

# A Fully Abstract Game Semantics for Countable Nondeterminism

W. J. Gowers

Department of Computer Science

University of Bath

Bath, United Kingdom

W.J.Gowers@bath.ac.uk

James Laird

Department of Computer Science

University of Bath

Bath, United Kingdom

J.D.Laird@bath.ac.uk

## Abstract

The concept of fairness for a concurrent program means that the program must be able to exhibit an unbounded amount of nondeterminism without diverging. Game semantics models of nondeterminism show that this is hard to implement; for example, Harmer and McCusker’s model only admits infinite nondeterminism if there is also the possibility of divergence. We solve a long standing problem by giving a fully abstract game semantics for a simple stateful language with a countably infinite nondeterminism primitive. We see that doing so requires us to keep track of infinitary information about strategies, as well as their finite behaviours. The unbounded nondeterminism gives rise to further problems, which can be formalized as a lack of continuity in the language. In order to prove adequacy for our model (which usually requires continuity), we develop a new technique in which we simulate the nondeterminism using a deterministic stateful construction, and then use combinatorial techniques to transfer the result to the nondeterministic language. Lastly, we prove full abstraction for the model; because of the lack of continuity, we cannot deduce this from definability of compact elements in the usual way, and we have to use a stronger universality result instead. We discuss how our techniques may also be applied to Tsukada and Ong’s model of PCF with finite nondeterminism, yielding an alternative proof of computational adequacy.

**Keywords** semantics, nondeterminism, games and logic

## 1 Introduction

Picture two concurrent processes  $P$  and  $Q$  with shared access to a variable  $v$  that holds natural numbers and is initialized to 0. The execution of  $P$  consists in an infinite loop that increments the value of  $v$  at each iteration. Meanwhile,  $Q$  performs some computation  $A$ , and then prints out the current value of  $v$  and terminates the whole program. Since we cannot predict in advance how many cycles of the loop

in  $P$  will have elapsed by the time the computation  $A$  has completed, the value that ends up printed to the screen may be arbitrarily large. Furthermore, under the basic assumption that the task scheduler is *fair*; i.e., any pending task must eventually be executed, we can observe that our program must always terminate by printing out some value to the screen.

We have therefore built an *unbounded nondeterminism* machine, that can print out arbitrarily large natural numbers but which never diverges, as distinct from finitary choice nondeterminism.<sup>1</sup> What we have just shown is that if we want to solve the problem of building a fair task scheduler, then we must in particular be able to solve the problem of building an unbounded nondeterminism machine.

This is an important observation to make about concurrent programming, because the task of implementing unbounded nondeterminism is difficult – indeed, considerably more so than that of implementing bounded nondeterminism. Dijkstra argues in [Dijkstra 1997, Ch. 9] that it is impossible to implement unbounded nondeterminism, showing that the natural constructs from which we construct imperative programs satisfy a *continuity* property that unbounded nondeterminism lacks. In fact, for semanticists, this lack of continuity is a problem in itself, since the standard proofs of computational adequacy and full abstraction typically make use, implicitly or otherwise, of the fact that composition within the model is continuous with respect to some ordering.

We shall explore some of the problems relating to unbounded nondeterminism, and how they may be solved, using game semantics to give a fully abstract model of a simple stateful language – Idealized Algol – enhanced with a countable nondeterminism primitive. We begin with a pair of examples that will illustrate the lack of continuity, from a syntactic point of view. Let  $\text{nat}$  be our number type and consider a sequence of functions  $\langle n: \text{nat} \rightarrow \text{nat} \mid n \in \mathbb{N} \rangle$  where  $\langle n \rangle k$  evaluates to 0 if  $k < n$  and diverges otherwise. In that case, the least

<sup>1</sup>Using recursion, we can build a program out of finite nondeterminism that can produce arbitrarily large natural numbers; however, this program also admits the possibility of divergence.

upper bound of the  $<n$  is the function that combines all their convergent behaviours; i.e., the function  $\lambda k.k; \emptyset$  that evaluates its input and then returns 0. If  $?: \text{nat}$  is an unbounded nondeterminism machine, then function application to  $?$  is not continuous; indeed,  $<m ?$  always has the possibility of divergence – since  $?$  may evaluate to  $m + 1$ , say. But  $(\lambda k.k; \emptyset); ?$  always converges to 0.

Lack of continuity is a problem because fixed-point combinators are typically built using least upper bounds, and proving adequacy of the model requires that these least upper bounds be preserved. In a non-continuous situation, we will need to come up with new techniques in order to prove adequacy without using continuity.

A closely connected problem with unbounded nondeterminism is that it leads to terms that may be distinguished only by their *infinitary* behaviour. A program that flashes a light and unboundedly nondeterministic number of times cannot reliably be distinguished in finite time from a program that flashes that light forever: however long we watch the light flash, there is always a chance that it will stop at some point in the future. From a game semantics point of view, this corresponds to the observation that it is not sufficient to consider sets of finite plays in order to define strategies: we must consider infinite sequences of moves as well.

## 1.1 Related Work

Our game semantics model bears closest resemblance to that of Harmer and McCusker [Harmer and McCusker 1999], which is a fully abstract model of Idealized Algol with *finite* nondeterminism. Indeed, our work can be viewed as an extension of the Harmer-McCusker model with the extra information on infinite plays that we need to model countable nondeterminism.

The idea of adding infinite traces into strategies in order to model unbounded nondeterminism goes back to Roscoe's work on CSP [Roscoe 1993], and is very similar to work by Levy [Levy 2008] on game semantics for a higher order language. In particular, we will need something similar to Levy's *liveliness* condition on strategies, which is a way of saying that a strategy is a union of deterministic strategies – something that is not automatic when we start tracking infinite plays.

An alternative approach to the game semantics of nondeterminism can be found in Tsukada and Ong's sheaf model of nondeterministic PCF [Tsukada and Ong 2015] and in the more general work on concurrency by Winskel et al. (e.g., see [Winskel 2013] and [Castellan et al. 2016]), in which there is a very natural interpretation of nondeterminism. Although we are able to give a model of Idealized Algol with countable nondeterminism in the more traditional Harmer-McCusker style, it seems necessary to introduce this extra

machinery in order to model stateless languages such as PCF (and certainly to model concurrency). In the last section of this paper, we will show how our methods can be applied under very general circumstances, and in particular to these models.

Related work by Laird [Laird 2015, 2016] discusses a semantics for PCF with unbounded nondeterminism based on sequential algorithms and explores the role played by continuity; however, this semantics is not fully abstract. Laird's work is interesting because it shows that we can obtain a traditional adequacy proof for a semantics with one-sided continuity: composition is continuous with respect to functions, but not with respect to arguments. We cannot use these techniques here, though, because our composition is not continuous on either side.

## 1.2 Contributions

The main concepts of game semantics and the steps we take to establish full abstraction are well-established, with a few exceptions. The idea of including infinitary information in strategies is not new, but this particular presentation, though closely related to that of [Levy 2008], has not been carried out in a traditional Hyland-Ong game semantics setting before.

There are two points in the traditional Full Abstraction proof that depend on composition being continuous, and we have had to come up with ways of getting round them. The easier of the two is that continuity is necessary to derive Full Abstraction from definability of compact strategies; in order to get around this, we have had to appeal to the stronger *universality* result of [Hyland and Ong 2000], that says that every *recursive* strategy is definable.

For the proof of adequacy, we have had to come up with a new technique. This technique can be thought of as a kind of synthesis between the two usual methods of proving adequacy – one involving logical relations and the other using more hands-on operational techniques. We do this by separating out the deterministic, continuous part of the strategy from the nondeterministic, discontinuous part. Using the stateful language, we can simulate individual evaluation paths of a nondeterministic program using deterministic programs, which allows us to appeal to the adequacy result for deterministic Idealized Algol. We then rely on more combinatorial techniques to factor the nondeterminism back in.

This new technique is actually very generally applicable. In the last section of the paper, we show that it may be used to prove adequacy for models of nondeterministic PCF under very mild assumptions. The Tsukada-Ong model, for example, satisfies these assumptions and so we obtain an adequacy result for its semantics.

## 2 Idealized Algol with Countable Nondeterminism

We describe a simple type theory and operational semantics for Idealized Algol with countable nondeterminism. This is similar to the approach adopted in [Harmer and McCusker 1999], which extends Idealized Algol with *finite* nondeterminism. The types of our language are defined inductively as follows:

$$T ::= \text{nat} \mid \text{com} \mid \text{Var} \mid T \rightarrow T.$$

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

$$\begin{aligned} M ::= & x \mid \lambda x.M \mid M M \mid Y_T M \mid \\ & n \mid \text{skip} \mid \text{succ } M \mid \text{pred } M \mid \\ & \text{If } \emptyset M M M \mid M; M \mid \\ & M := M \mid @M \mid \\ & \text{new}_T M \mid \text{mkvar } M M \mid ?. \end{aligned}$$

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

We define a small-step operational semantics for the language; this presentation is equivalent to the big-step semantics given in [Harmer and McCusker 1999], except with a different rule for the countable rather than finite nondeterminism. We give a selection of the appropriate rules in Figure 1. 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  $n$ .

If  $\langle \emptyset, M \rangle$  is a configuration with empty store, we call  $M$  a *closed term*. Given a closed term  $M$  of ground type com or nat, we write that  $M \Downarrow x$  (where  $x = \text{skip}$  in the com case and is a natural number in the nat case) if there is a finite sequence  $M \rightarrow M_1 \rightarrow \dots \rightarrow M_n = x$ . If there is no infinite sequence  $M \rightarrow M_1 \rightarrow M_2 \rightarrow \dots$ , then we say that  $M$  *must converge*, and write  $M \Downarrow^{\text{must}}$ . In general, we refer to a (finite or infinite) sequence  $M \rightarrow M_1 \rightarrow \dots$  that either terminates at an observable value or continues forever as an *evaluation*  $\pi$  of  $M$ . Since the only case where we have any choice in which rule to use is the application of the rule for ?,  $\pi$  may be completely specified by a finite or infinite sequence of natural numbers.

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

$$\begin{aligned} C[M] \Downarrow V &\Rightarrow C[N] \Downarrow V \\ C[M] \Downarrow^{\text{must}} &\Rightarrow C[N] \Downarrow^{\text{must}} \end{aligned}$$

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

## 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,
- $\lambda_A : m_A \rightarrow \{O, P\} \times \{Q, A\}$  designates each move as either an *O-move* or a *P-move*, and as either a *question* or an *answer*. We define  $\lambda_A^{OP} = \text{pr}_1 \circ \lambda_A$  and  $\lambda_A^{QA} = \text{pr}_2 \circ \lambda_A$ . We also define  $\neg : \{O, P\} \times \{Q, A\} \rightarrow \{O, P\} \times \{Q, A\}$  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, and 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  $\lambda_A^{QA}$  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.

$$\begin{array}{c}
\frac{}{\langle s, v := n \rangle \longrightarrow \langle \langle s \mid v \mapsto n \rangle, \text{skip} \rangle} \quad \frac{s(v) = n}{\langle s, @v \rangle \longrightarrow \langle s, n \rangle} \quad \frac{}{\langle s, \text{skip}; M \rangle \longrightarrow \langle s, M \rangle} \\
\frac{}{\langle s, \text{new}_T \lambda v. M \rangle \longrightarrow \langle \langle s \mid v \mapsto 0 \rangle, M \rangle} \quad \frac{}{? \longrightarrow n} \quad \frac{n \in \mathbb{N}}{M; N \longrightarrow M'; N} \quad \frac{M \longrightarrow M'}{MN \longrightarrow M'N}
\end{array}$$

**Figure 1.** Selected rules in the small-step operational semantics of Idealized Algol with countable nondeterminism

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  $s|_I \in P_A$ .

Our base games will be the games  $\mathbb{N}$  and  $\mathbb{C}$  on the arenas of the same names, where  $P_{\mathbb{N}} = \{\epsilon, q\} \cup \{qn : n \in \mathbb{N}\}$  and  $\mathbb{C} = \{\epsilon, q, qa\}$ .

### 3.2.1 Connectives

Let  $A, B$  be games. Then we may define games  $A \times B$ ,  $A \otimes B$ ,  $A \multimap B$  and  $!A$  as in [Abramsky and McCusker 1999]. As an example, we give the definition of  $A \multimap B$ :

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

### 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

$$\text{If } \emptyset ? \Omega \emptyset \quad \emptyset,$$

where the term on the right must converge (to  $\emptyset$ ), 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 doesn't work here:  $\text{If } \emptyset ? \Omega \emptyset$  and  $\emptyset$  both denote the strategy with maximal play  $q \emptyset$ ; the partiality in the former is 'hidden' by the move  $\emptyset$ .

We follow [Harmer and McCusker 1999] by modelling a strategy as a pair  $(T_\sigma, D_\sigma)$ , where  $T_\sigma$  is a nondeterministic strategy in the usual sense and  $D_\sigma$  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

$$M = Y_{\text{nat} \rightarrow \text{nat}}(\lambda f. \lambda n. n; (fn))$$

is given by a total strategy, without divergences: namely the strategy  $\mu$  with plays of the form

$$\begin{array}{c}
\mathbb{N}_1 \quad q \quad n_1 \quad q \quad n_2 \quad \cdots \\
\mathbb{N}_2 \quad q
\end{array}$$

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  $Mn$  diverges for any  $n$ . Semantically, this corresponds to the fact that we have a legal interaction  $q \ q \ n \ q \ n \ \cdots$  with an infinite tail in  $\mathbb{N}_1$ ; when we perform 'hiding' by restricting the interaction to  $\mathbb{N}$ , we have no reply to the initial move  $q$ .

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  $\sigma \parallel \tau$  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

$$N = Y_{\text{nat} \rightarrow \text{nat} \rightarrow \text{nat}}(\lambda g. \lambda mn. \text{If } \emptyset \ m \ \emptyset \ n; (g \text{ (pred } m) \ n))?$$

This term first chooses a natural number  $m$ , and then reads from its input  $n$  for a total of  $m$  times before eventually returning  $\emptyset$ . Thus, its denotation is the strategy  $\nu$  with maximal



plays of arbitrary length of the form:

$$\begin{array}{ccccccc} N_1 & & q & n_1 & \cdots & q & n_m \\ N_2 & q & & & & & 0 \end{array}$$

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

$$\text{If } 0 ? MN$$

has the same denotation as  $N$ , even though for any  $n$ ,  $Mn \Downarrow^{\text{must}}$ , while  $Nn \Downarrow^{\text{must}}$ . Moreover, if we try to compose  $\llbracket N \rrbracket$  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 moves. 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 arbitrarily 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  $\overline{P}_A$  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*  $\sigma$  for  $A$  is a pair  $(T_\sigma, D_\sigma)$ , where:

- $T_\sigma$  is a non-empty prefix-closed subset of  $\overline{P}_A$  such that if  $s \in T_\sigma$  is a  $P$ -position and  $sa \in P_A$  then  $sa \in T_\sigma$ .
- $D_\sigma \subseteq \overline{P}_A$  is a postfix-closed set of plays in  $\overline{P}_A$  that either end with an  $O$ -move or are infinite. We require  $D_\sigma$  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  $s$  of moves with justification pointers from all moves except the initial moves in  $C$ . Given such a string, we may form the restrictions  $s|_{A,B}$  and  $s|_{B,C}$  by removing all moves in either  $C$  or  $A$ , together with all justification pointers pointing into these games. We define  $s|_{A,C}$  to be the sequence formed by removing all moves from  $B$  from  $s$  and all pointers to moves in  $B$ , *unless* we have a sequence of pointers  $a \rightarrow b \rightarrow c$ , in which case we replace them with a pointer  $a \rightarrow c$ .

We call such a sequence  $s$  a *legal interaction* if  $s|_{A,B} \in P_{A \multimap B}$ ,  $s|_{B,C} \in P_{B \multimap C}$  and  $s|_{A,C} \in P_{A \multimap C}$ . We write  $\text{int}_\infty(A, B, C)$  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

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

and then set

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

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

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

We then set

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

where  $\text{pocl } X$  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  $\sigma$  and  $\tau$  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  $\sigma$  be a strategy for a game  $A$ . We say that  $\sigma$  is *complete* if  $T_\sigma = \overline{T_\sigma}$ ; i.e.,  $T_\sigma$  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  $\nu$  that we mentioned above has an

infinite increasing sequence of plays  $q0 \sqsubseteq q0q0 \sqsubseteq \dots$ , but has no infinite play corresponding to its limit. Nonetheless, we do not want to allow arbitrary strategies: for example, the strategy  $\mu$  above should include the infinite play  $qq0q0\dots$ ; the strategy  $\mu^\circ$  formed by removing this infinite play has no meaning in our language. Indeed, if we compose  $\mu^\circ$  with the strategy  $\emptyset$  for  $\mathbb{N}$  on the left, then the resulting strategy does not satisfy diverge-or-reply.

**Definition 3.2.** Let  $\sigma$  be a strategy for a game  $A$ . We say that  $\sigma$  is *locally complete* if it may be written as the union of countably many complete strategies; i.e., there exist  $\sigma_n$  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  $\nu'$ . Then we have  $\nu = \top_{\mathbb{N}}; \nu'$ , but  $\nu$  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  $\sigma$  for a game  $A$  is *deterministic* if

- it is complete;
- whenever  $sab, sac$  are  $P$ -plays in  $T_\sigma$  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  $\sigma$  and  $\tau$  are deterministic strategies and  $s \in T_{\sigma; \tau}$  then there is a unique minimal  $\mathfrak{s} \in T_\sigma \parallel T_\tau$  such that  $\mathfrak{s}|_{A,C} = s$ . That means that if  $s_1 \sqsubseteq s_2 \sqsubseteq \dots$  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  $\mathfrak{s}_1 \sqsubseteq \mathfrak{s}_2 \sqsubseteq \dots$ . 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  $\sigma$  and  $\tau$ . Therefore,  $s = \mathfrak{s}|_{A,C} \in T_{\sigma; \tau}$ .  $\square$

**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 establishing that diverge-or-reply holds for  $\sigma; \tau$ . Again, it is sufficient to prove this in the case that  $\sigma$  and  $\tau$  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  $T_\sigma$  or  $T_\tau$  or from ‘infinite chattering’ between  $\sigma$  and  $\tau$ . In the first case, the diverge-or-reply rule for  $\sigma$  and  $\tau$  gives us a divergence at  $s$  in  $\sigma; \tau$ . In the second case, an infinite chattering between  $\sigma$  and  $\tau$  corresponds to an infinite interaction  $\mathfrak{s} \in \text{int}(A, B, C)$  ending with infinitely many moves in  $B$  such that  $\mathfrak{s}|_{A,C} = s$ . Completeness for  $\sigma$  and  $\tau$  tells us that  $\mathfrak{s}|_{A,B} \in D_\sigma$  and  $\mathfrak{s}|_{B,C} \in D_\tau$  and therefore that  $\mathfrak{s}|_{A,C} \in D_{\sigma; \tau}$ .  $\square$

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 liveness, 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 with infinite nondeterminism. For example, if  $\nu$  is the strategy we defined above, and  $\emptyset$  is the ‘constant 0’ strategy on  $\mathbb{N}$ , then  $\emptyset; \nu$  has a divergence in the naive model, because the strategies  $\emptyset$  and  $\nu$  appear to be engaged in infinite chattering. In our model, we have fixed that problem, because the strategy  $\nu$  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  $\text{id}_A$  on  $A \multimap A$ , where  $T_{\text{id}_A}$  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  $D_\sigma$  is the set of all infinite plays in  $T_\sigma$ . 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 A Cartesian closed category

We follow the construction given in [Abramsky and McCusker 1999], using the connectives  $!$  and  $\times$  to build a Cartesian closed category  $\mathcal{G}_{ND}^!$  from  $\mathcal{G}_{ND}$  whose objects are the well-opened games in  $\mathcal{G}_{ND}$  and where a morphism from  $A$  to  $B$  in  $\mathcal{G}_{ND}^!$  is a morphism from  $!A$  to  $B$  in  $\mathcal{G}_{ND}$ .

This is very similar to the construction of a co-Kleisli category for a linear exponential comonad, but certain technical issues relating to well-openedness prevent us from displaying it in this way.

### 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  $\sigma$  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  $\mathbb{N} \rightarrow \mathbb{N}$ . 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. We can then define a *recursive* strategy to be one that is recursively presentable with respect to that enumeration of moves.

**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].  $\square$

### 3.7 Deterministic 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  $\sigma : I \rightarrow A$  be a strategy for a game  $A$  in  $\mathcal{G}_{ND}$ . Then we may write  $\sigma$  as  $\top_{\mathbb{N}}; \text{Det}(\sigma)$ , where  $\text{Det}(\sigma) : !\mathbb{N} \rightarrow A$  is a deterministic strategy and  $\top_{\mathbb{N}}$  is the strategy for  $!\mathbb{N}$  that is 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  $\text{code}_A$  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  $\sigma$  is complete. Then the strategy  $\text{Det}(\sigma)$  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  $b_1, b_2, \dots$ , where  $\text{code}_A(b_1) < \text{code}_A(b_2) < \dots$ . 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  $0 < j \leq \text{code}_A(b_1)$ , then play  $b_1$ .
- If  $\text{code}_A(b_n) < j \leq \text{code}_A(b_{n+1})$  then play  $b_{n+1}$ .
- If  $j = 0$  and  $sa \in D_\sigma$ , then play nothing, and put the resulting play inside  $D_{\text{Det}(\sigma)}$ . Otherwise, play  $b_1$ .

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

Lastly, if  $\sigma$  is the union of complete strategies  $\sigma_1, \sigma_2, \dots$ , 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  $\sigma_k$ .  $\square$

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

## 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  $M : T$  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  $! \mathbb{N} \rightarrow \llbracket T \rrbracket$  as in [Abramsky and McCusker 1999]. We define the denotation of  $M$  to be given by the composite

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

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

### 4.2 Computational Adequacy

The *computational adequacy* result for our model can be stated as follows.

**Proposition 4.1** (Computational Adequacy).  *$M \Downarrow \text{skip}$  if and only if  $qa \in T_{\llbracket M \rrbracket}$ .  $M \Downarrow^{must}$  if and only if  $D_{\llbracket M \rrbracket} = \emptyset$ .*

Traditional proofs of computational adequacy using logical relations make essential use of the continuity of composition with respect to a natural ordering on strategies (see, for example, [Harmer and McCusker 1999] and [Harmer 1999] for the finite nondeterminism case). In our case, since composition is not continuous in the language itself, we cannot use this technique. In order to prove adequacy, we use a new technique that involves using a deterministic stateful construction to model the nondeterminism inside a deterministic world in which continuity holds. We shall return to the

concept of an *evaluation* of a term as a sequence of natural numbers that we use to replace the constant  $?$ .

**Lemma 4.2.** *Let  $M = C[?]$  be a term of type  $\text{com}$ , where  $C[-]$  is a context of Idealized Algol. Write  $\sigma_M$  for the denotation of the term  $\lambda n.C[n]$ .*

- *If  $M \Downarrow \text{skip}$  then there exists some total deterministic strategy  $\sigma : ! \mathbb{N} \rightarrow \sigma_M$  such that  $qa \in T_{\sigma; \sigma_M}$ .*
- *If  $M \Downarrow^{must}$  then there exists some total deterministic strategy  $\sigma : ! \mathbb{N} \rightarrow \sigma_M$  such that  $D_{\sigma; \sigma_M} \neq \emptyset$ .*

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

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

Here,  $\text{case}_{k+1} a n_0 \dots n_k d$  is a new shorthand that evaluates to  $n_i$  if  $a$  evaluates to  $i$ , and evaluates to  $d$  if  $a$  evaluates to  $j > k$ . 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  $\pi$  be a finite evaluation  $\langle s, C[?] \rangle$  that converges to skip. Encode  $\pi$  as a sequence  $n_1, \dots, n_k$ . Let  $d$  be some arbitrary number. Then we can show that the following term also converges to skip in the same way:

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

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  $\pi$  is a finite evaluation of  $\langle s, C[?] \rangle$  that diverges (but nevertheless only involves finitely many calls to the nondeterministic oracle), then the term  $N_{n_1, \dots, n_k, d}(\lambda n.C[n])$  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  $\text{nat} \rightarrow \text{com}$  the denotation of  $N_{n_1, \dots, n_k, d} F$  is given by the composite

$$I \xrightarrow{\text{cell}_0} ! \text{Var} \xrightarrow{\llbracket \lambda v.v := (\text{suc } @v); \text{case}_{k+1} @v \Omega n_1 \dots n_k d \rrbracket} ! \mathbb{N} \xrightarrow{\llbracket F \rrbracket} \mathbb{C}.$$

We set  $\sigma_{\pi}$  to be the composite of the left two arrows. Observe that  $\sigma_{\pi}$  is the strategy with unique maximal infinite play as follows.

$$q n_1 \dots q n_k q d q d \dots$$

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



Lastly, we need to deal with the case that there is an infinite evaluation  $\pi = n_1, n_2, \dots$  of  $M$  that consults the nondeterministic oracle infinitely often. In this case,  $M$  must certainly diverge along the evaluation  $\pi$ . For each  $j$ , we define  $\pi_n^{(j)}$  to be the strategy for  $!N$  corresponding to the term  $N_{n_1, \dots, n_j, \Omega}$ . So  $\pi_n^{(j)}$  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  $N_{n_1, \dots, n_j, \Omega}(\lambda n. C[n])$  must diverge, since it will proceed according to the evaluation  $\pi$  and eventually reach the divergence (since  $\pi$  consults the oracle infinitely often). This implies that  $D_{\sigma_\pi^{(j)}; \sigma_M} \neq \emptyset$  for all  $j$ .

We define  $\sigma_\pi$  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  $D_{\sigma_\pi; \sigma_M} \neq \emptyset$ .

$\sigma_\pi$  has plays of the form

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

and so it is total.  $\square$

From this result, we can prove the converse, which we will also need.

**Lemma 4.3.** *Let  $M = C[?]$  be as before. Let  $\sigma: !\mathbb{N}$  be a total deterministic strategy.*

- *If  $qa \in T_{\sigma; \sigma_M}$  then  $M \Downarrow \text{skip}$ .*
- *If  $D_{\sigma; \sigma_M} \neq \emptyset$  then  $M \Downarrow^{\text{must}}$ .*

*Proof.* Since  $\sigma$  is total and deterministic, it must have a maximal infinite play  $s_\sigma$  of the form

$$q \ m_1 \ q \ n_2 \ \cdots,$$

where  $m_1, m_2, \dots$  is some infinite sequence of natural numbers. If the strategy  $\sigma_M$  contains some play  $s$  such that  $s|_{\mathbb{N}} = s_\sigma$ , then  $\sigma = \sigma_\pi$  for some infinite evaluation  $\pi$  of  $M$ . Otherwise, let  $t$  be the maximal sub-play of  $s$  such that  $s|_{\mathbb{N}} = t$  for some  $s \in \sigma_M$ . Then, if we replace  $\sigma$  with the strategy  $\sigma'$  that plays according to  $t$  and subsequently plays  $q \ d \ q \ d \ \cdots$  for our fixed value  $d$ , then we will have  $\sigma'; \sigma_M = \sigma; \sigma_M$ . Moreover,  $\sigma' = \sigma_\pi$  for some evaluation  $\pi$  of  $M$ .

Now suppose that there exists  $\sigma: !\mathbb{N}$  such that  $qa \in T_{\sigma; \sigma_M}$ . By the proof of Lemma 4.2, we may assume that  $\sigma = \sigma_\pi$  for some evaluation  $\pi$  of  $M$ . Therefore,  $qa \in T_{\sigma_\pi; \sigma_M}$ , which means that  $M \Downarrow \text{skip}$  along the evaluation  $\pi$ . The corresponding statement for must convergence follows in the same way.  $\square$

We can now prove our computational adequacy result.

*Proof of Proposition 4.1.* We prove this for must convergence; the corresponding proof for may convergence is very similar.

Let  $M = C[?]$  be a closed term, where  $C$  is a deterministic context. Then, by Lemmas 4.2 and 4.3, we see that  $M \Downarrow^{\text{must}}$  if and only if there exists some total deterministic  $\sigma: !\mathbb{N}$  such that  $D_{\sigma; \sigma_M} \neq \emptyset$ . By examining the definition of composition, we see that this is the case if and only if  $D_{\llbracket M \rrbracket} = D_{\tau_N; \sigma_M} \neq \emptyset$ .  $\square$

We define *extensional equivalence of strategies* as follows. If  $\sigma, \tau$  are two strategies for a game  $A$ , we say that  $\sigma \sim \tau$  if for all test morphisms  $\alpha: A \rightarrow \mathbb{C}$  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  $\llbracket M \rrbracket \sim \llbracket N \rrbracket$  then  $M \equiv_{m\&m} N$ .*

### 4.3 Universality

Let  $S, T$  be Idealized Algol types and let  $\sigma: S \rightarrow T$  be a morphism in  $\mathcal{G}_{ND, vis, rec}^1$ . We want to prove that  $\sigma$  is the denotation of some term.

By our nondeterministic factorization result, we know that  $\sigma = \tau_N; \text{Det}(\sigma)$ , where  $\text{Det}(\sigma)$  is a deterministic strategy. By universality for  $\mathcal{G}_{D, vis, rec}^1$ , we know that  $\text{Det}(\sigma) = \llbracket M \rrbracket$  for some closed term  $M: S \rightarrow T$ . Then  $\sigma = \tau_N; \text{Det}(\sigma) = \llbracket ? \rrbracket; \llbracket M \rrbracket = \llbracket M ? \rrbracket$ .

### 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  $\llbracket M \rrbracket \sim \llbracket N \rrbracket$ .*

*Proof.* Let  $A = \llbracket T \rrbracket$ . Suppose that  $\llbracket M \rrbracket \not\sim \llbracket N \rrbracket$ ; so there is some strategy  $\alpha: A \rightarrow \mathbb{C}$  such that  $\llbracket M \rrbracket; \alpha \neq \llbracket N \rrbracket; \alpha$ . By universality, we have  $A = \llbracket P \rrbracket$  for some closed term  $P$  of type  $T \rightarrow \text{com}$ . Then we have  $\llbracket M \rrbracket; \llbracket P \rrbracket \neq \llbracket N \rrbracket; \llbracket P \rrbracket$ ; by computational adequacy, it follows that  $M \not\equiv_{m\&m} N$ .  $\square$

Of course, this full abstraction holds just as well for  $\mathcal{G}_{ND, vis}^1$ , where we relax the recursivity condition.

## 5 Nondeterministic PCF

We conclude by making a few remarks about the situation when our base deterministic language is PCF rather than Idealized Algol.

Hyland and Ong [Hyland and Ong 2000] gave a model of PCF using games and *innocent strategies*. If  $sab \in P_A$ , where  $b$  is a  $P$ -move such that  $sab$  is visible at  $b$ , and if  $ta \in P_A$  is such that  $\ulcorner sa \urcorner = \ulcorner ta \urcorner$ , then it is possible to show that there

is a unique way to extend  $ta$  by  $b$  such that  $\ulcorner sab \urcorner = \ulcorner tab \urcorner$ . We will abuse notation and refer to this play as  $tab$ , omitting the justification pointer from  $b$ .

If  $\sigma$  is a strategy for  $A$  that is deterministic and  $P$ -visible, we say that  $\sigma$  is *innocent* if and only if whenever  $sab, ta \in \sigma$  are as above, we have  $tab \in \sigma$ .

Tsukada and Ong [Tsukada and Ong 2015] showed that traditional game semantics models are unsuitable for modelling *nondeterministic* PCF: while the definition of *visibility* of strategies can be extended to nondeterministic strategies without difficulty, innocence cannot.

Instead, they use a novel type of game semantics in which strategies are given not by sets of plays but by justified *trees* whose vertices are moves. The difference is subtle but important: from the point of view of countable nondeterminism it allows us to distinguish between terms that take an arbitrarily large finite number of steps to converge and terms that diverge. For example, the denotation of our term  $M$  above has an infinite branch in it, while the denotation of  $N$  has infinitely many finite branches of arbitrary length.

The main advantage of the tree-based model, however, is that it gives rise to a satisfactory synthetic definition of a *nondeterministic innocent* strategy based on sheaves. In fact, Tsukada and Ong do not prove full abstraction for PCF with countable nondeterminism (even though that language may be interpreted within their category), but for PCF with finite nondeterminism.

Having ourselves given a fully abstract model of Idealized Algol with countable nondeterminism, we shall contribute to the process of ‘completing the square’ by giving a sketch of how we can use our techniques to prove adequacy for the Tsukada-Ong model of PCF with countable nondeterminism. A side-effect of this will be to give an alternative proof of adequacy for their model of PCF with finite nondeterminism.

The first observation to make is that our Lemmas 4.2 and 4.3 are not really statements about the category  $\mathcal{G}_{ND,vis}$ , but about the deterministic model  $\mathcal{G}_{D,vis}$ .

For example, the first part of the lemmas says that if  $C[-]$  is an ordinary deterministic Idealized Algol context, then  $C[?] \Downarrow \text{skip}$  if and only if there exists some total deterministic strategy  $\sigma : !\mathbb{N}$  such that  $qa \in T_{\sigma;[\lambda n.C[n]]}$ . Although we have mentioned a term  $(C[?])$  living in nondeterministic Idealized Algol, this can be thought of as a statement about  $C[-]$  itself, which is part of deterministic Idealized Algol. Moreover, the strategy  $\sigma$  and the denotation of  $\lambda n.C[n]$  are both deterministic strategies, so we can interpret Lemmas 4.2 and 4.3 as telling us something about Idealized Algol and its game semantics. We can therefore forget about our nondeterminism model, with its divergence sets and infinite plays (neither of

which are part of the Tsukada-Ong model) and concentrate on the Abramsky-McCusker model of Idealized Algol. Note that although Lemmas 4.2 and 4.3 mention  $T_{\sigma;\sigma_M}$  and  $D_{\sigma;\sigma_M}$ , we can rephrase both of these inside the deterministic model, since the strategies involved are both deterministic.

We want a version of Lemmas 4.2 and 4.3 that can be applied to PCF contexts and the game semantics model  $\mathcal{G}_{inn}$  of PCF. Clearly, the lemma as currently stated does not hold in  $\mathcal{G}_{inn}$ , since the strategies  $\sigma$  that we define are not innocent in general.

Instead, we need to look at the combinatorial structure of the strategies. We observe that if  $\sigma_M : !\mathbb{N} \rightarrow \mathbb{C}$  is a strategy, then there exists a deterministic strategy  $\sigma : !\mathbb{N}$  such that  $qa \in T_{\sigma;\sigma_M}$  if and only if there exists some  $s \in T_{\sigma_M}$  such that  $s|_{\mathbb{C}} = qa$ . In addition, there exists a deterministic strategy  $\sigma : !\mathbb{N}$  such that  $D_{\sigma;\sigma_M} \neq \emptyset$  if and only if  $\sigma_M$  is not *winning*; i.e., either  $\sigma_M$  is not total or there exists some  $s \in T_{\sigma_M}$  with an infinite tail of moves in  $!\mathbb{N}$ . We recover the following version of Lemmas 4.2 and 4.3 which now applies to the interpretation of PCF in  $\mathcal{G}_{inn}$ :

**Lemma 5.1.** *Let  $M = C[?]$  be a term of type  $\text{com}$ . Write  $\sigma_M : !\mathbb{N} \rightarrow \mathbb{C}$  for the denotation of the term  $\lambda n.C[n]$ .*

- $M \Downarrow \text{skip}$  if and only if there exists  $s \in \sigma_M$  such that  $s|_{\mathbb{C}} = qa$ .
- $M \Downarrow^{must}$  if and only if  $\sigma_M$  is winning.

Now we have an inclusion functor  $J : \mathcal{G}_{inn}^! \hookrightarrow \mathcal{G}_{TO}$ , where  $\mathcal{G}_{TO}$  is the Tsukada-Ong category. Since the nondeterministic oracle  $?$  may also be interpreted as a tree-strategy  $\top_{\mathbb{N}}$  in  $\mathcal{G}_{TO}$ , this gives us a model of PCF with countable nondeterminism inside that category.

In order to prove adequacy for this model, we are only going to use two facts about the category  $\mathcal{G}_{TO}$ . The first fact is that the inclusion functor  $J$  preserves the structure of the model  $\mathcal{G}_{inn}$ ; i.e., it is faithful and strong monoidal. The second fact will capture the properties of the morphism  $\top_{\mathbb{N}} : I \rightarrow \mathbb{N}$  in  $\mathcal{G}_{TO}$ .

**Definition 5.2.** Let  $\sigma, \tau : \mathbb{N}_1 \rightarrow \mathbb{N}_2$  be morphisms in  $\mathcal{G}_{inn}^!$ . We say that  $\sigma \approx \tau$  if the following two conditions hold.

- For all  $n \in \omega$ , there exists  $s \in \sigma$  such that  $s|_{\mathbb{N}_2} = qn$  if and only if there exists  $t \in \tau$  such that  $t|_{\mathbb{N}_2} = qn$ .
- $\sigma$  is winning if and only if  $\tau$  is winning.

**Proposition 5.3.** *If  $\sigma, \tau : \mathbb{N} \rightarrow \mathbb{N}$  are morphisms in  $\mathcal{G}_{inn}^!$ , then  $\top_{\mathbb{N}}; J(\sigma) = \top_{\mathbb{N}}; J(\tau)$  in  $\mathcal{G}_{TO}$  if and only if  $\sigma \approx \tau$ .*

This is evidently true if we replace  $\mathcal{G}_{TO}$  with  $\mathcal{G}_{ND}$ , since a strategy  $\rho$  for  $\mathbb{N}$  is determined by the set of  $n$  such that  $qn \in T_{\rho}$  and whether or not  $D_{\rho}$  is empty. It is true in  $\mathcal{G}_{TO}$ , which

allows us to prove the following version of adequacy which is sufficient for the purpose of proving full abstraction.

**Theorem 5.4** (Adequacy for nondeterministic PCF). *Let  $M, N : \text{nat}$  be two terms of nondeterministic PCF. Suppose that for all  $n \in \omega$ ,  $M \Downarrow n$  if and only if  $N \Downarrow n$  and furthermore that  $M \Downarrow^{\text{must}}$  if and only if  $N \Downarrow^{\text{must}}$ . Then  $\llbracket M \rrbracket = \llbracket N \rrbracket$  in  $\mathcal{G}_{TO}$ .*

## Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. EP/K018868/1. 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 EPSRC.

## 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](https://doi.org/10.1016/S0304-3975(99)00047-X)
- Simon Castellan, Pierre Clairambault, and Glynn Winskel. 2016. Concurrent Hyland-Ong games. (Sept. 2016). <https://hal.archives-ouvertes.fr/hal-01068769> working paper or preprint.
- 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.
- Edsger Wybe Dijkstra. 1997. *A Discipline of Programming* (1st ed.). Prentice Hall PTR, Upper Saddle River, NJ, USA.
- 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>
- J. Laird. 2015. Sequential Algorithms for Unbounded Nondeterminism. *Electronic Notes in Theoretical Computer Science* 319 (2015), 271 – 287. <https://doi.org/10.1016/j.entcs.2015.12.017>
- James Laird. 2016. Higher-order Programs as Coroutines. (2016). to appear.
- 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>
- Takeshi Tsukada and C. H. Luke Ong. 2015. Nondeterminism in Game Semantics via Sheaves. In *Proceedings of the 2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) (LICS '15)*. IEEE Computer

- Society, Washington, DC, USA, 220–231. <https://doi.org/10.1109/LICS.2015.30>
- Glynn Winskel. 2013. Strategies as Profunctors. In *Foundations of Software Science and Computation Structures*, Frank Pfenning (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 418–433.