Full Title*

Subtitle†

W. J. Gowers‡

PhD Student

Department of Computer Science

University of Bath

Bath, United Kingdom

W.J.Gowers@bath.ac.uk

Abstract

Text of abstract ....

Keywords keyword1, keyword2, keyword3

1 Introduction

Text of paper ...

2 Idealized Algol with Countable Nondeterminism

The language that we will be modelling is the language Idealized Algol [Abramsky and McCusker 1999], extended with an additional constant ? representing countable nondeterminism. This is similar to the approach adopted in [Harmer and McCusker 1999], which extends Idealized Algol with *finite* nondeterminism. The types of the language are defined inductively as follows:

$$T ::= \mathsf{nat} \mid \mathsf{com} \mid \mathsf{Var} \mid T \to T\,.$$

Meanwhile, the terms are those given in [Abramsky and McCusker 1999], together with the nondeterministic choice:

$$\begin{aligned} M ::= {} & x \mid \lambda x.M \mid M\ M \mid \mathbf{Y}_T M \mid \\ & \mathsf{n} \mid \mathsf{skip} \mid \mathsf{suc}\ M \mid \mathsf{pred}\ M \mid \\ & \mathtt{If0}\ M\ M\ M \mid M; M \mid \\ & M := M \mid @M \mid \\ & \mathsf{new}_T\ M \mid \mathsf{mkvar}\ M\ M \mid ?\,. \end{aligned}$$

The typing rule for ? is $\Gamma \vdash ? : \mathsf{nat}$. We shall use the letter v to range over variables of type Var.

The value forms in the language are given by

$$V ::= \mathsf{skip} \mid \mathsf{n} \mid \lambda x.M \mid v \mid \mathsf{mkvar}$$

We define predicates $M \Downarrow V$ (M may converge to V) and $M \Downarrow^{\text{must}}$ (M must converge) inductively to give a big-step operational semantics for our language. We give a selection of the appropriate rules in Figure 1; this presentation is almost identical to that given in [Harmer and McCusker 1999], with a slightly different rule for the countable nondeterminism. In each rule, $\langle s, M\rangle$ is a *configuration* of the language, where M is a term, and s is a *store*; i.e., a function from the set of variables free in M to the set of natural numbers. If s is a store and v a variable, we write $\langle s \mid v \mapsto n\rangle$ for the state formed by updating the value of the variable v to n.

Given a term M of ground type com or nat, a proof π that $\langle s, M\rangle \Downarrow V$ gives rise to a (possibly infinite) sequence of natural numbers corresponding to a bottom-to-top, left-to-right reading of the natural numbers n used in the first rule for ?. We call such a sequence an *evaluation* of the configuration $\langle s, M\rangle$. It is perhaps easier to view this from the perspective of a small-step reduction: the sequence of numbers is formed by listing the different values that the nondeterminism constant ? decays to over the course of the evaluation π.

If $\langle \varnothing, M\rangle$ is a configuration with empty store, we call M a *closed term*. Let T be an Idealized Algol type, and let $M, N : T$ be closed terms. Then we write $M \sqsubseteq_{m\&m} N$ if for all compatible contexts $C[-]$ of ground type we have

$$C[M] \Downarrow V \Rightarrow C[N] \Downarrow V$$
$$C[M] \Downarrow^{\text{must}} \Rightarrow C[N] \Downarrow^{\text{must}}$$

We write $M \equiv_{m\&m} N$ if $M \sqsubseteq_{m\&m} N$ and $N \sqsubseteq_{m\&m} M$.

One aspect of the language that makes it particularly difficult to model is that function application is not continuous, either with respect to functions or with respect to arguments.

*with title note
†with subtitle note
‡with author1 note

LICS'18, 9-12 July, 2018, Oxford, UK
2018.

$$\frac{\langle s, N\rangle \Downarrow \langle s', \mathsf{n}\rangle \qquad \langle s', M\rangle \Downarrow \langle s'', v\rangle}{\langle s, M := N\rangle \Downarrow \langle \langle s'' \mid v \mapsto n\rangle, \mathsf{skip}\rangle} \qquad \frac{\langle s, M\rangle \Downarrow \langle s', v\rangle}{\langle s, @M\rangle \Downarrow \langle s', \mathsf{n}\rangle}\ s'(v) = n \qquad \frac{\langle s, M\rangle \Downarrow \langle s', \mathsf{skip}\rangle \qquad \langle s', N\rangle \Downarrow \langle s'', V\rangle}{\langle s, M; N\rangle \Downarrow \langle s'', V\rangle}$$

$$\frac{\langle \langle s \mid v \mapsto 0\rangle, M\rangle \Downarrow \langle \langle s' \mid v \mapsto n\rangle, V\rangle}{\langle s, \mathsf{new}_T\ \lambda v.M\rangle \Downarrow \langle s', V\rangle} \qquad \frac{\langle s, M\mathsf{n}\rangle \Downarrow \langle s', V\rangle}{\langle s, M?\rangle \Downarrow \langle s', V\rangle}\ n \in \mathbb{N} \qquad \frac{\forall n \in \mathbb{N}. \langle s, M\mathsf{n}\rangle \Downarrow^{\text{must}}}{\langle s, M?\rangle \Downarrow^{\text{must}}}$$

$$\frac{\langle s, M\rangle \Downarrow^{\text{must}} \qquad \forall \langle s', \lambda x.M'\rangle\ .\ \langle s, M\rangle \Downarrow \langle s', \lambda x.M'\rangle \Rightarrow \langle s', M'[N/x]\rangle \Downarrow^{\text{must}}}{\langle s, M\ N\rangle \Downarrow^{\text{must}}}$$

Figure 1. Operational semantics of Idealized Algol with Countable Nondeterminism

For example, it is easy to write a sequence of functions $<n : \mathsf{nat} \to \mathsf{nat}$ that return 0 if their argument is less than n and diverge otherwise:

$$\begin{aligned} <0 &= \lambda m.\Omega \\ <1 &= \lambda m.\mathtt{If0}\ m\ \mathtt{0}\ \Omega \\ <2 &= \lambda m.\mathtt{If0}\ m\ \mathtt{0}\ (\mathtt{If0}\ (\mathsf{pred}\ m)\ \mathtt{0}\ \Omega) \\ &\dots \end{aligned}$$

It is easy enough to see (for example, by the denotational semantics) that the least upper bound of these functions is the function $\lambda x.\mathtt{0}$. However, it is clear that $<n\ ?\ \Downarrow^{\text{must}}$ for each n, while $\lambda x.\mathtt{0}\ ?$ must converge to $\mathtt{0}$. Thus, $\lambda x.\mathtt{0}\ ?$ is not the least upper bound of the $<n\ ?$.

This is a bit of a problem, since continuity often plays an important role in full abstraction proofs – firstly, for proving Computational Adequacy of the recursion combinator, and, secondly, for deducing full abstraction from compact definability. Semantically, we shall deal with the first problem by adopting a novel approach to Computational Adequacy, and with the second problem by appealing to the stronger *universality* result: namely, that every *recursive* strategy is definable.

3 Game Semantics

We will use the Hyland-Ong version of Game Semantics, as in [Abramsky and McCusker 1999].

3.1 Arenas

An *arena* is given by a triple $A = (M_A, \lambda_A, \vdash_A)$, where

- M_A is a countable set of moves,
- $\lambda_A : m_A \to \{O, P\} \times \{Q, A\}$ designates each move as either an O-*move* or a P-*move*, and as either a *question* or an *answer*. We define $\lambda_A^{OP} = \mathrm{pr}_1 \circ \lambda_A$ and $\lambda_A^{QA} = \mathrm{pr}_2 \circ \lambda_A$. We also define $\neg : \{O, P\} \times \{Q, A\} \to \{O, P\} \times \{Q, A\}$ to be the function that reverses the values of O and P while leaving $\{Q, A\}$ unchanged.
- $\vdash_A$ is an *enabling relation* between $M_A + \{*\}$ and M_A satisfying the following rules:
  - If $a \vdash_A b$ and $a \neq b$, then $\lambda_A^{OP}(a) \neq \lambda_A^{OP}(b)$.
  - If $* \vdash_A a$, then $\lambda_A(a) = OQ$ and $b \not\vdash_A a$ for all $b \in M_A$.
  - If $a \vdash_A b$ and b is an answer, then a is a question.

  We say that a move $a \in M_A$ is *initial* in A if $* \vdash_A a$.

Our base arenas will be the *flat arenas* for the types nat and com. Given a set X, the flat arena on X is the arena with a single O-question q and a P-answer x for each $x \in X$, where $* \vdash q$ and $q \vdash x$ for each x. The denotation of the type nat will be the flat arena $\mathbb{N}$ on the set of natural numbers, while the denotation of the type com will be the flat arena $\mathbb{C}$ on the singleton set $\{a\}$.

Given an arena A, a *justified string* in A is a sequence s of moves in A, together with *justification pointers* that go from move to move in the sequence in such a way that every non-initial move m in s has exactly one justification pointer going back to an earlier move n in s such that $n \vdash_A m$. We say that n *justifies* m. It is easy to see that every justified string must begin with an initial move, an hence with an O-question.

A *legal play* s is a justified string in A that strictly alternates between O-moves and P-moves and is such that the corresponding QA-sequence formed by applying λ_A^{QA} to terms is well-bracketed. We write L_A for the set of legal plays in A.

3.2 Games and strategies

We follow the approach taken by Abramsky and McCusker [Abramsky and McCusker 1999] – a middle road between the *arenas* of Hyland and Ong and the *games* of [Abramsky et al. 2000] that makes the linear structure more apparent.

Let s be a legal play in some arena A. If m and n are moves in s such that there is a chain of justification pointers leading from m back to n, we say that n *hereditarily justifies* m. Given some set S of initial moves in s, we write $s|_S$ for the subsequence of s made up of all those moves that are hereditarily justified by some move in S.

A *game* is a tuple $A = (M_A, \lambda_A, \vdash_A, P_A)$, where $(M_A, \lambda_A, \vdash_A)$ is an arena and P_A is a non-empty prefix-closed set of legal plays in that arena such that if $s \in P_A$ and I is a non-empty set of initial moves in s, then $s|_I \in P_A$.

3.2.1 Multiplicatives

Let A, B be games. We define games $A \otimes B$ and $A \multimap B$ as follows.

$$
\begin{array}{rcl}
M_{A\otimes B} & = & M_A + M_B\,. \\
\lambda_{A\otimes B} & = & [\lambda_A, \lambda_B]\,. \\
* \vdash_{A\otimes B} n & \Leftrightarrow & * \vdash_A n \text{ or } * \vdash_B n\,. \\
m \vdash_{A\otimes B} n & \Leftrightarrow & m \vdash_A n \text{ or } m \vdash_B n\,. \\
P_{A\otimes B} & = & \{s \in L_{A\otimes B} \,:\, s|_A \in P_A \text{ and } s|_B \in P_B\}\,.
\end{array}
$$

$$
\begin{array}{rcl}
M_{A\multimap B} & = & M_A + M_B\,. \\
\lambda_{A\multimap B} & = & [\neg \circ \lambda_A, \lambda_B]\,. \\
* \vdash_{A\multimap B} n & \Leftrightarrow & * \vdash_B m\,. \\
m \vdash_{A\multimap B} n & \Leftrightarrow & \begin{array}{l} m \vdash_A n \text{ or } m \vdash_B n \\ \text{or (for } m \neq *) * \vdash_B m \text{ and } * \vdash_A n\,. \end{array} \\
P_{A\multimap B} & = & \{s \in L_{A\multimap B} \,:\, s|_A \in P_A \text{ and } s|_B \in P_B\}\,.
\end{array}
$$

3.2.2 Modelling countable nondeterminism

Our definition of a strategy will be modelled upon that given in [Harmer and McCusker 1999]. We model nondeterministic computations by relaxing the determinism constraint on strategies – so player P may have multiple replies to any given O-move.

In addition, we have to keep track of any possible divergence in the computation; this is so we can distinguish terms such as

$$\texttt{If0}\ ?\ \Omega\ \texttt{0} \qquad\qquad \texttt{0}\,,$$

where the term on the right must converge (to $\texttt{0}$), while the term on the left has a possible divergence. The traditional way of representing divergences in game semantics is by a partiality in the strategy; i.e., an O-move to which P has no reply, but this partiality will be obscured by the alternative behaviour in the denotation of the strategy on the left.

We follow [Harmer and McCusker 1999] by modelling a strategy as a pair (T_σ, D_σ), where T_σ is a nondeterministic strategy in the usual sense and D_σ is a set of O-plays after which there is a possibility of divergence.

Tracking divergences explicitly in this way requires some care when we compose strategies. Specifically, we need to be able to add new divergences into strategies when they arise through 'infinite chattering' or *livelock*. For example, the denotation of the term

$$M = \mathrm{Y}_{\mathsf{nat}\to\mathsf{nat}}(\lambda f.\lambda n.n; (f\,n))\,,$$

where $n; P$ is a shorthand for $\texttt{If0}\ n\ P\ P$, is given by a total strategy, without divergences: namely the strategy μ with plays of the form

$$
\begin{array}{cc}
\mathbb{N} & \mathbb{N} \\
 & q \\
q & \\
n_1 & \\
q & \\
n_2 & \\
\vdots &
\end{array}\,.
$$

However, when we compose this strategy with any total strategy for $\mathbb{N}$ on the left, we expect the resulting strategy to contain divergences, since the term $M\mathsf{n}$ diverges for any n.

The approach adopted in [Harmer and McCusker 1999] is to check specifically for infinite chattering between strategies $\sigma : A \multimap B$ and $\tau : B \multimap C$ by checking whether the set $\sigma \| \tau$ contains any infinite increasing sequence of plays ending with moves in B. If there is such a sequence, then it restricts to some O-position in $\sigma; \tau$ and we add in a divergence at that position.

This works very satisfactorily for finite nondeterminism, but not at all for countable nondeterminism. To see why, consider the term

$$N = \mathrm{Y}_{\mathsf{nat}\to\mathsf{nat}\to\mathsf{nat}}(\lambda g.\lambda m n.\texttt{If0}\ m\ \texttt{0}\ n; (g\ (\mathsf{pred}\ m)\ n))?$$

This term first chooses a natural number m, and then reads from its input n for a total of m times before eventually returning $\texttt{0}$. Thus, its denotation is the strategy ν with maximal plays of the form:

$$
\begin{array}{cc}
\mathbb{N} & \mathbb{N} \\
 & q \\
q & \\
n_1 & \\
\vdots & \\
q & \\
n_m & \\
 & 0
\end{array}\,.
$$

Note that this strategy strictly contains the one we considered before, and therefore that the denotation of

$$\texttt{If0}\ ?MN$$

has the same denotation as N, even though it has all the divergent evaluations of M, while $N\mathsf{n} \Downarrow^{\text{must}}$ for all n. Moreover, if we try to compose $[\![N]\!]$ with the strategy on $\mathbb{N}$ that

always returns 1, then we end up with an infinite increasing sequence of positions, which triggers the introduction of a divergence into the composite – even though no divergence occurs in the evaluation of N.

Aside from making violating soundness for the model, this example actually leads to composition not being associative if we naively extend the Harmer-McCusker model from finite to infinite nondeterminism (e.g., see [Harmer 1999, 4.4.1]).

Somehow, the crucial point is that we need to distinguish between terms like M, which contain infinite sequences of moves, and terms like N, which contain arbitrarily large finite sequences of oves. The way that we do this is by making the infinite sequences of moves explicit in our strategies, in the style of [Roscoe 1993] and [Levy 2008]. Then the denotation of M will contain an infinite sequence, while the denotation of N will contain arbitarily long finite sequences, but no infinite sequences.

The games in our model will be the same as those that we considered in the last section, but our definition of a strategy will change.

3.2.3 Strategies

Given an arena A, we define an *infinite justified string* in the obvious way. We define $\bar{P_A}$ to be P_A together with the set of all those infinite justified sequences that have all finite prefixes in P_A.

Let A be a game. A *strategy* σ for A is a pair (T_σ, D_σ), where:

- T_σ is a non-empty prefix-closed subset of $\bar{P_A}$ such that if $s \in T_\sigma$ is a P-position and $sa \in P_A$ then $sa \in T_\sigma$.
- $D_\sigma \subseteq \bar{P_A}$ is a postfix-closed set of plays in $\bar{P_A}$ that either end with an O-move or are infinite. We require D_σ to obey the following rules:

  Divergences come from plays If $d \in D_\sigma$ then there exists some $s \sqsubseteq d$ such that $s \in T_\sigma \cap D_\sigma$.

  Diverge-or-reply If $s \in T_\sigma$ is an O-position, then either $s \in D_\sigma$ or $sa \in T_\sigma$ for some legal play sa.

  Infinite positions are divergent If $s \in T_\sigma$ is infinite, then $s \in D_\sigma$.

3.2.4 Composition of strategies

Given games A, B, C, we define a justified string over A, B, C to be a sequence $\mathfrak{s}$ of moves with justification pointers from all moves except the initial moves in C. Given such a string, we may form the restrictions $\mathfrak{s}|_{A,B}$ and $\mathfrak{s}|_{B,C}$ by removing all moves in either C or A, together with all justification pointers pointing into these games. We define $\mathfrak{s}|_{A,C}$ to be the sequence formed by removing all moves from B from $\mathfrak{s}$ and all pointers to moves in B, *unless* we have a sequence of pointers $a \to b \to c$, in which case we replace them with a pointer $a \to c$.

We call such a sequence $\mathfrak{s}$ a *legal interaction* if $\mathfrak{s}|_{A,B} \in P_{A \multimap B}$, $\mathfrak{s}|_{B,C} \in P_{B \multimap C}$ and $\mathfrak{s}|_{A,C} \in P_{A \multimap C}$. We write $\mathrm{int}_\infty(A, B, C)$ for the set of (possibly infinite) legal interactions between A, B and C.

Now, given strategies $\sigma : A \multimap B$ and $\tau : B \multimap C$, we define

$$T_\sigma \| T_\tau = \{\mathfrak{s} \in \mathrm{int}_\infty(A, B, C) : \mathfrak{s}|_{A,B} \in T_\sigma,\ \mathfrak{s}|_{B,C} \in T_\tau\},$$

and then set

$$T_{\sigma;\tau} = \{\mathfrak{s}|_{A,C} : \mathfrak{s} \in T_\sigma \| T_\tau\}.$$

As for divergences in $\sigma;\tau$, our approach is actually simpler than that in [Harmer and McCusker 1999]; we set

$$D_\sigma \not\downarrow D_\tau = \left\{ \mathfrak{s} \in \mathrm{int}_\infty(A, B, C) \;\middle|\; \begin{array}{l} \textbf{either } \mathfrak{s}|_{A,B} \in D_\sigma \\ \quad \text{and } s|_{B,C} \in T_\tau \\ \textbf{or } \mathfrak{s}|_{A,B} \in T_\sigma \\ \quad \text{and } s|_{B,C} \in D_\tau \end{array} \right\}.$$

We then set

$$D_{\sigma;\tau} = \mathrm{pocl}_{A \multimap C}\{\mathfrak{s}|_{A,C} : \mathfrak{s} \in D_\sigma \not\downarrow D_\tau\},$$

where $\mathrm{pocl}\, X$ denotes the *postfix closure* of X; i.e., the set of all O-plays in $P_{A \multimap C}$ that have some prefix in X.

Note that there is no need to consider separately, as Harmer and McCusker do, divergences that arise through 'infinite chattering': in our model, a case of infinite chattering between strategies σ and τ is itself a legal interaction between the two strategies, which is necessarily divergent (because it is infinite) and therefore gives rise to some divergence in $\sigma;\tau$.

We need to impose one more condition on strategies:

Definition 3.1. Let σ be a strategy for a game A. We say that σ is *complete* if $T_\sigma = \bar{T_\sigma}$; i.e., T_σ contains an infinite position s if it contains every finite prefix of s.

Any finite-nondeterminism strategy in the sense of [Harmer and McCusker 1999] may be interpreted as a complete strategy by enlarging it with all its infinite limiting plays. However, when we introduce countable nondeterminism, we introduce the possibility of strategies that are not complete. For example, the strategy ν that we mentioned above has an infinite increasing sequence of plays $q0 \sqsubseteq q0q0 \sqsubseteq \cdots$, but has no infinite play corresponding to its limit. Nonetheless, we do not want to allow arbitrary strategies: for example, the strategy μ above should include the infinite play $qq0q0\ldots$; the strategy μ° formed by removing this infinite play has no meaning in our language. Indeed, if we compose μ° with the strategy $\mathsf{0}$ for $\mathbb{N}$ on the left, then the resulting strategy does not satisfy diverge-or-reply.

Definition 3.2. Let σ be a strategy for a game A. We say that σ is *locally complete* if it may be written as the union of countably many complete strategies; i.e., there exist σ_n such that $T_\sigma = \bigcup T_{\sigma_n}$ and $D_\sigma = \bigcup D_{\sigma_n}$.

From now on, we will use 'strategy' to mean *locally complete strategy*.

We need to show that the composition of locally complete strategies is locally complete. Note that this does not hold for *complete* strategies: for example, our term N above can be written as $N'\ ?$, where N' is a deterministic term with complete denotation ν'. Then we have $\nu = \top_{\mathbb{N}}; \nu'$, but ν is not complete. However, we can show that the composition of *deterministic* complete strategies is complete; since a locally complete strategy may always be written as the union of complete deterministic strategies, this is sufficient to show that the composition of locally complete strategies is locally complete.

Definition 3.3. We say that a strategy σ for a game A is *deterministic* if

- it is complete;
- whenever sab, sac are P-plays in T_σ we have $b = c$ and the justifier of b is the justifier of c;
- If $s \in D_\sigma$ then either s is infinite or there is no a such that $sa \in T_\sigma$.

Lemma 3.4. *Let A, B, C be games and let $\sigma : A \multimap B$, $\tau : B \multimap C$ be deterministic complete strategies. Then $\sigma; \tau$ is complete.*

Proof. The proof relies on a lemma from [Hyland and Ong 2000] that states (in our language) that if σ and τ are deterministic strategies and $s \in T_{\sigma;\tau}$ then there is a unique minimal $\mathfrak{s} \in T_\sigma \| T_\tau$ such that $\mathfrak{s}|_{A,C} = s$. That means that if $s_1 \sqsubseteq s_2 \sqsubseteq \cdots$ is an infinite increasing sequence of plays in $T_{\sigma;\tau}$, with infinite limit s, then there is a corresponding infinite increasing sequence of legal interactions $\mathfrak{s}_1 \sqsubseteq \mathfrak{s}_2 \sqsubseteq \cdots$. Then the limit of this sequence is an infinite legal interaction $\mathfrak{s}$ and we must have $\mathfrak{s}|_{A,B} \in \sigma$, $\mathfrak{s}|_{B,C} \in \tau$ by completeness of σ and τ. Therefore, $s = \mathfrak{s}|_{A,C} \in T_{\sigma;\tau}$. □

Corollary 3.5. *The composition of strategies $\sigma : A \multimap B$ and $\tau : B \multimap C$ is a well-formed strategy for $A \multimap C$.*

Proof. The only tricky point is eastablishing that diverge-or-reply holds for $\sigma; \tau$. Again, it is sufficient to prove this in the case that σ and τ are deterministic and complete. Then it essentially follows from the argument used in [Abramsky and Jagadeesan 1994] that shows that a partiality at an O-position $s \in T_{\sigma;\tau}$ must arise either from a partiality in T_σ or T_τ or from 'infinite chattering' between σ and τ. In the first case, the diverge-or-reply rule for σ and τ gives us a divergence at s in $\sigma; \tau$. In the second case, an infinite chattering between σ and τ corresponds to an infinite interaction $\mathfrak{s} \in \int(A, B, C)$ ending with infinitely many moves in B such that $\mathfrak{s}|_{A,C} = s$. Completeness for σ and τ tells us that $\mathfrak{s}|_{A,B} \in D_\sigma$ and $\mathfrak{s}|_{B,C} \in D_\tau$ and therefore that $\mathfrak{s}|_{A,C} \in D_{\sigma;\tau}$. □

Our proof for Corollary 3.5 really makes use of the fact that a locally complete strategy is *lively* in the sense of [Levy 2008]; i.e., locally deterministic. Our definition is slightly stronger than liveliness, because it insists that the union of complete strategies be *countable*. This will be essential to our definability result.

3.2.5 Associativity of composition

In fact, the proof of associativity of composition is pretty much the same in our model as it is in any other model of game semantics. However, it is worth saying a few words about it, since the model obtained by naively extending the Harmer-McCusker model to unbounded nondeterminism does not have an associative composition. The point is that this is not really a problem with associativity, but rather that this naive model gives the wrong result for the composition of strategies. For example, if ν is the strategy we defined above, and $\mathtt{0}$ is the 'constant 0' strategy on $\mathbb{N}$, then $\mathtt{0}; \nu$ has a divergence in the naive model, because the strategies $\mathtt{0}$ and ν appear to be engaged in infinite chattering. In our model, we have fixed that problem, because the strategy ν contains no infinite plays, and so no divergences arise in the composition.

3.3 A symmetric monoidal closed category

Given a game A, we define a strategy id_A on $A \multimap A$, where T_{id_A} is given by

$$\{s \in P_{A_1 \multimap A_2} \ : \ \text{for all even-length } t \sqsubseteq s,\ t|_{A_1} = t|_{A_2}\},$$

where we distinguish between the two copies of A by calling them A_1 and A_2, and where D_σ is the set of all infinite plays in T_σ. This is an identity for the composition we have defined, and so we get a category $\mathcal{G}_{ND}$ of games and nondeterministic strategies. Moreover, the connectives $\otimes$ and $\multimap$ exhibit $\mathcal{G}_{ND}$ as a symmetric monoidal closed category.

$\mathcal{G}_{ND}$ has an important subcategory $\mathcal{G}_D$ of deterministic complete strategies; this category is isomorphic to the category considered in [Abramsky and McCusker 1999].

3.4 Products and Exponentials

Let A, B be games We define a new game $A \times B$. The arena for $A \times B$ is the same as the arena for $A \otimes B$, but now $P_{A\times B}$ is the disjoint union of P_A and P_B inside that arena:

$$P_{A\times B} = \{s \in L_{A\otimes B} \ : \ s|_A \in P_A \text{ and } s|_B = \epsilon\}$$
$$\cup \{s \in L_{A\otimes B} \ : \ s|_A = \epsilon \text{ and } s|_B \in P_B\}.$$

Then $A \times B$ is the category-theoretic product of A and B in $\mathcal{G}_{ND}$.

We define a game $!A$ as follows. The arena for $!A$ is the same as the arena for A, but the set of plays is given by

$$P_{!A} = \{s \in L_A : s|_m \in P_A \text{ for each initial move } m\}.$$

There are strategies $\mathtt{mult}_A : !A \to !A \otimes !A$, $\supset : !(A \times B) \xrightarrow{\cong} !A \otimes !B$ and $\mathtt{der}_A : !A \to A$ that can be used to create a Cartesian closed category $\mathcal{G}^!_{ND}$, in which morphisms from A to B are strategies for the game $!A \multimap B$. This construction is essentially the co-Kleisli category on a comonad given by !, but certain technical issues prevent us from presenting it in this way. See [Abramsky and McCusker 1999] for full details.

3.5 Constraining strategies

Given a non-empty justified string s in an arena A, we define the *P-view* $\ulcorner s \urcorner$ of s inductively as follows.

$$\begin{aligned} \ulcorner sm \urcorner &= m, && \text{if } m \text{ is initial;} \\ \ulcorner sntm \urcorner &= \ulcorner s \urcorner nm, && \text{if } m \text{ is an } O\text{-move and } n \text{ justifies } m; \\ \ulcorner sm \urcorner &= \ulcorner s \urcorner m, && \text{if } m \text{ is a } P\text{-move.} \end{aligned}$$

We say that a play sm ending in a P-move is *P-visible* if the justifier of m is contained in $\ulcorner m \urcorner$. We say that a strategy σ for a game A is *visible* if every P-position $s \in T_\sigma$ is P-visible. It can be shown that the composition of visible strategies is visible, and that we can build a Cartesian closed category using our exponential.

The resulting category $\mathcal{G}^!_{D,vis}$ of games and deterministic visible strategies is a fully abstract model of Idealized Algol [Abramsky and McCusker 1999].

3.6 Recursive games and strategies

Most full abstraction results go via a definability result that says that all *compact* strategies are definable [Curien 2007]. However, deducing full abstraction from compact definability makes essential use of continuity properties that are absent when we deal with countable nondeterminism. We will therefore need to appeal to a stronger result – that of *universality*, which states that *every* strategy is definable. Clearly, universality does not hold for any of our categories of games, since there are many non-computable functions $\mathbb{N} \to \mathbb{N}$. However, Hyland and Ong proved in [Hyland and Ong 2000] that every *recursively presentable* innocent strategy is PCF-definable.

In order to define recursively presentable strategies, we need to work with *enumerated games*; i.e., games where the set of moves comes with an enumeration to the natural numbers. Clearly our base games $\mathbb{N}$ and $\mathbb{C}$ can be enumerated, as can the tensor product, linear implication, exponential and product of games.

Proposition 3.6. *Let $\mathcal{G}_{D,vis,rec}$ be the category of games and* recursive *visible strategies. Then $\mathcal{G}_{D,vis,rec}$ is a fully abstract model of Idealized Algol in which every morphism is definable.*

Proof. This follows from the corresponding results for PCF, together with the *innocent factorization* result of [Abramsky and McCusker 1999]. See also [Murawski and Tzevelekos 2013]. □

3.7 Determinisitic Factorization

Our definability results will hinge on a *factorization theorem*, showing that every nondeterministic strategy may be written as the composition of a deterministic strategy with the nondeterministic 'oracle' $\top_{\mathbb{N}}$. We can then deduce definability from definability in the model of deterministic Idealized Algol.

Note that our result is a bit simpler than the corresponding result in [Harmer and McCusker 1999]; this is because it is easier to model a countable source of nondeterminism than a 'finite but arbitrarily large' source.

Proposition 3.7. *Let $\sigma : I \to A$ be a strategy for a game A in $\mathcal{G}_{ND}$. Then we may write σ as $\top_{\mathbb{N}}; \mathrm{Det}(\sigma)$, where $\mathrm{Det}(\sigma) : !\mathbb{N} \to A$ is a deterministic strategy and $\top_{\mathbb{N}}$ is the strategy for $!\mathbb{N}$ given by*

- $T_{\top_{\mathbb{N}}} = P_{!\mathbb{N}}$.
- $D_{\top_{\mathbb{N}}}$ *is the set of infinite positions in* $T_{\top_{\mathbb{N}}}$.

Proof. We begin by fixing an injection code_A from the set of P-moves in A into the natural numbers. In the enumerated case, this is given to us already.

We first assume that the strategy σ is complete. Then the strategy $\mathrm{Det}(\sigma)$ is very easy to describe. For each O-position $sa \in T_\sigma$, we have some set B of possible replies to sa, which we order as $b_1, b_2, \cdots$, where $\mathrm{code}_A(b_1) < \mathrm{code}_A(b_2) < \cdots$. We insert a request to the oracle for a natural number; then, depending on her answer j, we play the next move as follows:

- If $0 < j \leq \mathrm{code}_A(b_1)$, then play b_1.
- If $\mathrm{code}_A(b_n) < j \leq \mathrm{code}_A(b_{n+1})$ then play b_{n+1}.
- If $j = 0$ and $sa \in D_\sigma$, then play nothing, and put the resulting play inside $D_{\mathrm{Det}(\sigma)}$. Otherwise, play b_1.

Lastly, we close under limits to make the strategy $\mathrm{Det}(\sigma)$ complete. $\mathrm{Det}(\sigma)$ is clearly nondeterministic. Checking that $\top_{\mathbb{N}}; \mathrm{Det}(\sigma) = \sigma$ is easy for finite plays; for infinite plays, it follows by completeness of σ.

Lastly, if σ is the union of complete strategies $\sigma_1, \sigma_2, \cdots$, we insert an additional request to the oracle immediately after the very first move by player O; after receiving a reply k, we play according to σ_k. □

Note that in the recursive case, $\mathrm{Det}(\sigma)$ is clearly recursively presentable if σ is. Furthermore, if σ is visible, then so is $\mathrm{Det}(\sigma)$.

4 Full abstraction

4.1 Denotational Semantics

The category in which we shall model our language is the category $\mathcal{G}^!_{ND,vis,rec}$ – the Cartesian closed category of (enumerated) games with nondeterministic, recursively presentable visible strategies. We have a natural embedding $\mathcal{G}^!_{D,vis,rec} \hookrightarrow \mathcal{G}^!_{ND,vis,rec}$, and we know that $\mathcal{G}^!_{D,vis,rec}$ is a universal and fully abstract model of Idealized Algol.

Any term $M\colon T$ of Idealized Algol with countable nondeterminism may be written as $M = C[?]$, where C is a context not involving the constant ?. Then the term $\lambda n.C[n]$ is a term of Idealized Algol, and therefore has a denotation $!\mathbb{N} \to [\![T]\!]$ as in [Abramsky and McCusker 1999]. We define the denotation of M to be given by the composite

$$I \xrightarrow{\top_{\mathbb{N}}} !\mathbb{N} \xrightarrow{[\![\lambda n.C[n]]\!]} [\![T]\!]$$

In other words, we interpret the constant ? using the strategy $\top_{\mathbb{N}}$ for $\mathbb{N}$.

4.2 Adequacy and soundness

We prove a *consistency* result for our model. Let M be a closed term of type com.

Lemma 4.1. *If $M \Downarrow$ skip then $qa \in T_{[\![M]\!]}$. If $M \Downarrow^{must}$ then $D_{[\![M]\!]} = \varnothing$.*

We can also prove the converse, *computational adequacy.*

Proposition 4.2. *If $qa \in T_{[\![M]\!]}$ then $M \Downarrow$ skip. If $D_{[\![M]\!]} = \varnothing$ then $M \Downarrow^{must}$.*

In order to prove these, we come back to the concept of an *evaluation* of a term as a sequence of natural numbers that we use to replace the constant ?.

Lemma 4.3. *Let $M = C[?]$ be a term of type* com*. Write σ_M for the denotation of the term $\lambda n.C[n]$. Let π be some evaluation of the configuration $\langle s, M\rangle$, where s is some state. Then there is a deterministic total strategy $\sigma_\pi\colon !\mathbb{N}$ such that*

- *π terminates at the value* skip *if and only if then $qa \in T_{\sigma_\pi;\sigma_M}$.*
- *π diverges if and only if $D_{\sigma_\pi;\sigma_M} \neq \varnothing$.*

Proof. Let $n_1, \ldots, n_k, d$ be a finite sequence of natural numbers. We define an Idealized Algol term $N_{n_1,\ldots,n_k,d}\colon (\mathsf{nat} \to \mathsf{com}) \to \mathsf{com}$ to be the following.

$$\lambda f.\mathsf{new}_{\mathsf{nat}}(\lambda v.f(v := (suc\ @v); \mathsf{case}_{k+1}\ @v\ \Omega\ n_1 \cdots n_k d))\,.$$

Here, $\mathsf{case}_{k+1}\ a\ n_0\ \cdots\ n_k\ d$ evaluates to n_i if a evaluates to i, and evaluates to d if a evaluates to $j > k$. Clearly, it can be built out of $\mathtt{If0}$ s. This term adds an extra variable v to the program; each time f is called, it increments the value of v and maps its value on to one of the n_i.

Now let π be a finite evaluation of $\langle s, C[?]\rangle \Downarrow$ skip. Encode π as a sequence $n_1, \ldots, n_k$. Let d be some arbitrary number. Then we can show that the following term also converges to skip in the same way:

$$N_{n_1,\ldots,n_k,d}(\lambda n.C[n])\,.$$

The idea here is similar to one used in testing; we want to test the behaviour of a nondeterministic program, and to do so we *mock* the random number generator in order to simulate a particular evaluation path using purely deterministic programs.

If instead π is a finite evaluation of $\langle s, C[?]\rangle \not\Downarrow^{\mathrm{must}}$; i.e., a divergent evaluation (that nevertheless only involves finitely many calls to the nondeterministic oracle), then the term $N_{n_1,\ldots,n_k,d}(\lambda n.C[n])$ will diverge according to the same execution path.

Digging into the construction of new within Idealized Algol, as given in [Abramsky and McCusker 1999], we see that for any term F of type $\mathsf{nat} \to \mathsf{com}$ the denotation of $N_{n_1,\ldots,n_k,d}F$ is given by the composite

$$I \xrightarrow{\mathrm{cell}_0} !\mathsf{Var} \xrightarrow{[\![\lambda v.v:=(\mathrm{suc}\ @v);\mathsf{case}_{k+1}\ @v\ \Omega\ n_1\cdots n_k d]\!]} !\mathbb{N} \xrightarrow{[\![F]\!]} \mathbb{C}\,.$$

We set σ_π to be the composite of the left two arrows. Observe that σ_π is the strategy with unique maximal infinite play as follows.

$$q\ n_1\ \cdots\ q\ n_k\ q\ d\ q\ d\ \cdots$$

Setting $F = \lambda n.C[n]$, we see that $[\![F]\!] = \sigma_M$. So, by soundness and adequacy for the Idealized Algol model, we see that $qa \in T_{\sigma_\pi;\sigma_M}$ if and only if $N_{n_1,\ldots,n_k,d}(\lambda n.C[n]) \Downarrow$ skip, which is the case if and only if $M \Downarrow$ skip along the evaluation π. Similarly, $D_{\sigma_\pi;\sigma_M} \neq \varnothing$ if and only if $N_{n_1,\ldots,n_k,d}(\lambda n.C[n])$ diverges, which is equivalent to saying that M diverges along the evaluation π.

Lastly, we need to deal with the case that π is an evaluation $n_1, n_2, \ldots$ that consults the nondeterministic oracle infinitely often. In this case, M must certainly diverge along the evaluation π. In that case, we define $\pi^{(j)}_n$ to be the strategy for $!N$ corresponding to the term $N_{n_1,\ldots,n_j,\Omega}$. So $\pi^{(j)}_n$ has a unique finite maximal play

$$q\ n_1\ q\ n_2\ \cdots\ q\ n_j\ q\,,$$

at which point the strategy has a partiality.

Evaluation of the term $N_{n_1,\ldots,n_j,\Omega}(\lambda n.C[n])$ must diverge, since it will proceed according to the evaluation π and eventually reach the divergence (since π consults the oracle infinitely often). This implies that $D_{\sigma_\pi^{(j)};\sigma_M} \neq \varnothing$ for all j.

We define σ_π to be the least upper bound of the $\sigma_\pi^{(j)}$ (e.g., in the sense of [Harmer and McCusker 1999]). Since composition is continuous for deterministic (!) strategies, we deduce that $D_{\sigma_\pi;\sigma_M} \neq \varnothing$.

σ_π has plays of the form

$$q\ n_1\ q\ n_2\ \cdots,$$

and so it is total. □

We can now prove our soundness and adequacy results.

Proof of Lemma 4.1. Suppose that that M is a closed term of type com and that $M \Downarrow$ skip. Let π be an evaluation such that $M \Downarrow$ skip along π. Then $qa \in T_{\sigma_\pi;\sigma_M}$ for some strategy σ_π. It follows that $qa \in T_{\top_{\mathbb{N}};\sigma_M}$.

Now suppose that $D_{[\![M]\!]} \neq \varnothing$. Then there is some interaction $\mathfrak{s} \in \int_\infty(I, !\mathbb{N}, \mathbb{C})$ such that $\mathfrak{s}|_{\mathbb{C}} \in D_{\sigma_M}$. Let σ be the minimal deterministic strategy for $!\mathbb{N}$ containing the play $\mathfrak{s}|_{!\mathbb{N}}$. By the proof of Lemma 4.3, $\sigma \subseteq \sigma_\pi$ for some evaluation π of M. Then we have $D_{\sigma_\pi;\sigma_M} \neq \varnothing$, so M diverges along π. □

Proof of Proposition 4.2. Suppose that M is a closed term of type com and that $qa \in T_{[\![M]\!]}$. Then there is some interaction $\mathfrak{s} \in \int_\infty(I, !\mathbb{N}, \mathbb{C})$ such that $qa \in \mathfrak{s}|_{\mathbb{C}}$. Let σ be the minimal deterministic strategy for $!\mathbb{N}$ containing the play $\mathfrak{s}|_{!\mathbb{N}}$. By the proof of Lemma 4.3, $\sigma \subseteq \sigma_\pi$ for some evaluation π of the term M. Then we have $qa \in T_{\sigma_\pi;\sigma_M}$, so $M \Downarrow$ skip along π.

Now suppse that $M \not\Downarrow^{\text{must}}$. Let π be a divergent evaluation of M. Then we have $D_{\sigma_\pi;\sigma_M} \neq \varnothing$. Moreover, since σ_π is total, it follows that $D_{\top_{\mathbb{N}};\sigma_M} \neq \varnothing$. □

We define *extensional equivalence of strategies* as follows. If σ, τ are two strategies for a game A, we say that σ sym τ if for all test morphisms $\alpha : A \to \mathbb{C}$ we have $\sigma;\alpha = \tau;\alpha$. Having defined this equivalence, we may prove *soundness* in the usual way.

Theorem 4.4 (Soundness). *Let M, N be two closed terms of type T. If $[\![M]\!]$ sym $[\![N]\!]$ then $M \equiv_{m\&m} N$.*

4.3 Universality

Let S, T be Idealized Algol types and let $\sigma : S \to T$ be a morphism in $\mathcal{G}^!_{ND,vis,rec}$. We want to prove that σ is the denotation of some term.

By our nondeterministic factorization result, we know that $\sigma = \top_{\mathbb{N}}; \mathrm{Det}(\sigma)$, where $\mathrm{Det}(\sigma)$ is a deterministic strategy. By universality for $\mathcal{G}^!_{D,vis,rec}$, we know that $\mathrm{Det}(\sigma) = [\![M]\!]$ for some closed term $M : S \to T$. Then $\sigma = \top_{\mathbb{N}}; \mathrm{Det}(\sigma) = [\![?]\!]\,;[\![M]\!] = [\![M\ ?]\!]$.

4.4 Full abstraction

Theorem 4.5 (Full abstraction). *Let M, N be two closed terms of type T. If $M \equiv_{m\&m} N$ then $[\![M]\!]$ sym $[\![N]\!]$.*

Proof. Let $A = [\![T]\!]$. Suppose that $[\![M]\!]$ /sym $[\![N]\!]$; so there is some strategy $\alpha : A \to \mathbb{C}$ such that $[\![M]\!]\,;\alpha \neq [\![N]\!]\,;\alpha$. By universality, we have $A = [\![P]\!]$ for some closed term P of type $T \to$ com. Then we have $[\![M]\!]\,;[\![P]\!] \neq [\![N]\!]\,;[\![P]\!]$; by consistency and adequacy, it follows that $M \not\equiv_{m\&m} N$. □

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. nnnnnnn and Grant No. mmmmmmm. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

References

Samson Abramsky and Radha Jagadeesan. 1994. Games and Full Completeness for Multiplicative Linear Logic. *The Journal of Symbolic Logic* 59, 2 (1994), 543–574. http://arxiv.org/abs/1311.6057

Samson Abramsky, Radha Jagadeesan, and Pasquale Malacaria. 2000. Full Abstraction for PCF. *Information and Computation* 163, 2 (2000), 409 – 470. https://doi.org/10.1006/inco.2000.2930

Samson Abramsky and Guy McCusker. 1999. Full Abstraction for Idealized Algol with Passive Expressions. *Theor. Comput. Sci.* 227, 1-2 (Sept. 1999), 3–42. https://doi.org/10.1016/S0304-3975(99)00047-X

Pierre-Louis Curien. 2007. Definability and Full Abstraction. *Electronic Notes in Theoretical Computer Science* 172 (2007), 301 – 310. https://doi.org/10.1016/j.entcs.2007.02.011 Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin.

Marco Grandis and Robert Paré. 1999. Limits in double categories. *Cah. Topologie Géom. Différ. Catégoriques* 40, 3 (1999), 162–220.

Pare Robert Grandis, Marco. 2004. Adjoint for double categories. *Cahiers de Topologie et Géométrie Différentielle Catégoriques* 45, 3 (2004), 193–240. http://eudml.org/doc/91684

R. Harmer and G. McCusker. 1999. A fully abstract game semantics for finite nondeterminism. In *Proceedings. 14th Symposium on Logic in Computer Science (Cat. No. PR00158)*. 422–430. https://doi.org/10.1109/LICS.1999.782637

Russell S. Harmer. 1999. *Games and full abstraction for nondeterministic languages.* Technical Report.

J.M.E. Hyland and C.-H.L. Ong. 2000. On Full Abstraction for PCF: I, II, and III. *Information and Computation* 163, 2 (2000), 285 – 408. https://doi.org/10.1006/inco.2000.2917

Martin Hyland and Andrea Schalk. 2002. Games on graphs and sequentially realizable functionals. Extended abstract. In *Logic in Computer Science, 2002. Proceedings. 17th Annual IEEE Symposium on.* IEEE, 257–264.

Paul Blain Levy. 2008. Infinite trace equivalence. *Annals of Pure and Applied Logic* 151, 2 (2008), 170 – 198. https://doi.org/10.1016/j.apal.2007.10.007

Andrzej S. Murawski and Nikos Tzevelekos. 2013. Deconstructing General References via Game Semantics. In *Foundations of Software Science and Computation Structures*, Frank Pfenning (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 241–256.

A. W. Roscoe. 1993. Unbounded Non-determinism in CSP. *Journal of Logic and Computation* 3, 2 (1993), 131. https://doi.org/10.1093/logcom/3.2.131

A Appendix

Text of appendix …