Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 173 (2007) 221–239
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Amb Breaks Well-Pointedness, Ground Amb Doesn't

Paul Blain Levy [1]

University of Birmingham, Birmingham B15 2TT, U.K.

Abstract

McCarthy's amb operator has no known denotational semantics, and its basic operational properties - the context lemma, the compatibility of refinement similarity and convex bisimilarity - have long been open. In this paper, we give a single example program that demonstrates the failure of each of these properties. This shows that there cannot be any well-pointed denotational semantics.
However, we show that, if amb is given at ground type only, then all of these operational properties do hold.

Keywords: McCarthy's amb, applicative simulation, Howe's method, fixpoint, CIU theorem, context lemma

1 Introduction

1.1 The Questions

McCarthy's amb [14] is a kind of fair nondeterminism: M `amb` M' can return any value that M or M' can return, and can diverge only if both M and M' can diverge. This differs from ordinary (*erratic*) nondeterminism $M \sqcap M'$, which can diverge if either M or M' can diverge. Despite its apparent simplicity, amb has been something of an embarrassment for semantics research. It has resisted both denotational modelling and a satisfactory operational treatment, leading to two substantial open problems [6].

The first problem arises from the notion of *applicative bisimulation*, introduced in [1] in the untyped setting and later studied in the typed setting [3]. Applicative bisimilarity was shown to be a congruence by an ingenious method [5]. This method works in both the deterministic and the erratically nondeterministic setting, but as explained in [8], it does not work in the presence of amb. So it has remained open whether applicative bisimilarity, in the presence of amb, is a congruence.

[1] Email: pbl@cs.bham.ac.uk

doi:10.1016/j.entcs.2007.02.036

A second problem is *contextual equivalence*, where we treat both convergence and divergence as observable. In the nondeterministic setting, this is known to be coarser than applicative bisimulation. The *context lemma* states that two terms M and M' that are contextually equivalent in any environment (i.e. under any closing substitution) must be contextually equivalent. This was shown in [5,6] in the erratically nondeterministic setting, but whether it holds in the presence of amb has remained open.

In this paper, we give a single example that simultaneously answers these questions—and some variants using preorders rather than equivalence relations—in the negative. We give two programs M and M' that in any environment must be regarded as equivalent, even when we use the finer relation of applicative bisimilarity. On the other hand, there is a context $\mathcal{C}[\cdot]$ such that $\mathcal{C}[M]$ may diverge and $\mathcal{C}[M']$ cannot. This shows that, in the setting of amb, it is impossible to regard a term as being a function from environments to behaviours. No denotational semantics founded on such a principle can work.

In order to formulate this example, we need to make use of amb at non-ground type. In a calculus that provides amb with ground type only, we shall show that the open questions can be answered affirmatively.

The structure of the paper is as follows. In Sect. 2, we describe our results using a small call-by-name (CBN) calculus, without function types. This makes the example program easy to understand. Then, in Sect. 3–4, to prove our positive results, we move to a call-by-value (CBV) calculus with function types and recursive types.

Remark 1.1 Our example program works for *typed* calculi (which may include recursive types). This is by contrast with [7], where the *untyped* lazy λ-calculus with amb is studied. For that calculus, our example does not work (unless sequencing is added), and the open questions remain open.

2 Small Call-By-Name Calculus

2.1 The Questions

In this section, we consider a call-by-name calculus with ground types and unary sum types, as shown in Fig. 1–2. We write L for the unary sum type constructor, and `pm` as an abbreviation for "pattern-match". We write `diverge` for `rec x. x`. The operational semantics as displayed in Fig. 2 follows the formulation of [16].

For each type A, we define a set $[A]$ as follows:

$$\begin{aligned}[\mathtt{bool}] &= \mathcal{P}\{\mathsf{true}, \mathsf{false}, \bot\} \\ [1] &= \mathcal{P}\{\top, \bot\} \\ [LA] &= \mathcal{P}(\{\mathsf{up}\ B \mid B \in [A]\} \cup \{\bot\})\end{aligned}$$

(We could choose to exclude the empty set from the powersets, but this does not substantially affect our argument.) For each closed term $M : A$ we define its *operational meaning* $[M] \in [A]$ by induction on A:

Types $A ::= \quad \mathtt{bool} \mid 1 \mid LA$

Terms

$$\frac{}{\Gamma \vdash \mathtt{x} : A}\,(\mathtt{x} : A) \in \Gamma \qquad \frac{\Gamma, \mathtt{x} : A \vdash M : A}{\Gamma \vdash \mathtt{rec}\ \mathtt{x}.M : A}$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash M' : A}{\Gamma \vdash M \sqcap M' : A} \qquad \frac{\Gamma \vdash M : A \quad \Gamma \vdash M' : A}{\Gamma \vdash M\ \mathtt{amb}\ M' : A}$$

$$\frac{}{\Gamma \vdash \mathtt{top} : 1} \qquad \frac{\Gamma \vdash M : 1 \quad \Gamma \vdash N : B}{\Gamma \vdash M; N : B}$$

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \mathtt{up}\ M : LA} \qquad \frac{\Gamma \vdash M : LA \quad \Gamma, \mathtt{x} : A \vdash N : B}{\Gamma \vdash \mathtt{pm}\ M\ \mathtt{as}\ \mathtt{up}\ \mathtt{x}.\ N : B}$$

Fig. 1. Syntax of Call-By-Name Language

- if $M : \mathtt{bool}$ then $[M] \stackrel{\text{def}}{=} \{\mathtt{true} \mid M \Downarrow \mathtt{true}\} \cup \{\mathtt{false} \mid M \Downarrow \mathtt{false}\} \cup \{\bot \mid M \Uparrow\}$
- if $M : 1$ then $[M] \stackrel{\text{def}}{=} \{\mathtt{top} \mid M \Downarrow \mathtt{top}\} \cup \{\bot \mid M \Uparrow\}$
- if $M : LA$ then $[M] \stackrel{\text{def}}{=} \{\mathtt{up}\ [N] \mid M \Downarrow \mathtt{up}\ N\} \cup \{\bot \mid M \Uparrow\}$.

We say two terms $M, M' : A$ are *convex bisimilar* when $[M] = [M']$. If A is a ground type, we say they are *behaviourally equivalent*.

Convex bisimilarity is robust, because of the following result, whose proof we defer to Sect. 3.

Proposition 2.1 *If closed terms $\vdash M, M' : A$ are convex bisimilar then $\mathcal{C}[M]$ and $\mathcal{C}[M']$ are convex bisimilar for any context $\mathcal{C}[\cdot]$ of any type, with hole of type A.*

Suppose we wish to identify closed *ground* terms precisely when they are behaviourally equivalent. As explained in [9], domain semantics, in which $\mathtt{diverge} \leqslant \mathtt{true}$, cannot be used. For then

$$\mathtt{true} \sqcap \mathtt{diverge} \leqslant \mathtt{true} \sqcap \mathtt{true} = \mathtt{true}$$

but, if amb is monotone, we also have

$$\begin{aligned} \mathtt{true} &= \mathtt{if}\ (\mathtt{false}\ \mathtt{amb}\ \mathtt{diverge})\ \mathtt{then}\ \mathtt{diverge}\ \mathtt{else}\ \mathtt{true} \\ &\leqslant \mathtt{if}\ (\mathtt{false}\ \mathtt{amb}\ \mathtt{true})\ \mathtt{then}\ \mathtt{diverge}\ \mathtt{else}\ \mathtt{true} \\ &= \mathtt{true} \sqcap \mathtt{diverge} \end{aligned}$$

Hence $\mathtt{true} \sqcap \mathtt{diverge} = \mathtt{true}$, contradicting behavioural equivalence. So in any domain semantics of nondeterminism, either $\mathtt{true} \sqcap \mathtt{diverge}$ and $\mathtt{true}$ are identified (as in Hoare's theory), or amb is not monotone (as in the theories of Smyth and Plotkin). In fact, no denotational model of ground behavioural equivalence for this calculus is known.

We say that two open terms $\Gamma \vdash M, M' : B$ are

The following closed terms are *terminal*

$$T ::= \quad \texttt{true} \mid \texttt{false} \mid \texttt{top} \mid \texttt{up}\ M$$

Convergence Relation $M \Downarrow T$—Inductive Definition

$$\frac{M \Downarrow T}{M \sqcap M' \Downarrow T} \qquad \frac{M' \Downarrow T}{M \sqcap M' \Downarrow T} \qquad \frac{M[\texttt{rec x}.M/\texttt{x}] \Downarrow T}{\texttt{rec x}.M \Downarrow T}$$

$$\frac{M \Downarrow T}{M\ \texttt{amb}\ M' \Downarrow T} \qquad \frac{M' \Downarrow T}{M\ \texttt{amb}\ M' \Downarrow T} \qquad \frac{M \Downarrow \texttt{true} \quad N \Downarrow T}{\texttt{if}\ M\ \texttt{then}\ \ \texttt{then}\ N\ \texttt{else}\ N' \Downarrow T}$$

$$\frac{}{\texttt{true} \Downarrow \texttt{true}} \qquad \frac{}{\texttt{false} \Downarrow \texttt{false}} \qquad \frac{M \Downarrow \texttt{false} \quad N' \Downarrow T}{\texttt{if}\ M\ \texttt{then}\ \ \texttt{then}\ N\ \texttt{else}\ N' \Downarrow T}$$

$$\frac{}{\texttt{top} \Downarrow \texttt{top}} \qquad \frac{M \Downarrow \texttt{top} \quad N \Downarrow T}{M; N \Downarrow T}$$

$$\frac{}{\texttt{up}\ M \Downarrow \texttt{up}\ M} \qquad \frac{M \Downarrow \texttt{up}\ P \quad N[P/\texttt{x}] \Downarrow T}{\texttt{pm}\ M\ \texttt{as up x}.\ N \Downarrow T}$$

Divergence Predicate $M \Uparrow$—Coinductive Definition

$$\frac{M \Uparrow}{M \sqcap M' \Uparrow} \qquad \frac{M' \Uparrow}{M \sqcap M' \Uparrow} \qquad \frac{M \Uparrow}{\texttt{if}\ M\ \texttt{then}\ N\ \texttt{else}\ N' \Uparrow}$$

$$\frac{M[\texttt{rec x}.M/\texttt{x}] \Uparrow}{\texttt{rec x}.M \Uparrow} \qquad \frac{M \Uparrow \quad M' \Uparrow}{M\ \texttt{amb}\ M' \Uparrow} \qquad \frac{M \Downarrow \texttt{true} \quad N \Uparrow}{\texttt{if}\ M\ \texttt{then}\ \ \texttt{then}\ N\ \texttt{else}\ N' \Uparrow}$$

$$\frac{M \Uparrow}{M; N \Uparrow} \qquad \frac{M \Downarrow \texttt{top} \quad N \Uparrow}{M; N \Uparrow} \qquad \frac{M \Downarrow \texttt{false} \quad N' \Uparrow}{\texttt{if}\ M\ \texttt{then}\ \ \texttt{then}\ N\ \texttt{else}\ N' \Uparrow}$$

$$\frac{M \Uparrow}{\texttt{pm}\ M\ \texttt{as up x}.\ N \Uparrow} \qquad \frac{M \Downarrow \texttt{up}\ P \quad N[P/\texttt{x}] \Uparrow}{\texttt{pm}\ M\ \texttt{as up x}.\ N \Uparrow}$$

Fig. 2. Big-Step Semantics For A Call-By-Name Calculus

(i) *convex applicatively bisimilar* when $M[\overrightarrow{N/\mathtt{x}}]$ and $M'[\overrightarrow{N/\mathtt{x}}]$ are bisimilar for every Γ-environment $\overrightarrow{N/\mathtt{x}}$

(ii) *contextually equivalent* when $\mathcal{C}[M]$ and $\mathcal{C}[M']$ are behaviourally equivalent for every ground context $\mathcal{C}[\cdot]$ with hole inhabiting $\Gamma \vdash B$

(iii) *CI equivalent* (CI stands for "closed instantiation") when $M[\overrightarrow{N/\mathtt{x}}]$ and $M'[\overrightarrow{N/\mathtt{x}}]$ are observationally equivalent for every Γ-environment $\overrightarrow{N/\mathtt{x}}$.

The two open problems of [6], stated there in a rich setting with function types and recursive types, are as follows.

(i) Is convex applicative bisimilarity a congruence?

(ii) Does CI equivalence imply contextual equivalence? (Such a result is called a *context lemma* or a *CI theorem*.)

There are also variants of these questions using preorders rather than equivalence relations. In the setting of erratic choice, all of these questions have been affirmatively answered [5,6,12]. But it did not seem possible to adapt these techniques to `amb` [8]. So the questions have remained open.

2.2 The Counterexample

We will now give a single example that answers both these questions (and the preorder variants) negatively. Define the terms $\mathtt{x} : L1 \vdash M, M' : L1$ as follows.

$$M \stackrel{\text{def}}{=} (\mathtt{up}\ \mathtt{top})\ \mathtt{amb}\ (\mathtt{pm}\ \mathtt{x}\ \mathtt{as}\ \mathtt{up}\ \mathtt{z}.\mathtt{up}\ (\mathtt{top} \sqcap \mathtt{z}))$$
$$M' \stackrel{\text{def}}{=} \mathtt{up}\ (\mathtt{top} \sqcap \mathtt{pm}\ (\mathtt{x}\ \mathtt{amb}\ \mathtt{up}\ \mathtt{top})\ \mathtt{as}\ \mathtt{up}\ \mathtt{y}.\mathtt{y})$$
$$M'' \stackrel{\text{def}}{=} M \sqcap M'$$

For any closed term $\vdash N : L1$, the terms $M[N/\mathtt{x}]$ and $M''[N/\mathtt{x}]$ are behaviourally equivalent. (This is true even if we introduce a constant at each type representing the empty set.)

- Neither is able to diverge.
- Both are able to return $\mathtt{up}\ P$, for some P such that $P \Downarrow \mathtt{top}$ but $P \not\Uparrow$.
- Neither is able to return $\mathtt{up}\ P$, for some P such that $P \not\Downarrow \mathtt{top}$.
- Both are able to return $\mathtt{up}\ P$, for some P such that $P \Downarrow \mathtt{top}$ and $P \Uparrow$, precisely if N is able to return $\mathtt{up}\ Q$ for some Q such that $Q \Uparrow$.

Thus M and M'' are convex applicative bisimilar. Hence, by Prop. 2.1, they are also CI equivalent. But they are not contextually equivalent; for example, they can be distinguished by the context

$$\mathcal{C}[\cdot] \stackrel{\text{def}}{=} \mathtt{pm}\ (\mathtt{up}\ \mathtt{top}\ \mathtt{amb}\ (\mathtt{rec}\ \mathtt{x}.[\cdot]))\ \mathtt{as}\ \mathtt{up}\ \mathtt{u}.\ \mathtt{u}\ \ : 1$$

We first observe that

(i) if $\mathtt{rec}\ \mathtt{x}.M \Downarrow \mathtt{up}\ N$, then, by induction on the evaluation, we have $N = (\mathtt{top} \sqcap\ )^n\ \mathtt{top}$, and so N cannot diverge

(ii) $\mathtt{rec}\ \mathtt{x}.M'' \Downarrow \mathtt{up}\ (\mathtt{top} \sqcap \mathcal{C}[M''])$ by taking the right-hand choice.

(i) gives us $\mathcal{C}[M] \not\Uparrow$. To show $\mathcal{C}[M'] \Uparrow$, we consistently take the right-hand choice. Formally, we have

$$\{\mathcal{C}M'', \mathtt{top} \sqcap \mathcal{C}M''\} \sqsubseteq \Uparrow$$

by simple coinduction, using (ii).

This example rules out any denotational semantics that is *well-pointed*, i.e. in which the semantics of a term is a function from environments. Operationally, M and M'' describe the same endofunction f on $[L1]$, mapping C to $\{\mathtt{up}\ \{\top\}, \mathtt{up}\ \{\top, \bot\}\}$ if $\exists D \in [1].\ (\bot \in D \wedge \mathtt{up}\ D \in C)$, and to $\{\mathtt{up}\ \{\top\}\}$ otherwise. But f has *two* fixpoints, viz. $\{\mathtt{up}\ \{\top\}\}$ and $\{\mathtt{up}\ \{\top\}, \mathtt{up}\ \{\top, \bot\}\}$. And the operational argument shows us that $[\mathtt{rec}\ \mathtt{x}.M]$ is the former, and $[\mathtt{rec}\ \mathtt{x}.M'']$ the latter. So there is no *right* way of computing the recursive fixpoint. (Cf. the fixpoint example in [13].)

2.3 Uses

A *use* is a special kind of ground context that can be applied to a closed term.

- A use of $\mathtt{bool}$ is a ground context $\mathtt{if}\ [\cdot]\ \mathtt{then}\ N\ \mathtt{else}\ N'$.
- A use of 1 is a ground context $[\cdot]; N$.
- A use of LA is a ground context $\mathtt{pm}\ [\cdot]\ \mathtt{as}\ \mathtt{up}\ \mathtt{x}.\ N$.

Two closed terms $\vdash M, M' : A$ are *uses equivalent* when $\mathcal{C}[M]$ and $\mathcal{C}[M]'$ are behaviourally equivalent for every use $\mathcal{C}[\cdot]$ of A. More generally, two open terms $\Gamma \vdash M, M' : A$ are *CIU equivalent* when $\mathcal{C}[M[\overrightarrow{V/\mathtt{x}}]]$ and $\mathcal{C}[M'[\overrightarrow{V/\mathtt{x}}]]$ are behaviourally equivalent for every Γ-environment $\overrightarrow{V/\mathtt{x}}$ and every use $\mathcal{C}[\cdot]$ of A.

A *uses theorem* states that uses equivalence implies contextual equivalence. A *CIU theorem* is the conjunction of a CI theorem and a uses theorem, stating that CIU equivalence implies contextual equivalence. This theorem (and preorder variants) is known to hold in the deterministic [18] and erratically nondeterministic [6] settings.

Like the CI theorem, the uses theorem fails in the presence of $\mathtt{amb}$. To see this, define terms $\vdash M, M' : L1$ as follows:

$$M \stackrel{\text{def}}{=} \mathtt{diverge} \sqcap \mathtt{up}\ \mathtt{top}$$
$$M' \stackrel{\text{def}}{=} M \sqcap \mathtt{up}\ (\mathtt{top} \sqcap \mathtt{diverge})$$

Now for any ground term $\mathtt{x} : 1 \vdash N : C$, the terms $M\ \mathtt{to}\ \mathtt{x}.\ N$ and $M'\ \mathtt{to}\ \mathtt{x}.\ N$ both diverge. Moreover, they converge to the same things, because M and M' are "may contextually equivalent" (see e.g. [6]). So M and M' are uses equivalent. But they are not contextually equivalent; for example, they can be distinguished by

$$\mathcal{C}[\cdot] = \mathtt{pm}\ ([\cdot]\ \mathtt{amb}\ \mathtt{up}\ \mathtt{top})\ \mathtt{as}\ \mathtt{x}.\ \mathtt{x} \quad : 1$$

$\mathcal{C}[M']$ may diverge, whereas $\mathcal{C}[M]$ cannot.

2.4 Ground Amb

In the examples in Sect. 1.1–2.3, crucial use was made of `amb` at the non-ground type $L1$. If we allow `amb` at ground type only, then all the questions can be answered affirmatively. We prove this in Sect. 4.

2.5 Strong and Weak Divergence

As suggested in [17], if we are concerned with branching-time behaviour, it might be reasonable to distinguish different kinds of divergence. When a term diverges, either

- convergence remains possible throughout, or
- it is eventually the case that only divergence is possible.

These two kinds of divergence are called *weak* and *strong* respectively. For example, the program P_n

> Choose $n+1$ booleans. If they're all true, then terminate, else:
>
> > choose $n+2$ booleans. If they're all true, then terminate, else:
> >
> > > choose $n+3$ booleans. If they're all true, then terminate, else:
> > >
> > > ...

can weakly diverge, but cannot strongly diverge. The same is true of $\mathcal{C}[M'']$.

Our claim that $M[N/\mathtt{x}]$ and $M''[N/\mathtt{x}]$ have the same range of behaviours for any N continues to hold even if we distinguish these kinds of divergence. And it seems likely that Prop. 2.1 could be adapted to a finer notion of bisimulation that makes this distinction. So the distinction does not destroy our example.

In order to encode λ-calculus with amb into the π-calculus, [2] takes this a step further: not merely distinguishing strong from weak divergence, but disregarding weak divergence entirely. Our example is not then applicable, because $\mathcal{C}[M'']$ cannot strongly diverge.

Remark 2.2 If we treat the boolean choices as probabilistic, with 0.5 probability of true, then the program P_n diverges with probability greater than $> 1-2^{-n}$, which is close to 1 if n is large. It seems hard to justify disregarding this divergence, if one cares about divergence in the first place.

3 A Call-By-Value Calculus

For the operational techniques in this paper, it is easiest to work with call-by-value. They can be adapted to call-by-push-value, and hence to call-by-name, but at the cost of some complication. The types of our calculus are as follows:

$$\textbf{coinductive definition} \qquad A ::= \sum_{i \in I} A_i \mid 1 \mid A \times A \mid A \to A$$

where I ranges over countable sets. We make the type syntax coinductive so that we get equirecursive types (i.e. equality $\mu \mathtt{X}.A = A[\mu \mathtt{X}.A/\mathtt{X}]$ rather than mere isomorphism). We define the *ground types* coinductively by

$$C ::= \quad \textstyle\sum_{i \in I} C_i \mid 1 \mid C \times C$$

We omit rules for 1 as they are analogous to those for $\times$.

We use a fine-grain call-by-value calculus[2] that explicitly distinguishes values from ordinary terms. So there are two judgements: $\Gamma \vdash M : B$ means that M is a term of type B, and $\Gamma \vdash^{\mathsf{v}} V : B$ means that V is a value of type B. The syntax is defined inductively in Fig. 3.

$$\frac{}{\Gamma, \mathtt{x} : A, \Gamma' \vdash^{\mathsf{v}} \mathtt{x} : A} \qquad \frac{\Gamma \vdash^{\mathsf{v}} V : A \quad \Gamma, \mathtt{x} : A \vdash M : B}{\Gamma \vdash \mathtt{let}\ V\ \mathtt{be}\ \mathtt{x}.\ M : B}$$

$$\frac{\Gamma \vdash^{\mathsf{v}} V : A}{\Gamma \vdash \mathtt{return}\ V : A} \qquad \frac{\Gamma \vdash M : A \quad \Gamma, \mathtt{x} : A \vdash N : B}{\Gamma \vdash M\ \mathtt{to}\ \mathtt{x}.\ N : B}$$

$$\frac{\Gamma \vdash^{\mathsf{v}} V : A \quad \Gamma \vdash^{\mathsf{v}} V' : A'}{\Gamma \vdash^{\mathsf{v}} \langle V, V' \rangle : A \times A'} \qquad \frac{\Gamma \vdash^{\mathsf{v}} V : A \times A' \quad \Gamma, \mathtt{x} : A, \mathtt{y} : A' \vdash M : B}{\Gamma \vdash \mathtt{pm}\ V\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y} \rangle.\ M : B}$$

$$\frac{\Gamma \vdash^{\mathsf{v}} V : A_{\hat{\imath}}}{\Gamma \vdash^{\mathsf{v}} \langle \hat{\imath}, V \rangle : \textstyle\sum_{i \in I} A_i}\ \hat{\imath} \in I \qquad \frac{\Gamma \vdash^{\mathsf{v}} V : \textstyle\sum_{i \in I} A_i \quad \Gamma, \mathtt{x} : A_i \vdash M_i : B\ \ (\forall i \in I)}{\Gamma \vdash \mathtt{pm}\ V\ \mathtt{as}\ \{\langle i, \mathtt{x} \rangle . M_i\}_{i \in I} : B}$$

$$\frac{\Gamma, \mathtt{f} : A \to B, \mathtt{x} : A \vdash M : B}{\Gamma \vdash^{\mathsf{v}} \mathtt{rec}\ \mathtt{f} \lambda \mathtt{x}.M : A \to B} \qquad \frac{\Gamma \vdash^{\mathsf{v}} V : A \to B \quad \Gamma \vdash^{\mathsf{v}} W : A}{\Gamma \vdash VW : B}$$

$$\frac{\Gamma \vdash M_i : B\ \ (\forall i \in I)}{\Gamma \vdash \mathtt{choose}_{\ i \in I}.M_i : B} \qquad \frac{\Gamma \vdash M_i : B\ \ (\forall i \in I)}{\Gamma \vdash\ \mathtt{amb}_{\ i \in I}.M_i : B}$$

Fig. 3. Syntax Of Fine-Grain CBV With Countable Nondeterminism

The operational semantics is given in Fig. 4. Instead of defining $\Downarrow$ coinductively, we define its complement $\Downarrow_{\Box}$ inductively. That is clearly equivalent, but makes reasoning easier.

Remark 3.1 We can treat the CBN calculus of Sect. 2 in precisely the same way as our CBV calculus. Indeed, the former is a fragment of the latter via the standard thunking transformation [4], translating LA as $1 \to \overline{A}$. But this only works because the CBN calculus lacks function types.

[2] For comparison with similar calculi such as Moggi's monadic metalanguage [15], see [11].

If we wished to include CBN function types, or, more generally, to work with call-by-push-value [10], we would require other techniques. As this is not specific to `amb`, we do not treat it in this paper.

May Convergence (inductive definition)

$$\frac{M[W/\mathtt{x}] \Downarrow V}{\mathtt{let}\ W\ \mathtt{be}\ \mathtt{x}.\ M \Downarrow V} \qquad \frac{M[\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M/\mathtt{f}, W/\mathtt{x}] \Downarrow V}{(\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M)W \Downarrow V}$$

$$\frac{}{\mathtt{return}\ V \Downarrow V} \qquad \frac{M \Downarrow W \quad N[W/\mathtt{x}] \Downarrow V}{M\ \mathtt{to}\ \mathtt{x}.\ N \Downarrow V}$$

$$\frac{M_{\hat{\imath}}[W/\mathtt{x}] \Downarrow V}{\mathtt{pm}\ \langle \hat{\imath}, W\rangle\ \mathtt{as}\ \{\langle i, \mathtt{x}\rangle.M_i\}_{i\in I} \Downarrow V}\ \hat{\imath} \in I \qquad \frac{M[W/\mathtt{x}, W'/\mathtt{y}] \Downarrow V}{\mathtt{pm}\ \langle W, W'\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M \Downarrow V}$$

$$\frac{M_{\hat{\imath}} \Downarrow V}{\mathtt{choose}_{i\in I} M_i \Downarrow V}\ \hat{\imath} \in I \qquad \frac{M_{\hat{\imath}} \Downarrow V}{\mathtt{amb}_{i\in I} M_i \Downarrow V}\ \hat{\imath} \in I$$

Must convergence (inductive definition)

$$\frac{}{\mathtt{return}\ V \Downarrow_\Box} \qquad \frac{M \Downarrow_\Box \quad \forall W(M \Downarrow W \Rightarrow N[W/\mathtt{x}] \Downarrow_\Box)}{M\ \mathtt{to}\ \mathtt{x}.\ N \Downarrow_\Box}$$

$$\frac{M[W/\mathtt{x}] \Downarrow_\Box}{\mathtt{let}\ W\ \mathtt{be}\ \mathtt{x}.\ M \Downarrow_\Box} \qquad \frac{M[\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M/\mathtt{f}, W/\mathtt{x}] \Downarrow_\Box}{(\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M)W \Downarrow_\Box}$$

$$\frac{M_{\hat{\imath}}[W/\mathtt{x}] \Downarrow_\Box}{\mathtt{pm}\ \langle \hat{\imath}, W\rangle\ \mathtt{as}\ \{\langle i, \mathtt{x}\rangle.M_i\}_{i\in I} \Downarrow_\Box}\ \hat{\imath} \in I \qquad \frac{M[W/\mathtt{x}, W'/\mathtt{y}] \Downarrow_\Box}{\mathtt{pm}\ \langle W, W'\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M \Downarrow_\Box}$$

$$\frac{M_{\hat{\imath}} \Downarrow_\Box}{\mathtt{choose}_{i\in I} M_i \Downarrow_\Box}\ \hat{\imath} \in I \qquad \frac{M_i \Downarrow_\Box \quad (\forall i \in I)}{\mathtt{amb}_{i\in I} M_i \Downarrow_\Box}\ \hat{\imath} \in I$$

Fig. 4. Big-Step Semantics For Fine-Grain CBV

Definition 3.2 (i) A *closed relation* R associates to each type A a binary relation on the closed terms inhabiting it, and a binary relation on the closed values inhabiting it.

(ii) An *open relation* $\mathcal{R}$ associates to each sequent $\Gamma \vdash A$ a binary relation on the terms inhabiting it, and to each value sequent $\Gamma \vdash^{\mathsf{v}} A$ a binary relation on the values inhabiting it, such that if $\Gamma \vdash M\,\mathcal{R}\,M' : B$ and $\Gamma \subseteq \Gamma'$ then $\Gamma' \vdash M\,\mathcal{R}\,M' : B$, and similarly for values.

(iii) We write id for the identity relation on terms and values, and idf for the identity relation restricted to identifiers.

(iv) We write $\mathcal{E}$ for the universal relation on terms and values (relating everything to everything).

(v) We write ; for relational composition, in diagrammatic order.

(vi) We write R^* for the reflexive transitive closure of R.

(vii) If $\mathcal{R}$ is an open relation, we write $\mathcal{R}_0$ for the restriction of $\mathcal{R}$ to closed terms and closed values.

(viii) Let R be a closed relation. We define R° (the *open extension* of R) to be the open relation that relates two terms $\Gamma \vdash M, N : B$ when $M[\overrightarrow{V/\mathtt{x}}]\, R\, N[\overrightarrow{V/\mathtt{x}}]$ for any substitution $\overrightarrow{V/\mathtt{x}}$ from Γ to the empty context.

(ix) Let R be a closed relation. We define R^{w} (the *weakening extension* of R) to be the open relation that relates two terms $\Gamma \vdash M, N : B$ when M and N are both closed and $M\, R\, N$.

Definition 3.3 (i) Let $\mathcal{R}$ and $\mathcal{S}$ be open relations. We define $\mathcal{R}[\mathcal{S}]$ (the *substitution of $\mathcal{S}$ into $\mathcal{R}$*) to be the open relation consisting of the pairs of terms $\Delta \vdash M[\overrightarrow{V/\mathtt{x}}], N[\overrightarrow{W/\mathtt{x}}] : B$ for every pair of terms $\Gamma \vdash M, N : B$ and pair of substitutions $\Gamma \xrightarrow{\overrightarrow{V/\mathtt{x}}} \Delta$ and $\Gamma \xrightarrow{\overrightarrow{W/\mathtt{x}}} \Delta$ such that $M\, \mathcal{R}\, N$ and $V_{\mathtt{x}}\, \mathcal{S}\, W_{\mathtt{x}}$ for each $(\mathtt{x} : A) \in \Gamma$.

(ii) An open relation $\mathcal{S}$ is *substitutive* when $\mathsf{idf} \subseteq \mathcal{S}$ and $\mathcal{S}[\mathcal{S}] \subseteq \mathcal{S}$.

Definition 3.4 Let $\mathcal{R}$ be an open relation.

(i) We define $\widehat{\mathcal{R}}$ (the *compatible refinement* of $\mathcal{R}$) to be the open relation that relates two terms $\theta\{M_i\}_{i\in I}$ and $\phi\{N_j\}_{j\in J}$ when $\theta = \phi$ (hence $I = J$), and $M_i\, \mathcal{R}\, N_i$ for each $i \in I$.

(ii) $\mathcal{S}$ is *compatible* when $\widehat{\mathcal{S}} \subseteq \mathcal{S}$.

(iii) We define $\mathcal{R}^{\mathsf{SC}}$ (the *substitutive compatible closure* of $\mathcal{R}$) to be the least substitutive compatible relation containing $\mathcal{R}$.

Lemma 3.5 *Let R be a closed relation. Then $R^{\mathsf{wSC}} \subseteq R^{\mathsf{w}} \cup \widehat{R^{\mathsf{wSC}}}$. Hence $R^{\mathsf{wSC}}{}_0 \subseteq R \cup \widehat{R^{\mathsf{wSC}}}_0$.*

Proof.

$$R^{\mathsf{wSC}} = R^{\mathsf{w}}[R^{\mathsf{wSC}}] \cup \widehat{R^{\mathsf{wSC}}} \subseteq R^{\mathsf{w}}[\mathcal{E}] \cup \widehat{R^{\mathsf{wSC}}} \subseteq R^{\mathsf{w}} \cup \widehat{R^{\mathsf{wSC}}}$$

□

For reasoning about operational semantics, the following variant of $\widehat{-}$ is useful.

Definition 3.6 If $\mathcal{R}$ is an open relation, we define $\grave{\mathcal{R}}$ to be the closed relation that relates

- $\mathtt{let}\ V\ \mathtt{be}\ \mathtt{x}.M$ to $\mathtt{let}\ V'\ \mathtt{be}\ \mathtt{x}.\ M'$, where $V\, \mathcal{R}\, V'$ and $M\, \mathcal{R}\, M'$

- $\texttt{return}\ V$ to $\texttt{return}\ V'$, where $V \mathcal{R} V'$
- $M_0\ \texttt{to}\ \texttt{x}.\ M_1$ to $M_0'\ \texttt{to}\ \texttt{x}.\ M_1'$, where $M_0 \mathcal{R} M_0'$ and $M_1 \mathcal{R} M_1'$
- $\texttt{pm}\ \langle V_0, V_1\rangle\ \texttt{as}\ \langle \texttt{x}, \texttt{y}\rangle.\ M$ to $\texttt{pm}\ \langle V_0', V_1'\rangle\ \texttt{as}\ \langle \texttt{x}, \texttt{y}\rangle.\ M'$, where $V_0 \mathcal{R} V_0'$ and $V_1 \mathcal{R} V_1'$ and $M \mathcal{R} M'$
- $\texttt{pm}\ \langle \hat{\imath}, V\rangle\ \texttt{as}\ \{\langle i, \texttt{x}\rangle.\ M_i\}_{i\in I}$ to $\texttt{pm}\ \langle \hat{\imath}, V'\rangle\ \texttt{as}\ \{\langle i, \texttt{x}\rangle.\ M_i'\}_{i\in I}$ where $V \mathcal{R} V'$ and $M_i \mathcal{R} M_i'$ for each $i \in I$
- $(\texttt{rec}\ \texttt{f}\lambda\texttt{x}.M)V$ to $(\texttt{rec}\ \texttt{f}\lambda\texttt{x}.M')V'$ where $M \mathcal{R} M'$ and $V \mathcal{R} V'$
- $\texttt{choose}_{\ i\in I}.\ M_i$ to $\texttt{choose}_{\ i\in I}.\ M_i'$, where $M_i \mathcal{R} M_i'$ for each $i \in I$
- $\texttt{amb}_{\ i\in I}.\ M_i$ to $\texttt{amb}_{\ i\in I}.\ M_i'$, where $M_i \mathcal{R} M_i'$ for each $i \in I$.

Definition 3.7 Let R be a closed relation.

(i) R *respects tuples* when
- $\langle \hat{\imath}, V\rangle\, R\, \langle \hat{\imath}', V'\rangle : \sum_{i\in I} A_i$ implies $\hat{\imath} = \hat{\imath}'$ and $V\, R\, V' : A_{\hat{\imath}}$,
- $\langle V_0, V_1\rangle\, R\, \langle V_0', V_1'\rangle : A_0 \times A_1$ implies $V_0\, R\, V_0' : A_0$ and $V_1\, R\, V_1' : A_1$.

(ii) R *respects functions* when $V\, R\, V' : A \to B$ implies $VW\, R\, V'W : B$ for every closed value $W : A$

(iii) We say that R is a *lower applicative simulation* when it respects tuples and functions, and $M\, R\, M'$ and $M \Downarrow V$ implies $M' \Downarrow V'$ for some V' such that $V\, R\, V'$. If, moreover, $M\, R\, M'$ and $M \Uparrow$ implies $M' \Uparrow$, then R is a *lower+divergence applicative simulation.*

(iv) We say that R is a lower (resp. lower+divergence) applicative *bisimulation* when R and R^{op} are both lower (resp. divergence) simulations.

(v) We say that R is a *lower+divergence applicative sesquisimulation* when it is a lower+divergence simulation and a lower bisimulation.

The dual of a lower+divergence simulation is called a *refinement simulation* in [6].

We define lower applicative *similarity* to be the greatest lower applicative simulation, and so forth for the other kinds of simulation.

It is convenient to define contextual equivalence (and inequality) without formally defining contexts.

Definition 3.8 Let R be a closed relation.

- R is *may-preadequate* when, if $M\, R\, M' : A$ where A is a ground type, and $M \Downarrow n$ then $M' \Downarrow n$. It is *may-adequate* when both R and R^{op} are may preadequate.
- R is *preadequate* when it is preadequate and, if $M\, R\, M' : A$ where A is a ground type, and $M \Uparrow$ then $M' \Uparrow$. It is *adequate* when both R and R^{op} are preadequate.

Definition 3.9 Let $\Gamma \vdash M, M' : A$ be terms. Write $\mathcal{R}_{(M,M')}$ for the substitutive compatible closure of the open relation that only relates $\Gamma' \vdash M, M' : A$ for $\Gamma' \supseteq \Gamma$. We say

- $M \sqsubseteq_\diamond M'$ when $\mathcal{R}_{(M,M')_0}$ is may-preadequate

- $M \simeq_\diamond M'$ when $\mathcal{R}_{(M,M')_0}$ is may-adequate
- $M \sqsubseteq_{\Uparrow} M'$ when $\mathcal{R}_{(M,M')_0}$ is preadequate
- $M \simeq_{\Uparrow} M'$ when $\mathcal{R}_{(M,M')_0}$ is adequate.

Definition 3.10 (i) Let $M, M' : A$ be closed terms. We say $M \sqsubseteq_{\Uparrow U} M'$ when for any ground type C and term $\mathtt{z} : A \vdash P : C$, the behaviours (values or divergence) of M `to` $\mathtt{z}$. P are contained in the behaviours of M' `to` $\mathtt{z}$. P.

(ii) Let $V, V' : A$ be closed values. We say $V \sqsubseteq_{\Uparrow U} V'$ when for any ground type B and term $\mathtt{z} : A \vdash P : B$, the behaviours (values or divergence) of $P[V/\mathtt{z}]$ are contained in the behaviours of $P'[V/\mathtt{z}]$.

Clearly contextual inequality $\sqsubseteq_{\Uparrow}$ is contained in $\sqsubseteq_{\Uparrow U}{}^\circ$.

The only task that we have in the setting of general `amb` is proving Prop. 2.1, or rather a corresponding statement in our CBV setting.

Definition 3.11 A closed relation R is said to be *ground on functions* when $V\, R\, V' : A \to B$ implies that A is a ground type.

Proposition 3.12 (i) *Let R be a lower+divergence applicative simulation that is ground on functions. Then ${R^{\mathsf{wSC}}}_0$ is a lower+divergence applicative simulation.*

(ii) *Let R be a lower+divergence applicative bisimulation that is ground on functions. Then ${R^{\mathsf{wSC}}}_0$ is a lower+divergence applicative bisimulation.*

Proof.

(i) Clearly ${R^{\mathsf{wSC}}}_0$ respects functions, and it is easy to show that it respects tuples. Hence if $W\, R^{\mathsf{wSC}}\, W' : A$ and A is a ground type, then $W = W'$. This is by induction on W.

We next show that ${R^{\mathsf{wSC}}}_0 \subseteq R \cup \grave{R^{\mathsf{wSC}}}$. Suppose $M\, {R^{\mathsf{wSC}}}_0\, M'$. By Lemma 3.5, either $M\, R\, M'$ or $M\, \widehat{R^{\mathsf{wSC}}}\, M'$. In the latter case, we show that either $M\, R\, M'$ or $M\, \grave{R^{\mathsf{wSC}}} M'$, by case analysis.

- Suppose $M = (\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M_0)W$ and $M' = (\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M'_0)W'$ and $\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M_0\, R^{\mathsf{wSC}}\, \mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M'_0$ and $W\, R^{\mathsf{wSC}}\, W'$. By Lemma 3.5, either
  - $M_0\, R^{\mathsf{wSC}}\, M'_0$, in which case we are done, or
  - $\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M_0\, R\, \mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M'_0$, in which case W has ground type so $W = W'$ by the first paragraph. Hence $M\, R\, M'$, since R respects functions.
- The other cases are trivial, using the fact that R^{wSC} respects tuples.

We next show that ${R^{\mathsf{wSC}}}_0$ is a lower applicative simulation. We need to show that if $M \Downarrow V$ and $M\, {R^{\mathsf{wSC}}}_0\, M'$ then there exists V' such that $M' \Downarrow V'$ and $V\, {R^{\mathsf{wSC}}}_0\, V'$. We do this by induction on $M \Downarrow V$. The case that $M\, R\, M'$ is trivial, so we suppose that $M\, \grave{R^{\mathsf{wSC}}}\, M'$, and go through the various cases of M. We omit the details, which are straightforward.

We next show that if $M' \Downarrow_\square$ and $M\, R^{\mathsf{wSC}}\, M'$ then $M \Downarrow_\square$; we do this by induction on $M' \Downarrow_\square$. The case that $M\, R\, M'$ is trivial, so we suppose that $M\, \grave{R^{\mathsf{wSC}}}\, M'$.

- Suppose $M = M_0\ \texttt{to x}.\ M_1$ and $M' = M'_0\ \texttt{to x}.\ M'_1$ and $M_0\, R^{\mathsf{wSC}}\, M'_0$ and $M_1\, R^{\mathsf{wSC}}\, M'_1$. Then $M'_0 \Downarrow_\Box$, which gives us $M_0 \Downarrow_\Box$. If $M_0 \Downarrow W$, then, since ${R^{\mathsf{wSC}}}_0$ is a lower simulation, there exists W' such that $M'_0 \Downarrow W'$ and $W\, R^{\mathsf{wSC}}\, W'$, and we have $M'_1[W'/\texttt{x}] \Downarrow_\Box$. Since $M_1[W/\texttt{x}]\, R^{\mathsf{wSC}}\, M'_1[W'/\texttt{x}]$ we have $M_1[W/\texttt{x}] \Downarrow_\Box$ by inductive hypothesis. Hence $M_0\ \texttt{to x}.\ M_1 \Downarrow_\Box$.

(ii) A corollary of (i).

□

4 Ground Amb

4.1 Aims

Our aim is to prove the following results.

Proposition 4.1 *When we restrict the use of* `amb` *to ground type,*

(i) *divergence applicative similarity is a substitutive precongruence*

(ii) *divergence applicative sesquisimilarity is a substitutive precongruence*

(iii) *divergence applicative bisimilarity is a substitutive congruence.*

(iv) $\sqsubseteq_{\Uparrow}$ *and* $\sqsubseteq_{\Uparrow U^\circ}$ *coincide, i.e.* ${\sqsubseteq_{\Uparrow U^\circ}}^{\mathsf{SC}}_0$ *is preadequate.*

4.2 Decomposing Over A Relation

The following will be useful in the following sections.

Definition 4.2 An open relation $\mathcal{S}$ *decomposes over* a closed relation R when $\mathcal{S} \subseteq \widehat{\mathcal{S}}; R^\circ$.

Proposition 4.3 *Let $\mathcal{S}$ be an open relation that decomposes over a closed relation R. Suppose that $\mathcal{S}$ respects tuples and R respects functions. Then $\mathcal{S}_0$, restricted to terms (i.e. not values), is contained in $\grave{\mathcal{S}}; R$.*

Proof. Suppose $M\, \mathcal{S}_0\, M'$. Since $\mathcal{S}$ decomposes over R, there exists M'' such that $M\, \widehat{\mathcal{S}}\, M''$ and $M''\, R\, M'$. We then reason by cases.

- Suppose $M = VW$ and $M'' = V'W'$ and $V\, \mathcal{S}\, V'$ and $W\, \mathcal{S}\, W'$. Then $V = \texttt{rec f}\lambda\texttt{x}.M_0$, so, by decomposition, there exists M''_0 such that $M_0\, \mathcal{S}\, M''_0$ and $\texttt{rec f}\lambda\texttt{x}.M''_0\, R\, V'$. Since R respects functions, $(\texttt{rec f}\lambda\texttt{x}.M''_0)W'\, R\, V'W'\, R\, M'$.
- In all other cases, $M\, \grave{\mathcal{S}}\, M''$, using the fact that $\mathcal{S}$ respects tuples.

□

4.3 Divergence Similarity Is A Precongruence

The goal of this section is to prove Prop. 4.1.

Definition 4.4 An open relation $\mathcal{S}$ is *Howe-suitable* over a closed relation R when

- $\mathcal{S}$ decomposes over R.

- $\mathcal{S}$ is reflexive, substitutive and respects functions
- $\mathcal{S}; R^\circ \subseteq \mathcal{S}$

Proposition 4.5 *Let R be a closed preorder and let $\mathcal{S}$ be an open relation Howe-suitable over R.*

(i) $R^\circ \subseteq \mathcal{S}$

(ii) *If $\mathcal{S}_0 \subseteq R$ (e.g. if $(\mathcal{S}^*)_0 \subseteq R$), then $R^\circ = \mathcal{S} = \mathcal{S}^*$.*

(iii) *If R respects tuples then so does $\mathcal{S}$.*

Proof.

(i) $R^\circ = \mathsf{id}; R^\circ \subseteq \mathcal{S}; R^\circ \subseteq \mathcal{S}$

(ii) For any open relation $\mathcal{S}$, we have $\mathcal{S} \subseteq \mathcal{S}[\mathsf{id}]_0{}^\circ$. In our case, since $\mathcal{S}$ is reflexive and substitutive, we have $\mathcal{S} \subseteq \mathcal{S}_0{}^\circ \subseteq R^\circ$.

(iii) Suppose $\langle \hat{\imath}, V\rangle \, \mathcal{S}_0 \, \langle \hat{\imath}', V'\rangle$. Then there exists V'' such that $V \, \mathcal{S}_0 \, V''$ and $\langle \hat{\imath}, V''\rangle \, R \, \langle \hat{\imath}', V'\rangle$. Because R respects values, $\hat{\imath} = \hat{\imath}'$ and $V'' \, R \, V'$ so $V \, \mathcal{S} \, V'$. Similarly at product types.

□

Definition 4.6 A closed relation R is an *upper simulation* when it respects values and tuples and $M \, R \, M'$ and $M \Downarrow_\Box$ implies $M' \Downarrow_\Box \wedge \forall V'.(M' \Downarrow V' \Rightarrow \exists V.(M \Downarrow V \wedge V \, R \, V'))$

Proposition 4.7 *Let $\mathcal{S}$ be an open relation Howe-suitable over a closed relation R respecting functions and tuples.*

(i) *If R is a lower simulation, then so is $\mathcal{S}_0$, and hence so is $\mathcal{S}_0^*$.*

(ii) *If R is an upper simulation and $\mathcal{S}_0^{\mathsf{op}}$ is may-preadequate, then $\mathcal{S}_0$ is an upper simulation, and hence so is $\mathcal{S}_0^*$.*

Proof. $\mathcal{S}$ respects functions by definition, and respects tuples by Prop. 4.5(iii). Hence Prop. 4.3 applies.

(i) Suppose that R is a lower simulation. We have to show that $M \, \mathcal{S}_0 \, M'$ and $M \Downarrow V$ implies $M' \Downarrow V''$ for some V'' such that $V \, \mathcal{S}_0 \, V''$. We proceed by induction on $M \Downarrow V$. This is standard.

(ii) Suppose that R is an upper simulation. We have to show that $M \, \mathcal{S}_0 M'$ and $M \Downarrow_\Box$ implies $M' \Downarrow_\Box \wedge \forall V'.(M' \Downarrow V' \Rightarrow \exists V.(M \Downarrow V \wedge V \, R \, V'))$ We prove this by induction on $M \Downarrow_\Box$.

We know that there exists M'' such that $M \, \grave{\mathcal{S}} \, M''$ and $M'' \, R \, M'$.

Suppose $M = \ \mathtt{amb}_{\ i \in I} M_i$ and $M'' = \ \mathtt{amb}_{\ i \in I} M_i'$ and $M_i \, \mathcal{S} \, M_i'$ for all $i \in I$. Then there exists $\hat{\imath} \in I$ such that $M_{\hat{\imath}} \Downarrow_\Box$. So $M_{\hat{\imath}}' \Downarrow_\Box$, so $M'' \Downarrow_\Box$, so $M' \Downarrow_\Box$. If $M' \Downarrow n$, then, since $M \, \mathcal{S}_0 \, M'$ and $\mathcal{S}_0^{\mathsf{op}}$ is may-preadequate, we have $M \Downarrow n$, and we know that $n \, \mathcal{S} \, n$.

Otherwise, we proceed as follows. We first show $M'' \Downarrow_\Box \wedge \forall V''.(M'' \Downarrow V'' \Rightarrow \exists V.(M \Downarrow V \wedge V \, R \, V''))$ in the following way.

- Suppose that $M = M_0$ `to x`. M_1 and $M'' = M'_0$ `to x`. M'_1 and $M_0 \mathcal{S} M'_0$ and $M_1 \mathcal{S} M'_1$. We have $M_0 \Downarrow_\Box$, so $M'_0 \Downarrow_\Box$. If $M'_0 \Downarrow W'$, then by the inductive hypothesis there exists W such that $M_0 \Downarrow W$ and $W \mathcal{S} W'$. So $M_1[W/\mathtt{x}] \Downarrow_\Box$, and $M_1[W/\mathtt{x}] \mathcal{S} M'_1[W'\mathtt{x}]$, so $M'_1[W'/\mathtt{x}] \Downarrow_\Box$.

  If M'_0 `to x`. $M'_1 \Downarrow V''$, then there exists W' such that $M'_0 \Downarrow W'$ and $M'_1[W'/\mathtt{x}] \Downarrow V''$. Then there exists W such that $M_0 \Downarrow W$ and $W \mathcal{S} W'$. Since $M_1[W/\mathtt{x}] \mathcal{S} M'_1[W'\mathtt{x}]$, there exists V such that $M_1[W/\mathtt{x}] \Downarrow V$ and $V \mathcal{S} V''$.
- The other cases are similar.

  It follows that:
- $M' \Downarrow_\Box$, as required
- if $M' \Downarrow V'$, then there exists V'' such that $M'' \Downarrow V''$ and $V'' R V'$, so there exists V such that $M \Downarrow V$ and $V \mathcal{S} V''$, so $V \mathcal{S} V'$, as required

□

Proposition 4.8 *Let R be a closed relation. Then there exist relations $R^{\rightarrow}$ and $R^{\leftarrow}$ such that*

- *$R^{\rightarrow}$ is Howe-suitable over R*
- *$R^{\leftarrow^{\mathsf{op}}}$ is Howe-suitable over R^{op}*
- *$R^{\rightarrow *} = R^{\leftarrow *}$*
- *$R^{\rightarrow} \cap R^{\leftarrow}$ is compatible.*

Proof. See [12]. For finitary syntax, one can use the standard Howe extension for $R^{\rightarrow}$ and the dual construction for $R^{\leftarrow}$. □

To prove Prop. 4.1(i), let R be divergence similarity. Then $R^{\rightarrow}$ is Howe-suitable over a lower simulation (viz. R), so ${R^{\rightarrow}}_0{}^*$ is a lower simulation, and hence may-preadequate. Hence ${R^{\leftarrow}}_0$, as it is contained in a preadequate relation (viz. ${R^{\leftarrow *}}_0$) is may-preadequate.

$R^{\leftarrow^{\mathsf{op}}}$ is Howe-suitable over the upper simulation R^{op}, and ${R^{\leftarrow}}_0$ is may-preadequate, so ${R^{\leftarrow}}_0{}^{\mathsf{op}*}$ is an upper simulation.

Since ${R^{\rightarrow *}}_0$ is both a lower simulation and the opposite of an upper simulation, it is a divergence simulation, hence contained in R. By Prop. 4.5(ii), we have $R^\circ = R^{\rightarrow} = R^{\rightarrow *}$. Hence $R^{\leftarrow} \subseteq R^{\leftarrow *} = R^\circ$ so $R^{\leftarrow} = R^\circ$. So $R^\circ = R^{\rightarrow} \cap R^{\leftarrow}$, which is compatible.

The proof of Prop. 4.1(ii)–(iii) is similar.

4.4 CIU Theorem

The goal of this section is to prove Prop. 4.1(iv).

Definition 4.9 A closed relation R is *closed under sequencing* when

- $V\, R\, V' : A$ implies $P[V/\mathtt{x}]\, R\, P[V'/\mathtt{x}]$ for any term $\mathtt{x} : A \vdash P : B$
- $M\, R\, M' : B$ implies M `to x`. $P\, R\, M'$ `to x`. P for any term $\mathtt{x} : A \vdash P : B$.

Clearly $\sqsubseteq_{\Uparrow U}$ is closed under sequencing.

Proposition 4.10 *Let R be a closed preorder. Then $R^{\circ \mathsf{SC}}$ decomposes over R°.*

Proof. [6] □

Definition 4.11 Let S be a closed relation, let A be a type and let $\mathcal{V}, \mathcal{V}'$ be sets of closed values of type A. We say $\mathcal{V}\, S^{\Box}\, \mathcal{V}'$ when $\forall V' \in \mathcal{V}'.\ \exists V \in \mathcal{V}.\ V\, S\, V'$.

Definition 4.12 Let A be a type, and let N be a closed term of type A.

(i) For a closed value $W : A$, we say $W \sqsubseteq_{\diamond} N$ when for every ground term $\mathtt{z} : A \vdash P : \sum_{i \in I} 1$, if $P[W/\mathtt{z}] \Downarrow n$ then N `to` $\mathtt{z}.\ P \Downarrow n$.

(ii) For a set $\mathcal{W}$ of closed values of type A, we say $\mathcal{W} \sqsubseteq_{\Box} N$ when, for every ground term $\mathtt{z} : A \vdash P : \sum_{i \in I} 1$, if $P[W/\mathtt{z}] \Downarrow_{\Box}$ for all $W \in \mathcal{W}$, then

$$N \texttt{ to } \mathtt{z}.\ P \Downarrow_{\Box} \wedge \forall n.(N \texttt{ to } \mathtt{z}.\ P \Downarrow n \Rightarrow \exists W \in \mathcal{W}.\ P[W/\mathtt{z}] \Downarrow n)$$

Proposition 4.13 (i) *$\mathcal{W} \sqsubseteq_{\Box} N$ implies $N \Downarrow_{\Box}$.*

(ii) *If $N \Downarrow_{\Box}$, then $\{W \mid N \Downarrow_{\Box} W\} \sqsubseteq_{\Box} N$*

Proof. Trivial. □

Definition 4.14 A closed relation R is *must-preadequate* when $M\, R\, M' : C$, where B is a ground type, and $M \Downarrow_{\Box}$, implies $M' \Downarrow_{\Box} \wedge \forall n.(M' \Downarrow n \Rightarrow M \Downarrow n)$.

Proposition 4.15 *Let R be a closed preorder that is closed under sequencing. Let $\mathcal{S}$ be a substitutive open relation that decomposes over R.*

(i) $\mathcal{S}_0 \subseteq \grave{\mathcal{S}}; R$.

(ii) *Suppose that R is may-preadequate. If $M \Downarrow V : A$ and $M\, \mathcal{S}_0\, M'$, there exists a closed value $V' : A$ such that $V\, \mathcal{S}_0\, V'$ and $V' \sqsubseteq_{\diamond} M'$*

(iii) *Suppose that R is must-preadequate. Suppose that $\mathcal{S}_0^{\mathsf{op}}$ is may-preadequate and $n\, \mathcal{S}\, n$ for each closed ground value n. If $M \Downarrow_{\Box}$ and $M\, \mathcal{S}_0\, M'$, then there exists a set $\mathcal{V}'$ of closed values of type A such that $\{V \mid M \Downarrow V\}\, \mathcal{S}_0^{\Box}\, \mathcal{V}'$ and $\mathcal{V}' \sqsubseteq_{\Box} M'$.*

Proof.

(i) Suppose $\mathtt{pm}\ \langle V, W\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M\, \mathcal{S}_0\, N$. Then there exists V', W', M' such that $\langle V, W\rangle\, \mathcal{S}\, \langle V', W'\rangle$ and $M\, \mathcal{S}\, M'$ and $\mathtt{pm}\ \langle V', W'\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M'\, R\, N$. Then there exists V'' and W'' such that $V\, \mathcal{S}\, V''$ and $W\, \mathcal{S}\, W''$ and $\langle V'', W''\rangle\, R\, \langle V', W'\rangle$. Then, since R is closed under sequencing, we have

$$\mathtt{pm}\ \langle V'', W''\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M'\, R\, \mathtt{pm}\ \langle V', W'\rangle\ \mathtt{as}\ \langle \mathtt{x}, \mathtt{y}\rangle.\ M'\, R\, N$$

The case $(\mathtt{rec}\ \mathtt{f}\lambda\mathtt{x}.M)V\, \mathcal{S}_0\, N$ is similar to the same case in Prop. 4.3.

- All the other cases are similar to these or trivial.

(ii) We proceed by induction on $M \Downarrow V$. We know that there exists M'' such that $M\, \grave{\mathcal{S}}\, M''$ and $M''\, R\, M'$. We show that there exists a closed value $V' : A$ such that $V\, \mathcal{S}\, V'$ and $V' \sqsubseteq_{\diamond} M''$, as follows.

- Suppose that $M = M_0$ `to` $\mathtt{x}.\ M_1$ and $M'' = M_0'$ `to` $\mathtt{x}.\ M_1'$ and $M_0\, \mathcal{S}\, M_0'$ and $M_1\, \mathcal{S}\, M_1'$. We have $M_0 \Downarrow W$ and $M_1[W/\mathtt{x}] \Downarrow V$. By inductive hypothesis, there

exists W' such that $W \mathcal{S} W'$ and $W' \sqsubseteq_\diamond M_0'$. Hence $M_1[W/\mathtt{x}] \mathcal{S} M_1'[W'/\mathtt{x}]$. By inductive hypothesis, there exists V' such that $V \mathcal{S} V'$ and $V' \sqsubseteq_\diamond M_1'[W'/\mathtt{x}]$. We require $V' \sqsubseteq_\diamond M_0'$ `to` $\mathtt{x}$. M_1'.

Given $\mathtt{z} : A \vdash P : \sum_{i \in I} 1$, suppose $P[V'/\mathtt{z}] \Downarrow n$. Then $M_1'[W'/\mathtt{x}]$ `to` $\mathtt{z}$. $P \Downarrow n$. So M_0 `to` $\mathtt{x}$. $(M_1'$ `to` $\mathtt{z}$. ${}^{\mathtt{x}}P) \Downarrow n$. So $(M_0'$ `to` $\mathtt{x}$. $M_1')$ `to` $\mathtt{z}$. $P \Downarrow n$.

- Similarly for the other cases.

We then deduce that $V' \sqsubseteq_\diamond M'$ by may-preadequacy of R.

(iii) We proceed by induction on $M \Downarrow_\Box$. We know that there exists M'' such that $M \grave{\mathcal{S}} M''$ and $M'' \, R \, M'$.

Suppose $M =$ `amb` $_{i \in I} M_i$ and $M'' =$ `amb` $_{i \in I} M_i'$ and $M_i \mathcal{S} M_i'$ for all $i \in I$. Then there exists $\hat{\imath} \in I$ such that $M_{\hat{\imath}} \Downarrow_\Box$. By inductive hypothesis and Prop. 4.13(i) $M_{\hat{\imath}}' \Downarrow_\Box$, so `amb` $_{i \in I} M_i' \Downarrow_\Box$, so $M' \Downarrow_\Box$. Set $\mathcal{V}'$ to be $\{n \mid M' \Downarrow n\}$. By Prop. 4.13(ii) we have $\mathcal{V}' \sqsubseteq_\Box M'$. To show $\{n \mid M \Downarrow n\} \mathcal{S}_0^\Box \mathcal{V}'$, we reason as follows. If $n \in \mathcal{V}'$ then $M' \Downarrow n$; since $M \mathcal{S} M'$ and $\mathcal{S}^{\mathrm{op}}$ is may-preadequate, $M \Downarrow n$, and $n \mathcal{S} n$ by assumption.

Otherwise we proceed as follows. We first show that there exists a set $\mathcal{V}'$ of closed values of type A such that $\{V \mid M \Downarrow V\} \mathcal{S}_0^\Box \mathcal{V}'$ and $\mathcal{V}' \sqsubseteq_\Box M''$, in the following way.

- Suppose that $M =$ `return` W, and $M'' =$ `return` W' and $W \mathcal{S} W'$. Define $\mathcal{V}'$ to be $\{W'\}$, so $\{V \mid M \Downarrow V\} = \{W\} \mathcal{S}_0^\Box \mathcal{V}'$. Prop. 4.13(ii) tells us that $\{W'\} \sqsubseteq_\Box$ `return` W'.
- Suppose that $M = M_0$ `to` $\mathtt{x}$. M_1 and $M'' = M_0'$ `to` $\mathtt{x}$. M_1' and $M_0 \mathcal{S} M_0'$ and $M_1 \mathcal{S} M_1'$. We have $M_0 \Downarrow_\Box$, so there exists $\mathcal{W}'$ such that

$$\{W \mid M_0 \Downarrow W\} \; \mathcal{S}_0^\Box \; \mathcal{W}' \tag{1}$$

$$\mathcal{W}' \sqsubseteq_\Box M_0' \tag{2}$$

Write L for the set of pairs (W, W') such that $M_0 \Downarrow W$ and $W' \in \mathcal{W}'$ and $W \mathcal{S} W'$. For each $(W, W') \in L$, we have $M_1[W/\mathtt{x}] \mathcal{S} M_1'[W'/\mathtt{x}]$ and $M_1[W/\mathtt{x}] \Downarrow_\Box$, so by the inductive hypothesis there exists a set $\mathcal{V}'_{W,W'}$ of closed values such that

$$\{V \mid M_1[W/\mathtt{x}] \Downarrow V\} \; \mathcal{S}_0^\Box \; \mathcal{V}'_{W,W'} \tag{3}$$

$$\mathcal{V}'_{W,W'} \sqsubseteq_\Box M_1'[W'/\mathtt{x}] \tag{4}$$

Define $\mathcal{V}'$ to be $\bigcup_{(W,W') \in L} \mathcal{V}'_{W,W'}$.

We show $\{V \mid M_0$ `to` $\mathtt{x}$. $M_1 \Downarrow V\} \mathcal{S}_0^\Box \mathcal{V}'$ as follows. If $V' \in \mathcal{V}'$ then there exists $(W, W') \in L$ such that $V' \in \mathcal{V}'_{W,W'}$. By (3), there exists V such that $M_1[W/\mathtt{x}] \Downarrow V$ and $V \mathcal{S} V'$. Since $M_0 \Downarrow W$, we have M_0 `to` $\mathtt{x}$. $M_1 \Downarrow V$.

To show $\mathcal{V}' \sqsubseteq_\Box M_0'$ `to` $\mathtt{x}$. M_1', suppose that $\mathtt{z} : A \vdash P : \sum_{i \in I} 1$ is a ground term such that $P[V'/\mathtt{z}] \Downarrow_\Box$ for all $V' \in \mathcal{V}'$. Define Q to be M_1' `to` $\mathtt{z}$. ${}^{\mathtt{x}}P$. For any $W' \in \mathcal{W}'$, (1) tells us that there exists W such that $(W, W') \in L$, and for any $V' \in \mathcal{V}'_{W,W'}$ we have $P[V'/\mathtt{z}] \Downarrow_\Box$, so by (4) we have $M_1'[W'\mathtt{x}]$ `to` $\mathtt{z}$. $P \Downarrow_\Box$, i.e. $Q[W'/\mathtt{x}] \Downarrow_\Box$.

· By (2) we have M_0' `to` $\mathtt{x}$. $Q \Downarrow_\Box$. Hence $M_0' \Downarrow_\Box$, and for each V' such that $M_0' \Downarrow V'$ we have $M_1'[V'/ttx]$ `to` $\mathtt{z}$. $P \Downarrow_\Box$, so $M_1'[V'/\mathtt{x}] \Downarrow_\Box$ and for each W' such that $M_1' \Downarrow W'$ we have $P[W'/\mathtt{z}] \Downarrow_\Box$. Hence M_0' `to` $\mathtt{x}$. $M_1' \Downarrow_\Box$. If M_0' `to` $\mathtt{x}$. $M_1' \Downarrow W'$

then there exists V' such that $M_0' \Downarrow V'$ and $M_1'[V'/\mathtt{x}] \Downarrow W'$, so $P[W'/\mathtt{z}] \Downarrow_\square$. Hence $(M_0' \mathtt{\ to\ x.\ } M_1') \mathtt{\ to\ z.\ } P \Downarrow_\square$.

- Suppose $(M_0' \mathtt{\ to\ x.\ } M_1') \mathtt{\ to\ z.\ } P \Downarrow n$. Then $M_0' \mathtt{\ to\ x.\ } Q \Downarrow n$. By (2) there exists $W' \in \mathcal{W}'$ such that $Q[W'/\mathtt{x}] \Downarrow n$, i.e. $M_1'[W'/\mathtt{x}] \mathtt{\ to\ z.\ } P \Downarrow n$. (1) tells us that there exists W such that $(W, W') \in L$. Since $P[V'/\mathtt{z}] \Downarrow_\square$ for every $V' \in \mathcal{V}'_{W,W'}$, (4) tells us that there exists $V' \in \mathcal{V}'_{W,W'}$ (hence $\in \mathcal{V}'$) such that $P[V'/\mathtt{z}] \Downarrow n$.

• The other cases are similar (but much easier).
We then deduce that $\mathcal{V}' \sqsubseteq_\square M''$ by must-preadequacy of R.

□

We now prove Prop. 4.1(iv). We know $\sqsubseteq_{\Uparrow U}{}^{\circ\mathsf{SC}}$ is substitutive and decomposes over $\sqsubseteq_{\Uparrow U}$, which is closed under sequencing. If $M \sqsubseteq_{\Uparrow U}{}^{\circ\mathsf{SC}}{}_0 M' : C$, where C is ground, and $M \Downarrow n$, then, since $\sqsubseteq_{\Uparrow U}$ is may-preadequate, Prop. 4.15(ii) tells us that $M' \Downarrow n$.

We also know $\sqsubseteq_{\Uparrow U}^{\mathsf{op}}{}^{\circ\mathsf{SC}}$ is substitutive and decomposes over $\sqsubseteq_{\Uparrow U}^{\mathsf{op}}$, which is closed under sequencing. If $M \sqsubseteq_{\Uparrow U}{}^{\circ\mathsf{SC}}{}_0 M' : C$, where C is ground, and $M' \Downarrow_\square$, then, since $\sqsubseteq_{\Uparrow U}^{\mathsf{op}}$ is must-preadequate and $\sqsubseteq_{\Uparrow U}{}^{\circ\mathsf{SC}}{}_0$ is reflexive and (we have just shown) may-preadequate, we obtain from Prop. 4.15(iii) that $M \Downarrow_\square$.

Acknowledgements

I thank Soren Lassen for his helpful comments.

References

[1] Abramsky, S., *The lazy λ-calculus*, in: *Research topics in Functional Programming*, Addison Wesley, 1990 pp. 65–117.

[2] Carayol, Hirschkoff and Sangiorgi, *On the representation of mccarthy's amb in the pi-calculus*, TCS: Theoretical Computer Science **330** (2005).

[3] Gordon, A. D., *Bisimilarity as a theory of functional programming*, Theor. Comput. Sci. **228** (1999), pp. 5–47.

[4] Hatcliff, J. and O. Danvy, *Thunks and the λ-calculus*, Journal of Functional Programming **7** (1997), pp. 303–319.

[5] Howe, D. J., *Proving congruence of bisimulation in functional programming languages*, Inf. and Comp. **124** (1996).

[6] Lassen, S., "Relational Reasoning about Functions and Nondeterminism," Ph.D. thesis, Univ. of Aarhus (1998).

[7] Lassen, S. B., *Normal form simulation for McCarthy's amb*, Electr. Notes Theor. Comput. Sci **155** (2006), pp. 445–465.
URL http://dx.doi.org/10.1016/j.entcs.2005.11.068

[8] Lassen, S. B. and A. K. Moran, *Unique fixed point induction for McCarthy's amb*, in: *Proceedings of the 24th International Symposium on Mathematical Foundations of Computer Science*, "LNCS" **1672** (1999), pp. 198–208.

[9] Levy, P., S. Lassen and P. Panangaden, *Divergence-least semantics of* `amb` *is Hoare* (2005), short presentation at the APPSEM II workshop, Frauenchimsee, Germany, full version in preparation.

[10] Levy, P. B., "Call-By-Push-Value. A Functional/Imperative Synthesis," Semantic Struct. in Computation, Springer, 2004.

[11] Levy, P. B., *Call-by-push-value: Decomposing call-by-value and call-by-name*, Higher-Order and Symbolic Computation **19** (2006), pp. 377–414.

[12] Levy, P. B., *Infinitary Howe's method*, in: *Proceedings, 8th International Workshop on Coalgebraic Methods in Computer Science, Vienna, Austria*, ENTCS **164(1)**, 2006, pp. 85–104.

[13] Levy, P. B., *Infinite trace equivalence*, in: *Proceedings, 21st Annual Conference in Mathematical Foundations of Computer Science, Birmingham, UK, 2005*, number 155 in ENTCS, 2006, pp. 467–496.

[14] McCarthy, J., *A basis for a mathematical theory of computation*, in: P. Brafford and D. Hirschberg, editors, *Computer Programming and Formal Systems*, North-Holland, 1963 .

[15] Moggi, E., *Notions of computation and monads*, Information and Computation **93** (1991), pp. 55–92.

[16] Moran, A. K., *Natural semantics for non-determinism*, Licentiate Thesis, Chalmers University of Technology and University of Göteborg, Sweden (1994).

[17] Natarajan and Cleaveland, *Divergence and fair testing*, in: *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 1995.

[18] Talcott, C., *Reasoning about functions with effects*, in: A. D. Gordon and A. M. Pitts, editors, *Higher Order Operational Techniques in Semantics*, Publications of the Newton Institute, Cambridge University Press, 1998 pp. 347–390.