Chapter 1

Parametric Monads and Full Abstraction

Let a monoidal category $\mathcal{X}$ act on a category $\mathcal{G}$, where $\mathcal{G}$ is a suitable model of some programming language. In this chapter we will investigate the adequacy and full abstraction properties of the resulting category $\mathcal{G}/\mathcal{X}$, as we did with Kleisli categories in Chapter **??**. Once again, we will pass to a special case of the general theory. As in Chapter **??**, we will require $\mathcal{G}$ to be a Cartesian closed category that admits a computationally adequate denotational semantics of Idealized Algol, and we shall require that $\mathcal{G}$ may be regarded as being enriched in algebraic directed-complete partial orders in such a way that every compact morphism between the denotations of types is the denotation of some term. As hinted at in Chapter **??**, we shall require the action of $\mathcal{X}$ on $\mathcal{G}$ to be a reader action corresponding to an oplax symmetric monoidal functor that satisfies the condition in Theorem **??**, so that the category $\mathcal{G}/\mathcal{X}$ is Cartesian closed.

We fix a symmetric monoidal category $\mathcal{X}$ and an oplax monoidal functor $j\colon \mathcal{X} \to \mathbf{Set}$ such that for any object p of $\mathcal{X}$ there are morphisms $h\colon p \to p \otimes p$ and $h_0\colon p \to I$ such that the composite

$$j(p) \xrightarrow{jh} j(p \otimes p) \xrightarrow{m^j_{p,p}} j(p) \times j(p)$$

is equal to the diagonal on $j(p)$.

We fix a model $\mathcal{G}$ of Idealized Algol as above, and suppose that the datatypes in $\mathcal{G}$ are interpreted via an oplax monoidal functor $\mathbf{Set} \to \mathcal{G}$. Then we get an oplax monoidal functor $\mathcal{X} \to \mathcal{G}$, inducing a reader action of $\mathcal{X}^{\mathrm{op}}$ on $\mathcal{G}$ such that the category $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$ is Cartesian closed. We will define a language and an interpretation of this language in the category $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$.

1.1 The language $\mathrm{IA}_{\mathcal{X}}$

Definition 1.1.1 (The language $\mathrm{IA}_{\mathcal{X}}$)**.** The language $\mathrm{IA}_{\mathcal{X}}$ is formed by taking Idealized Algol, and adding to it new constants

$$\mathsf{choose}_p$$

for each object p of $\mathcal{X}$ such that $j(p) \in \{\mathbb{C}, \mathbb{B}, \mathbb{N}\}$, with typing rule

$$\frac{}{\Gamma \vdash \mathsf{choose}_p \colon j(p)}\,.$$

The interpretation of choose_p is that it requests an element a of the set $j(p)$.

Let $\mathcal{G}$ be a model of Idealized Algol as described above, and suppose that there is an oplax monoidal functor $\mathbf{Set} \to \mathcal{G}$ that is used to interpret datatypes. We will use an underline to indicate thies functor; so, for example, the object of $\mathcal{G}$ that is used to denote the natural number type is written $\underline{\mathbb{N}}$.

By our description of $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$ as a lax colimit in **Cat** (i.e., Corollary **??**), we have a natual functor $J \colon \mathcal{G} \to \mathcal{G}/\mathcal{X}^{\mathrm{op}}$ and a natural transformation $\phi_{p,a} \colon J(jp \to a) \to Ja$. Our denotational semantics of $\mathrm{IA}_{\mathcal{X}}$ is then given in the category $\mathcal{G}/X^{\mathrm{op}}$ as follows. The denotation of any type T of Idealized Algol is given by $J(\llbracket T \rrbracket_{\mathcal{G}})$, where $\llbracket T \rrbracket_{\mathcal{G}}$ is the original denotation in $\mathcal{G}$. The denotation of any sequent $\Gamma \vdash M$ is given by $\llbracket \Gamma \vdash M \rrbracket = J(\llbracket \Gamma \vdash M \rrbracket_{\mathcal{G}})$, where $\llbracket - \rrbracket_{\mathcal{G}}$ is the original denotation in $\mathcal{G}$. The denotation of choose_p is given by the morphism $\omega_p \colon 1 \to j(p)$ given by the composite

$$I \xrightarrow{\Lambda(\mathrm{id}_{Jjp})} (Jjp \to Jjp) \to J(jp \to jp) \xrightarrow{\phi_{p,jp}} Jjp\,.$$

This denotation may alternatively be defined in a non-compositional way: given a term $\Gamma \vdash M \colon T$ in context of $\mathrm{IA}_{\mathcal{X}}$, we can write

$$M = N[\mathsf{choose}_p / x_p]\,,$$

where (x_p) is a finite collection of free variables in M.

Since the categories $\mathcal{G}$ and $\mathcal{G}/\mathcal{X}$ are Cartesian closed, the β-rule is valid in the semantics, and so if N is a term of $\mathrm{IA}_{\mathcal{X}}$ that refers to $(\mathsf{choose}_p)_{p \in \mathcal{P}}$ for some finite collection $\mathcal{P}$ of objects of $\mathcal{X}$, then we may write the denotation of $\Gamma \vdash N$ as the composite

$$\llbracket \Gamma \rrbracket \xrightarrow{\langle \mathrm{id}, (\omega_p) \rangle} \llbracket \Gamma, (x_p) \rrbracket \xrightarrow{\llbracket \Gamma, (x_p) \vdash N[x_p / \mathsf{choose}_p \rrbracket} \llbracket T \rrbracket\ ,$$

where the denotation at the right is that of ordinary Idealized Algol.

This is a morphism in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$. If we consider it as a morphism in $\mathcal{G}$, we see that it is given by the curried form of the composite

$$\llbracket \Gamma \rrbracket \times j\left(\bigotimes_p p\right) \xrightarrow{\llbracket \Gamma \rrbracket \times m^j} \llbracket \Gamma \rrbracket \times \prod_p j(p) \xrightarrow{\llbracket \Gamma, (x_p) \vdash N[x_p / \mathsf{choose}_p] \rrbracket} \llbracket T \rrbracket\ .$$

The example to have in mind is that of probability; here, the objects of our category $\mathcal{X}$ are discrete random variables, with $j(p)$ giving the codomain of the random variable, and the term $\mathsf{choose}_p \colon j(p)$ can be thought of as choosing an element of that set.

1.2 Operational Semantics

We inductively define a relation

$$\Gamma, s \vdash M \Downarrow_U c, s' ,$$

where Γ is a $\mathtt{Var}$-context, s, s' are Γ-stores, $\Gamma \vdash M, \Gamma \vdash c$ are $\mathrm{IA}_{\mathcal{X}}$ terms-in-context such that c is an IA canonical form, and U is a sequence of pairs of the form $(p : a)$, where p is an object of $\mathcal{X}$ and $a \in j(p)$. The definition of this rule is shown in Figure 1.1.

We notice immediately that all but one of these rules are exactly the same as the corresponding rules from IA_X, the only difference being the form the form that the associated sequence takes. The one difference is the rule for choose_p.

1.3 Translation into $\mathbf{IA}_X$

We make the connection between the languages IA_X and $\mathrm{IA}_{\mathcal{X}}$ more explicit in the following series of lemmas. In this section, we will make use of an encoding between an object of the form jp and an Idealized Algol datatype N. The case we have in mind is when jp is some finite set and N is the natural number object, so that we can choose some way of representing elements of jp as elements of N.

Definition 1.3.1. Let $p_1, \cdots, p_n$ be a sequence of objects of $\mathcal{X}$ and let N be an object of $\mathcal{X}$ such that $j(N)$ is a datatype of Idealized Algol (i.e., $j(N) \in \{\mathbb{C}, \mathbb{B}, \mathbb{N}\}$). Suppose we have a morphism

$$f \colon N \to p_1 \otimes \cdots \otimes p_n$$

in $\mathcal{X}$ such that jf is a surjection. Define functions $\pi_i \colon j(N) \to j(p_i)$ to be given by the composites

$$j(N) \xrightarrow{jf} j(p_1 \otimes \cdots \otimes p_n) \xrightarrow{m^j} j(p_1) \times \cdots \times j(p_n) \xrightarrow{\mathrm{pr}_i} j(p_i) .$$

Let $u \in j(N)^*$ be a sequence of elements of $j(N)$, and let U be a sequence of pairs $(p : a)$, where each p is one of the p_i. We say that u *covers* U *with respect to* f if U and u have the same length and if whenever $U^{(k)} = (p_i : a)$, we have $a = \pi_i(u^{(k)})$.

$$\frac{}{\Gamma, s \vdash c \Downarrow_{\epsilon} c, s} \qquad \frac{\Gamma, s \vdash M \Downarrow_U \lambda x.M', s' \qquad \Gamma, s' \vdash M'[N/x] \Downarrow_V c, s''}{\Gamma, s \vdash MN \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash M(\mathbf{Y}M) \Downarrow_U c, s'}{\Gamma, s \vdash \mathbf{Y}M \Downarrow_U c, s'} \qquad \frac{\Gamma, s \vdash M \Downarrow_U n, s'}{\Gamma, s \vdash \mathsf{succ}\, M \Downarrow_U n+1, s'}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U n+1, s'}{\Gamma, s \vdash \mathsf{pred}\, M \Downarrow_U n, s'} \qquad \frac{\Gamma, s \vdash M \Downarrow_U 0, s'}{\Gamma, s \vdash \mathsf{pred}\, M \Downarrow_U 0, s'}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U \mathsf{skip}, s' \qquad \Gamma, s' \vdash N \Downarrow_V c, s''}{\Gamma, s \vdash M; N \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U \mathbb{tt}, s' \qquad \Gamma, s' \vdash N \Downarrow_V c, s''}{\Gamma, s \vdash \mathsf{If}\, M \,\mathsf{then}\, N \,\mathsf{else}\, P \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U \mathbb{ff}, s' \qquad \Gamma, s' \vdash P \Downarrow_V c, s''}{\Gamma, s \vdash \mathsf{If}\, M \,\mathsf{then}\, N \,\mathsf{else}\, P \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U 0, s' \qquad \Gamma, s' \vdash N \Downarrow_V c, s''}{\Gamma, s \vdash \mathsf{If0}\, M \,\mathsf{then}\, N \,\mathsf{else}\, P \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_U n+1, s' \qquad \Gamma, s' \vdash P \Downarrow_V c, s''}{\Gamma, s \vdash \mathsf{If0}\, M \,\mathsf{then}\, N \,\mathsf{else}\, P \Downarrow_{U+\!\!+V} c, s''}$$

$$\frac{\Gamma, s \vdash E \Downarrow_U n, s' \qquad \Gamma, s' \vdash V \Downarrow_V x, s''}{\Gamma, s \vdash V \leftarrow E \Downarrow_{U+\!\!+V} \mathsf{skip}, (s''|x \mapsto n)}\ x \in \Gamma \qquad \frac{\Gamma, s \vdash V \Downarrow_U x, s'}{\Gamma, s \vdash !V \Downarrow_U n, s'}\ s'(x) = n$$

$$\frac{\Gamma, x\colon \mathtt{Var}, (s|x \mapsto 0) \vdash M \Downarrow_U c, (s'|x \mapsto n)}{\Gamma, s \vdash \mathsf{new}\, \lambda x.M \Downarrow_U c, s'}$$

$$\frac{\Gamma, s \vdash E \Downarrow_U n, s' \qquad \Gamma, s' \vdash V \Downarrow_V \mathsf{mkvar}\, WR, s'' \qquad \Gamma, s'' \vdash Wn \Downarrow_W \mathsf{skip}, s'''}{\Gamma, s \vdash V \leftarrow E \Downarrow_{U+\!\!+V+\!\!+W} \mathsf{skip}, s'''}$$

$$\frac{\Gamma, s \vdash V \Downarrow_U \mathsf{mkvar}\, WR, s' \qquad \Gamma, s' \vdash R \Downarrow_V n, s''}{\Gamma, s \vdash !V \Downarrow_{U+\!\!+V} n, s''}$$

$$\frac{}{\Gamma, s \vdash \mathsf{choose}_p \Downarrow_{(p:a)} a, s}\ a \in j(p)$$

Figure 1.1: Operational semantics for $\mathrm{IA}_{\mathcal{X}}$.

Recall that, in the definition of the category $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$, the Melliès morphisms are left unchanged by precomposing with a morphism in the image of the functor j; therefore, if $M\colon T$ is a closed term of $\mathrm{IA}_{\mathcal{X}}$ referring to $\mathsf{choose}_{p_1}, \cdots, \mathsf{choose}_{p_n}$, then we may write the denotation of M as the composite

$$j(N) \xrightarrow{jf} j(p_1 \otimes \cdots \otimes p_n) \xrightarrow{m^j} j(p_1) \times \cdots \times j(p_n) \xrightarrow{[\![x_1,\cdots,x_n \vdash M[x_i/\,\mathsf{choose}_{p_i}]]\!]_{\mathcal{G}}} [\![T]\!] \;;$$

i.e., as

$$j(N) \xrightarrow{\langle \pi_1,\cdots,\pi_n \rangle} j(p_1) \times \cdots \times j(p_n) \xrightarrow{[\![x_1,\cdots,x_n \vdash M[x_i/\,\mathsf{choose}_{p_i}]]\!]_{\mathcal{G}}} [\![T]\!] \;.$$

Lemma 1.3.2. *Let $\Gamma \vdash M$ be an $IA_{\mathcal{X}}$ term-in-context, where M refers to terms $\mathsf{choose}_{p_1}, \cdots, \mathsf{choose}_{p_n}$, and no other choose terms. Let N be an object of $\mathcal{X}$ such that $j(N)$ is an IA datatype and let $f\colon N \to p_1 \otimes \cdots \otimes p_n$ be a morphism, as in Definition 1.3.1. Suppose that the functions π_i are all definable in Idealized Algol; that is, that there are terms $\Pi_i\colon j(N) \to j(p_i)$ of IA such that the following inference is valid.*

$$\frac{\Gamma, s \vdash M \Downarrow m, s'}{\Gamma, s \vdash \Pi_i M \Downarrow \pi_i(m), s'}$$

Let s, s' be Γ-stores, and let $\Gamma \vdash c$ be a canonical form. Suppose U is a sequence such that we have

$$\Gamma, s \vdash M \Downarrow_U c, s' \,.$$

Then

$$\Gamma, s \vdash M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] \Downarrow_u c, s'$$

in $IA_{j(N)}$ for all sequences $u \in j(N)^*$ that cover U.

Proof. Induction on the derivation of $\Gamma, s \vdash M \Downarrow_U c, s'$. Suppose that the last rule in the derivation takes the following form.

$$\frac{\Gamma_1, s^{(0)} \vdash M_1 \Downarrow_{U_1} c_1, s^{(1)} \qquad \cdots \qquad \Gamma_n, s^{(n-1)} \vdash M \Downarrow_{U_n} c_n, s^{(n)}}{\Gamma, s^{(0)} \vdash M \Downarrow_{U_1 +\!\!+ \cdots +\!\!+ U_n} c, s^{(n)}}$$

Suppose a sequence u covers $U_1 +\!\!+ \cdots +\!\!+ U_n$. Then we may write $u = u_1 +\!\!+ \cdots +\!\!+ u_n$, where u_i covers U_i.

By induction, then, we may derive that

$$\Gamma_k, s^{(k)} \vdash M_k[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] \Downarrow_{u_k} c_k, s^{(k)}$$

for $k = 1, \cdots, n$. Now note that Lemma **??** still holds if we use the terms choose_{p_i} instead of the ask_X; this means that we have a valid $\mathrm{IA}_j(N)$ inference given by

$$\frac{\begin{array}{c}\Gamma_1, s^{(0)} \vdash M_1[\mathtt{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] \Downarrow_{u_1} c_1, s^{(1)} \\ \cdots \qquad \Gamma_n, s^{(n-1)} \vdash M_n[\mathtt{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] \Downarrow_{u_n} c_n, s^{(n)}\end{array}}{\Gamma, s^{(0)} \vdash M[(\lambda z.\Pi_i)\,\mathsf{ask}_{j(N)}\,.\,\mathsf{choose}_{p_i}] \Downarrow_u c, s^{(n)}} \;,$$

from which we can deduce that

$$\Gamma, s^{(0)} \vdash M[\texttt{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] \Downarrow_i c, s^{(n)}\,,$$

as desired.

The other possibility is that the final step in the derivation takes the form

$$\frac{}{\Gamma, s \vdash \mathsf{choose}_{p_j} \Downarrow_{(p_j:a)} a, s}\ .$$

Let U be a (length 1) sequence covering $(p_j : a)$. So $U = t$, where $t \in j(P)$ is such that $\pi_j(t) = a$.

Then

$$\mathsf{choose}_{p_j}[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/\,\mathsf{choose}_{p_i}] = \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v)\,,$$

and we may derive

$$\Gamma, s \vdash \texttt{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v) \Downarrow_t a, s\,. \qquad \square$$

To prove the converse, we prove a lemma about substitution analogous to Lemma **??**.

Lemma 1.3.3. *Let*

$$\frac{\Gamma, s^{(0)} \vdash M_1 \Downarrow_{u_1} c_1, s^{(1)} \qquad \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n \Downarrow_{u_n} c_n, s^{(n)}}{\Gamma, s^{(0)} \vdash M \Downarrow_{u_1 +\!\!+ \cdots +\!\!+ u_n} c, s^{(n)}}$$

be an inference of $IA_{j(N)}$, where every instance of $\mathsf{ask}_{j(N)}$ occurs as part of some term $\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)$, and suppose that $M \neq \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v)$ for any j. Suppose we have sequences $U_1, \cdots, U_n$ such that u_k covers U_k for $k = 1, \cdots, n$. Then

$$\frac{\begin{array}{c}\Gamma, s^{(0)} \vdash M_1[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_{U_1} c_1, s^{(1)} \\ \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_{U_n} c_n, s^{(n)}\end{array}}{\Gamma, s^{(0)} \vdash M[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_{U_1 +\!\!+ \cdots +\!\!+ U_n} c, s^{(n)}}$$

is a valid inference of $IA_{\mathcal{X}}$.

Proof. As in Lemma **??**, we can prove this by looking at cases. For example, consider the sequencing rule

$$\frac{\Gamma, s \vdash M \Downarrow_u \mathsf{skip}, s' \qquad \Gamma, s' \vdash N \Downarrow_v c, s''}{\Gamma, s \vdash M; N \Downarrow c, s''}\ .$$

We have

$$\begin{aligned} &(M;N)[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \\ = {}& M[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)]; \\ & N[\mathsf{choose}_{p_i}\,/\,\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)]\,, \end{aligned}$$

and so we certainly get a rule

$$\frac{\begin{array}{c}\Gamma, s \vdash M[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_U \mathsf{skip}, s' \\ \Gamma, s' \vdash N[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_V c, s''\end{array}}{\Gamma, s \vdash (M; N)[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow c, s''} \quad .$$

The only case where we need to be careful is for the new rule:

$$\frac{\Gamma, x, (s|x \mapsto 0) \vdash M \Downarrow_u c, (s'|x \mapsto n)}{\Gamma, s \vdash \mathsf{new}\, \lambda x.M \Downarrow_u c, s'} \quad .$$

If $\mathsf{new}\, \lambda x.M \neq \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v)$, then we have

$$\begin{aligned} &(\mathsf{new}\, \lambda x.M)[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \\ &= \mathsf{new}\, \lambda x.(M[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)]) \,. \end{aligned}$$

Then we can apply the rule

$$\frac{\Gamma, x, (s|x \mapsto 0) \vdash M[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow_U c, (s'|x \mapsto n)}{\Gamma, s \vdash (\mathsf{new}\, \lambda x.M)[\mathsf{choose}_{p_i} \,/\, \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)] \Downarrow Uc, s'} \quad .$$

□

We now prove the converse to Lemma 1.3.2.

Lemma 1.3.4. *Let $\Gamma, y_1 : j(p_1), \cdots, y_n : j(p_n) \vdash M : T$ be a term-in-context of ordinary Idealized Algol, where Γ is a $\mathtt{Var}$-context. Let U be a sequence and let N, π_i, Π_i be as above. Suppose that there exists some sequence $u \in j(N)^*$ such that u covers U and such that*

$$\Gamma, s \vdash M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/y_i] \Downarrow_u c, s' \,.$$

Then

$$\Gamma, s \vdash M[\mathsf{choose}_{p_i} /y_i] \Downarrow_U c, s' \,.$$

Proof. Induction on the derivation. Suppose that M is not one of the y_i; then $M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)/y_i]$ is not equal to $\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)$. Moreover, every instance of $\mathsf{ask}_{j(N)}$ in M occurs as part of an expression of the form $\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v)$, and so we win by Lemma 1.3.3 and the inductive hypothesis.

Otherwise, $M = \mathtt{new}\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v)$ for some j. Now, if we have

$$\Gamma, s \vdash \mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_j!v) \Downarrow_u c, s' \,,$$

then a simple examination of the reduction tells us that we must have $s' = s$, and that u must have length 1 – say $u = m$ – where the single element n of u satisfies $\pi_j(m) = c$.

But now we certainly have

$$\Gamma, s \vdash \mathsf{choose}_{p_j} \Downarrow_{(p_j:c)} c, s\,,$$

and the sequence m covers the sequence $(p_j : c)$. □

Lemmas 1.3.2 and 1.3.4 together prove the following.

Lemma 1.3.5. *Let $\Gamma, x_1, \cdots, x_n \vdash M$ be a term-in-context of Idealized Algol, where Γ is a* `Var`*-context. Then the following are equivalent.*

i) $\Gamma, s \vdash M[\mathsf{choose}_{p_i/x_i}] \Downarrow_U c, s'$.

ii) $\Gamma, s \vdash M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v/x_i] \Downarrow_u c, s'$ *for all u covering U.*

iii) $\Gamma, s \vdash M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i!v/x_i] \Downarrow_u c, s'$ *for some u covering U.*

Proof. (i) ⇒ (ii): Lemma 1.3.2.

(ii) ⇒ (iii): By assumption, the function $j(f) \colon N \to j(\bigotimes_i p_i)$ is surjective, so for any U there is some $u \in j(N)^*$ covering U.

(iii) ⇒ (i): Lemma 1.3.4. □

1.4 Computational Adequacy

We are now ready to make the definitions we need to state our Computational Adequacy result.

Recall that if σ was a Kleisli morphism $1 \to \mathbb{C}$ (i.e., a morphism $1 \to (X \to \mathbb{C})$ in the original category, where X was an Idealized Algol datatype), then we wrote $\sigma \downarrow_u$ if the composite

$$1 \xrightarrow{\sigma} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathrm{Var} \to \mathbb{N}) \xrightarrow{\mathsf{new}} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

was not equal to $\bot$, where η_u was the denotation of the Idealized Algol term-in-context

$$f \colon X \to \mathtt{com} \vdash \lambda v.v \leftarrow 0; f(v \leftarrow \mathsf{succ}\,!v; \mathrm{tr}_u\,!v); !v \colon \mathtt{Var} \to \mathtt{nat}\,.$$

We want to extend this definition to morphisms in the category $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$. There are a couple of problems here.

Firstly, the morphisms in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$ are equivalence classes of Melliès morphisms, and the equivalence relation does not respect this predicate $\downarrow_u$ – especially since the X in the above formula could change when we choose a different representative of the equivalence class.

Secondly, a morphism $1 \to \mathbb{C}$ in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$ is given by an (equivalence class of) morphisms $1 \to (j(p) \to \mathbb{C})$ in $\mathcal{G}$, and the object $j(p)$ need not be an Idealized Algol datatype.

To solve the second problem, we make an additional small assumption on our category $\mathcal{G}$. We require that there exist morphisms

$$\xi_u \colon (X \to \mathbb{C}) \to \mathbb{C}$$

for any set X and any finite sequence $u \in X^*$ such that for any function $f \colon X \to Y$, we have $(f \to \mathbb{C}); \xi_u = \xi_{f_* u}$, where $f_* u$ is the sequence formed by applying f pointwise to u, and such that if X is an IA datatype, then

$$\xi_u = (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathrm{Var} \to \mathbb{N}) \xrightarrow{\mathsf{new}} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}\,.$$

Example 1.4.1. In the category of games, the morphisms ξ_u are the strategies containing the plays ϵ, qq and plays of the form

$$\begin{array}{ccc} X & \mathbb{C} & \mathbb{C} \\ & & q \\ & q & \\ q & & \\ u^{(0)} & & \\ \vdots & & \\ q & & \\ u^{(k)} & & \end{array} \qquad\qquad \begin{array}{ccc} X & \mathbb{C} & \mathbb{C} \\ & & q \\ & q & \\ q & & \\ u^{(0)} & & \\ \vdots & & \\ q & & \\ u^{(|u|-1)} & & \\ & a & \\ & & a \end{array}$$

(so the strategy has no reply if player O asks the question in X fewer than $|u|$ times, or tries to ask it more than $|u|$ times).

Definition 1.4.2. Given a set X and a Melliès morphism $\sigma \colon 1 \to (X \to \mathbb{C})$, we say that σ *accepts* a sequence $u \in X^*$ if $\sigma; \xi_u \neq \bot$. We write $\mathrm{Acc}(\sigma)$ for the set of all sequences accepted by σ.

Recall that a morphism $1 \to \mathbb{C}$ in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$ is given by an equivalence class of Melliès morphisms $1 \to (j(p) \to \mathbb{C})$ in $\mathcal{G}$, where p ranges over the objects of $\mathcal{X}$, and where the equivalence relation is generated by identifying all pairs of morphisms $\sigma \colon 1 \to (j(p) \to \mathbb{C})$ and $\tau \colon 1 \to (j(q) \to \mathbb{C})$ such that there is a morphism $f \colon p \to q$ such that $\tau; (j(f) \to \mathbb{C}) = \sigma$.

Definition 1.4.3. We define an equivalence relation on pairs $(p,\mathcal{U})$, where p is an object of $\mathcal{X}$ and $\mathcal{U} \subseteq j(p)^*$ is a set of finite sequences drawn from $j(p)$ to be the equivalence relation generated by identifying $(p,\mathcal{U})$ and $(q,\mathcal{V})$ whenever there is a morphism $f \colon p \to q$ in $\mathcal{X}$ such that for all $u \in j(p)^*$, we have $u \in \mathcal{U}$ if and only if $j(f)_* u \in \mathcal{V}$.

It is instructive to consider the equivalence relation on pairs $(p, \mathcal{U})$ in the case that $\mathcal{X} = \mathbf{Rv}_\Omega$ is the category of random variables on some probability space Ω. Given a random variable V on a set X, we get an induced random variable taking values in X^*. If we have a random variable W on a set Y and a function $f \colon X \to Y$ such that $W = f \circ X$, and if $\mathcal{U} \subseteq X^*$ and $\mathcal{V} \subseteq Y^*$ are such that $u \in \mathcal{U}$ if and only if $f_* u \in \mathcal{V}$, then the induced probabilities of the sets $\mathcal{U}$ and $\mathcal{V}$ are the same. So, in this case, the equivalence relation on sets of sequences is subsumed into the very natural equivalence relation of having the same probability.

Proposition 1.4.4. *Let $\sigma \colon 1 \to (j(p) \to A)$, $\tau \colon 1 \to (j(q) \to A)$ be two representatives of the same morphism $1 \to A$ in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$. Then $(p, \mathrm{Acc}(\sigma))$ and $(q, \mathrm{Acc}(\tau)$ are equivalent.*

Proof. Since the relation on pairs $(p, \mathcal{U})$ is an equivalence relation, it suffices to assume that σ and σ' are related by the relation that generates the equivalence relation on Melliès morphisms; i.e., that there is a morphism $f \colon p \to q$ such that $\sigma = \tau; (j(f) \to \mathbb{C})$.

Let $u \in j(p)^*$. Then we have

$$\begin{aligned} u \in \mathrm{Acc}(\sigma) &\Leftrightarrow \sigma; \xi_u \neq \bot \\ &\Leftrightarrow \tau; (j(f) \to A); \xi_u \neq \bot \\ &\Leftrightarrow \tau \xi_{j(f)_* u} \neq \bot \\ &\Leftrightarrow j(f)_* u \in \mathrm{Acc}(\tau)\,. \end{aligned}$$

Therefore, $(p, \mathrm{Acc}(\sigma))$ and $(q, \mathrm{Acc}(\tau))$ are equivalent. □

We can now state and prove our Computational Adequacy result. For this result, given a term $M \colon \mathtt{com}$ mentioning objects $p_1, \cdots, p_n$, we shall assume the existence of some IA datatype N admitting a morphism $f \colon N \to p_1 \otimes \cdots \otimes p_n$ such that the definable projections π_i on to the objects $j(p_i)$ are IA-definable.

Definition 1.4.5. Let M be a closed term of $\mathrm{IA}_{\mathcal{X}}$ of type $\mathtt{com}$ mentioning $p_1, \cdots, p_n$. Let $S(M)$ be the set of all sequences U such that $M \Downarrow_U \mathsf{skip}$.

We define $B(M)$, the *behaviours of* M, to be the equivalence class corresponding to the pair

$$(p_1 \otimes \cdots \otimes p_n, \mathcal{U})\,,$$

where $\mathcal{U}$ is the set of all sequences $u \in j(p_1 \otimes \cdots \otimes p_n)^*$ that cover some sequence $U \in S(M)$, via the projections

$$j(p_1 \otimes \cdots \otimes p_n) \xrightarrow{m^j} j(p_1) \times \cdots \times j(p_n) \xrightarrow{\mathrm{pr}_i} j(p_i)\,.$$

Theorem 1.4.6 (Computational Adequacy for $\mathrm{IA}_{\mathcal{X}}$)**.** *Let $M \colon \mathtt{com}$ be a closed term of $IA_{\mathcal{X}}$ referring to $p_1, \cdots, p_n$. Suppose the denotation of M is given by a morphism $1 \to (j(p) \to \mathbb{C})$ in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$.*

Then $(p, \mathrm{Acc}([\![M]\!]))$ *is equivalent to* $B(M)$.

Proof. By Proposition 1.4.4, we may assume that the denotation of M is in a particular form, namely the (curried form of) the composite

$$j(N) \xrightarrow{\langle \pi_1, \cdots, \pi_n \rangle} j(p_1) \times \cdots \times j(p_n) \xrightarrow{[\![x_1, \cdots, x_n \vdash M[x_i / \,\mathsf{choose}_{p_i}]]\!]_{\mathcal{G}}} \mathbb{C}\,.$$

But if we consider this as a Kleisli morphism in the category $\mathrm{Kl}_{R_{j(N)}}\,\mathcal{G}$, then this is the denotation of the $\mathrm{IA}_{j(N)}$ term

$$M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i !v) / \,\mathsf{choose}_{p_i}]\,.$$

By Lemma 1.3.5, if $u \in j(N)^*$ is a sequence, then

$$M[\mathsf{new}(\lambda v.v \leftarrow \mathsf{ask}_{j(N)}; \Pi_i !v) / \,\mathsf{choose}_{p_i}] \Downarrow_u \mathsf{skip}$$

if and only if u covers a sequence U such that $M \Downarrow_U \mathsf{skip}$. By our Computational Adequacy result for IA_X (Propositions **??** and **??**), this means that for all $u \in j(N)^*$, $u \in \mathrm{Acc}([\![M]\!])$ (for this particular form of $[\![M]\!]$) if and only if $u \in \mathcal{U}$. Therefore, $(N, \mathrm{Acc}([\![M]\!])) = (N, \mathcal{U}')$, where $\mathcal{U}' \subseteq j(N)^*$ is the set of all sequences u that cover some U such that $M \Downarrow_U \mathsf{skip}$ via the projections π_i. Lastly, we note that $(N, \mathcal{U}')$ is equivalent to $B(M)$, through the morphism $f \colon N \to p_1 \otimes \cdots \otimes p_n$. □

1.5 Equational Soundness

We transfer to an Equational Soundness result in our standard way. First, we make a definition of observational equivalence of $\mathrm{IA}_{\mathcal{X}}$ terms.

Definition 1.5.1. Let M be a closed term of $\mathrm{IA}_{\mathcal{X}}$ of type `com` mentioning $p_1, \cdots, p_n$. Let $S(M)$ be the set of all sequences U such that $M \Downarrow_U \mathsf{skip}$.

We define $B(M)$, the *behaviours of* M, to be the equivalence class corresponding to the pair

$$(p_1 \otimes \cdots \otimes p_n, \mathcal{U})\,,$$

where $\mathcal{U}$ is the set of all sequences $u \in j(p_1 \otimes \cdots \otimes p_n)^*$ that cover some sequence $U \in S(M)$, via the projections

$$j(p_1 \otimes \cdots \otimes p_n) \xrightarrow{m^j} j(p_1) \times \cdots \times j(p_n) \xrightarrow{\mathrm{pr}_i} j(p_i)\,.$$

Definition 1.5.2 (Observational Equivalence)**.** Let $M, M' \colon T$ be closed terms of $\mathrm{IA}_{\mathcal{X}}$. We say that M and M' are *observationally equivalent* if $B(C[M])$ and $B(C[M'])$ are equivalent for all contexts $C \colon$ `com` with a hole of type T.

We then make definitions that will mirror this equivalence in the denotational semantics.

Definition 1.5.3 (Equivalence of morphisms $1 \to \mathbb{C}$)**.** Let $\sigma, \tau \colon 1 \to \mathbb{C}$ be morphisms in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$, considered as morphisms $\sigma \colon j(p) \to \mathbb{C}$ and $\tau \colon j(q) \to \mathbb{C}$ in $\mathcal{G}$. We say that $\sigma \approx \tau$ if $(p, \mathrm{Acc}(\sigma))$ is equivalent to $(q, \mathrm{Acc}(\tau))$.

Definition 1.5.4 (Intrinsic Equivalence)**.** Let $\sigma, \tau \colon A \to B$ be morphisms in $\mathcal{G}/\mathcal{X}^{\mathrm{op}}$. Then we say that $\sigma \sim \tau$ if for all $\alpha \colon (A \to B) \to \mathbb{C}$, we have $\Lambda(\sigma); \alpha \approx \Lambda(\tau); \alpha$.

Now we can prove Equational Soundness as we did in Proposition **??**.

Theorem 1.5.5 (Equational Soundness for $\mathrm{IA}_{\mathcal{X}}$)**.** *Let $M, M' : T$ be closed terms of $IA_{\mathcal{X}}$ such that $[\![M]\!] \sim [\![N]\!]$. Then M and M' are observationally equivalent.*

Proof. First suppose that M and M' are not observationally equivalent – so there is some context C such that $B(C[M])$ and $B(C[M'])$ are inequivalent. Now $B(C[M])$ is equivalent to $(N,\mathcal{U})$ and $B(C[M'])$ is equivalent to $(N,\mathcal{U}')$, where $\mathcal{U} \subseteq j(N)^*$ is the set of sequences that cover some $U \in S(C[M])$ and $\mathcal{U}'$ the set of sequences that cover some $U \in S(C[M'])$ via the projections π_i.

Let α be the denotation of the term-in-context $f \colon T \vdash C[f]$. Then $\Lambda([\![M]\!]); \alpha$ is the denotation of $C[M]$ and $\Lambda([\![M']\!]); \alpha$ the denotation of $C[M']$. By Theorem 1.4.6, the sets $(N, \mathrm{Acc}(\Lambda([\![M]\!]); \alpha))$ and $(N, \mathrm{Acc}(\Lambda([\![M']\!])))$ are inequivalent, and so $[\![M]\!] \not\sim [\![M']\!]$. □

Our setup is too general for us to prove Full Abstraction, but we will be able to prove a Full Abstraction result in an important special case: that of Probabilistic Algol.

1.6 Probability

We now specialize to the case where $\mathcal{X}$ is a category of random variables on some fixed probability space $(\Omega, \mathcal{F}, \mathbb{P})$, in order to model a probabilistic language. For our purposes, it will suffice to take Ω to be the real interval $(0,1)$ with its Borel σ-algebra and measure. A *random variable* on Ω is a measurable function $V \colon \Omega \to X$. Given such a random variable, and $A \subseteq X$, we write $\mathbb{P}(V \in A)$ for $\mathbb{P}(V^{-1}(A))$, and $\mathbb{P}(V = x)$ for $\mathbb{P}(V \in \{x\})$.

The category $\mathcal{X} = \mathbf{Rv}_{\Omega}^{FS}$ will then be the category whose objects are random variables of *finite support*; that is, measurable functions $V \colon \Omega \to X$, where X is a discrete space, such that there is some finite subset $Y \subseteq X$ such that $\mathbb{P}(V \in Y) = 1$.

The morphisms in $\mathbf{Rv}_{\Omega}^{FS}$ from $V \colon \Omega \to X$ to $W \colon \Omega \to Y$ are probability-preserving functions $X \to Y$; i.e., functions $X \to Y$ such that for all $A \subseteq Y$, we have $\mathbb{P}(f(V) \in A) = \mathbb{P}(W \in A)$.

Recall that the tensor product of two random variables $V\colon \Omega \to X$ and $W\colon \Omega \to Y$ is their pairing $V \otimes W = \langle V, W\rangle\colon \Omega \to X \times Y$.

We define a language Probabilistic Algol (PA) to be the sublanguage of $\mathrm{IA}_{\mathbf{Rv}_\Omega^{FS}}$ generated by the terms of Idealized Algol and the terms

$$\mathsf{choose}_{V_p}\ ,$$

where $p \in [0,1]$, and where we have identified V_p is the Bernoulli random variable

$$\Omega \to \mathbb{B}$$

that returns $\mathbb{t}$ if its input is less than p and $\mathbb{f}$ if it is greater than or equal to p.

The denotation of any term of PA, then, will be an (equivalence class of) morphisms

$$\underline{\mathbb{B}^n} \xrightarrow{m} \underline{\mathbb{B}}^n \to [\![T]\!]\ ,$$

together with some random variable taking values in $\mathbb{B}^n$. We have used an underline to distinguish between the object $\underline{\mathbb{B}^n}$ of $\mathcal{G}$ corresponding to the set $\mathbb{B}^n$ of n-tuples of booleans and the n-fold Cartesian power $\underline{\mathbb{B}}^n$ in $\mathcal{G}$ of the object $\mathbb{B}$ corresponding to the set of booleans.

Lastly, given such a random variable $V\colon \Omega \to \mathbb{B}^n$, there is a random variable $\tilde{V}\colon \Omega \to \mathbb{N}$ such that for each $\vec{v} \in \mathbb{B}^n$, we have

$$\mathbb{P}\left(\tilde{V} = \sum_{i=1}^{n} 2^{i-1}\vec{v}_i\right) = \mathbb{P}(V = \vec{v})$$

and such that $\mathbb{P}(\tilde{V} = k) = 0$ for any $k \geq 2^n$. Then we have a function $f\colon \mathbb{N} \to \mathbb{B}^n$ that sends $\sum_{i=1}^{n} 2^{i-1}a_i$ to $(a_1, \cdots, a_n)$ and sends $k \geq 2^n$ to some fixed value (say, $(\mathbb{f}, \cdots, \mathbb{f})$), and then we have

$$f \circ \tilde{V} = V\ .$$

Moreover, $\tilde{V}$ has finite support.

Now suppose that X is a finite discrete probability space. Then the set X^ω of all infinite sequences of elements of X may be given the product topology, and equipped with the resulting Borel σ-algebra. A basic open subset of X^ω is a set $\mathfrak{S} \subseteq X^\omega$ for which there exists some n such that if $s \in \mathfrak{S}$ and t is a sequence such that s and t are identical on the first n terms, then $t \in \mathfrak{S}$. We can define a pre-probability measure on these basic open sets by setting

$$\mathbb{P}(\mathfrak{S}) = \sum_{u \in \mathfrak{S}|_n} \prod_{i=0}^{n-1} \mathbb{P}(u^{(i)})\,,$$

where $\mathfrak{S}|_n$ is the set of all length-n prefixes of elements of $\mathfrak{S}$.

Then the Carathéodory Extension Theorem tells us that there is a unique extension of this to a probability measure on the whole space (see, for example, [Shr04, 1.1.4]).

If $V\colon \Omega \to Z$ is a finitely-supported random variable, then V induces a probability measure on its support $\mathrm{Im}(V) \subseteq Z$. This gives us a probability measure on $\mathrm{Im}(V)^*$, which we can extend to a probability measure on Z^* by setting

$$\mathbb{P}(A) = \mathbb{P}(A \cap \mathrm{Im}(V)^*)$$

for any $A \subseteq Z^*$.

Definition 1.6.1. Let $V\colon \Omega \to X$ be a finitely supported random variable and let $\mathcal{U} \subseteq X^*$ be a set of sequences. Then we define

$$\mathbb{P}(V,\mathcal{U}) = \mathbb{P}(\mathcal{U}^\omega)\,,$$

where $\mathcal{U}^\omega \subseteq X^\omega$ is the set of all infinite sequences having some prefix in $\mathcal{U}$. Note that $\mathcal{U}^\omega$ is an open subset of X^ω, so is in particular measurable.

An easier way to define $\mathbb{P}(V,\mathcal{U})$ is that it is the sum of the probabilities of all the sequences in $\mathcal{U}$; i.e.:

$$\mathbb{P}(V,\mathcal{U}) = \sum_{u\in\mathcal{U}} \prod_{i=0}^{|u|-1} \mathbb{P}(u^{(i)})\,,$$

where the infinite sum refers to the supremum of the sums of all finite subsets of $\mathcal{U}$.

Proposition 1.6.2. *Suppose that $(V,\mathcal{U})$ and $(W,\mathcal{V})$ are equivalent pairs, in the sense of Definition 1.4.3, where $V\colon \Omega \to X$, $W\colon \Omega \to Y$ are finitely-supported random variables, and $\mathcal{U} \subseteq X^*$, $\mathcal{V} \subseteq Y^*$ are sets of sequences. Then $\mathbb{P}(V,\mathcal{U}) = \mathbb{P}(W,\mathcal{V})$.*

Proof. Without loss of generality, we may assume that there is a probability-preserving function $f\colon X \to Y$; i.e., a function such that for any $A \subseteq Y$ we have

$\mathbb{P}(W \in A) = \mathbb{P}(f(V) \in A)$ and such that $\mathcal{U} = f_*^{-1}(\mathcal{V})$. Then we have

$$\begin{aligned}
\mathbb{P}(V,\mathcal{U}) &= \mathbb{P}(V, f_*^{-1}(\mathcal{V})) \\
&= \sum_{\substack{u \in X^* \\ f_* u \in \mathcal{V}}} \prod_{i=0}^{|u|-1} \mathbb{P}(V = u^{(i)}) \\
&= \sum_{v \in \mathcal{V}} \sum_{\substack{u \in X^* \\ f_* u = v}} \prod_{i=0}^{|u|-1} \mathbb{P}(V = u^{(i)}) \\
&= \sum_{v \in \mathcal{V}} \prod_{i=0}^{|v|-1} \sum_{\substack{x \in X \\ f(x) = v}} \mathbb{P}(V = x) \\
&= \sum_{v \in \mathcal{V}} \prod_{i=0}^{|v|-1} \mathbb{P}(f(V) = v^{(i)}) \\
&= \sum_{v \in \mathcal{V}} \prod_{i=0}^{|v|-1} \mathbb{P}(W = v^{(i)}) \\
&= \mathbb{P}(W, \mathcal{V})\,. \qquad\qquad \square
\end{aligned}$$

We now make a definition relating the operational behaviour we have defined for $\mathrm{IA}_{\mathcal{X}}$ to probability.

Definition 1.6.3. Let $M \colon \mathtt{com}$ be a closed term of PA mentioning probabilities $p_1, \cdots, p_n$. We define $\mathbb{P}(M \Downarrow)$ to be $\mathbb{P}(B(M))$; i.e.,

$$\mathbb{P}(V_{p_1} \otimes \cdots \otimes V_{p_n}, \mathcal{U})\,,$$

where $\mathcal{U}$ is the set of all sequences $u \in j(V_{p_1} \otimes \cdots \otimes V_{p_n})^*$ that cover some sequence U such that $M \Downarrow_U \mathsf{skip}$.

We can define a corresponding notion for morphisms in the denotational semantics.

Definition 1.6.4. Let $\sigma \colon 1 \to \mathbb{C}$ be a morphism in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$, considered as a morphism $\sigma \colon 1 \to (X \to \mathbb{C})$ in $\mathcal{G}$, together with a finitely-supported random variable $V \colon \Omega \to X$.

Then we define $\mathbb{P}(\sigma \downarrow)$ to be

$$\mathbb{P}(V, \mathrm{Acc}(\sigma))\,.$$

Remark 1.6.5. By Propositions 1.6.2 and 1.4.4, Definitions 1.6.3 and 1.6.4 are well defined.

Now we are ready to prove computational adequacy.

Proposition 1.6.6 (Computational Adequacy for PA)**.** *Let $M\colon \texttt{com}$ be a closed term of PA. Then $\mathbb{P}(M \Downarrow) = \mathbb{P}(\llbracket M \rrbracket \downarrow)$.*

Proof. By Theorem 1.4.6, $B(M)$ is equivalent to $(p, \mathrm{Acc}(\llbracket M \rrbracket))$. Therefore, by Proposition 1.6.2, $\mathbb{P}(M \Downarrow) = \mathbb{P}(B(M)) = \mathbb{P}(V, \mathrm{Acc}(\llbracket M \rrbracket)) = \mathbb{P}(\llbracket M \rrbracket \downarrow)$. □

We can define observational equivalence for terms.

Definition 1.6.7. Let $M, N\colon T$ be closed terms of PA. Then we say that M and N are (probabilistically) *observationally equivalent* if for all contexts $C\colon \texttt{com}$ with a hole of type T, we have

$$\mathbb{P}(C[M] \Downarrow) = \mathbb{P}(C[N] \Downarrow)\,.$$

We then have the usual corresponding definition in the denotational semantics.

Definition 1.6.8. Let $\sigma, \tau\colon A \to B$ be morphisms in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$. We write $\sigma \sim_{\mathbb{P}} \tau$ if for all morphisms $\alpha\colon (A \to B) \to \mathbb{C}$ in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$ we have

$$\mathbb{P}(\Lambda(\sigma); \alpha \downarrow) = \mathbb{P}(\Lambda(\tau); \alpha \downarrow)\,.$$

Then, by our standard argument, we may derive Equational Soundness from Computational Adequacy.

Proposition 1.6.9. *Let $M, N\colon T$ be closed terms of PA such that $\llbracket M \rrbracket \sim_{\mathbb{P}} \llbracket N \rrbracket$. Then M and N are probabilistically observationally equivalent.*

Our next goal will be to prove the converse to this result: Full Abstraction.

1.7 Full Abstraction for Probabilistic Algol

Proposition 1.7.1. *Let $V\colon \Omega \to X$ be a finitely supported random variable. Then there exist $p_1, \cdots, p_n$ and a function*

$$f\colon \mathbb{B}^n \to X$$

such that for all $x \in X$ we have $\mathbb{P}(V = x) = \mathbb{P}(f(V_{p_1}, \cdots, V_{p_n}) = x)$.

Proof. Recall that the V_p are not independent in our formulation; indeed, if $p < q$, then $V_p = \mathtt{t} \Rightarrow V_q = \mathtt{t}$.

Enumerate those elements $x \in X$ such that $\mathbb{P}(V = x) \neq 0$ as $x_1, \cdots, x_n$, and for each $k = 1, \cdots, n$, define

$$p_k = \sum_{i=1}^{n} \mathbb{P}(X = x_i)\,.$$

Note that we must have $p_n = 1$. Then we define

$$f(\vec{b}) = \begin{cases} x_1 & \text{if } \vec{b} = \vec{\mathbb{f}} \\ \min\{k \,:\, b_k = \mathbb{t}\} & \text{otherwise}\,. \end{cases}$$

Fix $x \in X$. If x is not one of the x_i, then we have $\mathbb{P}(f(V_{p_1}, \cdots, V_{p_n}) = x) = 0 = \mathbb{P}(V = x)$. Otherwise, suppose $x = x_k$. If $\omega \in \Omega$ and $p_{k-1} \leq \omega < p_k$, then $V_{p_k}(\omega) = \mathbb{t}$, and $V_{p_i}(\omega) = \mathbb{f}$ for all $i \leq k$. So $f((V_{p_1} \otimes \cdots \otimes V_{p_n})(\omega)) = x_k$. If $\omega < p_{k-1}$, then $V_{p_{k-1}}(\omega) = \mathbb{t}$, so $f((V_{p_1} \otimes \cdots \otimes V_{p_n})(\omega)) \neq x_k$. If $\omega \geq p_k$, then $V_{p_k}(\omega) = \mathbb{f}$, so $f((V_{p_1} \otimes \cdots \otimes V_{p_n})(\omega)) \neq x_k$. Therefore,

$$\mathbb{P}(f(V_{p_1}, \cdots, V_{p_k}) = x_k) = \mathbb{P}([p_{k-1}, p_k)) = p_k - p_{k-1} = \mathbb{P}(X = x_k)\,.$$

It follows that f is probability preserving in the sense required. □

The most important consequence of Proposition 1.7.1 is that it tells us that any morphism $A \to B$ in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$ may be considered as a pair

$$(V_{p_1} \otimes \cdots \otimes V_{p_n}, f \colon A \to (\mathbb{B}^n \to B))$$

for appropriately chosen $p_1, \cdots, p_n$.

Definition 1.7.2. Let $\sigma \colon A \to B$ be a morphism in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$. We say that σ is *compact* if it is compact when considered as a morphism in $\mathcal{G}$.

Remark 1.7.3. When we say 'considered as a morphism in $\mathcal{G}$' in the above definition, we mean 'in at least one of its possible interpretations as a morphism in $\mathcal{G}$'. Note, however, that the continuous image of a compact element is compact, and so if we pass to a new representative of σ by composing on the left by the image of some morphism in $\mathbf{Rv}_\Omega^{FS}$, then the resulting representative of σ will also be compact.

Note that if $\mathcal{G}$ is the category of games, this compactness property is invariant under the choice of representative for σ.

Proposition 1.7.4 (Compact definability)**.** *Let T be an Idealized Algol type and let $\sigma \colon 1 \to \llbracket T \rrbracket$ be a compact morphism in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$. Then there is some closed term $M \colon T$ such that $\sigma = \llbracket M \rrbracket$.*

Proof. Let $(V, \sigma \colon 1 \to (X \to \llbracket T \rrbracket)$ be a compact representative of σ, where X is a set and V is a finitely-supported random variable taking values in X. By Proposition 1.7.1, we may choose $p_1, \cdots, p_n$ such that there is a probability-preserving function

$$f \colon V_{p_1} \otimes \cdots \otimes V_{p_n} \to \llbracket T \rrbracket\;.$$

After composing on the right by $(\sigma \to \llbracket T \rrbracket)$, we may assume that σ is of the form

$$(V_{p_1} \otimes \cdots \otimes V_{p_n}, \sigma \colon 1 \to (\underline{\mathbb{B}^n} \to \llbracket T \rrbracket))\,.$$

Now this σ necessarily factors as

$$1 \xrightarrow{\hat{\sigma}} (\mathbb{B}^n \to [\![T]\!]) \xrightarrow{(m \to [\![T]\!])} (\underline{\mathbb{B}^n} \to [\![T]\!])\,,$$

where $\hat{\sigma}$ is compact. Then, by compact definability in $\mathcal{G}$, $\hat{\sigma}$ is the denotation of some term $N\colon \texttt{bool} \to \cdots \to \texttt{bool} \to T$, and it follows that our original morphism σ in $\mathcal{G}/(\mathbf{Rv}_{\Omega}^{FS})^{\mathrm{op}}$ is the denotation of

$$N\ \mathsf{choose}_{p_1}\ \cdots\ \mathsf{choose}_{p_n}\ . \qquad \square$$

Theorem 1.7.5 (Full Abstraction for PA)**.** *Let $M, N\colon T$ be observationally equivalent terms of PA. Then $[\![M]\!] \sim_{\mathbb{P}} [\![N]\!]$.*

Proof. Suppose that $[\![M]\!] \not\sim_{\mathbb{P}} [\![N]\!]$. So there is some $\alpha\colon [\![T]\!] \to \mathbb{C}$ such that $\mathbb{P}([\![M]\!]\,;\alpha\downarrow) \neq \mathbb{P}([\![N]\!]\,;\alpha\downarrow)$.

Let $\mathbb{P}([\![M]\!]\,;\alpha\downarrow) = p$ and $\mathbb{P}([\![N]\!]\,;\alpha\downarrow) = q$, and suppose without loss of generality that $p > q$. Now there must be some finite subset $\mathcal{V}$ of $\mathrm{Acc}([\![M]\!]\,;\alpha\downarrow)$ such that the combined probability of the sequences in $\mathcal{V}$ is still greater than q. For each $u \in \mathcal{V}$, we can choose some compact $\alpha_u \subseteq \alpha$ such that u is still accepted by $[\![M]\!]\,;\alpha_u$, by algebraicity. Since the set of compact elements below α is directed, there is some $\alpha' \subseteq \alpha$ such that $\alpha_u \subseteq \alpha'$ for each $u \in \mathcal{V}$. Then we have

$$\mathbb{P}([\![M]\!]\,;\alpha'\downarrow) > q \qquad\qquad \mathbb{P}([\![N]\!]\,;\alpha'\downarrow) \leq q\,,$$

and therefore $\mathbb{P}([\![M]\!]\,;\alpha'\downarrow) \neq \mathbb{P}([\![N]\!]\,;\alpha'\downarrow)$.

By Proposition 1.7.4, α' is the denotation of some term $L\colon T \to \texttt{com}$, and our Computational Adequacy result (Proposition 1.6.6) then tells us that

$$\mathbb{P}(L\,M\Downarrow) = \mathbb{P}([\![M]\!]\,;\alpha'\downarrow) \neq \mathbb{P}([\![N]\!]\,;\alpha'\downarrow) = \mathbb{P}(L\,N\Downarrow)\,.$$

Therefore, M and N are not observationally equivalent. $\square$

1.8 Comparison with a Kleisli Category Model

An alternative way to model probability is using the Kleisli category construction that we considered in Chapter **??**. Specifically, we can consider the language $\mathrm{IA}_{\mathbb{B}}$ as a probabilistic Algol variant, by treating the term $\mathsf{ask}_{\mathbb{B}}$ as a coin flip that returns $\mathbb{t}$ or $\mathbb{f}$ each with probability $\frac{1}{2}$.

Given a closed term $M\colon \texttt{com}$ of $\mathrm{IA}_{\mathbb{B}}$, we define

$$\mathbb{P}(M\Downarrow) = \sum_{u \in \mathbb{B}^*\,:\ M \Downarrow_u \mathsf{skip}} 2^{-|u|}\,,$$

since $2^{-|u|}$ is the probability of a particular sequence u of $\mathbb{t}$ and $\mathbb{f}$ values occurring. Here, the infinite sum means the supremum over all sums of finite subsets.

Similarly, given a Kleisli morphism $\sigma\colon 1 \to \mathbb{C}$ – i.e., a morphism $\sigma\colon 1 \to (\mathbb{B} \to \mathbb{C})$ in $\mathcal{G}$, we can define

$$\mathbb{P}(\sigma \downarrow) = \sum_{u \in \mathrm{Acc}(\sigma)} 2^{-|u|}\,.$$

Our Computational Adequacy result for IAX (Propositions **??** and **??**) then gives us a Computational adequacy result for this model.

Proposition 1.8.1. *Let $M\colon$ `com` be a closed term of $IA_{\mathbb{B}}$. Then $\mathbb{P}(M \Downarrow) = \mathbb{P}([\![M]\!] \downarrow)$.*

Proof. Propositions **??** and **??** tell us that the set of sequences u such that $M \Downarrow_u \mathsf{skip}$ is the same as the set $\mathrm{Acc}([\![M]\!])$. □

We can define probabilistic observational equivalence and the probabilistic intrinsic equivalence $\sim_{\mathbb{P}}$ in exactly the same way as we did for PA. Then the same argument we used in Theorem 1.7.5 proves Full Abstraction for this model.

Theorem 1.8.2. *Let $M, N\colon T$ be closed terms of $IA_{\mathbb{B}}$. Then M and N are probabilistically observationally equivalent if and only if $[\![M]\!] \sim_{\mathbb{P}} [\![N]\!]$.*

This model is much easier to realize. What do we gain, then, from our more complicated model?

The most obvious answer is that our original model allowed us to work with arbitrary probabilities, rather than using a fixed coin with probability $\frac{1}{2}$. This is not such a great advantage as it might seem, since if $p \in [0, 1]$ is any real number whose binary expansion is computable as a function $\mathbb{N} \to \mathbb{B}$, then we can simulate choose_p within the probabilistic version of $\mathrm{IA}_{\mathbb{B}}$[1].

Perhaps a better way of thinking about the difference between the two models, then, is to consider what the denotation of a term actually looks like. In the language $\mathrm{IA}_{\mathbb{B}}$, we can define a term that converges to $\mathbb{t}$ with probability $\frac{2}{3}$ and to $\mathbb{f}$ with probability $\frac{1}{3}$ by

$$\mathbf{Y}_{\mathtt{bool}}(\lambda b.\, \mathsf{If}\ \mathsf{choose}_{\frac{1}{2}}\ \mathsf{then}\ \mathbb{t}\ \mathsf{else}\ (\mathsf{If}\ \mathsf{choose}_{\frac{1}{2}}\ \mathsf{then}\ b\ \mathsf{else}\ \mathbb{f}))\,.$$

Here, we have renamed $\mathsf{ask}_{\mathbb{B}}$ to $\mathsf{choose}_{\frac{1}{2}}$ to give a better idea of what the term does in the probabilistic setup.

Now the denotation of this term in $\mathrm{Kl}_{R_{\mathbb{B}}}\,\mathcal{G}$ is given by the denotation of the term-in-context

$$c\colon \mathtt{bool} \vdash \mathbf{Y}_{\mathtt{bool}}(\lambda b.\, \mathsf{If}\ c\ \mathsf{then}\ \mathbb{t}\ \mathsf{else}\ (\mathsf{If}\ c\ \mathsf{then}\ b\ \mathsf{else}\ \mathbb{f}))$$

[1] Idea: build up a sequence of intervals I_n of width 2^n by repeatedly flipping the coin and using the result to choose either the lower or the upper half of I_{n-1}. If at any point the upper bound of I_n is less than or equal to p (which can be checked by computing the first n terms of the binary expansion of p, then return $\mathbb{t}$. If at any point the lower bound of I_n is greater than or equal to p, return $\mathbb{f}$.

in $\mathcal{G}$. If $\mathcal{G}$ is the category of games, then this morphism is the strategy with maximal plays taking one of the following two forms.

$$q(q\mathbb{f}q\mathbb{t})^n q\mathbb{t}\mathbb{t} \qquad\qquad q(q\mathbb{f}q\mathbb{t})^n q\mathbb{f}q\mathbb{f}\mathbb{f}$$

In other words, it is not at all clear from the denotation that the term should give $\mathbb{t}$ with probability $\frac{2}{3}$ and $\mathbb{f}$ with probability $\frac{1}{3}$.

In $\mathcal{G}/\mathbf{Rv}_\Omega^{FS}$, however, we can model a term that has the same behaviour using the morphism

$$\left(V_{\frac{2}{3}}, \mathrm{id}_{\mathbb{B}}\right) ,$$

which makes it much clearer what the probabilistic behaviour is.

1.9 Game Semantics and Probability

We now specialize to the case that $\mathcal{G}$ is the category of arenas and single-threaded strategies that we developed in Chapters **??** and **??**. This will allow us to capture the close relationship between the sequences u that we have been considering and the plays in a strategy.

Definition 1.9.1. Let X be a set and let $u \in X^*$ be a sequence. Consider X as an arena $\underline{X}$. Then we write qu for the play in $\underline{X}$ given by

$$q\, u^{(1)} \cdots q\, u^{(|u|-1)} .$$

Note that any P-position in $\underline{X}$ is of the form qu for some sequence u.

Definition 1.9.2. Let A be an arena, let V be a random variable taking values in a set X, and let $\sigma\colon X \to A$ be a single-threaded strategy. We may consider X as a game $\underline{X}$. Let s be a legal play of A. If $t \in \sigma$, we write t/s if $t|_A = s$ and if the last move of t is the last move of s (this implies in particular that $t|_{\underline{X}}$ is a P-position in $\underline{X}$). Then we define

$$\mathrm{Acc}_s(\sigma) = \{u \in X^* \,:\, \exists t \in \sigma \,.\, t/s,\, t|_{\underline{X}} = qu\} .$$

We define

$$\mathbb{P}_V(s \in \sigma) = \mathbb{P}(V, \mathrm{Acc}_s(\sigma)) .$$

We would like use this definition to define $\mathbb{P}(s \in \sigma)$ for σ a morphism in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$, but we first need to check that this is well-defined with respect to the equivalence relation on Melliès morphisms.

Proposition 1.9.3. *Let*

$$(V\colon \Omega \to X, \sigma\colon \underline{X} \to A) \qquad\qquad (W\colon \Omega \to Y, \sigma\colon \underline{Y} \to A)$$

be representatives of the same morphism $A \to B$ in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$, where X and Y are sets. Let s be a legal play of A. Then $(V, \mathrm{Acc}_s(\sigma))$ and $(W, \mathrm{Acc}_s(\sigma'))$ are equivalent as pairs in the sense of Definition 1.4.3.

Proof. It suffices by induction to prove this in the case that the two representatives are related by the relation that generates the equivalence relation on morphisms; i.e., that there is a probability-preserving function $f\colon X \to Y$ such that $\sigma = \sigma'; (j(f) \to A)$.

Let $u \in X^*$. Then we have

$$\begin{aligned} u \in \mathrm{Acc}_s(\sigma) &\Leftrightarrow \exists t \in \sigma \;.\; t/s,\, t|_{\underline{X}} = qu \\ &\Leftrightarrow \exists t \in \sigma'; (j(f) \to A) \;.\; t/s,\, t|_{\underline{X}} = qu \\ &\Leftrightarrow \exists t' \in \sigma' \;.\; t/s,\, t|_{\underline{Y}} = q(f_* u) \\ &\Leftrightarrow f_* u \in \mathrm{Acc}_s(\sigma')\,. \end{aligned}$$

Therefore, $(V, \mathrm{Acc}_s(\sigma))$ and $(W, \mathrm{Acc}_s(\sigma'))$ are equivalent. □

It follows by Proposition 1.6.2 that $\mathbb{P}_V(s \in \sigma) = \mathbb{P}_W(s \in \sigma')$ for all s. Therefore, the following is well-defined.

Definition 1.9.4. Let $\sigma\colon A \to B$ be a morphism in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$, where $\mathcal{G}$ is the category of arenas and single-threaded strategies, and suppose that σ is given (after currying) by a morphism

$$\tilde{\sigma}\colon \underline{X} \to (A \to B)$$

in $\mathcal{G}$, together with a random variable V taking values in X. Then we define

$$\mathbb{P}(s \in \sigma) = \mathbb{P}_V(s \in \tilde{\sigma})\,.$$

Definition 1.9.5. Let $\sigma, \sigma'\colon A \to B$ be morphisms in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$, where $\mathcal{G}$ is the category of arenas and single-threaded strategies. We say that $\sigma \approx_{\mathbb{P}} \sigma'$ if for all legal plays s of $A \to B$ we have

$$\mathbb{P}(s \in \sigma) = \mathbb{P}(s \in \sigma')\,.$$

We now relate this definition to Melliès composition of strategies.

Definition 1.9.6. Let A, B, C be arenas and let s be a play in $A \to C$. We write

$$\mathrm{wit}_B(s) = \{\mathfrak{s} \in \mathrm{int}(A, B, C) \;:\; \mathfrak{s}|_{A,C} = s\}\,.$$

Proposition 1.9.7. *Let $\sigma\colon A \to B$, $\tau\colon B \to C$ be morphisms in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$. Let s be a legal play in $A \to C$. Then*

$$\mathbb{P}(s \in \sigma; \tau) = \sum_{\mathfrak{s} \in \mathrm{wit}_B(s)} \mathbb{P}(\mathfrak{s}|_{A,B} \in \sigma)\mathbb{P}(\mathfrak{s}|_{B,C} \in \tau)\,.$$

Proof. Suppose that σ and τ are given by (equivalence classes of) pairs

$$(V\colon \Omega \to X, \tilde{\sigma}\colon A \to (\underline{X} \to B)) \qquad (W\colon \Omega \to Y, \tilde{\tau}\colon B \to (\underline{Y} \to C))\,,$$

where V and W are random variables and $\tilde{\sigma}, \tilde{\tau}$ are strategies in $\mathcal{G}$. Then the composition $\sigma;\tau$ in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$ is given by $V \otimes W\colon \Omega \to X \times Y$, together with the Melliès composition

$$A \xrightarrow{\tilde{\sigma}} (\underline{X} \to B) \xrightarrow{\underline{X} \to \tilde{\tau}} (\underline{X} \to (\underline{Y} \to C)) \to ((\underline{X} \times \underline{Y}) \to C) \xrightarrow{\mu \to C} (\underline{X \times Y} \to C)\,,$$

where μ is $\langle \underline{\mathrm{pr}_X}, \underline{\mathrm{pr}_Y} \rangle$.

First suppose that s is a sequence in $A \to C$, and let $\mathfrak{s} \in \mathrm{wit}_B(s)$. Let $\mathfrak{t}$ be a sequence in $\tilde{\sigma} \| (\underline{X} \to \tau)$ such that $\mathfrak{t}|_{A,B,C} = \mathfrak{s}$. Then $\mathfrak{t}|_{A,\underline{X} \to B} \in \tilde{\sigma}$ and $\mathfrak{t}|_{B,\underline{Y},C} \in \tilde{\tau}$.

Moreover, since we have $\mathfrak{t}|_{A,B} = \mathfrak{s}|_{A,B}$ and $\mathfrak{t}|_{B,C} = \mathfrak{s}|_{B,C}$, we must have

$$\mathfrak{t}|_{\underline{X}} \in \mathrm{Acc}_{\mathfrak{s}|_{A,B}}(\tilde{\sigma}) \qquad \mathfrak{t}|_{\underline{Y}} \in \mathrm{Acc}_{\mathfrak{s}|_{B,C}}(\tilde{\tau})\,,$$

where we have identified a play qu occurring in the arena $\underline{X}$ with its underlying sequence u of elements of X, and likewise for Y.

This gives us a function

$$\{\mathfrak{t} \in \tilde{\sigma} \| (\underline{X} \to \tilde{\tau}) : \ \mathfrak{t}|_{A,B,C} = \mathfrak{s}\} \to \mathrm{Acc}_{\mathfrak{s}|_{A,B}}(\tilde{\sigma}) \times \mathrm{Acc}_{\mathfrak{s}|_{B,C}}(\tilde{\tau})\,.$$

We claim that this function is a bijection.

Indeed, suppose that $\mathfrak{t}, \mathfrak{t}'$ are two interactions in $\tilde{\sigma} \| (\underline{X} \to \tilde{\tau})$ such that $\mathfrak{t}|_{A,B,C} = \mathfrak{t}'|_{A,B,C} = \mathfrak{s}$, $\mathfrak{t}|_{\underline{X}} = \mathfrak{t}'|_{\underline{X}}$ and $\mathfrak{t}|_{\underline{Y}} = \mathfrak{t}'|_{\underline{Y}}$. We claim that $\mathfrak{t} = \mathfrak{t}'$.

Indeed, suppose for a contradiction that $\mathfrak{t} \neq \mathfrak{t}'$: then there are prefixes $\mathfrak{r}p \sqsubseteq \mathfrak{t}$ and $\mathfrak{r}q \sqsubseteq \mathfrak{t}'$, where $\mathfrak{r}$ is the longest common subsequence of $\mathfrak{t}$ and $\mathfrak{t}'$ and $p \neq q$ are moves.

By our earlier analysis (see, for example, the proof of **??**), we know that p and q must either both occur in the $A \to (\underline{X} \to B)$-component, or both in the $(\underline{X} \to B) \to (\underline{X} \to (\underline{Y} \to C))$-component. But since $\mathfrak{t}, \mathfrak{t}' \in \tilde{\sigma} \| (\underline{X} \to \tilde{\tau})$ are both interactions of deterministic strategies, we also know that they must both be O-moves in that component – otherwise, they would have to be equal. In particular, neither p nor q may be a move in the middle component $\underline{X} \to B$, since then it would be a P-move in one of the two components.

Therefore, p and q are both O-moves in one of the outer components A and $\underline{X} \to (\underline{Y} \to C)$. By Corollary **??**, we know that only Player P may switch between games in $\underline{X} \to (\underline{Y} \to C)$, and therefore p and q must occur in the same component game – i.e., both in A, both in $\underline{X}$, both in $\underline{Y}$ or both in C. But now the conditions that $\mathfrak{t}|_{A,B,C} = \mathfrak{t}'|_{A,B,C}$, $\mathfrak{t}|_{\underline{X}} = \mathfrak{t}'|_{\underline{X}}$ and $\mathfrak{t}|_{\underline{Y}} = \mathfrak{t}'|_{\underline{Y}}$ mean that we must have $p = q$. For example, if p and q are both moves in C, then we have

$\mathfrak{r}|_C p \sqsubseteq \mathfrak{t}|_C$ and $\mathfrak{r}|_C q \sqsubseteq \mathfrak{t}'|_C$; since $\mathfrak{t}|_C = \mathfrak{t}'|_C$, we must have $p = q$. This is the desired contradiction.

For surjectivity, let $u \in \mathrm{Acc}_{\mathfrak{s}|_{A,B}}(\sigma)$ and $v \in \mathrm{Acc}_{\mathfrak{s}|_{B,C}}(\tau)$. We seek a sequence $\mathfrak{t} \in \tilde{\sigma} \| (\underline{X} \to \tilde{\tau})$ such that $\mathfrak{t}|_{A,B,C} = \mathfrak{s}$, $\mathfrak{t}|_{\underline{X}} = qu$ and $\mathfrak{t}|_{\underline{Y}} = qv$.

Since $u \in \mathrm{Acc}_{\mathfrak{s}|_{A,B}}(\sigma)$, there is some sequence $s \in \sigma$ such that $s|_{A,B} = \mathfrak{s}|_{A,B}$ and $s|_{\underline{X}} = qu$. Similarly, since $v \in \mathrm{Acc}_{\mathfrak{s}|_{B,C}}(\tau)$, there is some sequence $t \in \tau$ such that $t|_{B,C} = \mathfrak{s}|_{B,C}$ and $t|_{\underline{Y}} = qv$. We form the sequence $\mathfrak{t}$ as a suitable interleaving of s and t, noting that they have the same B-components: we start with the sequence $\mathfrak{s}$, and then insert the appropriate moves from (the left-hand copy of) $\underline{X}$ and $\underline{Y}$ between the corresponding moves from A, B and C. Lastly, we insert moves from the right-hand copy of $\underline{X}$ adjacent to the corresponding moves in the right-hand copy, inserting an O-move q in the right-hand copy of $\underline{X}$ immediately after each O-move q in the left-hand copy, and a P-move x in the right-hand copy immediately before each P-move x in the left-hand copy.

This tells us that we have

$$\mathbb{P}(\mathfrak{s}|_{A,B} \in \sigma)\mathbb{P}(\mathfrak{s}|_{B,C} \in \tau)$$

$$= \left(\sum_{u \in \mathrm{Acc}_{\tilde{\sigma}}(\mathfrak{s}|_{A,B})} \prod_{i=0}^{|u|-1} \mathbb{P}(V = u^{(i)}) \right) \left(\sum_{v \in \mathrm{Acc}_{\tilde{\tau}}(\mathfrak{s}|_{A,B})} \prod_{i=0}^{|v|-1} \mathbb{P}(W = v^{(i)}) \right)$$

$$= \sum_{(u,v) \in \mathrm{Acc}_{\tilde{\sigma}}(\mathfrak{s}|_{A,B}) \times \mathrm{Acc}_{\tilde{\tau}}(\mathfrak{s}|_{B,C})} \prod_{i=0}^{|u|-1} \mathbb{P}(V = u^{(i)}) \prod_{i=1}^{|v|-1} \mathbb{P}(W = v^{(i)})$$

$$= \sum_{\substack{\mathfrak{t} \in \tilde{\sigma} \| (\underline{X} \to \tilde{\tau}) \\ \mathfrak{t}|_{A,B,C} = \mathfrak{s}}} \left[\prod_{i=1}^{|u|-1} \mathbb{P}(V = u^{(i)}) \prod_{i=0}^{|v|-1} \mathbb{P}(W = v^{(i)}) \;\middle|\; \begin{array}{l} \text{where} \\ \mathfrak{t}|_{\underline{X}} = qu \\ \mathfrak{t}|_{\underline{Y}} = qv \end{array} \right] .$$

Now let $s \in \mathcal{L}_{A \to C}$ and let $t \in \sigma;\tau$ be such that t/s. By the argument in Proposition **??**, there is a unique interaction sequence $S \in \sigma \| (\underline{X} \to \tau) \| (\Lambda^{-1};\mu)$ such that $S|_{A,\underline{X \times Y} \to C} = t$. Define $\mathfrak{t} = S|_{A,\underline{X} \to B,\underline{X} \to (\underline{Y} \to C)}$, and $\mathfrak{s} = \mathfrak{t}|_{A,B,C}$. Now we must have $\mathfrak{s}|_{A,C} = t|_{A,C} = s$, so $\mathfrak{s} \in \mathrm{wit}_B(s)$.

Now consider $\mathfrak{t}|_{\underline{X},\underline{Y}}$, which has the same length as $S|_{\underline{X \times Y}} = t|_{\underline{X \times Y}}$. This sequence is made up of pairs of moves qx for $x \in X$ or qy for $y \in Y$.

By the definition of μ, we know that if the i-th pair of moves in $\mathfrak{t}|_{\underline{X},\underline{Y}}$ is qx for $x \in X$, then the i-th pair of moves in $t|_{\underline{X \times Y}}$ is $q(x, y_0)$ for some y_0, and if the i-th pair of moves in $\mathfrak{t}|_{\underline{X},\underline{Y}}$ is qy for $y \in Y$, then the i-th pair of mvoes in $t|_{\underline{X \times Y}}$ is $q(x_0, y)$ for some $x_0 \in X$. Moreover, if t' is some other sequence such that t'/s and such that t' differs only from t in the choice of the 'irrelevant' moves

x_0, y_0, then there is some $S' \in \sigma \| (\underline{X} \to \tau) \| (\Lambda^{-1}; \mu)$ such that $S|_{A, \underline{X \times Y} \to C} = t'$ and $S|_{A, \underline{X} \to (\underline{Y} \to C)} = \mathfrak{t}$. Then the combined probability of all such sequences is given by

$$\left[\prod_{i=1}^{|u|-1} \mathbb{P}(V = u^{(i)}) \prod_{i=0}^{|v|-1} \mathbb{P}(W = v^{(i)}) \,\middle|\, \begin{array}{l} \text{where} \\ \mathfrak{t}|_{\underline{X}} = qu \\ \mathfrak{t}|_{\underline{Y}} = qv \end{array} \right] ,$$

and we can combine this with our calculations above to get the desired result. □

A consequence of Proposition 1.9.7 is that the probabilistic equivalence relation defined in 1.9.5 is respected by composition of strategies. We may therefore take the quotient of this category by the probabilistic equivalence relation to form a new category

$$(\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}) \backslash \approx_{\mathbb{P}} \ .$$

Then next proposition shows that we do not lose anything by doing this, since the probabilistic equivalence relation gets subsumed into our intrinsic equivalence.

Proposition 1.9.8. *Suppose that $[\sigma], [\tau] \colon A \to B$ are morphisms in the quotiented category, given by equivalence classes of strategies in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\mathrm{op}}$. Then $[\sigma]$ and $[\tau]$ are probabilistically intrinsically equivalent in the quotiented category if and only if σ and τ are probabilistically intrinsically equivalent in the original category.*

Proof. If σ, τ are not intrinisically equivalent, then there is some $\alpha \colon (A \to B) \to \mathbb{C}$ such that $\mathbb{P}(\Lambda^{-1}(\sigma); \alpha \downarrow) \neq \mathbb{P}(\Lambda^{-1}(\tau); \alpha; \downarrow)$. Then we have $\mathbb{P}(qa \in \Lambda^{-1}(\sigma); \alpha) \neq \mathbb{P}(qa \in \Lambda^{-1}(\tau); \alpha)$, and therefore $\Lambda^{-1}(\sigma); \alpha \not\approx_{\mathbb{P}} \Lambda^{-1}(\tau); \alpha$.

Conversely, if $[\sigma], [\tau]$ are not intrinsically equivalent in the quotiented category, then there is some $[\alpha] \colon (A \to B) \to \mathbb{C}$ such that

$$[\Lambda^{-1}(\sigma); \alpha] \not\approx_{\mathbb{P}} [\Lambda^{-1}(\tau); \alpha] \, .$$

It follows that

$$\mathbb{P}(qa \in \Lambda^{-1}(\sigma); \alpha) \neq \mathbb{P}(qa \in \Lambda^{-1}(\tau); \alpha) \, ;$$

i.e., that

$$\mathbb{P}(\Lambda^{-1}(\sigma); \alpha \downarrow) \neq \mathbb{P}(\Lambda^{-1}(\tau); \alpha \downarrow) \, ,$$

and so σ and τ are not intrinsically equivalent in the original category. □

1.10 The Probabilistic Game Semantics of Danos and Harmer

The work in the previous section shows that it suffices to consider equivalence classes of strategies under the relation $\approx_{\mathbb{P}}$, which suggests that we may take the quantities $\mathbb{P}(s \in \sigma)$ as primitives, rather than defining them indirectly.

This is the approach taken by Danos and Harmer in [DH00] – the original game semantics for a probabilistic variant of Algol. Danos and Harmer define an arena as we do, but define a probabilistic strategy on an arena A to be given by a function

$$\sigma \colon \mathcal{L}_A^{\text{even}} \to [0,1]$$

such that for any even-length s, and any extension sa, we have

$$\sigma(s) \geq \sum_{sab \in \mathcal{L}_A} \sigma(sab)\,.$$

for any even-length s, and any extension sa, we have

$$\sigma(s) \geq \sum_{sab \in \mathcal{L}_A} \sigma(sab)\,.$$

These quantites $\sigma(s)$ take the role of our $\mathbb{P}(s \in \sigma)$, but now they are part of the *definition* of the strategy σ, rather than being a calculated quantity.

Proposition 1.10.1. *For any Melliès strategy $\sigma \colon A \to B$ given by a random variable V taking values in a set X and a strategy $\tilde{\sigma} \colon A \to (\underline{X} \to B)$, we get a probabilistic strategy in the sense of Danos and Harmer by setting*

$$\sigma(s) = \mathbb{P}(s \in \sigma)\,.$$

Proof. We need to check that for any odd-length legal play $sa \in \mathcal{L}_A$ we have

$$\mathbb{P}(s \in \sigma) \geq \sum_{sab \in \mathcal{L}_A} \mathbb{P}(sab \in \sigma)\,.$$

But for any $u \in \mathrm{Acc}_{sab}(\sigma)$, there must be some prefix v of u such that $v \in \mathrm{Acc}_s(\sigma)$. Then all the sequences u arising in this way that have v as a prefix are pairwise incomparable (since $\tilde{\sigma}$ is a deterministic strategy), and so their combined probability is at most the probability of v. □

Clearly, two morphisms in $\mathcal{G}/(\mathbf{Rv}_\Omega^{FS})^{\text{op}}$ give rise to the same probabilistic strategy in this way if and only if they are probabilistically equivalent.

Danos and Harmer then *define* the composition of two probabilistic strategies using the formula that we derived in Proposition 1.9.7:

Definition 1.10.2. Let $\sigma \colon A \to B$, $\tau \colon B \to C$ be probabilistic strategies. Then their composition $\sigma;\tau$ is given by

$$(\sigma;\tau)(s) = \sum_{\mathfrak{s} \in \mathrm{wit}_B(s)} \sigma(\mathfrak{s}|_{A,B})\tau(\mathfrak{s}|_{B,C})\,.$$

By Proposition 1.9.7, the composition of strategies in the quotiented category agrees with this composition of Danos and Harmer. Our proof above then gives an alternative proof of Full Abstraction for Danos and Harmer's probabilistic game semantics.

Bibliography

[DH00] V. Danos and R. Harmer. Probabilistic game semantics. In *Proceedings Fifteenth Annual IEEE Symposium on Logic in Computer Science (Cat. No.99CB36332)*, pages 204–213, June 2000.

[Shr04] Steven E Shreve. *Stochastic calculus for finance 2, Continuous-time models*. Springer, New York, NY; Heidelberg, 2004.