Probabilistic Lambda Calculi
Research Project

Pedro Amorim and Eric Jackson

1 Abstract

In section 2, we introduce a probabilistic version of Call-By-Push Value. In section 3, we introduce two probabilistic lambda-calculi, λ_{IID} and λ_{PC}, which correspond to independent and identically distributed sampling and perfectly correlated sampling, respectively.

2 Probabilistic Call-By-Push-Value

2.1 Syntax

Types

CBPV types are given by $\tau = A \,|\, B$ where A and B are defined inductively according to the following rules:

$$A ::= U\underline{B} \,|\, A + A \,|\, A \times A \,|\, 1 \,|\, \mathbb{R}$$
$$\underline{B} ::= FA \,|\, \underline{B} \times \underline{B} \,|\, A \to \underline{B}$$

As discussed in Levy's thesis, A can be thought of as defining values and B computations.

Expressions

$$\begin{aligned}
V, M ::= {} & \mathsf{x} \\
& |() \\
& |\lambda \mathsf{x} \,.\, M \\
& |\mathsf{let}\ \mathsf{x}\ \mathsf{be}\, V.\, M \\
& |V`M \\
& |\mathsf{produce}\, V \\
& |M\ \mathsf{to}\ \mathsf{x} \,.\, N \\
& |\mathsf{thunk}\, M \\
& |\mathsf{force}\, V \\
& |(M, M) \\
& |\ \#1\, M \\
& |\ \#2\, M \\
& |\ \mathsf{pm}\, V\ \mathsf{as}\, (\mathsf{x},\ \mathsf{y}).\, M \\
& |\mathsf{inl}_{\,A+A} V \\
& |\mathsf{inr}_{\,A+A} V \\
& |\ \mathsf{pm}\, V\ \mathsf{as}\, \{\mathsf{x}.M,\ \mathsf{y}.M\} \\
& |\mathsf{coin} \\
& |\mathsf{rand}
\end{aligned}$$

2.2 Static Semantics

Unit

$$\frac{}{\Gamma \vdash^v () : 1}$$

Functions and Application

$$\frac{\Gamma_{\mathsf{x}:A} \vdash^v M : \underline{B}}{\Gamma \vdash^c \lambda \mathsf{x}.\, M : A \to \underline{B}}$$

$$\frac{\Gamma \vdash^v V : A \qquad \Gamma_{V:A} \vdash^c M : A \to \underline{B}}{\Gamma \vdash^c V`M : \underline{B}}$$

$$\frac{\Gamma \vdash^v V : A \qquad \Gamma_{V:A} \vdash^c M : A \to \underline{B}}{\Gamma \vdash^c \mathsf{let}\ \mathsf{x}\ \mathsf{be}\, V.\, M : \underline{B}}$$

Produce and To

$$\frac{\Gamma \vdash^v V : A}{\Gamma \vdash^c \mathsf{produce}\, V : FA}$$

$$\frac{\Gamma \vdash^c M : FA \qquad \Gamma_{\mathsf{x}:A} \vdash^c N : \underline{B}}{\Gamma \vdash^c M\, \mathsf{to}\ \mathsf{x}.\, N : \underline{B}}$$

Thunk and Force

$$\frac{\Gamma \vdash^c M : \underline{B}}{\Gamma \vdash^v \mathsf{thunk}\, M : U\underline{B}}$$

$$\frac{\Gamma \vdash^v V : U\underline{B}}{\Gamma \vdash^c \mathsf{force}\, V : \underline{B}}$$

Products

$$\frac{\Gamma \vdash^c M : \underline{B} \qquad \Gamma \vdash^c M' : \underline{B}'}{\Gamma \vdash^c (M, M') : \underline{B} \times \underline{B}'}$$

$$\frac{\Gamma \vdash^c M : \underline{B} \times \underline{B}'}{\Gamma \vdash^c \ \#1\, M : \underline{B}}$$

$$\frac{\Gamma \vdash^c M : \underline{B} \times \underline{B}'}{\Gamma \vdash^c \ \#1\, M : \underline{B}'}$$

$$\frac{\Gamma \vdash^c (M, M') : \underline{B} \times \underline{B}' \qquad \Gamma_{\mathsf{x}:\underline{B},\, \mathsf{y}:\underline{B}'} \vdash^c M : \underline{B}}{\Gamma \vdash^c \ \mathsf{pm}\, V\, \mathsf{as}\, (\mathsf{x},\ \mathsf{y}).\, M : \underline{B}}$$

Sums

$$\frac{\Gamma \vdash^v V : A}{\Gamma \vdash^v \mathsf{inl}_{\,A+A'} V : \tau_1 + \tau_2}$$

$$\frac{\Gamma \vdash^v V : A}{\Gamma \vdash^v \mathsf{inr}_{\,A+A'} V : \tau_1 + \tau_2}$$

$$\frac{\Gamma \vdash^v V : A + A' \qquad \Gamma_{\mathsf{x}:A,\, \mathsf{y}:A'} \vdash^c M : \underline{B}}{\Gamma \vdash^c \ \mathsf{pm}\, V\, \mathsf{as}\, \{\mathsf{x}.M,\ \mathsf{y}.M\} : \underline{B}}$$

Random Variables

$$\frac{}{\Gamma \vdash^c \mathsf{coin}\ : F\,\mathbb{R}}$$

$$\frac{}{\Gamma \vdash^c \mathsf{rand}\ : F\,\mathbb{R}}$$

2.3 Denotational Semantics

3 λ_{IID} and λ_{PC}

3.1 Syntax

Types

The types of λ_{IID} and λ_{PC} are defined according to the following rules

$$\tau ::= \mathsf{unit} \mid \mathbb{R} \mid \tau \to \tau \mid \tau + \tau \mid \tau \times \tau$$

Expressions

The expressions of λ_{IID} and λ_{PC} of the following form

$$\begin{aligned}
e ::= {} & x \\
& \mid () \\
& \mid \lambda \mathsf{x} : \tau.\, e \\
& \mid \mathsf{let}\ \mathsf{x}\ = e\ \mathsf{in}\ e \\
& \mid e\, e \\
& \mid \mathsf{coin} \\
& \mid \mathsf{rand} \\
& \mid \mathsf{inl}_{\,\tau_1+\tau_2} e \\
& \mid \mathsf{inr}_{\,\tau_1+\tau_2} e \\
& \mid \mathsf{case}\ e\ \mathsf{of}\ e \mid e \\
& \mid (e,\, e) \\
& \mid \#\mathsf{1}\, e \\
& \mid \#\mathsf{2}\, e \\
& \mid e\ \mathsf{to}\ \mathsf{x}\ \mathsf{in}\ e
\end{aligned}$$

3.2 Static Semantics

4 Translating λ_{IID} and λ_{PC} to CBPV

Rather than defining denotational semantics for λ_{IID} and λ_{PC}, we will define a translation from each of these languages into CBPV. Then, we can use the CBPV semantics to generate denotational semantics.

4.1 Types

We begin with defining type translations from λ_{IID} and λ_{PC} to CBVP. These translations are essentially identical to the translations of CBN and CBV to CBPV presented in Levy's thesis.

λ_{IID}

$$
\begin{aligned}
[\![\mathsf{unit}]\!]_{\mathsf{IID}} &\triangleq F1 \\
[\![\mathbb{R}]\!]_{\mathsf{IID}} &\triangleq F\,\mathbb{R} \\
[\![\tau_1 \to \tau_2]\!]_{\mathsf{IID}} &\triangleq (U[\![\tau_1]\!]_{\mathsf{IID}}) \to [\![\tau_2]\!]_{\mathsf{IID}} \\
[\![\tau_1 + \tau_2]\!]_{\mathsf{IID}} &\triangleq F(U[\![\tau_1]\!]_{\mathsf{IID}} + U[\![\tau_2]\!]_{\mathsf{IID}}) \\
[\![\tau_1 \times \tau_2]\!]_{\mathsf{IID}} &\triangleq [\![\tau_1]\!]_{\mathsf{IID}} \times [\![\tau_2]\!]_{\mathsf{IID}}
\end{aligned}
$$

λ_{PC}

$$
\begin{aligned}
[\![\mathsf{unit}]\!]_{\mathsf{PC}} &\triangleq 1 \\
[\![\mathbb{R}]\!]_{\mathsf{PC}} &\triangleq \mathbb{R} \\
[\![\tau_1 \to \tau_2]\!]_{\mathsf{PC}} &\triangleq U([\![\tau_1]\!]_{\mathsf{PC}} \to F[\![\tau_2]\!]_{\mathsf{PC}}) \\
[\![\tau_1 + \tau_2]\!]_{\mathsf{PC}} &\triangleq U[\![\tau_1]\!]_{\mathsf{PC}} + U[\![\tau_2]\!]_{\mathsf{PC}} \\
[\![\tau_1 \times \tau_2]\!]_{\mathsf{PC}} &\triangleq U(F[\![\tau_1]\!]_{\mathsf{PC}} \times F[\![\tau_2]\!]_{\mathsf{PC}})
\end{aligned}
$$

4.2 Expressions

Now, we define translations from expressions in IID and PC to CBPV.

IID

$$
\begin{aligned}
[\![x]\!]_{\mathsf{IID}} &\triangleq \mathsf{force}\, x \\
[\![\lambda x.\, e]\!]_{\mathsf{IID}} &\triangleq \lambda x.\, [\![e]\!]_{\mathsf{IID}} \\
[\![\mathsf{let}\, x = e_1 \,\mathsf{in}\, e_2]\!]_{\mathsf{IID}} &\triangleq \mathsf{let}\, x \,\mathsf{be\,thunk}\, [\![e_1]\!]_{\mathsf{IID}}.\, [\![e_2]\!]_{\mathsf{IID}} \\
[\![e_1\, e_2]\!]_{\mathsf{IID}} &\triangleq (\mathsf{thunk}\, [\![e_2]\!]_{\mathsf{IID}})`\, [\![e_1]\!]_{\mathsf{IID}} \\
[\![\mathsf{coin}]\!]_{\mathsf{IID}} &\triangleq \mathsf{coin} \\
[\![\mathsf{rand}]\!]_{\mathsf{IID}} &\triangleq \mathsf{rand} \\
[\![\mathsf{inl}_{\,\tau_1+\tau_2} e]\!]_{\mathsf{IID}} &\triangleq \mathsf{produce\,inl\,thunk}\, [\![e]\!]_{\mathsf{IID}} \\
[\![\mathsf{inr}_{\,\tau_1+\tau_2} e]\!]_{\mathsf{IID}} &\triangleq \mathsf{produce\,inr\,thunk}\, [\![e]\!]_{\mathsf{IID}} \\
[\![\mathsf{case}\, e_1 \,\mathsf{of}\, e_2 \mid e_3]\!]_{\mathsf{IID}} &\triangleq [\![e_1]\!]_{\mathsf{IID}} \,\mathsf{to}\, z.\ \mathsf{pm}\, z \,\mathsf{as}\, \{\mathsf{inl}\, x.\, [\![e_2]\!]_{\mathsf{IID}}, \mathsf{inr}\, x.\, [\![e_3]\!]_{\mathsf{IID}}\} \\
[\![(e_1, e_2)]\!]_{\mathsf{IID}} &\triangleq \\
[\![\#1\, e]\!]_{\mathsf{IID}} &\triangleq \\
[\![\#2\, e]\!]_{\mathsf{IID}} &\triangleq \\
[\![e_1 \,\mathsf{to}\, x \,\mathsf{in}\, e2]\!]_{\mathsf{IID}} &\triangleq \mathsf{let}\, x = [\![e_1]\!]_{\mathsf{PC}} \,\mathsf{in}\, [\![e_2]\!]_{\mathsf{IID}}
\end{aligned}
$$

PC

$$
\begin{aligned}
[\![()]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,()\\
[\![x]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,x\\
[\![\lambda x.\,e]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,\mathsf{thunk}\,\lambda x.\,[\![e]\!]_{\mathsf{PC}}\\
[\![\mathsf{let}\,x = e_1\,\mathsf{in}\,e_2]\!]_{\mathsf{PC}} &\triangleq [\![e_1]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\,[\![e_2]\!]_{\mathsf{PC}}\\
[\![e_1\,e_2]\!]_{\mathsf{PC}} &\triangleq [\![e_2]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\,[\![e_1]\!]_{\mathsf{PC}}\,\mathsf{to}\,f.\,x`(\mathsf{force}\,f)\\
[\![\mathsf{coin}\,]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,\mathsf{coin}\\
[\![\mathsf{rand}\,]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,\mathsf{rand}\\
[\![\mathsf{inl}\,_{\tau_1+\tau_2}e]\!]_{\mathsf{PC}} &\triangleq [\![e]\!]_{\mathsf{PC}}\,\mathsf{to}\,z.\,\mathsf{produce}\,\mathsf{inl}\,z\\
[\![\mathsf{inr}\,_{\tau_1+\tau_2}e]\!]_{\mathsf{PC}} &\triangleq [\![e]\!]_{\mathsf{PC}}\,\mathsf{to}\,z.\,\mathsf{produce}\,\mathsf{inr}\,z\\
[\![\mathsf{case}\,e_1\,\mathsf{of}\,e_2\mid e_3\,]\!]_{\mathsf{PC}} &\triangleq [\![e_1]\!]_{\mathsf{PC}}\,\mathsf{to}\,z.\;\mathsf{pm}\,z\,\mathsf{as}\,\{\mathsf{inl}\,x.\,[\![e_2]\!]_{\mathsf{PC}},\ \mathsf{inl}\,y,\ [\![e_3]\!]_{\mathsf{PC}}\}\\
[\![(e_1,e_2)]\!]_{\mathsf{PC}} &\triangleq \mathsf{produce}\,\mathsf{thunk}\,([\![e_1]\!]_{\mathsf{PC}},\ [\![e_2]\!]_{\mathsf{PC}})\\
[\![\,\#1\,e]\!]_{\mathsf{PC}} &\triangleq [\![e]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\;\#1\,(\mathsf{force}\,x)\\
[\![\,\#2\,e]\!]_{\mathsf{PC}} &\triangleq [\![e]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\;\#2\,(\mathsf{force}\,x)\\
[\![e_1\,\mathsf{to}\,x\,\mathsf{in}\,e_2]\!]_{\mathsf{PC}} &\triangleq
\end{aligned}
$$

4.3 Contexts

IID

PC

Theorem.

- *If* $\Gamma \vdash_{\mathsf{IID}} e : \tau$ *then* $[\![\Gamma]\!]_{\mathsf{IID}} \vdash_c [\![e]\!]_{\mathsf{IID}} : [\![\tau]\!]_{\mathsf{IID}}$.
- *If* $\Gamma \vdash_{\mathsf{PC}} e : \tau$ *then* $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}}$.

Proof.

We proceed by mutual induction on $\Gamma \vdash_{\mathsf{IID}} e : \tau$ and $\Gamma \vdash_{\mathsf{PC}} e : \tau$.

- $\Gamma \vdash_{\mathsf{PC}} () : \mathsf{unit}$. We would like to show $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![()]\!]_{\mathsf{PC}} : F[\![\mathsf{unit}\,]\!]_{\mathsf{PC}}$. By the expression and type translation rules, this is equal to $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce}\,() : F1$ which holds by the CBPV produce and unit type rules.
- $\Gamma \vdash_{\mathsf{PC}} x : \tau$. We would like to show $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![x]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}}$. By the expression and type translation rules, this is equal to $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce}\,x : F$. By inspection $\Gamma(x) = \tau$, so by the context rule $[\![\Gamma]\!]_{\mathsf{PC}}(x) = [\![\tau]\!]_{\mathsf{PC}}$. Thus, this typing holds.
- $\Gamma \vdash_{\mathsf{PC}} \lambda x : \tau.\, e : \tau \to \tau'$. We have

  $$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![\lambda x : \tau.\, e]\!]_{\mathsf{PC}} : F[\![\tau \to \tau']\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce}\,\mathsf{thunk}\,\lambda x : [\![\tau]\!]_{\mathsf{PC}}.\, [\![e]\!]_{\mathsf{PC}} : FU([\![\tau]\!]_{\mathsf{PC}} \to F[\![\tau']\!]_{\mathsf{PC}})$$

  By the inductive hypothesis, $[\![\Gamma_{x:\tau}]\!]_{\mathsf{PC}} \vdash_c [\![e]\!]_{\mathsf{PC}} : [\![\tau']\!]_{\mathsf{PC}}$, thus this typing is valid.
- $\Gamma \vdash_{\mathsf{PC}} \mathsf{let}\,x = e_1\,\mathsf{in}\,e_2 : \tau$. We have

  $$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![\mathsf{let}\,x = e_1\,\mathsf{in}\,e_2]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e_1]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\,[\![e_2]\!]_{\mathsf{PC}} : F[\![\tau']\!]_{\mathsf{PC}}$$

  By inspection, $\Gamma \vdash_{\mathsf{PC}} e_1 : \tau'$ and $\Gamma_{x:\tau'} \vdash_{\mathsf{PC}} e_2 : \tau$. Thus by the inductive hypothesis $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_{\mathsf{PC}} [\![e_1]\!]_{\mathsf{PC}} : F[\![\tau']\!]_{\mathsf{PC}}$ and $[\![\Gamma_{x:\tau'}]\!]_{\mathsf{PC}} \vdash_{\mathsf{PC}} [\![e_2]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}}$. Thus, by the CVPB to rule, this typing holds.
- $\Gamma \vdash_{\mathsf{PC}} e_1\,e_2 : \tau$. We have

  $$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e_1\,e_2]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e_2]\!]_{\mathsf{PC}}\,\mathsf{to}\,x.\,[\![e_1]\!]_{\mathsf{PC}}\,\mathsf{to}\,f.\,x'(\mathsf{force}\,f) : F[\![\tau']\!]_{\mathsf{PC}}$$

  By inspection, $\Gamma \vdash_{\mathsf{PC}} e_1 : \tau \to \tau'$ and $\Gamma \vdash_{\mathsf{PC}} e_2 : \tau$. By the inductive hypothesis, $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e_1]\!]_{\mathsf{PC}} : F[\![\tau \to \tau']\!]_{\mathsf{PC}}$ and $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![e_2]\!]_{\mathsf{PC}} : F[\![\tau]\!]_{\mathsf{PC}}$. Checking the to and force type rules allows us to verify that this typing is valid.
- $\Gamma \vdash_{\mathsf{PC}} \mathsf{coin}\; : \mathbb{R}$.

  $$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![\mathsf{coin}\,]\!]_{\mathsf{PC}} : F[\![\mathbb{R}]\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce}\,\mathsf{coin}\; : F\,\mathbb{R}$$

  which clearly holds by the CBPV typing rules for coin and produce.

- $\Gamma \vdash_{\mathsf{PC}} \mathsf{rand} : \mathbb{R}$.

$$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![\mathsf{rand}]\!]_{\mathsf{PC}} : F[\![\mathbb{R}]\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce\,rand} : F\,\mathbb{R}$$

  which clearly holds by the CBPV typing rules for coin and produce.

- $\Gamma \vdash_{\mathsf{PC}} (e_1, e_2) : \tau_1 \times \tau_2$.

$$[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c [\![(e_1,\, e_2)]\!]_{\mathsf{PC}} : F[\![\tau_1 \times \tau_2]\!]_{\mathsf{PC}} = [\![\Gamma]\!]_{\mathsf{PC}} \vdash_c \mathsf{produce\,thunk}\,([\![e_1]\!]_{\mathsf{PC}},\, [\![e_2]\!]_{\mathsf{PC}}) : FU(F[\![\tau_1]\!]_{\mathsf{PC}},\, F[\![\tau_2]\!]_{\mathsf{PC}})$$

  By the inductive hypothesis, $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c e_1 : F[\![\tau_1]\!]_{\mathsf{PC}}$ and $[\![\Gamma]\!]_{\mathsf{PC}} \vdash_c e_2 : F[\![\tau_2]\!]_{\mathsf{PC}}$. Thus, by the CBPV typing rules, this typing holds.

QED

Theorem. *If* $\Gamma \vdash_{\mathsf{IID}} e : \tau_1 \times \tau_2$ *then* $[\![\, e \,]\!] = \mu_1 \times \mu_2$.

Proof. TODO! **QED**

5 Potential Applications

5.1 System Security

5.2 Key Reuse

5.3 Psuodo-Number Generators

5.4 Random Variables