1 Monads and Kleisli categories

??

1.1 Monads

Let $\mathcal{C}$ be a category. Then the category $[\mathcal{C}, \mathcal{C}]$ of functors $\mathcal{C} \to \mathcal{C}$ and natural transformations has a (strict) monoidal structure given by composition. A *monad* [Mac71, §VI] in $\mathcal{C}$ is a monoid in $[\mathcal{C}, \mathcal{C}]$.

In other words, it is a functor $M\colon \mathcal{C} \to \mathcal{C}$ together with natural transformations $m_a\colon MMa \to Ma$ and $u_a\colon a \to Ma$ such that the following diagrams commute for all objects a of $\mathcal{C}$.

$$\begin{tikzcd}
MMMa \arrow[r, "Mm_a"] \arrow[d, "m_{Ma}"] & MMa \arrow[d, "m_a"] \\
MMa \arrow[r, "m_a"] & Ma
\end{tikzcd}
\qquad
\begin{tikzcd}
Ma \arrow[r, "Mu_a"] \arrow[dr, "id"'] & MMa \arrow[d, "m_a"] \\
& Ma
\end{tikzcd}
\qquad
\begin{tikzcd}
Ma \arrow[r, "u_{Ma}"] \arrow[dr, "id"'] & MMa \arrow[d, "m_a"] \\
& Ma
\end{tikzcd}$$

Example 1.1. In the category of sets, the *nonempty powerset functor* $\mathcal{P}_+$ sends a set A to the set of nonempty subsets of A. This has the structure of a monad on **Set**, since we have a natural transformation (union) from $\mathcal{P}_+\mathcal{P}_+A \to \mathcal{P}_+A$ and a natural transformation (singleton) from $A \to \mathcal{P}_+A$ that obey the diagrams given above.

Example 1.2. Let $\mathcal{M}$ be a monoidal category and let x be a monoid in $\mathcal{M}$. The *writer monad* W_x on $\mathcal{M}$ is defined by $W_x y = y \otimes x$, with natural transformations

$$m_y\colon y \otimes x \otimes x \to y \otimes x \qquad\qquad u_y\colon y \to y \otimes x$$

given by the monoid structure on x.

Going the other way, if $\mathcal{M}$ is monoidal closed with inner hom $\multimap$, and if z is a comonoid in $\mathcal{M}$, then the *reader monad* R_z is given by $R_z y = z \multimap y$. Then the monadic coherences

$$m_y\colon z \multimap z \multimap y \to z \multimap y \qquad\qquad u_y\colon y \to z \multimap y$$

are induced from the comonoid structure on z. This second example is particularly important in Cartesian closed categories, in which every object has the structure of a comonoid.

Example 1.3. If $\mathcal{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathcal{D}$ with $\perp$ is an adjunction with counit $\epsilon\colon LR \to 1$ and unit $\eta\colon 1 \to RL$, then the composite $RL\colon \mathcal{C} \to \mathcal{C}$ has the structure of a monoid on $\mathcal{C}$, where the multiplication and unit are given by

$$R\epsilon L\colon RLRL \to RL \qquad\qquad \eta\colon 1 \to RL\,.$$

We will see in the next section that every monad is induced by an adjunction in this way.

As an example, if $\mathcal{M}$ is a monoidal closed category and w is an object of $\mathcal{M}$, then the *state monad* S_w on $\mathcal{M}$ is defined by

$$S_w x = w \multimap (x \otimes w)\,.$$

Example 1.4. Another example that arises from an adjunction is the *list monad* on **Set** that arises from the adjunction between the category of sets and the category of (set-valued) monoids. The underlying set of the free monoid on a set A is the set A^* of finite lists of elements of A, and the functor $A \mapsto A^*$ inherits a monoid structure where the multiplication $m_A \colon (A^*)^* \to A^*$ concatenates a list of lists into a single list and the unit $u_a \colon A \to A^*$ forms a list with a single element.

Example 1.5. A monad on $\mathcal{C}^{\mathrm{op}}$ is called a *comonad* on $\mathcal{C}$. The carrier of a comonad is still a functor $M \colon \mathcal{C} \to \mathcal{C}$, but now the multiplication and unit are natural transformations $M \Rightarrow MM$ and $M \Rightarrow 1$, rather than the other way round.

An adjunction $\mathcal{C} \mathrel{\underset{\xleftarrow[R]{}}{\overset{\xrightarrow{L}}{\bot}}} \mathcal{D}$ gives rise to a comonad structure on LR in much the same way as it gives rise to a monad structure on RL. So, for example, we have the *store comonad* S'_r for any object r of a monoidal closed category $\mathcal{M}$, given by

$$S'_r x = (r \multimap x) \otimes x\,.$$

1.2 Kleisli Categories

Let $\mathcal{C}$ be a category and let M be a monad on $\mathcal{C}$. Then [Kle65] there is a category Kl_M, called the *Kleisli category* of M, whose objects are the objects of $\mathcal{C}$ and where a morphism from an object a to an object b is a morphism $a \to Mb$ in $\mathcal{C}$.

Identity arrows are given by the morphisms $u_c \colon c \to Mc$ (considered as a morphism $c \to c$ in Kl_M) and the composition of arrows $f \colon a \to Mb$ and $g \colon b \to Mc$ is given by the following composite in $\mathcal{C}$.

$$a \xrightarrow{f} Mb \xrightarrow{Mg} MMc \xrightarrow{m_c} Mc$$

There is a natural identity-on-objects functor $J \colon \mathcal{C} \to \mathrm{Kl}_M$ that sends a morphism $f \colon a \to b$ in $\mathcal{C}$ to the composite

$$a \xrightarrow{f} b \xrightarrow{u_b} Mb\,,$$

considered as a morphism $a \to b$ in Kl_M.

In the other direction, we have a functor $S\colon \mathrm{Kl}_M \to \mathcal{C}$ that sends an object a of Kl_M to the object Ma of $\mathcal{C}$ and sends a morphism $f\colon a \to Mb$ from a to b in Kl_M to the composite

$$Ma \xrightarrow{Mf} MMb \xrightarrow{m_b} Mb$$

in $\mathcal{C}$. Note that $SJ = M$, by one of our coherence conditions on m and u. Meanwhile, JS is the functor $\mathrm{Kl}_M \to \mathrm{Kl}_M$ that sends an object a to Ma and sends a morphism $f\colon a \to Mb$ from a to b to the morphism $Mf\colon Ma \to MMb$ from Ma to Mb.

Proposition 1.6 ([Kle65])**.** *S is a right adjoint to J. The unit of the adjunction is $u\colon \mathrm{id} \Rightarrow M$. The counit $e_a\colon J(Sa) \to a$ is given by the identity morphism $Ma \to Ma$ in $\mathcal{C}$, considered as a morphism $Ma \to a$ in Kl_M.*

Given a monad M on a category $\mathcal{C}$ and a functor $F\colon \mathcal{C} \to \mathcal{D}$, where $\mathcal{D}$ is another category, we say that a natural transormation $\psi_a\colon FMa \to Fa$ is *M-multiplicative* if it makes the following diagrams commute.

$$\begin{tikzcd}
FMMa \arrow[r, "\psi_{Ma}"] \arrow[d, "Fm_a"'] & FMa \arrow[d, "\psi_a"] \\
FMa \arrow[r, "\psi_a"] & Fa
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
Fa \arrow[r, "Fu_a"] \arrow[dr, "\mathrm{id}"'] & FMa \arrow[d, "\psi_a"] \\
 & Fa
\end{tikzcd}$$

Given two triples $(\mathcal{D}, F, \psi), (\mathcal{D}', F', \psi')$, where $F\colon \mathcal{C} \to \mathcal{D}, F'\colon \mathcal{C}' \to \mathcal{D}'$ are functors and $\psi\colon FM \Rightarrow F, \psi'\colon F'M \Rightarrow F'$ are functors, we define a *morphism* from $(\mathcal{D}', F', \psi')$ to $(\mathcal{D}, F, \psi)$ to be a functor $H\colon \mathcal{D}' \to \mathcal{D}$ such that $F = HF'$ and $\psi = H\psi'$. This gives us a category.

A defining property of the Kleisli category is that it is initial among such triples $(\mathcal{D}, F, \psi)$:

Proposition 1.7 ([Str72])**.** *i) Given an object a of $\mathcal{C}$, the identity morphism $Ma \to Ma$ may be considered as a morphism $\phi_a\colon JMa \to Ja$ in Kl_M. ϕ_a is an M-multiplicative natural transformation.*

ii) Let $\mathcal{D}$ be a category, let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor and suppose that $\psi_a\colon FMa \to Ma$ is an M-multiplicative natural transformation. Then there is a unique functor $\hat{F}\colon \mathrm{Kl}_M \to \mathcal{D}$ such that $F = \hat{F}J$ and $\psi = \hat{F}\phi$.

Another way to characterize the Kleisli category Kl_M is to say that the the adjunction we described above is initial among all adjunctions giving rise to the monad M. This can be deduced from Proposition 1.7 using the following result.

Lemma 1.8 ([Str72])**.** *Let $\mathcal{C}$ be a category and let M be a monad on $\mathcal{C}$. If $\mathcal{C} \mathrel{\underset{\xleftarrow[R]{}}{\overset{\xrightarrow{L}}{\perp}}} \mathcal{D}$ is an adjunction (with counit ϵ and unit η), we say it* gives rise to *M if $M = RL$, $m = R\epsilon L$ and $u = \eta$.*

Any such adjunction gives rise to an M-multiplicative natural transformation $\psi\colon LM \Rightarrow L$. This gives us a fully faithful functor from the category of adjunctions giving rise to M to the category of triples $(\mathcal{D}, F, \psi)$ where ψ is M-multiplicative.

The proof of Proposition 1.7 essentially comes down to the following factorization result. If $f\colon a \to b$ is a morphism in Kl_M, then f may be factorized as

$$f = a \xrightarrow{Jf} Mb \xrightarrow{\phi_b} b\,,$$

where we use 'f' to refer both to the morphism $a \to b$ in Kl_M and to the underlying morphism $a \to Mb$ in $\mathcal{C}$. Indeed, if we compute this composite inside $\mathcal{C}$, we get

$$a \xrightarrow{f} Mb \xrightarrow{u_{Mb}} MMb \xrightarrow{M\,\mathrm{id}} MMb \xrightarrow{m_b} Mb\,,$$

which is equal to f by the coherence conditions on m and u. This means that the Kleisli category may be thought of as being freely generated from the original category $\mathcal{C}$ and a multiplicative natural transformation ϕ.

Example 1.9. The morphisms in the Kleisli category for the nonempty powerset monad $\mathcal{P}_+$ on **Set** are functions $A \to \mathcal{P}_+B$, which can be thought of as nondeterministic functional programs. Given a set A, the morphism $\phi_A\colon \mathcal{P}_+A \to A$ in $\mathrm{Kl}_{\mathcal{P}_+}$ can be interpreted as a 'nondeterministic choice' function that accepts a nonempty set of elements of A and nondeterministically chooses one of them. The factorization then means that the category is freely generated over $\mathcal{C}$ by these nondeterministic choice morphisms.

Example 1.10. Let $\mathcal{C}$ be a Cartesian closed category and let z be some fixed object of $\mathcal{C}$. Then the Kleisli category for the reader monad R_z on $\mathcal{C}$ is generated over $\mathcal{C}$ by a natural transformation $\phi_y\colon (z \to y) \to y$. By the enriched Yoneda lemma, such a natural transformation is always given by precomposition with some fixed morphism $\mathsf{ask}_z\colon 1 \to z$. This means that Kl_{R_z} is suitable for modelling any situation in which we are generally working in $\mathcal{C}$, but need the ability to request a value of type z (for example, a config file, a piece of user input or something else that isn't being passed into the function in question).

A particularly important fact about the reader monad in Cartesian closed categories is the following.

Theorem 1.11 ([Lam74])**.** *Let $\mathcal{C}$ be a Cartesian closed category and let z be an object of $\mathcal{C}$. Then the Kleisli category Kl_{R_z} for the reader monad over z on $\mathcal{C}$ is Cartesian closed.*

The *functional completeness* theorem [Lam74] can be thought of as a special case of our remarks above.

1.3 Denotational Semantics

From now till the end of the chapter, we fix an (order-enriched) Cartesian closed category $\mathcal{G}$ that admits a denotational semantics of Idealized Algol satisfying Computational Adequacy and in which every compact element is definable. The prototypical example, of course, will be the category of games and visible strategies, but we will not exploit any properties of this model beyond the ones we have already mentioned, mentioning it only in examples where appropriate.

Let $X \in \{\mathbb{B}, \mathbb{N}, \mathbb{C}\}$ be a set that has an interpretation as an Idealized Algol type X, and write X also for the corresponding object of $\mathcal{G}$. Write $\mathcal{G}_X$ as a shorthand for $\mathrm{Kl}_{R_X} \mathcal{G}$, the Kleisli category for the reader monad on $\mathcal{G}$ corresponding to the object X. The purpose of the rest of this chapter will be to define a new language, give it a denotational semantics in $\mathcal{G}_X$, and prove a full abstraction result for this denotational semantics.

Definition 1.12 (The language IA_X)**.** The language IA_X is formed by taking Idealized Algol, and adding to it a new constant

$$\mathsf{ask}_X$$

with typing rule

$$\frac{}{\Gamma \vdash \mathsf{ask}_X \colon X} \, .$$

From Proposition 1.7, we know that there is a distinguished natural transformation $\phi_A \colon (X \to A) \to A$ in $\mathcal{G}_X$; in particular, we have a morphism

$$\phi = \phi_X(\mathrm{id}_X) \colon 1 \to X \, ,$$

which will be the denotation of the term choose_X. Together with the existing denotational semantics of Idealized Algol within $\mathcal{G}$, this gives us an inductively defined denotational semantics of IA_X within $\mathcal{G}_X$.

Clearly any term-in-context of IA_X is of the form

$$\Gamma \vdash M[\mathsf{ask}_X / x] \colon T \, ,$$

where

$$\Gamma, x \colon X \vdash M \colon T$$

is a judgement of Idealized Algol. Given such a term-in-context, we know that the denotation of

$$\Gamma \vdash (\lambda x.M) \, \mathsf{ask}_X \colon T$$

is given by the composite

$$1 \xrightarrow{\phi} X \xrightarrow{[\![\Gamma, x \vdash M]\!]} [\![T]\!] \, .$$

Now this last term is β-equivalent to our original term-in-context $\Gamma \vdash M$. Since $\mathcal{G}_X$ is Cartesian closed (by Theorem 1.11), the β rule is valid in $\mathcal{G}_X$, and this means that the composite above is an alternative definition of the denotation of $\Gamma \vdash M$.

1.4 Operational Semantics

We now define the operational semantics of IA_X and prove a computational adequacy result for our denotational semantics.

Definition 1.13 (Operational semantics of IA_X)**.** Let X^* be the free monoid on the set X; i.e., the set of all finite strings of elements of X. Given $u, v \in X^*$ we shall write $u +\!\!+ v$ for their product in X^*; i.e., the concatenation of the two strings. We shall write ϵ for the unit in X^*; i.e., the empty string.

If $u \in X^*$,we write $|u|$ for the length of u. If $0 \leq n < |u|$, then we write $u^{(n)}$ for the corresponding element of u, numbering from 0.

We inductively define a relation $\Gamma, s \vdash M \Downarrow_u c, s'$, where Γ is a $\mathtt{Var}$-context, M, c are terms of IA_X with all free variables in Γ, where c is an IA canonical form, s, s' are Γ-stores and $u \in X^*$. The definition of this relation is shown in Figure 1.

We can define this semantics in an alternative, indirect way. Note that each rule from ordinary Idealized Algol takes the form

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

Here, we have interpreted each IA rule as an infinite scheme of rules ranging over the different terms M_i, M that the rule can apply to. We first extend this rule to a rule for IA_X, by allowing the M_i, M to range over terms of IA_X. We then replace the rule with the new rule

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

to give us an operational rule for IA_X (if $n = 0$, then we treat the empty string ϵ as the empty concatenation). Lastly, we add the rule for the new constant ask_X:

$$\frac{}{\Gamma, s \vdash \mathsf{ask}_X \Downarrow_x x, s} \; x \in X \quad .$$

This rule is the only nondeterministic one in our language, as well as being the only one in which the sequence annotating the $\Downarrow$ symbol at the bottom is not formed from concatenating together the sequences on the top.

Example 1.14. If $X = \mathbb{C}$, then, since X has a single element, a sequence n of elements of X may be identified with its length n. In this case, the language IA_X gives us a way to model time complexity, and the term ask_X may be considered as a constant $\mathsf{sleep}\colon \mathsf{com}$ whose semantics is to wait for some fixed period of time before continuing. In this case,

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

is interpreted to say that 'M converges to c in time n'.

$$\frac{}{\Gamma, s \vdash c \Downarrow_{\epsilon} c, s} \qquad \frac{\Gamma, s \vdash M \Downarrow_u \lambda x.M', s' \qquad \Gamma, s' \vdash M'[N/x] \Downarrow_v c, s''}{\Gamma, s \vdash MN \Downarrow_{u+\!\!+v} c, s''}$$

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

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

$$\frac{\Gamma, s \vdash M \Downarrow_u \mathsf{skip}, s' \qquad \Gamma, s' \vdash N \Downarrow_v c, s''}{\Gamma, s \vdash M; N \Downarrow_{u+\!\!+v} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_u \mathbb{t}, s' \qquad \Gamma, s' \vdash N \Downarrow_v c, s''}{\Gamma, s \vdash \mathsf{If}\, M\, \mathsf{then}\, N\, \mathsf{else}\, P \Downarrow_{u+\!\!+v} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_u \mathbb{f}, s' \qquad \Gamma, s' \vdash P \Downarrow_v c, s''}{\Gamma, s \vdash \mathsf{If}\, M\, \mathsf{then}\, N\, \mathsf{else}\, P \Downarrow_{u+\!\!+v} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_u 0, s' \qquad \Gamma, s' \vdash N \Downarrow_v c, s''}{\Gamma, s \vdash \mathtt{If0}\, M\, \mathsf{then}\, N\, \mathsf{else}\, P \Downarrow_{u+\!\!+v} c, s''}$$

$$\frac{\Gamma, s \vdash M \Downarrow_u n+1, s' \qquad \Gamma, s' \vdash P \Downarrow_v c, s''}{\Gamma, s \vdash \mathtt{If0}\, M\, \mathsf{then}\, N\, \mathsf{else}\, P \Downarrow_{u+\!\!+v} c, s''}$$

$$\frac{\Gamma, s \vdash E \Downarrow_u n, s' \qquad \Gamma, s' \vdash V \Downarrow_v x, s''}{\Gamma, s \vdash V \leftarrow E \Downarrow_{u+\!\!+v} \mathsf{skip}, (s''|x \mapsto n)}\ x \in \Gamma \qquad \frac{\Gamma, s \vdash V \Downarrow_u x, s'}{\Gamma, s \vdash !V \Downarrow_u n, s'}\ s'(x) = n$$

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

$$\frac{\Gamma, s \vdash E \Downarrow_u n, s' \qquad \Gamma, s' \vdash V \Downarrow_v \mathsf{mkvar}\, WR, s'' \qquad \Gamma, s'' \vdash Wn \Downarrow_w \mathsf{skip}, s'''}{\Gamma, s \vdash V \leftarrow E \Downarrow_{u+\!\!+v+\!\!+w} \mathsf{skip}, s'''}$$

$$\frac{\Gamma, s \vdash V \Downarrow_u \mathsf{mkvar}\, WR, s' \qquad \Gamma, s' \vdash R \Downarrow_v n, s''}{\Gamma, s \vdash !V \Downarrow_{u+\!\!+v} n, s''}$$

$$\frac{}{\Gamma, s \vdash \mathsf{ask}_X \Downarrow_x x, s}\ x \in X$$

Figure 1: Operational semantics for IA_X. All the rules except the last one are deterministic and may be obtained from the corresponding rules of Idealized Algol by suitably annotating the $\Downarrow$ relation with sequences from X^*.

Example 1.15. If $X \in \{\mathbb{B}, \mathbb{N}\}$, then the language IA_X gives us a way to model nondeterminism, where ask_X behaves as a *nondeterministic oracle*; i.e., a device that nondeterministically returns an element of X.

If $X = \mathbb{B}$ then we have a model of binary (i.e., finite) nondeterminism, whereas if $X = \mathbb{N}$ then we have a model of countable nondeterminism.

We interpret the relation

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

as saying that M converges to c in the case that the sequence of values returned by the nondeterministic oracle is given by the sequence u.

1.5 Soundness

To prove our adequacy result for the operational semantics of IA_X, we first give some definitions.

Definition 1.16. Fix some constant value $\top \in X$ (the precise value does not matter). We inductively define terms in context $\mathrm{tr}_u \colon \mathtt{nat} \to X$ of *ordinary deterministic* Idealized Algol for each $u \in X^*$ as follows.

$$\mathrm{tr}_\epsilon = \lambda n.\top \qquad \mathrm{tr}_{xu} = \lambda n.\, \mathsf{new}(\lambda v.v \leftarrow n; \mathtt{If0}!v \;\mathsf{then}\; x \;\mathsf{else}\; \mathrm{tr}_u(\mathtt{pred}!v))$$

Proposition 1.17. *Let $u \in X^*$ and let $n < |u|$. Then it is possible to deduce that*

$$\frac{\Gamma, s \vdash M \Downarrow n, s'}{\Gamma, s \vdash \mathrm{tr}_u\, M \Downarrow u^{(n)}, s'}$$

in Idealized Algol.

Proof. Induction on $|u|$ and on n. Since $n < u$, u must be non-empty, of the form xu'.

Suppose $n = 0$. Then $u^{(n)} = x$, and we have a derivation of $\Gamma, s \vdash \mathrm{tr}_{xu}\, M \Downarrow x, s'$ from $\Gamma, s \vdash M \Downarrow n, s'$ as shown in Figure 2a.

Now suppose that $n = m + 1$. Then $(xu)^{(m+1)} = u^{(m)}$. Then we have a derivation of $\Gamma, s \vdash \mathrm{tr}_{xu}\, M \Downarrow u^{(m)}, s'$ from $\Gamma, s \vdash M \Downarrow n, s'$ in Figure 2b, using the inductive hypothesis to tell us that we may derive

$$\frac{\Gamma, v, (s'|v \mapsto m+1) \vdash \mathtt{pred}!v \Downarrow m, (s'|v \mapsto m+1)}{\Gamma, v, (s'|v \mapsto m+1) \vdash \mathrm{tr}_u(\mathtt{pred}!v) \mapsto u^{(m)}, (s'|v \mapsto m+1)} \;. \qquad \square$$

We need a small lemma to help us deal with substitution.

$$\dfrac{\dfrac{\dfrac{\Gamma, v, (s|v \mapsto 0) \vdash M \Downarrow 0, (s'|v \mapsto 0) \quad \dfrac{}{\Gamma, v, (s'|v \mapsto 0) \vdash v \Downarrow v, (s'|v \mapsto 0)}}{\Gamma, v, (s|v \mapsto 0) \vdash v \leftarrow M \Downarrow \mathsf{skip}, (s'|v \mapsto 0)} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, v, (s'|v \mapsto 0) \vdash v \Downarrow v, (s'|v \mapsto 0)}}{\Gamma, v, (s'|v \mapsto 0) \vdash !v \Downarrow 0, (s'|v \mapsto 0)} \quad \dfrac{}{\Gamma, v, (s'|v \mapsto 0) \vdash x \Downarrow x, (s'|v \mapsto 0)}}{\Gamma, v, (s'|v \mapsto 0) \vdash \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v) \Downarrow x, (s'|v \mapsto 0)}}{\dfrac{\Gamma, v, (s|v \mapsto 0) \vdash v \leftarrow M; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v) \Downarrow x, (s'|v \mapsto 0)}{\Gamma, s \vdash \mathsf{new}(\lambda v.v \leftarrow M; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v)) \Downarrow x, s'}}}{\Gamma, s \vdash \lambda n.\ \mathsf{new}(\lambda v.v \leftarrow n; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v))M \Downarrow x, s'}$$

(a) IA derivation that if $M \Downarrow 0$ then $\mathrm{tr}_u\, M$ converges to the first element of the sequence u.

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\dfrac{}{\Gamma, v, (s'|v \mapsto 0) \vdash v \Downarrow v, (s'|v \mapsto 0)} \\ \Gamma, v, (s|v \mapsto 0) \vdash M \Downarrow m+1, (s'|v \mapsto 0)\end{array}}{\Gamma, v, (s|v \mapsto 0) \vdash v \leftarrow M \Downarrow \mathsf{skip}, (s'|v \mapsto m+1)} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, v, (s'|v \mapsto m+1) \vdash v \Downarrow v, (s'|v \mapsto m+1)}}{\Gamma, v, (s'|v \mapsto m+1) \vdash !v \Downarrow m+1, (s'|v \mapsto m+1)} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, v, (s'|v \mapsto m+1) \vdash v \Downarrow v, (s'|v \mapsto m+1)}}{\Gamma, v, (s'|v \mapsto m+1) \vdash !v \Downarrow m+1, (s'|v \mapsto m+1)}}{\Gamma, v, (s'|v \mapsto m+1) \vdash \mathsf{pred!}v \Downarrow m, (s'|v \mapsto m+1)}}{\Gamma, v, (s'|v \mapsto m+1) \vdash \texttt{tr}_u(\mathsf{pred!}v) \Downarrow u^{(m)}, (s'|v \mapsto m+1)}}{\Gamma, v, (s'|v \mapsto m+1) \vdash \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v) \Downarrow u^{(m)}, (s'|v \mapsto m+1)}}{\Gamma, v, (s|v \mapsto 0) \vdash v \leftarrow M; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v) \Downarrow u^{(m)}, (s'|v \mapsto m+1)}}{\Gamma, s \vdash \mathsf{new}(\lambda v.v \leftarrow M; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v)) \Downarrow u^{(m)}, s'}}{\Gamma, s \vdash \lambda n.\texttt{new}(\lambda v.v \leftarrow n; \texttt{If0!}v\ \mathsf{then}\ x\ \mathsf{else}\ \texttt{tr}_u(\mathsf{pred!}v))M \Downarrow u^{(m)}, s'}$$

(b) IA derivation that if $M \Downarrow m+1$ then $\mathrm{tr}_u\, M$ converges to the $m+1$-th element of the sequence u.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, v, (s|v \mapsto k) \vdash v \Downarrow v, (s|v \mapsto k)}}{\Gamma, v, (s|v \mapsto k) \vdash !v \Downarrow k, (s|v \mapsto k)}}{\Gamma, v, (s|v \mapsto k) \vdash \mathsf{succ!}v \Downarrow k+1, (s|v \mapsto k)} \quad \dfrac{}{\Gamma, v, (s|v \mapsto k) \vdash v \Downarrow v, (s|v \mapsto k)}}{\Gamma, v, (s|v \mapsto k) \vdash v \leftarrow \mathsf{succ!}v \Downarrow \mathsf{skip}, (s|v \mapsto k+1)} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, v, (s|v \mapsto k+1) \vdash v \Downarrow v, (s|v \mapsto k+1)}}{\Gamma, v, (s|v \mapsto k+1) \vdash !v \Downarrow k+1, (s|v \mapsto k+1)}\ \textsc{Prop. 1.17}}{\Gamma, v, (s|v \mapsto k+1) \vdash \texttt{tr}_w!v \Downarrow x, (s|v \mapsto k+1)}}{\Gamma, v, (s|v \mapsto k) \vdash v \leftarrow \mathsf{succ!}v; \texttt{tr}_w!v \Downarrow x, (s|v \mapsto k+1)}$$

(c) IA derivation that $(x \mapsto k), v \leftarrow \texttt{succ!}v; \mathrm{tr}_w!v$ converges to the $k+1$-th term of w.

Lemma 1.18. *Let*

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

be an inference, where the M_i,M are terms of IA_X and the whole inference satisfies one of the patterns of the Idealized Algol rules. Let Q be a fixed term of type X. Then

$$\frac{\Gamma, s^{(0)} \vdash M_1[Q/\,\mathsf{ask}_X] \Downarrow c_1, s^{(1)} \qquad \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n[Q/\,\mathsf{ask}_X] \Downarrow c_n, s^{(n)}}{\Gamma, s^{(0)} \vdash M[Q/\,\mathsf{ask}_X] \Downarrow c, s^{(n)}},$$

is a valid inference of Idealized Algol.

Proof. The real reason this is true is that the term ask_X is not mentioned anywhere in the IA rules, so substitution of the term N for ask could not possibly break the pattern. Formally, we can show this by inspection on each of the different rules. For instance, if the original rule is the one for sequencing:

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

then we have $(M;N)[Q/\,\mathsf{ask}_X] = M[P/\,\mathsf{ask}_X]; N[P/\,\mathsf{ask}_X]$ and the inference

$$\frac{\Gamma, s \vdash M[Q/\,\mathsf{ask}_X] \Downarrow \mathsf{skip}, s' \qquad \Gamma, s' \vdash N[Q/\,\mathsf{ask}_X] \Downarrow c, s''}{\Gamma, s \vdash M[Q/\,\mathsf{ask}_X]; N[P/\,\mathsf{ask}_X] \Downarrow c, s''}$$

is still a valid instance of the sequencing rule. □

We can now state and prove our soundness lemma.

Lemma 1.19. *Suppose that*

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

in IA_X. Fix $k \in \mathbb{N}$ and let $w \in X^*$ be a sequence such that u is a subsequence of w starting at position $k+1$ (i.e., $u^{(j)} = w^{(k+j+1)}$ for each $j = 0, \cdots, |u|-1$). Then

$$\Gamma, v\colon \mathtt{Var}, (s|v \mapsto k) \vdash M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_w!v/\,\mathsf{ask}_v] \Downarrow c, (s'|v \mapsto k + |u|)$$

in Idealized Algol.

Proof. Structural induction on the derivation.

Suppose that the last rule we use comes from one of the Idealized Algol rules. That is, there is an inference

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

derived from one of the Idealized Algol schemas, and we have replaced it with the rule

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

where each of the relations $\Gamma, s^{(i-1)} \vdash M_i \Downarrow_{u_i} c_i, s^{(i)}$ is derivable in IA_X.

Fix $k \in \mathbb{N}$ and a sequence w such that $u_1 +\!\!+ \cdots +\!\!+ u_n$ is a subsequence of w starting at position $k{+}1$. In particular, for each $i = 1, \cdots, n$, u_i is a subsequence of w starting at position $k + \sum_{j=1}^{i-1} |u_j| + 1$.

Then by the inductive hypothesis, we know that for each $i = 1, \cdots, n$, the relation

$$\Gamma, v, (s^{(i-1)}|v \mapsto k + \sum_{j=1}^{i-1} |u_j|) \vdash M_i[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/\,\mathsf{ask}_v] \Downarrow c, (s^{(i)}|v \mapsto k + \sum_{j=1}^{i} |u_j|)$$

is derivable in Idealized Algol. Then we may apply the Idealized Algol inference and Lemma 1.18 to deduce that

$$\Gamma, v, (s^{(0)}|v \mapsto k) \vdash M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/\,\mathsf{ask}_v] \Downarrow c, (s^{(n)}|v \mapsto k + \sum_{i=1}^{n} |u_n|) \,,$$

as desired.

Now suppose instead that the last rule was the new one for ask_X; i.e.,

$$\frac{}{\Gamma, s \vdash \mathsf{ask}_X \Downarrow_x x, s} \,,$$

where $x \in X$. Fix some $k \in \mathbb{N}$ and some w such that the single term x is a subsequence of w starting at position $k+1$; i.e., that $x = w^{(k+1)}$. Then we would like to derive that

$$\Gamma, v, (s|v \mapsto k) \vdash v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v \Downarrow x, (s|v \mapsto k+1) \,,$$

which we can do using the derivation in Figure 2c, where we have used Proposition 1.17 to deal with the tr_w term.

This completes the induction. □

In light of Lemma 1.19, we can state our soundness result.

First recall the statement of Computational Adequacy for $\mathcal{G}$:

Proposition 1.20. *Let $M\colon$ `com` be a closed term of Idealized Algol and suppose that*

$$, () \vdash M \Downarrow \mathsf{skip}, () \,.$$

Then $[\![M]\!] \neq \bot$.

Definition 1.21. Let $u \in X^*$. Let $u^\top$ be the sequence formed by appending some fixed value $\top \in X$ to the start of u, so that u is the subsequence of $u^\top$ running from position 1 up to position $|u|$. Define a morphism

$$\eta_u = [\![f \colon X \to \mathtt{com} \vdash \lambda v. f(v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v); !v]\!] : (X \to \mathbb{C}) \to (\mathtt{Var} \to \mathbb{N})$$

in $\mathcal{G}$.

Definition 1.22. Let n be a natural number. We define terms $\mathrm{test}_n \colon \mathtt{nat} \to \mathtt{com}$ inductively by

$$\mathrm{test}_0 = \lambda m.\, \mathtt{If0}\, m \;\mathsf{then\ skip\ else}\; \Omega$$

$$\mathrm{test}_{n+1} = \lambda m.\, \mathtt{If0}\, m \;\mathsf{then}\; \Omega \;\mathsf{else}\; \mathrm{test}_n(\mathtt{pred}\, m)\,.$$

So test_n converges if its input evaluates to n and diverges otherwise.

We then define $t_n \colon \mathbb{N} \to \mathbb{C}$ to be the denotation of test_n in $\mathcal{G}$.

Proposition 1.23 (Soundness). *Let $M \colon \mathtt{com}$ be a closed term of IA_X, let $u \in X^*$ be a sequence and suppose that*

$$, () \vdash M \Downarrow_u \mathsf{skip}, ()\,.$$

Let the denotation $[\![M]\!] : 1 \to \mathtt{com}$ in $\mathcal{G}_X$ be considered as a morphism $1 \to (X \to \mathbb{C})$ in $\mathcal{G}$. Then the composite

$$1 \xrightarrow{[\![M]\!]} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

is not equal to $\perp$.

Proof. Since the β rule is valid in $\mathcal{G}_X$, this composite is equal to the denotation of the term

$$\mathrm{test}_{|u|}(\mathtt{new}(\lambda v. M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \mathsf{ask}_X]; !v))$$

in IA. By the adequacy result for Idealized Algol, it suffices to show that this term converges to skip; i.e., that the term

$$\mathtt{new}(\lambda v. M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \mathsf{ask}_X]; !v)$$

converges to $|u|$ in IA.

We can prove this using the following derivation tree.

$$\dfrac{\dfrac{\textsc{Lem. } 1.19 \quad \dfrac{}{v, (v \mapsto 0) \vdash M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \mathsf{ask}_x] \Downarrow \mathsf{skip}, (v \mapsto |u|)} \qquad \dfrac{\dfrac{}{v, (v \mapsto |u|) \vdash v \Downarrow v, (v \mapsto |u|)}}{v, (v \mapsto |u|) \vdash !v \Downarrow |u|, (v \mapsto |u|)}}{v, (v \mapsto 0) \vdash M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \mathsf{ask}_X]; v \Downarrow |u|, (v \mapsto |u|)}}{, () \vdash \mathtt{new}(\lambda v. M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \mathsf{ask}_X]; !v) \Downarrow |u|, ()}$$

□

The statement of Proposition 1.23 looks a bit strange. This is because the level of generality we are operating at (i.e., $\mathcal{G}$ being a fairly general model for Idealized Algol) does not give us much room to define things other than in terms of the denotations of Idealized Algol terms.

If $\mathcal{G}$ is the category of games and visible strategies, then the statements of Proposition 1.23 (and our later Adequacy and Full Abstraction results) become clearer. Observe that if $\sigma\colon 1 \to (X \to \mathbb{C})$ is a strategy in $\mathcal{G}$ (considered as a strategy for $!X \multimap \mathbb{C}$, then the maximal plays in the interaction

$$\sigma || (\eta_u ; [\![\mathsf{new}]\!])$$

take the form

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

for $k \leq |u|$ or

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

for $k > |u|$, where the component in $X, \mathbb{C}$ is a valid play of σ. Moreover, the strategy t_n is the one with maximal plays of the form

$$\begin{array}{cc} \mathbb{N} & \mathbb{C} \\ & q \\ q & \\ n & \\ & a \end{array}$$

or

$$\begin{array}{cc} \mathbb{N} & \mathbb{C} \\ & q \\ q & \\ m & \end{array}$$

for $m \neq n$.

This means that the composite

$$1 \xrightarrow{\sigma} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_n} \mathbb{C}$$

is not equal to $\perp$ if and only if σ contains the sequence

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

Since complete plays in the game $!X \multimap \mathbb{C}$ are always of the form q, followed by some sequence of pairs of the form qx_i for $x \in X$, followed by a, this is a very natural condition to consider when dealing with a strategy $\sigma\colon !X \multimap \mathbb{C}$.

1.6 Computational Adequacy

Now we want to prove Computational Adequacy; i.e., the converse to Proposition 1.23. To do this, we need to prove a converse to Lemma 1.19.

First of all, we need to prove a reverse result to Lemma 1.18 that deals with substitution in the opposite direction; i.e., instead of telling us what happens when we substitute a term for ask_X, we will look at what happens when we substitute a term for $v \leftarrow \mathtt{succ}!v; \mathrm{tr}_u!v$.

In most cases, this will not disrupt the structure of the IA rule. For instance, we always have

$$(!V)[Q/v \leftarrow \mathtt{succ}!v; \mathrm{tr}_u!v] =!(V[Q/v \leftarrow \mathtt{succ}!v; \mathrm{tr}_u!v])\,,$$

and so the derivation

$$\frac{\Gamma, s \vdash V[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow v, s'}{\Gamma, s \vdash !V[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow n, s'}\ s'(v) = n$$

still follows the pattern of the Idealized Algol rule for variable dereference.

There is only one case where this breaks down. Consider the following instance of the sequencing rule.

$$\frac{\Gamma, v, s \vdash v \leftarrow \mathsf{succ}!v \Downarrow \mathsf{skip}, s' \qquad \Gamma, v, s' \vdash \mathrm{tr}_u!v \Downarrow x, s''}{\Gamma, v, s \vdash v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v \Downarrow x, s''}$$

In this case, substituting some term Q for $v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v$ in the top two terms will have no effect, whereas it will replace the whole of the bottom with Q, invalidating the whole inference.

We have proved the following.

Lemma 1.24. *Let*

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

be an inference of Idealized Algol. Let $u \in X^*$ and let $Q \colon X$ be a term of IA_X. Fix an unused variable name v and suppose that $M \neq v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v$. Then

$$\frac{\begin{array}{c}\Gamma, s^{(0)} \vdash M_1[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow c_1, s^{(1)} \\ \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow c_n, s^{(n)}\end{array}}{\Gamma, s^{(0)} \vdash M[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow c, s^{(n)}}$$

conforms to the same Idealized Algol pattern. In particular, if $w_1, \cdots, w_n \in X^*$, then

$$\frac{\begin{array}{c}\Gamma, s^{(0)} \vdash M_1[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow_{w_1} c_1, s^{(1)} \\ \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow_{w_n} c_n, s^{(n)}\end{array}}{\Gamma, s^{(0)} \vdash M[Q/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v] \Downarrow_{w_1 +\!\!+ \cdots +\!\!+ w_n} c, s^{(n)}}$$

is a valid inference of IA_X.

We need one more lemma to help us deal with substitution.

Lemma 1.25. *Suppose that $\Gamma, y \vdash M \colon T$ is a typing judgement of Idealized Algol, where Γ is a* `Var`*-context and y is a free variable of type X. Fix $u \in X^*$. Suppose that $M \neq y$ and that we have some inference*

$$\frac{\Gamma, s^{(0)} \vdash N_1 \Downarrow c_1, s^{(1)} \qquad \cdots \qquad \Gamma, s^{(n-1)} \vdash N_n \Downarrow c_n, s^{(n)}}{\Gamma, s^{(0)} \vdash M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y] \Downarrow c, s^{(n)}}.$$

of Idealized Algol. Then each N_i may be written as $M_i[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y]$ for some $\Gamma, y \vdash M_i$.

Proof. This can be checked case-by-case. The most interesting is the case for sequencing: if $M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y] \neq v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v$, then we must have

$$M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y] = N[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y]; P[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y]\,,$$

which is deduced from $N[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y]$ and $P[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y]$. □

Now we can state and prove our adequacy lemma.

Lemma 1.26. *Suppose that $w \in X^*$ is a sequence of length greater than or equal to k, l and that*

$$\Gamma, v, (s|v \mapsto k) \vdash M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y] \Downarrow c, (s'|v \mapsto l)$$

is derivable in Idealized Algol, where v is not free in M and y is a variable name of type X. Then $l \geq k$ and

$$\Gamma, s \vdash M[\mathsf{ask}_X\,/y] \Downarrow_u c, s'$$

in IA_X, where u is the subsequence of w consisting of all terms from $k+1$ up to l.

Proof. Induction on the derivation.

Suppose that $M \neq y$. Then, by Lemma 1.25, the last step in the derivation of $M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y]$ must be of the form

$$\frac{\begin{array}{c}\Gamma, s^{(0)} \vdash M_1[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y] \Downarrow c_1, s^{(1)} \\ \cdots \qquad \Gamma, s^{(n-1)} \vdash M_n[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y] \Downarrow c_n, s^{(n)}\end{array}}{\Gamma, s^{(0)} \vdash M[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y] \Downarrow c, s^{(n)}}\,,$$

where each $M_i[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_w!v/y]$ is derivable in Idealized Algol.

By the inductive hypothesis, $s^{(i-1)}(v) \leq s^{(i)}(v)$ for each i and so $s^{(0)}(v) \leq s^{(n)}(v)$, as desired (in the case that there are no premises – i.e., the case of the rule for canonical forms – we have $s^{(0)}(v) = s^{(0)}(v)$). Moreover, by the inductive hypothesis, it is derivable that

$$\Gamma, s^{(i-1)} \vdash M_i[\mathsf{ask}_X\,/y] \Downarrow_{u_i} c_i, s^{(i)}\,,$$

where u_i is the subsequence of w going from term $s^{(i-1)}(v)+1$ up to $s^{(i)}(v)$.

Now for any term $\Gamma, y \vdash P$, we have

$$P[\mathsf{ask}_X\,/y] = P[v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v/y][\mathsf{ask}_X\,/v \leftarrow \mathsf{succ}!v; \mathrm{tr}_u!v]\,,$$

and so by Lemma 1.24 we may derive

$$\Gamma, s^{(0)} \vdash M[\mathsf{ask}_X\,/y] \Downarrow_{u_1 +\!\!+ \cdots +\!\!+ u_n} c, s^{(n)}\,.$$

But $u_1 +\!\!+ \cdots +\!\!+ u_n$ is precisely the subsequence of w going from term $s^{(0)}(v)+1$ up to $s^{(n)}(v)$!

This completes the first case. The second case is where $M = y$. Suppose, then, that

$$\Gamma, v, (s|v \mapsto k) \vdash v \leftarrow \mathtt{succ}!v; \mathrm{tr}_w!v \Downarrow x, (s'|v \mapsto l)$$

is derivable in Idealized Algol.

Since IA is a deterministic language (so if $\Gamma, s \vdash M \Downarrow c, s'$ and $\Gamma, s \vdash M \Downarrow c', s''$ then $c = c'$ and $s' = s''$), then the derivation of this term must agree with the valid IA derivation given in Figure 2c. It follows that $l = k+1$ (so, in particular, $l \geq k$) and that x is the $(k+1)$-th term of w, so the single-term sequence x is the subsequence of w going from $k+1$ to l.

Then we have the derivation

$$\frac{}{\Gamma, s \vdash \mathsf{ask}_X \Downarrow_x x, s'}$$

in IA_X. This completes the induction. □

We can now prove computational adequacy for our model.

Proposition 1.27 (Computational adequacy)**.** *Let $M \colon \mathtt{com}$ be a closed term of IA_X. Consider the denotation $[\![M]\!] : 1 \to \mathbb{C}$ in $\mathcal{G}_X$ as a morphism $1 \to (X \to \mathbb{C})$ in $\mathcal{G}$. Let $u \in X^*$ be a sequence and suppose that the composite*

$$1 \xrightarrow{[\![M]\!]} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

is not equal to $\bot$. Then

$$, () \vdash M \Downarrow_u \mathsf{skip}, () \,.$$

Proof. As before, the composite given in the statement is the denotation of the term

$$\mathrm{test}_{|u|}(\mathtt{new}(\lambda v. M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \,\mathsf{ask}_X]; !v)), .$$

By the adequacy result for Idealized Algol, the fact that this denotation is not equal to $\bot$ means that the term converges to skip, from which we can deduce that

$$\mathtt{new}(\lambda v. M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \,\mathsf{ask}_X]; !v$$

converges to $|u|$.

It is easy to see that this is equivalent to derivability of the following relation in Idealized Algol.

$$v, (v \mapsto 0) \vdash M[v \leftarrow \mathtt{succ}!v; \mathrm{tr}_{u^\top}!v / \,\mathsf{ask}_X] \Downarrow \mathsf{skip}, (v \mapsto |u|)$$

Now u is the subsequence of $u^\top$ going from position 1 to position $|u|$. So Lemma 1.26 tells us that we must have

$$, () \vdash M \Downarrow_u \mathsf{skip}, ()$$

in IA$_X$. □

1.7 Full abstraction

To prove full abstraction of our semantics for IA$_X$, we introduce the usual intrinsic equivalence on terms.

Definition 1.28. Let $\sigma, \tau \colon A \to B$ be morphisms in $\mathcal{G}_X$. By currying, we may consider A and B as morphisms $1 \to (A \to B)$ in $\mathcal{G}_X$. We say that $\sigma \sim \tau$ if for all morphisms $\alpha \colon (A \to B) \to \mathbb{C}$ and for all sequences $u \in X^*$, if we regard the $\alpha; \sigma, \alpha; \tau \colon 1 \to \mathbb{C}$ as morphisms $X \to \mathbb{C}$ in $\mathcal{G}$, then the composites

$$1 \xrightarrow{\alpha;\sigma} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

$$1 \xrightarrow{\alpha;\tau} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

are equal.

Theorem 1.29 (Full abstraction)**.** *Let $M, N \colon T$ be closed terms of IA$_X$. Then M, N are observationally equivalent – i.e., for all contexts $C[-] \colon \mathtt{com}$ of IA$_X$ with a hole of type T and for all sequences $u \in X^*$,*

$$, () \vdash C[M] \Downarrow_u \mathsf{skip}, () \Longleftrightarrow, () \vdash C[N] \Downarrow_u \mathsf{skip}, () \text{ –}$$

if and only if $[\![M]\!] \sim [\![N]\!]$.

Proof. First, suppose that $[\![M]\!] \sim [\![N]\!]$. Let $C[-] \colon \mathtt{com}$ be a context with a hole of type T. Then the denotation of $t \vdash C[t]$ is a morphism $\alpha \colon [\![T]\!] \to \mathbb{C}$. Moreover, the denotation of $C[M]$ is the composite $\alpha; [\![M]\!]$ and that of $C[N]$ is the composite $\alpha; [\![N]\!]$, by functional completeness.

Then the composites

$$1 \xrightarrow{\alpha;\sigma} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

$$1 \xrightarrow{\alpha;\tau} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

are equal, so $C[M] \Downarrow_u \mathsf{skip}$ if and only if $C[N] \Downarrow_u \mathsf{skip}$ by Propositions 1.23 and 1.27.

Conversely, suppose that $M \not\sim N$. So there is some $\alpha \colon [\![T]\!] \to \mathbb{C}$ in $\mathcal{G}_X$ and some sequence u such that (without loss of generality),

$$(\alpha; [\![M]\!]); \eta_u; [\![\mathsf{new}]\!]\,; t_{|u|} \neq \bot \qquad\qquad (\alpha; [\![N]\!]); \eta_u; [\![\mathsf{new}]\!]\,; t_{|u|} = \bot\,.$$

Here, we have enclosed $\alpha; \llbracket M \rrbracket$ and $\alpha; \llbracket N \rrbracket$ in brackets to indicate that the composition is taken in the Kleisli category $\mathcal{G}_X$, and then the whole thing is considered as a morphism $1 \to (X \to \mathbb{C})$ in $\mathcal{G}$.

More specifically, these composites are given by the composites

$$1 \xrightarrow{\llbracket M \rrbracket} (\mathbb{C} \to \llbracket T \rrbracket) \xrightarrow{\mathbb{C} \to \alpha} (\mathbb{C} \to (\mathbb{C} \to \mathbb{C})) \xrightarrow{\mu} (\mathbb{C} \to \mathbb{C})$$

$$1 \xrightarrow{\llbracket N \rrbracket} (\mathbb{C} \to \llbracket T \rrbracket) \xrightarrow{\mathbb{C} \to \alpha} (\mathbb{C} \to (\mathbb{C} \to \mathbb{C})) \xrightarrow{\mu} (\mathbb{C} \to \mathbb{C})$$

in $\mathcal{G}$, where μ indicates precomposition with the diagonal.

Now α is the least upper bound of its compact approximans, so it follows that there is some compact $\alpha' \subseteq \alpha$ such that

$$\llbracket M \rrbracket \,; (\mathbb{C} \to \alpha'); \mu; \eta_u; \llbracket \mathsf{new} \rrbracket \,; t_{|u|} \neq \bot \qquad \llbracket N \rrbracket \,; (\mathbb{C} \to \alpha'); \mu; \eta_u; \llbracket \mathsf{new} \rrbracket \,; t_{|u|} = \bot \,.$$

Then, by compact definability in $\mathcal{G}$, α' is the denotation of some IA term $x\colon T \vdash C[x]\colon X \to \mathtt{com}$, which is therefore the denotation of the term $x\colon T \vdash C[x]\ \mathsf{ask}_X\colon \mathtt{com}$ in $\mathcal{G}_X$. So we get

$$\llbracket C[M] \rrbracket \,; \eta_u; \llbracket \mathsf{new} \rrbracket \,; t_{|u|} \neq \bot \qquad\qquad \llbracket C[N] \rrbracket \,; \eta_u; \llbracket \mathsf{new} \rrbracket \,; t_{|u|} = \bot \,,$$

and so $C[M] \Downarrow_u \mathsf{skip}$ by Proposition 1.27, while $C[N] \not\Downarrow_u \mathsf{skip}$ by Proposition 1.23. Therefore, M and N are observationally inequivalent in IA_X. □

1.8 Comparison with Ghica's slot games

Let us suppose now that $\mathcal{G}$ is the category of games and visible strategies, and that $X = \mathbb{C}$. As we remarked above, this means that IA_X can be interpreted as a language for modelling time complexity.

We compare our approach to a different one, due to Dan Ghica [Ghi05]. Given a game A, Ghica defines a *play with costs* in A to be a justified sequence $s \in (M_A + \{\textcircled{\$}\})^*$ such that $s|_{M_A} \in P_A$. Here, $\textcircled{\$}$ is a special symbol called a *slot* or *token-action*, which can be interleaved throughout the play $s|_{M_A}$ from A. We shall additionally impose the requirement that an occurrence of the special symbol $\textcircled{\$}$ must take place either after an O-move in A or after another instance of $\textcircled{\$}$. The token actions do not carry justification pointers.

Following Ghica, we define a *strategy with costs* to be a prefix-closed set σ of plays with costs such that the set $\sigma|_{M_A} = \{s|_{M_A} \,:\, s \in \sigma\}$ is a valid visible strategy for A.

The identity strategy with costs is the usual identity strategy, without any token actions. Given an interleaving $\mathfrak{s} \in (M_A + M_B + M_C + \{\textcircled{\$}\})^*$ of two justified plays with costs for $A \multimap B$ and $B \multimap C$, write $\mathfrak{s}|_{A,B}$ for the subsequence consisting of all those moves in A and B, together with all token actions such that the previous move was an O-move in $A \multimap B$. Define $\mathfrak{s}|_{B,C}$ similarly. Then if $\sigma\colon A \multimap B$ and $\tau\colon B \multimap C$ are strategies with costs, we define $\sigma\|\tau$ to be the set of all such sequences $\mathfrak{s}$ such that $\mathfrak{s}|_{A,B} \in \sigma$ and $\mathfrak{s}|_{B,C} \in \tau$. Lastly, we define $\sigma;\tau$ to be the set of all sequences obtained by taking a sequence $\mathfrak{s} \in \sigma\|\tau$ and removing all the moves in B (but retaining all the token actions, including those that arise between moves in B). The usual arguments apply to show that this is indeed a category.

This seems like a purely combinatorial construction, but it can actually be subsumed into our category-theoretic apparatus.

Proposition 1.30. *Let A be a game. Then there is a bijection*

$$c\colon \{\textit{normal strategies for } !\mathbb{C} \multimap A\} \leftrightarrow \{\textit{strategies with costs for } A\}$$

Moreover, this bijection respects composition: let $\sigma\colon !\mathbb{C} \multimap (A \to B)$ and $\tau\colon !\mathbb{C} \multimap (B \to C)$ be strategies. Write $\sigma;\tau$ for the Kleisli composition of σ and τ in $\mathcal{G}_{\mathbb{C}}$; i.e., the composite

$$!\mathbb{C} \xrightarrow{\mu} !\mathbb{C} \otimes !\mathbb{C} \xrightarrow{\sigma\otimes\tau} (A \multimap B) \otimes (B \multimap C) \xrightarrow{;} (A \multimap C)\,.$$

Then $c(\sigma;\tau) = c(\sigma);c(\tau)$. Moreover, $c(\mathrm{id}_A)$ is the identity in the category of games and strategies with costs.

Proof. The map c is the unique functor given by the functional completeness theorem that sends the canonical strategy $\mathrm{id}\colon !\mathbb{C} \to \mathbb{C}$ to the strategy with costs for $\mathbb{C}$ with maximal play

$$q\text{\textcircled{\$}}a\,.$$

More synthetically, we get from a strategy for $\sigma\colon !\mathbb{C} \multimap A$ to a strategy with costs for A by replacing each occurrence of the pair qa occurring in the $\mathbb{C}$ component with the token action \textcircled{\$} in each play of σ.

This functor is the identity on objects, and it is fully faithful, since it has an obvious inverse, given by taking a strategy with costs and replacing each occurrence of the token action with a pair of moves qa in $!\mathbb{C}$. Since each token action must always occur after an opponent move or after another token action, and since player O has no reply to the move q other than the move a, this always gives us a legal strategy. □

Therefore, we see that the category of games and strategies with costs is isomorphic to the Kleisli category $\mathcal{G}_{\mathbb{C}}$, which we have already shown to be fully abstract for a language with time complexity.

1.9 Alternative reduction rules - may testing

We remarked above that if $X \in \{\mathbb{B}, \mathbb{N}\}$, then IA_X is a model of nondeterminism, finite in the case of $\mathbb{B}$ and countable in the case of $\mathbb{N}$. However, our operational semantics is not the usual one for these languages.

For example, the terms

$$\mathsf{If}\ \mathsf{ask}_{\mathbb{B}}\ \mathsf{then}\mathbb{t}\ \mathsf{else}\ \mathbb{f}\colon \mathtt{bool} \qquad\qquad \mathsf{If}\ \mathsf{ask}_{\mathbb{B}}\ \mathsf{then}\mathbb{f}\ \mathsf{else}\ \mathbb{t}\colon \mathtt{bool}$$

are not observationally equivalent in our operational semantics; indeed, we have

$$\mathsf{If}\ \mathsf{ask}_{\mathbb{B}}\ \mathsf{then}\mathbb{t}\ \mathsf{else}\ \mathbb{f} \Downarrow_{\mathbb{t}} \mathbb{t} \qquad\qquad \mathsf{If}\ \mathsf{ask}_{\mathbb{B}}\ \mathsf{then}\mathbb{f}\ \mathsf{else}\ \mathbb{t} \Downarrow_{\mathbb{t}} \mathbb{f}\,.$$

However, these terms (which both nondeterministically choose either the true or the false value), *should* be observationally equivalent in any sensible nondeterministic semantics. The issue is the labelling on the reduction relations, which is saving too much information about the reduction of the term. Indeed, this is sort of the point of nondeterminism: we should be able to make nondeterministic choices without recording which value we used for that choice.

Definition 1.31 ([HM99])**.** If $X \in \{\mathbb{B}, \mathbb{N}\}$, we define an operational relation $\Downarrow$ ('may converge') on the language IA_X as follows. The rules for $\Downarrow$ are identical to the operational rules for Idealized Algol, with the addition of the following rule for the primitive ask_X.

$$\frac{}{\Gamma, s \vdash \mathsf{ask}_X \Downarrow x, s}\ x \in X$$

It is clear that these rules are exactly the same as our original operational semantics for IA_X, but with the sequences u removed. Moreover, if we have a valid derivation of $\Gamma, s \vdash M \Downarrow u, s'$, then it is clear (by induction) that we may annotate all the occurrences of $\Downarrow$ with suitable sequences in order to obtain a derivation of $\Gamma, s \vdash M \Downarrow_u c, s'$ for some $u \in X^*$. So we get the following alternative definition of may convergence.

Definition 1.32. We say that $\Gamma, s \vdash M \Downarrow c, s'$ if there is some $u \in X^*$ such that $\Gamma, s \vdash M \Downarrow_u c, s'$.

We can reflect this operational relation in the semantics by modifying the definition of intrinsic equivalence.

Firstly, an obvious consequence of Propositions 1.23 and 1.27 is that we have

Corollary 1.33. *Let $M\colon \mathtt{com}$ be a closed term of IA_X. Consider the denotation $[\![M]\!] : 1 \to \mathbb{C}$ in $\mathcal{G}_X$ as a morphism $1 \to (X \to \mathbb{C})$ in $\mathcal{G}$. Then there exists some sequence $u \in X^*$ such that the composite*

$$1 \xrightarrow{[\![M]\!]} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\mathtt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

if and only if

$$, () \vdash M \Downarrow \mathsf{skip}, ()\,.$$

In light of this result, we can define a new intrinsic equivalence on morphisms in $\mathcal{G}_X$:

Definition 1.34. Let $\sigma, \tau \colon A \to B$ be morphisms in $\mathcal{G}_X$, considered as morphisms $1 \to (A \to B)$ in $\mathcal{G}_X$. We say that $\sigma \sim_{\text{may}} \tau$ if for all $u \in X^*$ there exists $v \in X^*$ such that the composites

$$1 \xrightarrow{\alpha;\sigma} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\texttt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

$$1 \xrightarrow{\alpha;\tau} (X \to \mathbb{C}) \xrightarrow{\eta_v} (\texttt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|v|}} \mathbb{C}$$

are equal, and vice versa.

Then exactly the same argument as before gives us a full abstraction result for may-equivalence.

Theorem 1.35. *Let $M, N \colon T$ be closed terms of IA_X. Then M, N are may-observationally equivalent – i.e., for all contexts $C[-] \colon$ `com` of IA_X with a hole of type T,*

$$, () \vdash C[M] \Downarrow \mathsf{skip}, () \Leftrightarrow, () \vdash C[N] \Downarrow \mathsf{skip}, () \text{ –}$$

if and only if $[\![M]\!] \sim_{\text{may}} [\![N]\!]$.

Proof. Suppose that $[\![M]\!] \sim_{\text{may}} [\![N]\!]$. Let $C[-]$ be a context of IA_X, interpreted as a morphism $\alpha \colon [\![T]\!] \to \mathbb{C}$.

Suppose that $, () \vdash C[M] \Downarrow \mathsf{skip}, ()$. So there is some sequence $u \in X^*$ such that $, () \vdash C[M] \Downarrow_u \mathsf{skip}, ()$ and therefore the composite

$$1 \xrightarrow{\alpha;[\![M]\!]} (X \to \mathbb{C}) \xrightarrow{\eta_u} (\texttt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|u|}} \mathbb{C}$$

is not equal to $\bot$. Therefore, there exists some $v \in X^*$ such that the composite

$$1 \xrightarrow{\alpha;[\![N]\!]} (X \to \mathbb{C}) \xrightarrow{\eta_v} (\texttt{Var} \to \mathbb{N}) \xrightarrow{[\![\mathsf{new}]\!]} \mathbb{N} \xrightarrow{t_{|v|}} \mathbb{C}$$

Therefore, $, () \vdash C[N] \Downarrow_v \mathsf{skip}, ()$ and so $, () \vdash C[N] \Downarrow \mathsf{skip}, ()$. The reverse direction is identical.

Conversely, suppose that M, N are may-observationally equivalent. Then, as before, we can take α to be compact, whence definable, in Definition 1.34, and the proof continues as in the first part, but in reverse. □

Let us examine what this means in the category of games. If $\sigma \colon !X \multimap \mathbb{C}$ is a strategy, then, by our discussion at the end of §1.5, we know that, for any sequence u, the composite

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

is not equal to $\perp$ if and only if σ contains the play

$$q(qu^{(i)})_{i=0}^{|u|-1}a\,.$$

Moreover, since any complete play in $!X \multimap \mathbb{C}$ must take this form, we can see there exists such a u making the composite above not equal to $\perp$ if and only if

$$qa \in \{s|_{\mathbb{C}} \,:\; s \in \sigma \text{ is complete}\}\,.$$

This suggests a general equivalence relation on Kleisli morphisms in $\mathcal{G}_X$: given a strategy $\sigma\colon !X \multimap A$, we write $\sigma|A$ for the set

$$\{s|_A \,:\; s \in \sigma \text{ is complete}\}\,.$$

We say that two strategies $\sigma, \tau\colon !X \multimap A$ are may-equivalent, and write $\sigma \approx_{\text{may}} \tau$, if

$$\sigma|_A = \tau|_A\,.$$

In this case, Corollary 1.33 tells us that $M \Downarrow \mathsf{skip}$ if and only if $\sigma \approx_{\text{may}} \tau$.

We need to show that this respects composition, so that we get a category if we take the quotient by this equivalence relation.

Proposition 1.36. *Let $\sigma, \sigma'\colon A \to B$, $\tau, \tau'\colon B \to C$ be morphisms in $\mathcal{G}_X$. Suppose that $\sigma \approx_{\text{may}} \sigma'$ and $\tau \approx_{\text{may}} \tau'$. Then $\sigma;\tau \approx_{\text{may}} \sigma';\tau'$.*

Proof. A complete play in $\sigma;\tau$ is given by a sequence $\mathfrak{s}|_{X,A,C}$, where $\mathfrak{s} \in (M_X + M_A + M_B + M_C)^*$ that is a legal interaction of a complete play in τ with a collection of complete plays in σ, with B-components being identified. Then $\mathfrak{s}|_{A,C}$ can alternatively be characterized as $\mathfrak{t}|_{A,C}$, where $\mathfrak{t} \in (M_A + M_B + M_C)^*$ is a legal interaction of a sequence from $\tau|_{B,C}$ with a collection of sequences from $\sigma|_{A,B}$.

It follows that if $\sigma|_{A,B} = \sigma'|_{A,B}$ and $\tau|_{B,C} = \tau'|_{B,C}$, then $\sigma;\tau|_{A,C} = \sigma';\tau'|_{A,C}$. □

Now we can also see that this equivalence we have just defined is subsumed into the intrinsic equivalence.

Proposition 1.37. *Let $\sigma, \tau\colon !X \multimap A$ be strategies. If $\sigma \approx_{\text{may}} \tau$ then $\sigma \sim_{\text{may}} \tau$.*

Proof. Given strategies $\sigma, \tau\colon A$ in $\mathcal{G}_X$, we have $\sigma \sim_{\text{may}} \tau$ if and only if $\alpha;\sigma \approx_{\text{may}} \alpha;\tau$ for any morphism $\alpha\colon !A \multimap \mathbb{C}$ in $\mathcal{G}_X$. If $\sigma \approx_{\text{may}} \tau$, we have

$$\alpha;\sigma|_{\mathbb{C}} = \alpha;(\sigma|_{\mathbb{C}}) = \alpha;(\tau|_{\mathbb{C}}) = \alpha;\tau|_{\mathbb{C}}\,.$$ □

Note that it is also the case that if $\alpha \approx_{\mathrm{may}} \alpha'$ and $\sigma \approx_{\mathrm{may}} \tau$ then $\alpha;\sigma \approx_{\mathrm{may}} \alpha';\tau$. Therefore, the Full Abstraction result we have just proved applies to the quotiented category.

The definition of the relation $\approx_{\mathrm{may}}$ suggests that we might forget about the $!X$ component of a strategy $\sigma\colon !X \multimap A$ altogether, and consider only the set $\sigma|_A$. This set is not a strategy, since it does not satisfy the determinism requirement, but it satisfies every other requirement.

Definition 1.38. Given a game A, a *nondeterministic strategy* is a prefix-closed set of even-length legal plays from A.

We can compose nondeterministic strategies using ‘parallel composition plus hiding’, just as for deterministic ones, and we get a Cartesian closed category in the same way. We interpret all the Idealized Algol terms in the usual way as deterministic strategies, interpreting the nondeterministic primitive ask_X as the nondeterministic strategy for X with maximal plays

$$qx$$

for every $x \in X$.

It is already known (see [HM99]) that this model is fully abstract for (finitely or countably) nondeterministic Idealized Algol with may-contextual equivalence.

1.10 Alternative reduction rules - must testing

A more interesting, and more complicated, reduction rule for nondeterministic IA is the *must-convergence* relation.

We shall define this indirectly via its negation.

Definition 1.39. We shall define a relation

$$\Gamma, s \vdash M \Uparrow$$

between `Var`-contexts Γ, Γ-stores s and terms $\Gamma \vdash M \colon T$ of Idealized Algol.

References

[Ghi05] Dan R. Ghica. Slot games: A quantitative model of computation. In *Proceedings of the 32Nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL ’05, pages 85–97, New York, NY, USA, 2005. ACM.

[HM99] R. Harmer and G. McCusker. A fully abstract game semantics for finite nondeterminism. In *Proceedings. 14th Symposium on Logic in Computer Science (Cat. No. PR00158)*, pages 422–430, 1999.

[Kle65] H. Kleisli. Every standard construction is induced by a pair of adjoint functors. *Proceedings of the American Mathematical Society*, 16(3):544–546, 1965.

[Lam74] J. Lambek. Functional completeness of cartesian categories. *Annals of Mathematical Logic*, 6(3):259 – 292, 1974.

[Mac71] Saunders MacLane. *Categories for the Working Mathematician.* Springer-Verlag, New York, 1971. Graduate Texts in Mathematics, Vol. 5.

[Str72] Ross Street. The formal theory of monads. *Journal of Pure and Applied Algebra*, 2(2):149 – 168, 1972.