Simple Proofs and Semantics for a Simple Probabilistic Language

Alex Simpson

(incorporating jww Janez Ignacij Jereb & Jure Mihelčič Žnidaršič)

FMF, University of Ljubljana
IMFM, Ljubljana

MFPS XLII, Ljubljana

3rd June 2026

A simple probabilistic language: pwhile

Integer expressions E

Boolean expressions B

Distribution expressions $d(E_1, \ldots, E_n)$

Commands C:

$$
\begin{array}{rcl}
C & ::= & X \leftarrow E \mid \mathsf{skip} \mid C; C \mid \\
& & \mathsf{if}\ B\ \mathsf{then}\ C\ \mathsf{else}\ C \mid \mathsf{while}\ B\ \mathsf{do}\ C \mid \\
& & X \stackrel{\$}{\leftarrow} d(E_1, \ldots, E_n) \qquad \text{(sample)}
\end{array}
$$

Example program

$$
\begin{aligned}
&X \leftarrow 1\,; \\
&Y \xleftarrow{\$} \mathsf{coin}()\,; \\
&\textsf{while } Y = 1 \textsf{ do} \\
&\quad X \leftarrow X + 1\,; \\
&\quad Y \xleftarrow{\$} \mathsf{coin}()
\end{aligned}
$$

Simple small-step operational semantics

State: a partial function $\sigma : \mathrm{Var} \rightharpoonup \mathbb{Z}$ with finite domain.

$$\frac{}{X \leftarrow E \,,\, \sigma \longrightarrow \sigma[X \mapsto n]} \; [\![E]\!]_\sigma = n$$

$$\frac{}{X \leftarrow E \,,\, \sigma \longrightarrow \text{fault}} \; \mathrm{Var}(E) \not\subseteq \mathrm{Dom}(\sigma)$$

$$\frac{}{X \xleftarrow{\$} d(E_1, \ldots, E_n) \,,\, \sigma \xrightarrow{d(n)} \sigma[X \mapsto n]} \; [\![d(E_1, \ldots, E_n)]\!]_\sigma = d \,,\, n \in \mathrm{Supp}(d)$$

$$\frac{}{\text{while } B \text{ do } C \,,\, \sigma \longrightarrow \sigma} \; [\![B]\!]_\sigma = \text{ff}$$

$$\frac{}{\text{while } B \text{ do } C \,,\, \sigma \longrightarrow C \,;\, \text{while } B \text{ do } C \,,\, \sigma} \; [\![B]\!]_\sigma = \text{tt}$$

3 semantic styles for imperative probabilistic languages

Kleisli

$$[\![C]\!] : \text{State} \to \text{Dist}(\text{State})$$

Distribution transformer

$$[\![C]\!] : \text{Dist}(\text{State}) \to \text{Dist}(\text{State})$$

Random variable transformer

$$[\![C]\!] : \text{RV}(\text{State}) \to \text{RV}(\text{State})$$

Random state

Random state: a function $\Sigma : \Omega \to \mathsf{State}$, where the sample space Ω is a (discrete) probability space.

(Almost-sure) termination

$$C, \Sigma \text{ terminates} :\Longleftrightarrow \Pr[C \text{ terminates from } \Sigma] = 1 .$$

If C, Σ terminates, it terminates in a final random state $\mathsf{T}_{C,\Sigma}$

$$\Omega \xleftarrow{q_{C,\Sigma}} \Omega_{C,\Sigma} \xrightarrow{\mathsf{T}_{C,\Sigma}} \mathsf{State}$$

Random state transformer

$$\begin{array}{rcl} [\![C]\!] : \mathsf{RV}(\mathsf{State}) & \to & \mathsf{RV}(\mathsf{State}) \\ \Sigma & \mapsto & \mathsf{T}_{C,\Sigma} \end{array}$$

Desiderata for a program logic

- General purpose.
- Natural specifications, e.g., Hoare triples $\{\,\Phi\,\}\,C\,\{\,\Psi\,\}$.
- Expressive assertions Φ, Ψ .
- Compositional proof rules with clear meaning.
- The proof system deals with program-based reasoning, deferring mathematical side-arguments for separate verification.

Semantic assertions

A semantic assertion Φ is given by a **partial** function

$$\Sigma \mapsto (\Sigma \models \Phi) : \text{RState} \rightharpoonup \{\text{tt}, \text{ff}\}$$

satisfying:

(SA1) $\Sigma \sqsubseteq \Sigma'$ and $(\Sigma \models \Phi)\downarrow$ implies $(\Sigma \models \Phi) \Leftrightarrow (\Sigma' \models \Phi)$.

(SA2) Φ has an associated finite set $\mathrm{FV}(\Phi) \subseteq \text{Var}$, its footprint variables, satisfying

$$(\Sigma \models \Phi)\downarrow \iff \Sigma \text{ is } \mathrm{FV}(\Phi)\text{-total.}$$

(Σ is U-total if, $\forall X \in U,\ \Pr[\Sigma(X)\downarrow] = 1$.)

(SA3) If $q : \Omega' \twoheadrightarrow \Omega$ is probability preserving, then $(\Sigma \circ q \models \Phi) \simeq (\Sigma \models \Phi)$.

Example semantic assertions

$[B]$ ($B = \mathsf{tt}$ holds with probability 1)

$$\begin{aligned} \mathrm{FV}([B]) &:= \mathrm{Var}(B) \\ \Sigma \models [B] &:\Longleftrightarrow \Pr[[\![B]\!]_\Sigma = \mathsf{tt}] = 1\,. \end{aligned}$$

$E \sim d$ (E is distributed according to distribution d)

$$\begin{aligned} \mathrm{FV}(E \sim d) &:= \mathrm{Var}(E) \\ \Sigma \models E \sim d &:\Longleftrightarrow [\![E]\!]_\Sigma \sim d\,. \end{aligned}$$

$E \triangleright \Phi$ [1] (Φ holds conditionally on the value of E)

$$\begin{aligned} \mathrm{FV}(E \triangleright \Phi) &:= \mathrm{Var}(E) \cup \mathrm{FV}(\Phi) \\ \Sigma \models E \triangleright \Phi &:\Longleftrightarrow \forall n \in \mathrm{Supp}([\![E]\!]_\Sigma),\ \Sigma|_{E=n} \models \Phi\,. \end{aligned}$$

[1] Based on the *conditioning modality* from *Lilac: a Modal Separation Logic for Conditional Probability* [Li, Ahmed & Holtzen, PACMPL, 2023].

Specifications $\{\,\Phi\,\}\,C\,\{\,\Psi\,\}$

Safety: we ask specifications to guarantee fault-freeness:

$$C, \Sigma \text{ fault-free} :\Longleftrightarrow \Pr[C, \Sigma \text{ faults}] = 0$$

N.B., C, Σ terminates $\Longrightarrow$ C, Σ fault-free.

Partial and total correctness for $\{\,\Phi\,\}\,C\,\{\,\Psi\,\}$.

Partial correctness: If $\Sigma \models \Phi$ then

- C, Σ is fault-free (safety), and
- if C, Σ terminates then $\mathsf{T}_{C,\Sigma} \models \Psi$.

Total correctness: If $\Sigma \models \Phi$ then

- C, Σ terminates and $\mathsf{T}_{C,\Sigma} \models \Psi$.

Example specification

$$
\begin{aligned}
&X \leftarrow 1\,; \\
&Y \xleftarrow{\$} \mathsf{coin}()\,; \\
&\textsf{while } Y = 1 \textsf{ do} \\
&\quad X \leftarrow X + 1\,; \\
&\quad Y \xleftarrow{\$} \mathsf{coin}()
\end{aligned}
$$

Example specification

$\{\}$

$X \leftarrow 1\,;$

$Y \xleftarrow{\$} \mathrm{coin}()\,;$

while $Y = 1$ do

$\quad X \leftarrow X + 1\,;$

$\quad Y \xleftarrow{\$} \mathrm{coin}()$

$\{\forall n \geq 1,\ \Pr[X = n] = 2^{-n}\}$

Partial correctness rule for while [2]

$$\frac{\{\Phi\}\,\text{if } B \text{ then } C \text{ else skip}\,\{\Phi\}}{\{\Phi\}\,\text{while } B \text{ do } C\,\{\Psi \wedge [\neg B]\}} \quad \begin{array}{l}\Phi \Rightarrow \Psi \\ \Psi \text{ closed under } \rightarrow_{\text{a.s.}}\end{array}$$

Justification

Suppose while B do C, Σ terminates.

Define

$$\begin{aligned}\Sigma_0 &:= \Sigma \\ \Sigma_{n+1} &:= \mathsf{T}_{\text{if } B \text{ then } C \text{ else skip}, \Sigma_n}\,.\end{aligned}$$

Then

$$\Sigma_n \rightarrow_{\text{a.s.}} \mathsf{T}_{\text{while } B \text{ do } C, \Sigma}\,.$$

[2] Similar rules involving closedness requirements on the postcondition appear in *An Assertion-Based Program Logic for Probabilistic Programs* [Barthe *et. al.*, ESOP 2018].

Example verification

$\{\}$

$X \leftarrow 1\,;$

$Y \xleftarrow{\$} \mathrm{coin}()\,;$

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

while $Y = 1$ do

$X \leftarrow X + 1\,;$

$Y \xleftarrow{\$} \mathrm{coin}()$

$\{\,(\,(\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n})$

$\vee\ \forall n \geq 1,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\,)$

$\wedge\,[Y \neq 1]\,\}$

$\{\forall n \geq 1,\ \Pr[X = n] = 2^{-n}\}$

Φ in purple Ψ in red

More proof rules

$$\frac{}{\{\Psi[E/X]\}\, X \leftarrow E\, \{\Psi\}}\ \Psi[E/X] \Rightarrow \mathrm{FV}(E)\!\downarrow$$

$$\frac{}{Z\triangleright \vdash\ \{\,[Z = E]\,\}\, X \xleftarrow{\$} d(E)\, \{X \sim d(Z)\}}$$

$$\frac{\{\,\Phi\,\}\ C\ \{\,\Psi\,\}}{\{\,\Phi \wedge \Theta\,\}\ C\ \{\,\Psi \wedge \Theta\,\}}\ \mathrm{FV}(\Theta) \cap \mathrm{MV}(C) = \emptyset$$

Example verification (continued)

$\{\}$

$X \leftarrow 1\,;$

$\{\,[X = 1]\,\}$

$Y \xleftarrow{\$} \mathrm{coin}()\,;$

$\{\,[X = 1] \wedge Y \sim \mathrm{coin}()\,\}$

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

while $Y = 1$ do

$X \leftarrow X + 1\,;$

$Y \xleftarrow{\$} \mathrm{coin}()$

$\{\,(\,(\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n})$

$\vee\ \forall n \geq 1,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\,)$

$\wedge\,[Y \neq 1]\,\}$

$\{\forall n \geq 1,\ \Pr[X = n] = 2^{-n}\}$

Example verification (continued)

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

if $Y = 1$ do

then

$X \leftarrow X + 1$;

$Y \xleftarrow{\$} \mathsf{coin}()$

else

skip

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

Proof rule for if ... then ... else

$$\frac{Z \triangleright \vdash \{[Z = X] \wedge [B(Z)] \wedge \Phi\}\ C_1\ \{\Psi\} \qquad Z \triangleright \vdash \{[Z = X] \wedge [\neg B(Z)] \wedge \Phi\}\ C_2\ \{\Psi\}}{Z \triangleright \vdash \{[Z = X] \wedge \Phi\}\ \text{if}\ B(X)\ \text{then}\ C_1\ \text{else}\ C_2\ \{\Psi\}}$$

Proof rule for if ... then ... else

$$\frac{\Xi;\Gamma,Z\triangleright\vdash\{[Z=X]\wedge[B(Z)]\wedge\Phi\}\,C_1\,\{\Psi\}\quad\Xi;\Gamma,Z\triangleright\vdash\{[Z=X]\wedge[\neg B(Z)]\wedge\Phi\}\,C_2\,\{\Psi\}}{\Xi\,;\,\Gamma\,,\,Z\triangleright\vdash\,\{[Z=X]\wedge\Phi\}\,\text{if}\;B(X)\;\text{then}\;C_1\;\text{else}\;C_2\,\{\Psi\}}$$

Proof rule for if ... then ... else

$$\frac{\Xi;\Gamma, Z \triangleright \vdash \{[Z = X] \wedge [B(Z)] \wedge \Phi\}\ C_1\ \{\Psi\} \quad \Xi;\Gamma, Z \triangleright \vdash \{[Z = X] \wedge [\neg B(Z)] \wedge \Phi\}\ C_2\ \{\Psi\}}{\Xi\,;\,\Gamma\,,\,Z \triangleright \vdash\ \{[Z = X] \wedge \Phi\}\,\text{if}\ B(X)\ \text{then}\ C_1\ \text{else}\ C_2\,\{\Psi\}}$$

The general format of specifications

$$\Xi\,;\,\Gamma \vdash\ \{\Phi\}\,C\,\{\Psi\}$$

- Ξ is a finite set of ghost variables (i.e., variables not in C).
- Γ is a finite sequence of $S_1, \ldots, S_n$, where each S_i is either a semantic assertion with $\mathrm{FV}(S_i) \subseteq \Xi$ or a conditioning modality $E \triangleright$ with $\mathsf{Var}(E) \subseteq \Xi$.

Example verification (continued)

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

$m, Z\ ;\ m \geq 1,\ \Pr[Z = 0] = 1 - 2^{-m},\ \Pr[Z = 1] = 2^{-m},\ Z \triangleright \vdash$

$\{\,[Z = Y] \wedge (\,(\,[Z = 1] \wedge [X = m]\,) \vee$

$(\,[Z = 0] \wedge \forall n = 1 \ldots m,\ \Pr[X = n] = 2^{m+1-n}/(2^{m+1} - 1)\,)\,\}$

if $Y = 1$ do

then

$\{\,[Z = 1] \wedge [X = m]\,\}$

$X \leftarrow X + 1\ ;\ Y \xleftarrow{\$} \mathsf{coin}()$

$\{\,[Z = 1] \wedge Y \sim \mathsf{coin}() \wedge [X = m + 1]\,\}$

else skip

$\{\,[Z = 0] \wedge [Y = 0] \wedge \forall n = 1 \ldots m,\ \Pr[X = n] = 2^{m+1-n}/(2^{m+1} - 1)\,\}$

$\{\,(\,[Z = 1] \wedge Y \sim \mathsf{coin}() \wedge [X = m + 1]\,) \vee$

$(\,[Z = 0] \wedge [Y = 0] \wedge \forall n = 1 \ldots m,\ \Pr[X = n] = 2^{m+1-n}/(2^{m+1} - 1)\,)\,\}$

$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$

Context manipulation

$$\frac{\Xi ; \Gamma \vdash \{\Phi'\}\, C\, \{\Psi'\}}{\Xi ; \Gamma \vdash \{\Phi\}\, C\, \{\Psi\}} \quad \begin{array}{l} \Xi; \Gamma \vdash \Phi \Rightarrow \Phi' \\ \Xi; \Gamma \vdash \Psi' \Rightarrow \Psi \end{array}$$

$$\frac{\Xi ; \Gamma, Z \triangleright \vdash \{\Phi\}\, C\, \{\Psi\}}{\Xi ; \Gamma \vdash \{Z \triangleright \Phi\}\, C\, \{Z \triangleright \Psi\}}$$

$$\frac{\Xi ; \Gamma, \Theta \vdash \{\Phi\}\, C\, \{\Psi\}}{\Xi ; \Gamma \vdash \{\Theta \wedge \Phi\}\, C\, \{\Theta \wedge \Psi\}}$$

$$\frac{\Xi, Z ; \Gamma \vdash \{\Phi\}\, C\, \{\Psi\}}{\Xi ; \Gamma \vdash \{\exists Z, \Phi\}\, C\, \{\Psi\}} \quad Z \notin \mathrm{FV}(\Gamma, \Psi)$$

Example verification (continued)

$$m, Z\,;\ m \geq 1,\ \Pr[Z=0] = 1-2^{-m},\ \Pr[Z=1] = 2^{-m},\ Z \triangleright \vdash$$
$$\{\,(\,[Z=1] \wedge Y \sim \mathsf{coin}() \wedge [X = m+1]\,) \vee$$
$$(\,[Z=0] \wedge [Y=0] \wedge \forall n = 1 \ldots m,\ \Pr[X=n] = 2^{m+1-n}/(2^{m+1}-1)\,)\,\}$$

$$\{\,\exists m \geq 1,\ \exists Z,\ \Pr[Z=0] = 1-2^{-m} \wedge \Pr[Z=1] = 2^{-m} \wedge$$
$$Z \triangleright\ (\,[Z=1] \wedge Y \sim \mathsf{coin}() \wedge [X = m+1]\,) \vee$$
$$(\,[Z=0] \wedge [Y=0] \wedge \forall n = 1 \ldots m,\ \Pr[X=n] = 2^{m+1-n}/(2^{m+1}-1)\,)\,\}$$

$$\{\exists m \geq 1,\ \Pr[X = m \wedge Y = 1] = 2^{-m} \wedge \forall n = 1 \ldots m,\ \Pr[X = n \wedge Y = 0] = 2^{-n}\}$$

Independent conjunction

$\Phi * \Psi$:

$$\mathrm{FV}(\Phi * \Psi) \;:=\; \mathrm{FV}(\Phi) \cup \mathrm{FV}(\Psi)$$

$$\begin{aligned}
\Sigma \models \Phi * \Psi \;:\Longleftrightarrow\; & \Sigma \models \Phi \text{ and } \Sigma \models \Psi \text{ and } \Sigma\restriction_{\mathrm{FV}(\Phi)} \perp\!\!\!\perp \Sigma\restriction_{\mathrm{FV}(\Psi)}. \\
\Longleftrightarrow\; & \Sigma\restriction_{\mathrm{FV}(\Phi)} \models \Phi \text{ and } \Sigma\restriction_{\mathrm{FV}(\Psi)} \models \Psi \\
& \quad \text{and } \Sigma\restriction_{\mathrm{FV}(\Phi)} \perp\!\!\!\perp \Sigma\restriction_{\mathrm{FV}(\Psi)} \\
\Longleftrightarrow\; & \exists U, V \subseteq \mathrm{Var} \text{ s.t. } \Sigma\restriction_{U} \models \Phi \text{ and } \Sigma\restriction_{V} \models \Psi \\
& \quad \text{and } \Sigma\restriction_{U} \perp\!\!\!\perp \Sigma\restriction_{V}
\end{aligned}$$

U, V are not required to be disjoint. However, if $\Sigma \models \Phi * \Psi$ holds, then Σ is necessarily deterministic on all variables in $U \cap V$.

The probabilistic frame rule

$$\frac{\Xi ; \Gamma \vdash \{ \Phi \}\ C\ \{ \Psi \}}{\Xi ; \Gamma \vdash \{ \Phi * \Theta \}\ C\ \{ \Psi * \Theta \}}\ \mathrm{FV}(\Theta) \cap \mathrm{MV}(C) = \emptyset$$

Safety is crucial to the proof of the soundness of the frame rule.

IP for graph non-isomorphism

Two graphs G_1, G_2 are encoded as $n \times n$ adjacency matrices A_1, A_2.

An interactive proof for Prover to convince Verifier that $G_1 \not\cong G_2$.

V

Randomly sample $i \xleftarrow{\$} \text{coin}()$ and $\pi \xleftarrow{\$} \text{unif}(\text{Perm}(n))$ (i.e., π is sampled from the uniform distribution on permutations on $[n]$). Compute the adjacency matrix A for $\pi(G_i)$.

P(A_1, A_2, A)

Return the unique j such that A and A_j are adjacency matrices for isomorphic graphs.

V

Accept if $j = i$.
Reject if $j \neq i$.

Completeness and soundness

Completeness If $G_1 \ncong G_2$ then the interaction of V with P on the previous slide leads to V accepting with probability 1.

Soundness If $G_1 \cong G_2$ then the interaction of V with any putative prover P^* leads to V rejecting with probability $\geq \frac{1}{2}$.

(In this case V, in fact, always rejects with probability $= \frac{1}{2}$.)

Verification of soundness

We require P^* to satisfy

$$\{A_1, A_2, A \text{ are } n \times n \text{ arrays}\}\, \mathsf{P}^*\, \{[j = 0] \vee [j = 1]\}\,.$$
$$i \notin \mathrm{MV}(\mathsf{P}^*)$$

Verification:

$\{A_1 \cong A_2\}$

$i \xleftarrow{\$} \mathsf{coin}()$

$\pi \xleftarrow{\$} \mathsf{unif}(\mathsf{Perm}(n))$

$A \leftarrow \pi(A_i)$

$\{A_1 \cong A_2 \wedge i \sim \mathsf{coin}() \wedge \pi \sim \mathsf{unif}(\mathsf{Perm}(n)) \wedge [A = \pi(A_i)]\}$

$\{i \sim \mathsf{coin}() * (A_1 \cong A_2 \wedge A \sim \mathsf{unif}(\mathsf{Perm}(A_1)))\}$

P^*

$\{i \sim \mathsf{coin}() * [j = 0 \vee j = 1]\}$

$\{i \sim \mathsf{coin}() \wedge [j = 0 \vee j = 1] \wedge i \perp\!\!\!\perp j\}$

$\{\Pr[i = j] = 1/2\}$

if $i = j$ then Accept else Reject

$\{\Pr[\mathsf{Reject}] = 1/2\}$

Thank you!