with Theorem Proving

Kangfeng Ye, Simon Foster, Jim Woodcock

University of York, UK

November 04, 2021

UNIVERSITY of York

UKRI Engineering and Physical Sciences Research Council

robostar.cs.york.ac.uk

Overview

Background

- RoboChart[1]: DSL for robotics (state machines: reactive+time+probability), unification of semantics (Unifying Theories of Programming or UTP)

[1] https://robostar.cs.york.ac.uk/notations/

Overview

Background

- RoboChart[1]: DSL for robotics (state machines: reactive+time+probability), unification of semantics (Unifying Theories of Programming or UTP)
- Recent work[2]: probabilistic semantics to RoboChart (He et al.'s relational model[3]): sequential+probability

[1] https://robostar.cs.york.ac.uk/notations/
[2] Woodcock et al.: Probabilistic semantics for RoboChart - A weakest completion approach. UTP 2019
[3] He et al.: Deriving probabilistic semantics via the 'weakest completion'. ICFEM 2004

Overview

Background

- RoboChart[1]: DSL for robotics (state machines: reactive+time+probability), unification of semantics (Unifying Theories of Programming or UTP)
- Recent work[2]: probabilistic semantics to RoboChart (He et al.'s relational model[3]): sequential+probability

Our contributions

- A formalisation of the proof that embedding sequential composition is a homomorphism,

Overview

Background

- RoboChart[1]: DSL for robotics (state machines: reactive+time+probability), unification of semantics (Unifying Theories of Programming or UTP)
- Recent work[2]: probabilistic semantics to RoboChart (He et al.'s relational model[3]): sequential+probability

Our contributions

- A formalisation of the proof that embedding sequential composition is a homomorphism,
- A mechanisation of probabilistic designs in Isabelle/UTP for automated reasoning,

Overview

Background

- RoboChart[1]: DSL for robotics (state machines: reactive+time+probability), unification of semantics (Unifying Theories of Programming or UTP)
- Recent work[2]: probabilistic semantics to RoboChart (He et al.'s relational model[3]): sequential+probability

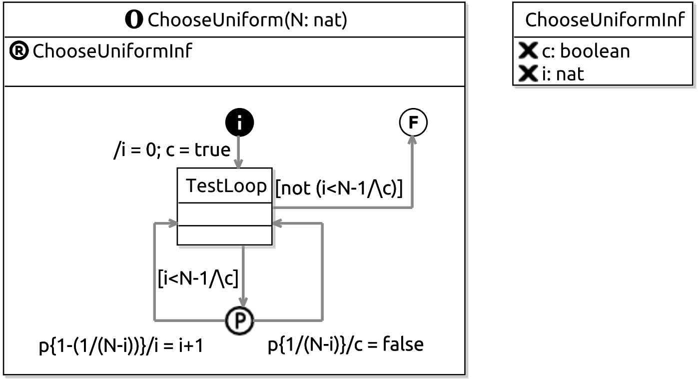
Our contributions

- A formalisation of the proof that embedding sequential composition is a homomorphism,
- A mechanisation of probabilistic designs in Isabelle/UTP for automated reasoning,
- With mechanisation, more interesting details are disclosed.
  - PMFs are convex-closed,
  - Probabilistic choice is not idempotent in general,
  - Embedding sequential composition is a homomorphism only for finite state space.

Outline

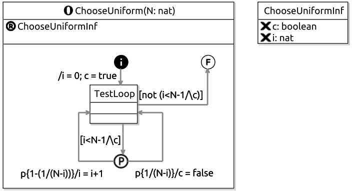
A RoboChart algorithm

Goal: a randomisation algorithm (the same probability $1/N$ to choose i from $[0, N-1]$)



A RoboChart algorithm

Question: does this model correctly implement the randomisation algorithm for any N?

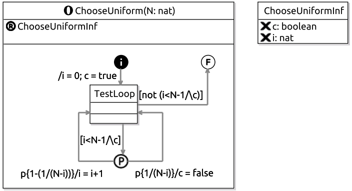


Analysis by PRISM on a Linux server:

- $N = 100$: model construction (4s) + checking (0.002s);
- $N = 10,000$: 8s + 0.004s;
- $N = 100,000$: 830s + 0.011s;
- $N = 1,000,000$: not finished after several hours;
- $N = 1, \ldots\ldots\ldots\ldots$: ?

A RoboChart algorithm

Question: does this model correctly implement the randomisation algorithm for any N?



Analysis by PRISM on a Linux server:

- $N = 100$: model construction (4s) + checking (0.002s);
- $N = 10,000$: 8s + 0.004s;
- $N = 100,000$: 830s + 0.011s;
- $N = 1,000,000$: not finished after several hours;
- $N = 1,$............: ?

Our solution: theorem proving

Nondeterministic probabilistic sequential programming language

pGCL[1]

$$P \quad ::= \quad \bot \mid I\!I \mid x := e \mid P \lhd b \rhd Q \mid P \sqcap Q \mid P \oplus_r Q \mid P \, ; \, Q \mid \mu X \bullet P(X)$$

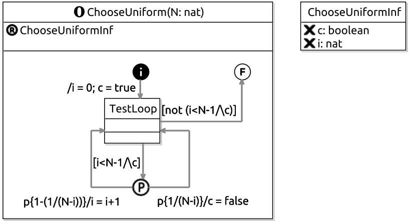
[1] McIver,A.,Morgan,C.: Introduction to pGCL: Its logic and its model. Springer (January 2005)

Nondeterministic probabilistic sequential programming language

pGCL[1]

$$P \quad ::= \quad \bot \mid I\!I \mid x := e \mid P \lhd b \rhd Q \mid P \sqcap Q \mid P \oplus_r Q \mid P \,;\, Q \mid \mu X \bullet P(X)$$

Randomisation algorithm in *pGCL*



$$\begin{aligned} &ChooseUniform(N) \triangleq \\ &\quad i := 0 \,;\ c := true \,; \\ &\quad \mu X \bullet \left(\begin{array}{l} ((c := false) \oplus_{1/(N-i)} (i := i+1)) \,;\ X \\ \lhd (i < (N-1) \wedge c) \rhd I\!I \end{array} \right) \end{aligned}$$

[1] McIver,A.,Morgan,C.: Introduction to pGCL: Its logic and its model. Springer (January 2005)

Outline

Relational semantics [He et al.] of sequential probabilistic programs

Embedding

$\mathcal{K}(D) \triangleq D/\rho$ $\quad$ $D \triangleq (p \vdash_n R)$ $\quad$ Embeddeding

Relational semantics of sequential probabilistic programs

Embedding

$$Y/K \triangleq \neg(\neg Y;\ K^{-})$$

Weakest prespecification

$$\mathcal{K}(D) \triangleq D/\rho \qquad D \triangleq (p \vdash_n R)$$

Embeddeding

Relational semantics of sequential probabilistic programs

Embedding

$$Y/K \triangleq \neg\, (\neg\, Y;\ K^{-})$$ Weakest prespecification

$$\rho \triangleq \left(true \vdash prob(s') > 0\right) \qquad prob : PROB\, (\triangleq S \to [0,1])$$ Forgetful function

$$\mathcal{K}(D) \triangleq D/\rho \qquad D \triangleq (p \vdash_n R)$$ Embeddeding

Relational semantics of sequential probabilistic programs

Embedding

$Y/K \triangleq \neg\,(\neg\, Y;\ K^{-})$		Weakest prespecification
$\rho \triangleq \big(true \vdash prob(s') > 0\big)$	$prob : PROB\,(\triangleq S \to [0,1])$	Forgetful function
$\mathcal{K}(D) \triangleq D/\rho$	$D \triangleq (p \vdash_n R)$	Embeddeding

$$
\begin{tikzcd}
S \arrow[r, "P"] \arrow[dr, "D"'] & PROB \arrow[d, "\rho"] \\
 & S
\end{tikzcd}
$$

Relational semantics of sequential probabilistic programs

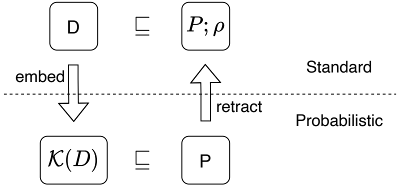
Embedding

$$Y/K \triangleq \neg\,(\neg\, Y;\ K^{-})$$ Weakest prespecification

$$\rho \triangleq \left(true \vdash prob(s') > 0\right) \qquad prob : PROB\,(\triangleq S \to [0,1])$$ Forgetful function

$$\mathcal{K}(D) \triangleq D/\rho \qquad D \triangleq (p \vdash_n R)$$ Embeddeding

$$\begin{tikzcd} S \arrow[r, "P"] \arrow[dr, "D"'] & PROB \arrow[d, "\rho"] \\ & S \end{tikzcd}$$



$$\mathcal{K}(D);\ \rho = D$$ Retraction

$$D \sqsubseteq (P;\ \rho) \Leftrightarrow (D/\rho) \sqsubseteq P$$

Relational semantics (embedding: a homomorphism)

Homomorphism on the structure of standard programs

$$\mathcal{K}(\bot) = \bot \qquad \mathcal{K}(x := e) = \left(true \vdash prob'(\mathbf{v}[e/x]) = 1\right)$$

$$\mathcal{K}(I\!I) = \left(\textbf{\textit{true}} \vdash prob'(\mathbf{v}) = 1\right) \qquad \mathcal{K}(P \lhd b \rhd Q) = \mathcal{K}(P) \lhd b \rhd \mathcal{K}(Q)$$

$$(P \oplus_r Q) = \ldots \qquad \mu X \bullet P(X) = \bigsqcap\{X \mid X \sqsupseteq P(X)\}$$

$$\mathcal{K}(P \sqcap Q) = \left(\bigsqcap r \in [0..1] \bullet \mathcal{K}(P) \oplus_r \mathcal{K}(Q)\right) \qquad (\sqsubseteq \mathcal{K}(P) \oplus_r \mathcal{K}(Q)) \qquad \text{Nondeterminism}^{*}$$

$$\mathcal{K}(P;\ Q) = \mathcal{K}(P);\uparrow \mathcal{K}(Q)$$

Relational semantics (previous [Woodcock et al.], a new contribution)

Homomorphism on the structure of standard programs

$$\mathcal{K}(\bot) = \bot \qquad \mathcal{K}(x := e) = \left(\mathit{true} \vdash \mathit{prob}'(\mathbf{v}[e/x]) = 1\right)$$

$$\mathcal{K}(I\!I) = \left(\textbf{\textit{true}} \vdash \mathit{prob}'(\mathbf{v}) = 1\right) \qquad \mathcal{K}(P \lhd b \rhd Q) = \mathcal{K}(P) \lhd b \rhd \mathcal{K}(Q)$$

$$(P \oplus_r Q) = \ldots \qquad \mu X \bullet P(X) = \bigsqcap \{X \mid X \sqsupseteq P(X)\}$$

$$\mathcal{K}(P \sqcap Q) = \left(\bigsqcap r \in [0..1] \bullet \mathcal{K}(P) \oplus_r \mathcal{K}(Q)\right) \qquad (\sqsubseteq \mathcal{K}(P) \oplus_r \mathcal{K}(Q))$$ Nondeterminism*

$$\mathcal{K}(P;\ Q) = \mathcal{K}(P);\uparrow \mathcal{K}(Q) \qquad (P \sqsubseteq Q \Rightarrow (\uparrow P) \sqsubseteq (\uparrow Q))$$ Sequential composition+

Outline

Probabilistic state space and probabilistic choice

Probabilistic state space

- $prob :: [\alpha]pmf$ (Isabelle measure-based pmf).
- Probabilistic designs:

$$\mathcal{K}\,(p \vdash R(S,S)) = \left(p \vdash \left(\Sigma i \in S \mid (R\ \textbf{\textit{wp}}\ (\mathbf{v} = i)) \bullet prob'(i)\right) = 1\right)$$

Probabilistic state space and probabilistic choice

Probabilistic state space

- $prob :: [\alpha]pmf$ (Isabelle measure-based pmf).
- Probabilistic designs:

$$\mathcal{K}\,(p \vdash R(S,S)) = \left(p \vdash \left(\Sigma i \in S \mid (R\ \textbf{wp}\ (\mathbf{v} = i)) \bullet prob'(i)\right) = 1\right)$$

Probabilistic choice

- $[S]pmf$ is convex-closed in terms of distribution combination operator $+_r$;
- $+_r$ is idempotent: $p +_r p = p$;
- $\oplus_r$ is not idempotent: $P \oplus_r P = P$ only if $prob'$ in $P(s, prob')$ is convex-closed.
  - the distribution of a deterministic probabilistic program (singleton);
  - the distributions of embedding nondeterministic choice.

Sequential composition

Kleisli lifting

$$\uparrow (q \vdash R) \triangleq \left(\begin{array}{l} (\Sigma i \in [\![q]\!] \bullet prob\,(i) = 1) \vdash \\ \exists\, Q \bullet \left(\begin{array}{l} (\forall\, ss \bullet prob'(ss) = \mathbf{\Sigma} t \bullet prob(t) * (Q(t))(ss)) \wedge \\ \left(\forall\, s \bullet \left(\begin{array}{l} \neg\ (prob(\mathbf{v}') > \mathbf{0} \wedge \mathbf{v}' = s) \,; \\ (\neg\ R \,;\ (\forall\, t \bullet prob(t) = (Q(s))(t))) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

Sequential composition

Kleisli lifting

$$\uparrow (q \vdash R) \triangleq \left(\begin{array}{l} (\Sigma i \in [\![q]\!] \bullet prob\,(i) = 1) \vdash \\ \exists\, Q \bullet \left(\begin{array}{l} (\forall\, ss \bullet prob'(ss) = \mathbf{\Sigma} t \bullet prob(t) * (Q(t))(ss)) \wedge \\ \left(\forall\, s \bullet \left(\begin{array}{l} \neg\ (prob(\mathbf{v}') > \mathbf{0} \wedge \mathbf{v}' = s)\, ; \\ (\neg\ R\, ;\ (\forall\, t \bullet prob(t) = (Q(s))(t))) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

Lifting

$$\uparrow (\mathcal{K}\,(\mathit{II})) = (\textbf{\textit{true}} \vdash prob' = prob)$$

$$P \sqsubseteq Q \Rightarrow \uparrow P \sqsubseteq \uparrow Q$$

Sequential composition

Kleisli lifting

$$\uparrow(q \vdash R) \triangleq \left(\begin{array}{l} (\Sigma i \in [\![q]\!] \bullet prob\,(i) = 1) \vdash \\ \exists\, Q \bullet \left(\begin{array}{l} (\forall\, ss \bullet prob'(ss) = \mathbf{\Sigma} t \bullet prob(t) * (Q(t))(ss)))\ \wedge \\ \left(\forall\, s \bullet \left(\begin{array}{l} \neg\ (prob(\mathbf{v}') > \mathbf{0} \wedge \mathbf{v}' = s)\,; \\ (\neg\, R\,;\ (\forall\, t \bullet prob(t) = (Q(s))(t))) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

Lifting

$$\uparrow(\mathcal{K}\,(\mathit{I\!I})) = \left(\textbf{\textit{true}} \vdash prob' = prob\right)$$

$$P \sqsubseteq Q \Rightarrow \uparrow P \sqsubseteq \uparrow Q$$

Sequential composition

$$P\,;_p\,Q \triangleq P;\ \uparrow Q$$

$$P\,;_p\,\mathcal{K}\,(\mathit{I\!I}) = P = \mathcal{K}\,(\mathit{I\!I})\ ;_p\,P \qquad \text{(left/right unit)}$$

$$\mathcal{K}(P;\ Q) = \mathcal{K}(P)\,;_p\,\mathcal{K}(Q) \qquad \text{Only if } S \text{ is finite}$$

Recursion

Theorem (Refinement introduction)

We assume

- R *is a well-founded relation:* $\mathbf{wf}\, R$;
- F *is monotonic:* $\forall\, P\ Q \bullet [\![P \sqsubseteq Q;\ P \textit{ is } \mathbf{N};\ Q \textit{ is } \mathbf{N}]\!] \Rightarrow F(P) \sqsubseteq F(Q)$;
- F *is a* $\mathbf{N}$*-healthy function:* $F \in \mathbf{N} \to \mathbf{N}$;
- *Induct step:* $\forall\, st \bullet ((p \wedge e = st) \vdash Q) \sqsubseteq F\,((p \wedge (e, st) \in R) \vdash Q)$;

then

$$(p \vdash Q) \sqsubseteq \mu\ F$$

Outline

Example 1

Probabilistic choice[1]

$$P1 \triangleq \left(\mathcal{K}\,(x := 0) \oplus_{1/3} \mathcal{K}\,(x := 1)\right)$$

$$P2 \triangleq \left(\mathcal{K}\,(x := x + 2) \oplus_{1/2} \mathcal{K}\,(x := x + 3)\right)$$

$$P3 \triangleq \left(\mathcal{K}\,(x := x + 4) \oplus_{1/4} \mathcal{K}\,(x := x + 5)\right)$$

$$P1 \,;_p\, (P2 \lhd x = 0 \rhd P3) = \left(\textit{\textbf{true}} \vdash \left(\begin{array}{l} prob'\,(\mathbf{v}[2/x]) = 1/6 \land prob'\,(\mathbf{v}[3/x]) = 1/6 \land \\ prob'\,(\mathbf{v}[5/x]) = 1/6 \land prob'\,(\mathbf{v}[6/x]) = 1/2 \end{array}\right)\right)$$

[1] Hehner, E.C.R.: Probabilistic predicative programming. MPC2004

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}\,(x := 0) \sqcap \mathcal{K}\,(x := 1))$$

$$Q \triangleq \left(\mathcal{K}\,(y := 0) \oplus_{1/2} \mathcal{K}\,(y := 1)\right)$$

$$P ;_p Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ \\ \end{array} \right)\right)$$

$$Q ;_p P = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} \\ \\ \\ \end{array} \right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}\,(x := 0) \sqcap \mathcal{K}\,(x := 1))$$

$$Q \triangleq \left(\mathcal{K}\,(y := 0) \oplus_{1/2} \mathcal{K}\,(y := 1)\right)$$

$$P \,;_p\, Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

$$Q \,;_p\, P = \left(\textbf{\textit{true}} \vdash \left(\qquad \right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}(x := 0) \sqcap \mathcal{K}(x := 1))$$

$$Q \triangleq \left(\mathcal{K}(y := 0) \oplus_{1/2} \mathcal{K}(y := 1)\right)$$

$$P ;_p Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} (prob'(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

$$Q ;_p P = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} (prob'(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ \\ \\ \end{array}\right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}\,(x := 0) \sqcap \mathcal{K}\,(x := 1))$$

$$Q \triangleq \left(\mathcal{K}\,(y := 0) \oplus_{1/2} \mathcal{K}\,(y := 1)\right)$$

$$P \,;_p\, Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

$$Q \,;_p\, P = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ \\ \\ \end{array}\right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}\,(x := 0) \sqcap \mathcal{K}\,(x := 1))$$

$$Q \triangleq \left(\mathcal{K}\,(y := 0) \oplus_{1/2} \mathcal{K}\,(y := 1)\right)$$

$$P \,;_p\, Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

$$Q \,;_p\, P = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \vee \\ \end{array}\right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 2

Probabilistic choice and nondeterministic choice[1]

$$P \triangleq (\mathcal{K}\,(x := 0) \sqcap \mathcal{K}\,(x := 1))$$

$$Q \triangleq \left(\mathcal{K}\,(y := 0) \oplus_{1/2} \mathcal{K}\,(y := 1)\right)$$

$$P \,;_p\, Q = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

$$Q \,;_p\, P = \left(\textbf{\textit{true}} \vdash \left(\begin{array}{c} (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[0, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[0, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \vee \\ (prob'\,(\mathbf{v}[1, 0/x, y]) = 1/2 \wedge prob'\,(\mathbf{v}[1, 1/x, y]) = 1/2) \end{array}\right)\right)$$

[1] Jifeng, H., Seidel, K., McIver, A.: Probabilistic models for the guarded command language. SCP 1997

Example 3: the randomisation algorithm in RoboChart

Assume $N \geq 1$,

$$\left(\textbf{\textit{true}} \vdash \left(\left(\begin{array}{l} c \wedge i < (N-1) \Rightarrow \\ \quad \left(\left(\begin{array}{l} \forall j < (N-i-1) \bullet \\ \quad prob' \, (\mathbf{v}[j+i, \mathit{false}/i, c]) = 1/(N-i) \end{array} \right) \wedge \right. \\ \quad\quad prob' \, (\mathbf{v}[N-1, \mathit{true}/i, c] = 1/(N-i))) \end{array} \right) \wedge \right. \right. \\ \left. \left. (\neg \, (c \wedge i < (N-1)) \Rightarrow prob'(\mathbf{v}) = 1) \right) \right)$$

$$\sqsubseteq (\mu X \bullet \mathit{ChooseUniformBody}(N, X))$$

Choose in Theorem (refinement introduction): $e = N - i - (0 \lhd c \rhd 1)$ and $R = \{(x, y).x < y\}$

Example 3: the randomisation algorithm in RoboChart

Assume $N \geq 1$,

$$\left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} \left(\begin{array}{l} c \wedge i < (N-1) \Rightarrow \\ \quad \left(\left(\begin{array}{l} \forall j < (N-i-1) \bullet \\ \quad prob' \, (\mathbf{v}[j+i, \mathit{false}/i, c]) = 1/(N-i) \end{array} \right) \wedge \right. \\ \quad \left. prob' \, (\mathbf{v}[N-1, \mathit{true}/i, c] = 1/(N-i))) \right) \end{array} \right) \wedge \\ (\neg \, (c \wedge i < (N-1)) \Rightarrow prob'(\mathbf{v}) = 1) \end{array} \right) \right)$$

$$\sqsubseteq (\mu X \bullet \mathit{ChooseUniformBody}(N, X))$$

Choose in Theorem (refinement introduction): $e = N - i - (0 \lhd c \rhd 1)$ and $R = \{(x, y).x < y\}$

$$\left(\textbf{\textit{true}} \vdash \left(\begin{array}{l} (\forall j \bullet j < (N-1) \Rightarrow (prob' \, (\mathbf{v}[j, \mathit{false}/i, c] = 1/N))) \wedge \\ prob' \, (\mathbf{v}[(N-1), \mathit{true}/i, c]) = 1/N \end{array} \right) \right)$$

$$\sqsubseteq \mathit{ChooseUniform}(N)$$

Outline

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;
- Mechanisation shows that

  (1) PMFs are convex-closed;

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;
- Mechanisation shows that

  (1) PMFs are convex-closed;

  (2) the probabilistic choice is not idempotent in general;

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;
- Mechanisation shows that
  (1) PMFs are convex-closed;
  (2) the probabilistic choice is not idempotent in general;
  (3) embedding distributes through sequential composition for finite state space.

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;
- Mechanisation shows that
  (1) PMFs are convex-closed;
  (2) the probabilistic choice is not idempotent in general;
  (3) embedding distributes through sequential composition for finite state space.
- Analysed several examples;

Conclusion

- Formalisation of the proof that embedding sequential composition is a homomorphism;
- Mechanisation of the relational semantics in Isabelle/UTP;
- Mechanisation shows that
  (1) PMFs are convex-closed;
  (2) the probabilistic choice is not idempotent in general;
  (3) embedding distributes through sequential composition for finite state space.
- Analysed several examples;
- Future work: lift probabilistic designs to deal with reactive (instead of sequential) probabilistic systems.

Thank you!

https://robostar.cs.york.ac.uk/