A Probabilistic and Non-Deterministic Call-by-Push-Value Language*

Jean Goubault-Larrecq†

April 8, 2019

Abstract

There is no known way of giving a domain-theoretic semantics to higher-order probabilistic languages, in such a way that the involved domains are continuous or quasi-continuous—the latter is required to do any serious mathematics. We argue that the problem naturally disappears for languages with two kinds of types, where one kind is interpreted in a Cartesian-closed category of continuous dcpos, and the other is interpreted in a category that is closed under the probabilistic powerdomain functor. Such a setting is provided by Paul B. Levy's call-by-push-value paradigm. Following this insight, we define a call-by-push-value language, with probabilistic choice sitting inside the value types, and where conversion from a value type to a computation type involves demonic non-determinism. We give both a domain-theoretic semantics and an operational semantics for the resulting language, and we show that they are sound and adequate. With the addition of statistical termination testers and parallel if, we show that the language is even fully abstract—and those two primitives are required for that.

Keywords: domain theory; PCF; call-by-push-value; probabilistic choice; non-deterministic choice; full abstraction.

1 Introduction

A central problem of domain theory is the following: is there any full Cartesian-closed subcategory of the category **Cont** of continuous dcpos that is closed under the probabilistic powerdomain functor $\mathbf{V}_{\leq 1}$ [14]? Solving the question in the positive would allow for a simple semantics of probabilistic higher-order languages, where types are interpreted as certain continuous dcpos.

However, we have a conundrum here. The category **Cont** itself is closed under $\mathbf{V}_{\leq 1}$ [13], but is not Cartesian-closed [2, Exercise 3.3.12(11)]. Among the

*This research was partially supported by Labex DigiCosme (project ANR-11-LABEX-0045-DIGICOSME) operated by ANR as part of the program "Investissement d'Avenir" Idex Paris-Saclay (ANR-11-IDEX-0003-02).

†LSV, ENS Paris-Saclay, CNRS, Université Paris-Saclay. Address: ENS Paris-Saclay, 61 avenue du président Wilson, 94230 Cachan, France. Email: `goubault@lsv.fr`

Cartesian-closed categories of continuous domains, none is known to be closed under $\mathbf{V}_{\leq 1}$, and most, such as the category of bc-domains or the category **CLatt** of continuous complete lattices, definitely are not [14].

Instead of solving this problem, one may wonder whether there are other kinds of domain-theoretic semantics that would be free of the issue. Typically, can we imagine having *two* classes of types? One would be interpreted in a category of continuous dcpos that is closed under $\mathbf{V}_{\leq 1}$—**Cont** for example, although we will prefer the category **PCCont** of pointed coherent continuous dcpos (see below). The other would be interpreted in a Cartesian-closed category of continuous dcpos, and we will use **CLatt**. Such a division in two classes of types is already present in Paul B. Levy's *call-by-push-value* [17] (a.k.a. *CBPV*), and although the division is justified there as to be between *value* types and *computation* types, the formal structure will be entirely similar.

Outline We briefly review some related work in Section 2, and give a few basic working definitions in Section 3. We define our probabilistic call-by-push-value languages in Section 4, explaining the design decisions we had to make in the process—notably the extra need for demonic non-determinism. We give domain-theoretic and operational semantics there, too. We establish soundness in Section 5 and adequacy in Section 6, to the effect that for every ground term M of the specific type $\mathtt{FVunit}$, the probability $\Pr(M\downarrow)$ that M must terminate, as defined from the operational semantics, coincides with a similar notion of probability defined from the denotational semantics. In Section 7, we review a few useful consequences of adequacy, among which the coincidence between the applicative preorder $\precsim_{\tau}^{app}$ and the contextual preorder $\precsim_{\tau}$ (both will be defined there), a fact sometimes called Milner's Context Lemma in the context of PCF (see [20, Theorem 8.1]). We show that, among the languages we have defined, CBPV($\mathtt{D},\mathtt{P}$) is not (inequationally) fully abstract in Section 8, and that adding a parallel if operator **`pifz`** does not make it fully abstract, but that adding both **`pifz`** and a statistical termination tester operator $\bigcirc_{>b}$ (as in [11]) results in an (inequationally) fully abstract language. The latter is proved in Section 9. We conclude and list a few remaining open questions in Section 10.

Acknowledgments I wish to thank Zhenchao Lyu and Xiaodong Jia, who participated in many discussions on the theme of this paper; Ohad Kammar, who kindly pointed me to [23]; and the anonymous referees of the LICS'19 conference.

2 Related Work

Call-by-push-value (CBPV) is the creation of Paul B. Levy [17] (see also the book [18]), and is a typed higher-order pure functional language. It was originally meant as a subsuming paradigm, embodying both call-by-value and call-by-name disciplines.

The first probabilistic extension of CBPV was proposed recently by Ehrhard and Tasson [4], and its denotational semantics rests on probabilistic coherence spaces. Their typing discipline is inspired by linear logic, and they also include a treatment of general recursive types, which we will not. In contrast, our extension of CBPV will have first-class types of subprobability distributions $\mathtt{V}\sigma$, and will also include a type former for demonic non-determinism (a.k.a., must-non-determinism).

Statistical probabilistic programming has attracted quite some attention recently, and quasi-Borel spaces and predomains have recently been used to give adequate semantics to typed and untyped probabilistic programming languages, see [23]. The latter describes another way of circumventing the problem we stated in the introduction. One important point that Vákár, Kammar and Staton achieve is the commutativity of the probabilistic choice monad, at all, even higher-order, types. In standard domain theory, the $\mathbf{V}_{\leq 1}$ monad is known to be commutative in full subcategories of **Cont** only. That would be enough motivation to attempt to solve the problem stated in the introduction, of finding a Cartesian-closed category, closed under $\mathbf{V}_{\leq 1}$ [14]. We also implement a commutative $\mathbf{V}_{\leq 1}$ monad in a higher-order setting; our way of circumventing the problem is merely different.

There is a large body of literature concerned with the question of full abstraction for PCF-like languages. The first paper on the subject is due to G. Plotkin [19], who defined the language PCF, asked all the important questions (soundness, adequacy, full abstraction, definability), and answered all of them, except for the question of finding a fully abstract denotational model of PCF *without* parallel if, a question that was solved later, through game semantics notably [12, 1]. Th. Streicher's book [20] is an excellent reference on the subject.

Probabilistic coherence spaces provide a fully abstract semantics for a version of PCF with probabilistic choice, as shown by Ehrhard, Tasson, and Pagani [5]. The already cited paper of Ehrhard and Tasson [4] gives an analogous result for their probabilistic version of CBPV. Our work is concerned with languages with domain-theoretic semantics instead, and our former work [11] gives soundness, adequacy and full abstraction results for PCF plus angelic non-determinism, and for PCF plus probabilistic choice and angelic non-determinism plus so-called statistical termination testers. We will see that CBPV naturally calls for a form of demonic, rather than angelic, non-determinism.

3 Preliminaries

We refer to [8, 2, 10] for material on domain theory and topology. A dcpo is *pointed* if and only if it has a least element $\perp$. Dcpos are always equipped with their Scott topology. $\overline{\mathbb{R}}_+ = \mathbb{R}\cup\{\infty\}$ and $[0,1]$ are dcpos, with the usual ordering. The *way-below* relation is written $\ll$: $x \ll y$ if and only if for every directed family $(x_i)_{i\in I}$ such that $y \leq \sup_{i\in I} x_i$, there is an $i \in I$ such that $x \leq x_i$. A dcpo X is *continuous* if and only if every element is the supremum of a directed family of elements way-below it. In that case, the sets $\mathord{\uparrow\!\!\uparrow} x = \{y \in X \mid x \ll y\}$ form a base of open sets of the Scott topology. We recall that a *base* of a topology is a family $\mathcal{B}$ of open sets such that every open set is a union of sets from $\mathcal{B}$. A *subbase* is a family $\mathcal{S}$ such that the finite intersections of elements of $\mathcal{S}$ form a base.

A *basis* B of a dcpo X (not to be confused with a base) is a set of elements of X such that, for every $x \in X$, $\{b \in B \mid b \ll x\}$ is directed and has x as supremum. A dcpo is continuous if and only if it has a basis. Then the sets $\mathord{\uparrow\!\!\uparrow} b$, $b \in B$, also form a base of the Scott topology.

We write $\leq$ for the specialization ordering of a T_0 topological space. For a dcpo X, that is the original ordering on X. A subset of a topological space is *saturated* if and only if it is upwards-closed in $\leq$, if and only if it is the intersection of its open neighborhoods. A topological space X is locally compact if and only if for every $x \in X$, for every open neighborhood U of x, there is a compact saturated set Q such that $x \in \mathrm{int}(Q) \subseteq Q \subseteq U$. ($\mathrm{int}(Q)$ denotes the interior of Q.) In that case, for every compact saturated subset Q and every open neighborhood U of Q, there is a compact saturated set Q' such that $Q \subseteq \mathrm{int}(Q') \subseteq Q' \subseteq U$. A topological space is *coherent* if and only if the intersection of any two compact saturated subsets is compact. It is *well-filtered* if and only if for every filtered family of compact saturated sets $(Q_i)_{i \in I}$ (*filtered* meaning directed for reverse inclusion), every open neighborhood U of $\bigcap_{i \in I} Q_i$ already contains some Q_i. In a well-filtered space, the intersection $\bigcap_{i \in I} Q_i$ of such a filtered family is compact saturated. A *stably compact* space is a T_0, well-filtered, locally compact, coherent and compact space X. Then the complements of compact saturated sets form another topology on X, the *cocompact topology*, and X with the cocompact topology is the *de Groot dual* X^{d} of X. For every stably compact space, $X^{\mathsf{dd}} = X$. Every pointed, coherent, continuous dcpo is stably compact.

Given two dcpos X and Y, $[X \to Y]$ denotes the dcpo of all Scott-continuous maps from X to Y, ordered pointwise. Directed suprema are also pointwise, namely $(\sup_{i \in I} f_i)(x) = \sup_{i \in I}(f_i(x))$ for every directed family $(f_i)_{i \in I}$ in $[X \to Y]$.

4 The Languages CBPV($\mathtt{D}, \mathtt{P}$) and CBPV($\mathtt{D}, \mathtt{P}$) + pifz + $\bigcirc$

The first language we introduce is called CBPV($\mathtt{D}, \mathtt{P}$): it is a call-by-push-value language with Demonic non-determinism and Probabilistic choice. We will explain below why we do not consider just probabilistic choice, but also demonic non-determinism.

4.1 Types and their Semantics

We consider the following grammar of types:

$$\sigma, \tau, \ldots ::= \mathtt{U}\underline{\tau} \mid \mathtt{unit} \mid \mathtt{int} \mid \sigma \times \tau \mid \mathtt{V}\tau$$
$$\underline{\sigma}, \underline{\tau}, \ldots ::= \mathtt{F}\tau \mid \sigma \to \underline{\tau}.$$

The types σ, τ, ..., are the *value* types, and the types $\underline{\sigma}$, $\underline{\tau}$, ..., are the *computation* types, following Levy [17]. Our types differ from Levy's: we do not have countable sums in value types or countable products in computation types, we write $\mathtt{unit}$ instead of 1, and we have a primitive type $\mathtt{int}$ of integers; the main difference is the $\mathtt{V}\tau$ construction, denoting the type of subprobability valuations on the space of elements of type τ.

We write $\overline{\sigma}$, $\overline{\tau}$ for types when it is not important whether they are value types or computation types.

We have already said in the introduction that computation types will be interpreted in the category **CLatt** of continuous complete lattices. Value types τ will give rise to pointed, coherent, continuous dcpos $[\![\tau]\!]$:

- for every computation type $\underline{\tau}$, we will define $[\![\mathtt{U}\underline{\tau}]\!]$ as $[\![\underline{\tau}]\!]$: being a continuous complete lattice, it is in particular pointed, coherent, and a continuous dcpo;
- $[\![\mathtt{unit}]\!]$ will be *Sierpiński space* $\mathbb{S} = \{\bot, \top\}$ with $\bot < \top$;
- $[\![\mathtt{int}]\!]$ will be $\mathbb{Z}_\bot = \mathbb{Z} \cup \{\bot\}$, with the ordering that makes $\bot$ least and all integers be pairwise incomparable;
- $[\![\mathtt{V}\tau]\!]$ will be $\mathbf{V}_{\leq 1}([\![\tau]\!])$, where $\mathbf{V}_{\leq 1}X$ denotes the dcpo of all subprobability valuations on the space X.

A *subprobability valuation* on X is a map ν from the lattice $\mathcal{O}X$ of open subsets of X to $[0,1]$ which is strict ($\nu(\emptyset) = 0$), Scott-continuous, and modular ($\nu(U \cup V) + \nu(U \cap V) = \nu(U) + \nu(V)$). When X is a continuous dcpo, so is $\mathbf{V}_{\leq 1}X$ [13, Corollary 5.4]. It is pointed, since the zero valuation is least in $\mathbf{V}_{\leq 1}X$. If X is also coherent, then $\mathbf{V}_{\leq 1}X$ is stably compact, see below. Hence $[\![\mathtt{V}\tau]\!]$ is indeed a pointed, coherent continuous dcpo.

The fact that $\mathbf{V}_{\leq 1}X$ is stably compact for every coherent continuous dcpo X is folklore. We argue as follows. The lift $X_\bot$ of X, obtained by adding a fresh bottom element $\bot$ to X, is stably compact. Then the space $\mathbf{V}_1 X_\bot$ of all probability valuations ν, i.e., such that $\nu(X_\bot) = 1$, is stably compact in the weak upwards topology [3, Theorem 39]. The latter has a subbase of open sets of the form $[U > r] = \{\nu \mid \nu(U) > r\}$, for every open subset U of X and $r \in \mathbb{R}_+ \setminus \{0\}$. The restriction map $\nu \mapsto \nu_{|\mathcal{O}X}$ is a homeomorphism from $\mathbf{V}_1 X_\bot$ onto $\mathbf{V}_{\leq 1}X$, both with their weak upwards topology, with inverse $\nu \mapsto \nu + (1 - \nu(X))\delta_\bot$. Hence $\mathbf{V}_{\leq 1}X$ is stably compact in its weak upwards topology. Since X is continuous, the latter coincides with the Scott topology, as shown by [16, Satz 8.6], see also [22, Satz 4.10].

It might seem curious that probabilistic non-determinism arises, as $\mathbf{V}\sigma$, among the *value* types. I have no philosophical backing for that, but this is somehow forced upon us by the mathematics.

Similarly, computation types $\underline{\tau}$ will give rise to continuous complete lattices $[\![\underline{\tau}]\!]$—notably $[\![\sigma \to \underline{\tau}]\!]$ will be the continuous complete lattice $[[\![\sigma]\!] \to [\![\underline{\tau}]\!]]$ of all Scott-continuous maps $[[\![\sigma]\!] \to [\![\underline{\tau}]\!]]$ from $[\![\sigma]\!]$ to $[\![\underline{\tau}]\!]$—, but we have to decide on an interpretation of types of the form $\mathbf{F}\tau$.

If we had decided to interpret computation types as bc-domains instead of continuous complete lattices, then a natural choice would be to define $[\![\mathbf{F}\tau]\!]$ as Ershov's *bc-hull* of $[\![\tau]\!]$ [7]. (Bc-domains are, roughly speaking, continuous complete lattices that may lack a top element.) As Ershov notices, "the construction of a bc-hull in the general case is highly nonconstructive (using a Zorn's lemma)" (ibid., page 13). Fortunately, the bc-hull of a space X is a natural subspace of the *Smyth powerdomain* $\mathcal{Q}(X)$ of X, at least when X is a coherent algebraic dcpo (ibid., Corollary B), and $\mathcal{Q}(X)$ is easier to work with. Explicitly, $\mathcal{Q}(X)$ is the poset of all non-empty compact saturated subsets of X, ordered by reverse inclusion, and is used to interpret demonic non-determinism in denotational semantics. When X is well-filtered and locally compact, $\mathcal{Q}(X)$ is also a continuous dcpo, and it is a bc-domain provided X is also compact and coherent. We shall see below that $\mathcal{Q}^\top(X)$, the poset of all (possibly empty) compact saturated subsets of X—alternatively, $\mathcal{Q}(X)$ plus an additional top element $\top = \emptyset$—, is a continuous complete lattice whenever X is a stably compact space, and that would make $\mathcal{Q}^\top([\![\tau]\!])$ a good candidate for $[\![\mathbf{F}\tau]\!]$.

For technical reasons related to adequacy, we will need a certain map f^* below to be strict, i.e., to map $\perp$ to $\perp$. (Technically, this is needed so that the denotational semantics of the construction M **to** x_σ **in** N, to be introduced below, be strict in that of M, in order to validate the fact that M **to** x_σ **in** N loops forever if M does.) This will be obtained by defining $[\![\mathbf{F}\tau]\!]$ as $\mathcal{Q}^\top_\perp([\![\tau]\!])$ instead, where $\mathcal{Q}^\top_\perp(X)$ is the *lift* of $\mathcal{Q}^\top(X)$, obtained by adding a fresh element $\perp$ below all others.

We recapitulate:

- $[\![\sigma \to \underline{\tau}]\!] = [[\![\sigma]\!] \to [\![\underline{\tau}]\!]]$;
- $[\![\mathbf{F}\sigma]\!] = \mathcal{Q}^\top_\perp([\![\sigma]\!])$.

Let us check that $\mathcal{Q}^\top_\perp([\![\sigma]\!])$ has the required property of being a continuous complete lattice, and let us prove some additional properties that we will need later. We start with the similar properties of $\mathcal{Q}^\top([\![\sigma]\!])$. We let $\eta^{\mathcal{Q}} \colon X \to \mathcal{Q}^\top(X)$ map every x to $\uparrow x$.

Proposition 4.1 *Let X be a stably compact space. Then:*

1. *$\mathcal{Q}^\top(X)$ is a continuous complete lattice, and Q is way-below Q' if and only if $Q' \subseteq int(Q)$;*
2. *For every continuous complete lattice L, for every continuous map $f \colon X \to L$, there is a Scott-continuous map $f^* \colon \mathcal{Q}^\top(X) \to L$ such that $f^* \circ \eta^{\mathcal{Q}} = f$, and it is defined by $f^*(Q) = \bigwedge_{x \in Q} f(x)$.*

3. $f^*(\emptyset) = \top$, $f^*(Q_1 \cup Q_2) = f^*(Q_1) \wedge f^*(Q_2)$.

Proof. 1. This is well-known, but here is a brief argument. The elements of $\mathcal{Q}^\top(X)$ are exactly the closed subsets in the de Groot dual of X, and the closed sets of any topological space always form a complete lattice. Note that the supremum of an arbitrary family $(Q_i)_{i\in I}$ in $\mathcal{Q}^\top(X)$ is $\bigcap_{i\in I} Q_i$.

Given any compact saturated subset Q' of X, the family $N(Q')$ of compact saturated neighborhoods Q'' of Q' is filtered, and has Q' as intersection. Indeed, since Q' is saturated, it is the intersection of its open neighborhoods; for every open neighborhood U of Q', local compactness implies that there is a compact saturated set Q'' such that $Q' \subseteq \mathrm{int}(Q'') \subseteq Q'' \subseteq U$; applying this to $U = X$ shows that $N(Q')$ is non-empty, and given $Q_1, Q_2 \in N(Q')$, applying it to $U = \mathrm{int}(Q_1) \cap \mathrm{int}(Q_2)$, shows that $N(Q')$ contains an element included in both Q_1 and Q_2.

It follows that, if $Q \ll Q'$, then Q contains an element of $N(Q')$, hence in particular an open neighborhood of Q'. Conversely, if $Q \supseteq U \supseteq Q'$ where U is open, then for every directed family $(Q_i)_{i\in I}$ in $\mathcal{Q}^\top(X)$ such that $Q' \supseteq \bigcap_{i\in I} Q_i$, U contains some Q_i by well-filteredness, hence $Q \supseteq Q_i$. Therefore $Q \ll Q'$.

Finally, since every Q' in $\mathcal{Q}^\top(X)$ is the filtered intersection of the elements of $N(Q')$, it is the supremum of the directed family $N(Q')$, and we have just argued that every element of $N(Q')$ is way-below Q', showing that $\mathcal{Q}^\top(X)$ is continuous.

2. We define $f^*(Q)$ as $\bigwedge_{x\in Q} f(x)$. This satisfies $f^* \circ \eta^{\mathcal{Q}} = f$, and is monotonic. Note that this is defined even when Q is empty, in which case $f^*(Q)$ is the top element of L. In order to show that f^* is Scott-continuous, let $(Q_i)_{i\in I}$ be a directed family in $\mathcal{Q}^\top(X)$, and $Q = \bigcap_{i\in I} Q_i$. We wish to show that $f^*(Q) \leq \sup_{i\in I} f^*(Q_i)$; the converse inclusion is by monotonicity. To this end, we let y be an element of L way-below $f^*(Q)$. Since $y \ll f(x)$ for every $x \in Q$, every element of Q is in the open set $f^{-1}(\twoheaduparrow y)$. Then $Q = \bigcap_{i\in I} Q_i$ is included in $f^{-1}(\twoheaduparrow y)$, so by well-filteredness some Q_i is also included in $f^{-1}(\twoheaduparrow y)$. Then $y \ll f(x)$ for every $x \in Q_i$, so $y \leq \bigwedge_{x\in Q_i} f(x) = f^*(Q_i)$. Since that holds for every $y \ll f^*(Q)$, the desired inequality follows.

3. Easy check. □

Note that item 2 does not state that f^* is *unique*; we have just chosen the largest one. A similar construction is well-known for $\mathcal{Q}(X)$. Proposition 4.1 establishes the essential properties needed to show that $\mathcal{Q}^\top$ defines a monad on the category of stably compact spaces, and that is not only well-known, but we will not require as much.

We turn to $\mathcal{Q}^\top_\perp(\llbracket\tau\rrbracket)$. We again write $\eta^{\mathcal{Q}}$ for the function that maps x to $\uparrow x$, this time from X to $\mathcal{Q}^\top_\perp(\llbracket X\rrbracket)$. Below, we again write f^* for the extension of f to $\mathcal{Q}^\top_\perp(X)$. This should not cause any confusion with the map f^* of Proposition 4.1, since the two maps coincide on $\mathcal{Q}^\top(X)$. Note that f^* is now strict.

Proposition 4.2 *Let X be a stably compact space. Then:*

1. *$\mathcal{Q}^\top_\perp(X)$ is a continuous complete lattice, and Q is way-below Q' if and only if $Q = \perp$, or $Q, Q' \neq \perp$ and $Q' \subseteq \mathrm{int}(Q)$;*

2. *For every continuous complete lattice L, for every continuous map $f\colon X \to L$, there is a strict Scott-continuous map $f^*\colon \mathcal{Q}^\top_\perp(X) \to L$ such that $f^* \circ \eta^{\mathcal{Q}} = f$. This is defined by $f^*(\perp) = \perp$, and for every $Q \neq \perp$, $f^*(Q) = \bigwedge_{x\in Q} f(x)$.*

3. *$f^*(\emptyset) = \top$, $f^*(Q_1 \wedge Q_2) = f^*(Q_1) \wedge f^*(Q_2)$.*

4. *For every stably compact space Y, for every Scott-continuous map $f\colon X \to \mathcal{Q}^\top_\perp(Y)$, and for every Scott-continuous map g from Y to a continuous complete lattice L, $g^* \circ f^* = (g^* \circ f)^*$.*

Proof. 1. The lift of a continuous complete lattice is a continuous complete lattice, and $\perp$ is always way-below every element.

2. Easy.

3. We check the second inequality. That follows from Proposition 4.1, item 3 if $Q_1, Q_2 \neq \perp$. If $Q_1 = \perp$, then $f^*(Q_1 \wedge Q_2) = f^*(\perp) = \perp$ and $f^*(Q_1) \wedge f^*(Q_2) = \perp \wedge f^*(Q_2) = \perp$. Similarly if $Q_2 = \perp$.

4. Fix $Q \in \mathcal{Q}^\top_\perp(X)$. If $Q = \perp$, then $g^*(f^*(Q)) = \perp = (g^* \circ f)^*(Q)$ by strictness. Henceforth, we assume that $Q \neq \perp$.

If $f(x) = \perp$ for some $x \in Q$, then $f^*(Q) = \perp$, so $g^*(f^*(Q)) = \perp$, and $(g^* \circ f)^*(Q) = \bigwedge_{x\in Q} g^*(f(x)) \leq g^*(\perp) = \perp$, since g^* is strict. Henceforth, we assume that $f(x) \neq \perp$ for every $x \in Q$.

We claim that $\bigcup_{x\in Q} f(x)$ is compact. Let $(V_i)_{i\in I}$ be a directed family of open subsets of Y whose union contains $\bigcup_{x\in Q} f(x)$. For every $x \in Q$, $f(x)$ is compact and included in $\bigcup_{i\in I} V_i$, so $f(x) \subseteq V_i$ for some $i \in I$. Hence $Q \subseteq \bigcup_{i\in I} f^{-1}(V_i)$. Since Q is compact, $Q \subseteq f^{-1}(V_i)$ for some $i \in I$, whence $\bigcup_{x\in Q} f(x) \subseteq V_i$.

$\bigcup_{x\in Q} f(x)$ is also saturated in Y, hence an element of $\mathcal{Q}^\top(Y)$, and therefore also of $\mathcal{Q}^\top_\perp(Y)$. It follows that this is the infimum of the elements $f(x)$, $x \in Q$, hence is equal to $f^*(Q)$. Therefore $g^*(f^*(Q)) = \bigwedge_{y\in f^*(Q)} g(y) = \bigwedge_{x\in Q, y\in f(x)} g(y) = \bigwedge_{x\in Q} g^*(f(x)) = (g^* \circ f)^*(Q)$. ☐

Item 4 above is part of the properties needed to check that $\mathcal{Q}^\top_\perp$ defines a monad on **CLatt**. We will not expand on that.

4.2 Syntax

We define the syntax of our language CBPV(`D`,`P`) together with its typing discipline, inductively, as in Figure 1, using the notation $M\colon \overline{\tau}$ to say "M is a term of type $\overline{\tau}$". There are countably infinitely many variables x_τ, y_τ, ... of each value type τ.

We extend the notation M **`to`** x_σ **`in`** N to the case where N has an arbitrary computation type by: for every $N\colon \lambda \to \underline{\tau}$, M **`to`** x_σ **`in`** $N = \lambda y_\lambda.M$ **`to`** x_σ **`in`** $(N y_\lambda)$, where y_λ is fresh. Similarly, we extend $\mathtt{abort}_{\mathtt{F}\tau}$ to all computation types by letting $\mathtt{abort}_{\lambda\to\underline{\tau}} = \lambda x_\lambda.\mathtt{abort}_{\underline{\tau}}$.

The variable x_σ is binding in $\lambda x_\sigma.M$, in N **`to`** x_σ **`in`** M, and in **`rec`** $x_\sigma.M$, and its scope is M in all three cases. We omit the standard definition of α-renaming and of capture-avoiding substitution.

$$\frac{}{x_\tau : \tau} \qquad \frac{}{\underline{*} : \mathtt{unit}} \qquad \frac{}{\underline{n} : \mathtt{int}}\,(n \in \mathbb{Z}) \qquad \frac{}{\mathtt{abort}_{\mathtt{F}\tau} : \mathtt{F}\tau}$$

$$\frac{M : \underline{\tau}}{\lambda x_\sigma . M : \sigma \to \underline{\tau}} \qquad \frac{M : \sigma \to \underline{\tau} \quad N : \sigma}{MN : \underline{\tau}} \qquad \frac{M : \sigma}{\mathtt{rec}\, x_\sigma . M : \sigma}$$

$$\frac{M : \mathtt{int}}{\mathtt{succ}\, M : \mathtt{int}} \qquad \frac{M : \mathtt{int}}{\mathtt{pred}\, M : \mathtt{int}} \qquad \frac{M : \underline{\tau}}{\mathtt{thunk}\, M : \mathtt{U}\underline{\tau}} \qquad \frac{M : \mathtt{U}\underline{\tau}}{\mathtt{force}\, M : \underline{\tau}}$$

$$\frac{M : \mathtt{unit} \quad N : \overline{\sigma}}{M ; N : \overline{\sigma}} \qquad \frac{M : \mathtt{int} \quad N : \overline{\sigma} \quad P : \overline{\sigma}}{\mathtt{ifz}\ M\ N\ P : \overline{\sigma}}$$

$$\frac{M : \sigma \times \tau}{\pi_1 M : \sigma} \qquad \frac{M : \sigma \times \tau}{\pi_2 M : \tau} \qquad \frac{M : \sigma \quad N : \tau}{\langle M, N \rangle : \sigma \times \tau}$$

$$\frac{M : \mathtt{V}\tau \quad N : \mathtt{V}\tau}{M \oplus N : \mathtt{V}\tau} \qquad \frac{M : \tau}{\mathtt{ret}\, M : \mathtt{V}\tau} \qquad \frac{M : \mathtt{V}\sigma \quad N : \mathtt{V}\tau}{\mathtt{do}\, x_\sigma \leftarrow M ; N : \mathtt{V}\tau}$$

$$\frac{M : \mathtt{F}\tau \quad N : \mathtt{F}\tau}{M \owedge N : \mathtt{F}\tau} \qquad \frac{M : \sigma}{\mathtt{produce}\, M : \mathtt{F}\sigma} \qquad \frac{M : \mathtt{F}\sigma \quad N : \mathtt{F}\tau}{M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N : \mathtt{F}\tau}$$

Figure 1: The syntax of CBPV($\mathtt{D}, \mathtt{P}$)

Using recursion at value types may seem strange, but this allows us to define some interesting values. For example, we can define the uniform distribution on $\{0, 1, 2\}$ by the term $\mathtt{rec}\, x_{\mathtt{Vint}} . (\mathtt{ret}\, \underline{0} \oplus \mathtt{ret}\, \underline{1}) \oplus (\mathtt{ret}\, \underline{2} \oplus x_{\mathtt{Vint}})$, which operates via a form of rejection sampling.

We will also consider an extension of CBPV($\mathtt{D}, \mathtt{P}$) called CBPV($\mathtt{D}, \mathtt{P}$)+$\mathtt{pifz}$+$\bigcirc$, obtained by admitting the following additional clauses:

$$\frac{M : \mathtt{FVunit}}{\bigcirc_{>b} M : \mathtt{unit}}\,(b \in \mathbb{Q} \cap (0,1)) \qquad \frac{M : \mathtt{int} \quad N : \mathtt{F}\tau \quad P : \mathtt{F}\tau}{\mathtt{pifz}\ M\ N\ P : \mathtt{F}\tau}$$

$\bigcirc_{>b}$ is the *statistical termination tester*, and $\mathtt{pifz}$ is *parallel if*. We extend the notation $\mathtt{pifz}\ M\ N\ P$ to the case where N and P have an arbitrary computation type $\underline{\tau}$ by letting $\mathtt{pifz}\ M\ N\ P$ denote $\lambda x_\sigma . \mathtt{pifz}\ M\ (N x_\sigma)\ (P x_\sigma)$ when N, P have type $\sigma \to \underline{\tau}$, where x_σ is a fresh variable.

The language CBPV($\mathtt{D}, \mathtt{P}$) + $\mathtt{pifz}$ is obtained by admitting only the second one as extra clause, while CBPV($\mathtt{D}, \mathtt{P}$) + $\bigcirc$ only admits the first one as extra clause.

4.3 Denotational Semantics

Let *Env*, the dcpo of *environments*, be the product of the dcpos $[\![\sigma]\!]$ over all variables x_σ. Its elements are maps ρ from variables x_σ to values $\rho(x_\sigma)$. The denotational semantics is given by a family of Scott-continuous maps $[\![M]\!]$, one

$$
\begin{aligned}
[\![x_\sigma]\!]\,\rho &= \rho(x_\sigma) \\
[\![\lambda x_\sigma.M]\!]\,\rho &= V \in [\![\sigma]\!] \mapsto [\![M]\!]\,(\rho[x_\sigma \mapsto V]) \qquad [\![MN]\!]\,\rho = [\![M]\!]\,\rho([\![N]\!]\,\rho) \\
[\![\mathtt{produce}\,M]\!]\,\rho &= \eta^{\mathcal{Q}}([\![M]\!]\,\rho) \\
[\![M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N]\!]\,\rho &= (V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^*([\![M]\!]\,\rho) \\
[\![\mathtt{thunk}\,M]\!]\,\rho &= [\![M]\!]\,\rho \qquad [\![\mathtt{force}\,M]\!]\,\rho = [\![M]\!]\,\rho \\
[\![\underline{*}]\!]\,\rho &= \top \qquad [\![\underline{n}]\!]\,\rho = n \\
[\![\mathtt{succ}\,M]\!]\,\rho &= \begin{cases} n+1 & \text{if } n = [\![M]\!]\,\rho \neq \bot \\ \bot & \text{otherwise} \end{cases} \\
[\![\mathtt{pred}\,M]\!]\,\rho &= \begin{cases} n-1 & \text{if } n = [\![M]\!]\,\rho \neq \bot \\ \bot & \text{otherwise} \end{cases} \\
[\![\mathtt{ifz}\ M\ N\ P]\!]\,\rho &= \begin{cases} [\![N]\!]\,\rho & \text{if } [\![M]\!]\,\rho = 0 \\ [\![P]\!]\,\rho & \text{if } [\![M]\!]\,\rho \neq 0, \bot \\ \bot & \text{if } [\![M]\!]\,\rho = \bot \end{cases} \\
[\![M;N]\!]\,\rho &= \begin{cases} [\![N]\!]\,\rho & \text{if } [\![M]\!]\,\rho = \top \\ \bot & \text{otherwise} \end{cases} \\
[\![\pi_1 M]\!]\,\rho &= m, [\![\pi_2 M]\!]\,\rho = n \text{ where } [\![M]\!]\,\rho = (m,n) \\
[\![\langle M, N\rangle]\!]\,\rho &= ([\![M]\!]\,\rho, [\![N]\!]\,\rho) \\
[\![\mathtt{ret}\,M]\!]\,\rho &= \delta_{[\![M]\!]\rho} \\
[\![\mathtt{do}\,x_\sigma \leftarrow M; N]\!]\,\rho &= (V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^\dagger([\![M]\!]\,\rho) \\
[\![M \oplus N]\!]\,\rho &= \frac{1}{2}([\![M]\!]\,\rho + [\![N]\!]\,\rho) \\
[\![M \owedge N]\!]\,\rho &= [\![M]\!]\,\rho \wedge [\![N]\!]\,\rho \qquad [\![\mathtt{abort}_{\mathtt{F}\tau}]\!]\,\rho = \emptyset \\
[\![\mathtt{rec}\,x_\sigma.M]\!]\,\rho &= \mathrm{lfp}(V \in [\![\sigma]\!] \mapsto [\![M]\!]\,\rho[x_\sigma \mapsto V])
\end{aligned}
$$

$$
\begin{aligned}
[\![\mathtt{pifz}\ M\ N\ P]\!]\,\rho &= \begin{cases} [\![N]\!]\,\rho & \text{if } [\![M]\!]\,\rho = 0 \\ [\![P]\!]\,\rho & \text{if } [\![M]\!]\,\rho \neq 0, \bot \\ [\![N]\!]\,\rho \wedge [\![P]\!]\,\rho & \text{if } [\![M]\!]\,\rho = \bot \end{cases} \\
[\![\bigcirc_{>b} M]\!]\,\rho &= \begin{cases} \top & \text{if } [\![M]\!]\,\rho \neq \bot \text{ and} \\ & b \ll \nu(\{\top\}) \text{ for every } \nu \in [\![M]\!]\,\rho \\ \bot & \text{otherwise} \end{cases}
\end{aligned}
$$

Figure 2: Denotational semantics

for each $M : \overline{\tau}$, from Env to $[\![\overline{\tau}]\!]$: see Figure 2, where the bottom two clauses are specific to CBPV($\mathtt{D},\mathtt{P}$) + **pifz**, resp. to CBPV($\mathtt{D},\mathtt{P}$) + $\bigcirc$, and the two of them together are specific to CBPV($\mathtt{D},\mathtt{P}$) + **pifz** + $\bigcirc$. We use the notation $V \in X \mapsto f(V)$ to denote the function that maps each $V \in X$ to $f(V)$. For every $\rho \in Env$, and every $V \in [\![\sigma]\!]$, we write $\rho[x_\sigma \mapsto V]$ for the environment that maps x_σ to V and every variable $y \neq x_\sigma$ to $\rho(y)$. The operator $\mathrm{lfp}\colon [X \to X] \to X$ maps every Scott-continuous map f from a pointed dcpo to itself, to its least fixed point $\mathrm{lfp}\, f = \sup_{n\in\mathbb{N}} f^n(\bot)$. The *Dirac mass* δ_x at x is the probability valuation such that $\delta_x(U) = 1$ if $x \in U$, 0 otherwise. For every continuous map $f\colon X \to \mathbf{V}_{\leq 1}Y$, $f^\dagger$ is the continuous map from $\mathbf{V}_{\leq 1}X$ to $\mathbf{V}_{\leq 1}Y$ defined by $f^\dagger(\nu)(V) = \int_{x\in X} f(x)(V)d\nu$ for every open subset V of Y. For future reference, we note that $f^\dagger(\delta_a) = f(a)$, and that, for every continuous map $h\colon Y \to \overline{\mathbb{R}}_+$,

$$\int_{y\in Y} h(y)df^\dagger(\nu) = \int_{x\in X} \left(\int_{y\in Y} h(y)df(x)\right) d\nu. \qquad (1)$$

Implicit here is the fact that the map $x \in X \mapsto \int_{y\in Y} h(y)df(x)$ is itself continuous. Also, integration is linear in both the integrated function h and the continuous valuation ν, and Scott-continuous in each. These facts can be found in Jones' PhD thesis [13].

The fact that the semantics $[\![M]\!]\rho$ is well-defined and continuous in ρ is standard. Note the use of binary infimum ($\wedge$) in the semantics of $\oslash$ and of **pifz**, for which we use the following lemma.

Lemma 4.3 *Let L be a continuous complete lattice.*

1. *The infimum map $\wedge\colon L \times L \to L$ is Scott-continuous.*
2. *For any two continuous maps $f, g\colon X \to L$, where X is a any topological space, the infimum $f \wedge g$ is computed pointwise: $(f \wedge g)(x) = f(x) \wedge g(x)$.*

Proof. Item 1 is well-known. Explicitly, one must show that for every directed family $(x_i)_{i\in I}$ with supremum x in M, for every $y \in L$, $y \wedge \sup_{i\in I} x_i \leq \sup_{i\in I}(y \wedge x_i)$: for every $z \ll y \wedge \sup_{i\in I} x_i$, z is below y and below some x_i, hence below $y \wedge x_i$ for some $i \in I$.

As for item 2, the composition of $\wedge$ with $x \mapsto (f(x), g(x))$ is continuous by item 1, is below f and g, and is clearly above any lower bound of f and g. $\square$

4.4 Operational Semantics

We choose an operational semantics in the style of [11]. It operates on configurations, which are pairs $C \cdot M$ of an evaluation context C and a term M. The deterministic part of the calculus will be defined by rewrite rules $C \cdot M \to C' \cdot M'$ between configurations. For the probabilistic and non-deterministic part of the calculus, we will rely on judgments $C \cdot M \downarrow a$, which state, roughly, that the probability that computation terminates, starting from $C \cdot M$, is larger than a.

The *elementary contexts*, together with their types $\overline{\sigma} \vdash \overline{\tau}$ (where $\overline{\sigma}$, $\overline{\tau}$ are value or computation types) are defined by:

- $[\_N] \colon (\sigma \to \underline{\tau}) \vdash \underline{\tau}$, for every $N \colon \sigma$ and every computation type $\underline{\tau}$;
- $[\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N] \colon \mathbf{F}\sigma \vdash \mathbf{F}\tau$ for every $N \colon \mathbf{F}\tau$;
- $[\mathbf{force}\ \_] \colon \mathbf{U}\underline{\tau} \vdash \underline{\tau}$, for every computation type $\underline{\tau}$;
- $[\mathbf{succ}\ \_], [\mathbf{pred}\ \_] \colon \mathbf{int} \vdash \mathbf{int}$;
- $[\mathbf{ifz}\ \_\ N\ P] \colon \mathbf{int} \vdash \overline{\sigma}$ for all $N, P \colon \overline{\sigma}$;
- $[\_; N] \colon \mathbf{unit} \vdash \overline{\sigma}$ for every $N \colon \overline{\sigma}$;
- $[\pi_1 \_] \colon \sigma \times \tau \vdash \sigma$ and $[\pi_2 \_] \colon \sigma \times \tau \vdash \tau$, for all value types σ and τ;
- $[\mathbf{do}\ x_\sigma \leftarrow \_; N] \colon \mathbf{V}\sigma \vdash \mathbf{V}\tau$, for every $N \colon \sigma \to \mathbf{V}\tau$.

The *initial contexts* are $[\_] \colon \overline{\sigma} \vdash \overline{\sigma}$, $[\mathbf{produce}\ \_] \colon \sigma \vdash \mathbf{F}\sigma$ and $[\mathbf{produce}\,\mathbf{ret}\ \_] \colon \sigma \vdash \mathbf{FV}\sigma$. For every elementary or initial context $E \colon \overline{\sigma} \vdash \overline{\tau}$ and every $M \colon \overline{\sigma}$, we write $E[M]$ for the result of replacing the unique occurrence of the hole $\_$ in E (after removing the outer square brackets) by M. E.g, $[\mathbf{succ}\ \_][\underline{3}] = \mathbf{succ}\ \underline{3}$.

A *context* (of type $\overline{\sigma} \vdash \overline{\tau}$) is a finite list $E_0 E_1 E_2 \cdots E_n$ ($n \in \mathbb{N}$) where E_0 is an initial context, $E_1, \ldots, E_n$ are elementary contexts, and $E_i \colon \overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$, $\overline{\sigma}_{n+1} = \overline{\sigma}$, and $\overline{\sigma}_0 = \overline{\tau}$. We then write $C[M]$ for $E_0[E_1[E_2[\cdots E_n[M] \cdots]]]$.

Note that the contexts are defined in exactly the same way for CBPV$(\mathtt{D},\mathtt{P})$ and for CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz}$, CBPV$(\mathtt{D},\mathtt{P}) + \bigcirc$, and CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz} + \bigcirc$.

The *configurations* of the operational semantics are pairs $C \cdot M$ where $C \colon \overline{\sigma} \vdash \mathbf{FVunit}$ and $M \colon \overline{\sigma}$. The rules of the operational semantics are given in Figure 3. The last row is specific to CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz}$, CBPV$(\mathtt{D},\mathtt{P}) + \bigcirc$, or to CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz} + \bigcirc$. The first rewrite rule—the *redex discovery rule* $C \cdot E[M] \to CE \cdot M$—applies provided E is an elementary context. The notation $N[x_\sigma := M]$ denotes capture-avoiding substitution of M for x_σ in N.

The judgments $C \cdot M \downarrow a$ are defined for all terms $M \colon \overline{\sigma}$, contexts $C \colon \overline{\sigma} \vdash \mathbf{FVunit}$, and $a \in \mathbb{Q} \cap [0, 1)$, and mean that a is way-below the probability of termination of $C \cdot M$ (i.e., either $a = 0$ or a is strictly less than the probability that $C \cdot M$ terminates). Since $\circledS$ induces non-deterministic choice, we really mean the probability of *must*-termination, namely that, in whichever way the non-determinism involved in the use of the $\circledS$ operator is resolved (evaluating left, or right), the final probability is larger than a.

We write $\Pr(C \cdot M\!\downarrow)$ for $\sup\{a \in \mathbb{Q} \in [0, 1) \mid C \cdot M \downarrow a \text{ is derivable}\}$, where sups are taken in $[0, 1]$. This leads to the following central notion, which we only state for ground terms. A term is *ground* if and only if it has no free variable. (We define *ground* contexts similarly.) The case of non-ground terms can be dealt with using appropriate quantifications over substitutions, but will not be needed.

Definition 4.4 *The* contextual preorder $\precsim_{\overline{\sigma}}$ *between ground CBPV*$(\mathtt{D},\mathtt{P})$ *terms of type* $\overline{\sigma}$ *is defined by* $M \precsim_{\overline{\sigma}} N$ *if and only if for every ground evaluation context* $C \colon \overline{\sigma} \vdash \mathbf{FVunit}$*,* $Pr(C \cdot M\!\downarrow) \leq Pr(C \cdot N\!\downarrow)$*.*

$$
\begin{array}{rlrl}
C \cdot E[M] \to CE \cdot M & & C[\_N] \cdot \lambda x_\sigma.M \to C \cdot M[x_\sigma := N] \\
C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot \mathtt{produce}\, M \to C \cdot N[x_\sigma := M] & & C[\mathtt{force}\ \_] \cdot \mathtt{thunk}\, M \to C \cdot M \\
[\_] \cdot \mathtt{produce}\, M \to [\mathtt{produce}\ \_] \cdot M & & \\
C[\mathtt{pred}\ \_] \cdot \underline{n} \to C \cdot \underline{n-1} & & C[\mathtt{succ}\ \_] \cdot \underline{n} \to C \cdot \underline{n+1} \\
C[\mathtt{ifz}\ \_\ N\ P] \cdot \underline{0} \to C \cdot N & & C[\mathtt{ifz}\ \_\ N\ P] \cdot \underline{n} \to C \cdot P \quad (n \neq 0) \\
C[\_; N] \cdot \underline{*} \to C \cdot N & & \\
C[\pi_1\_] \cdot \langle M, N\rangle \to C \cdot M & & C[\pi_2\_] \cdot \langle M, N\rangle \to C \cdot N \\
C[\mathtt{do}\ x_\sigma \leftarrow \_; N] \cdot \mathtt{ret}\, M \to C \cdot N[x_\sigma := M] & & [\mathtt{produce}\ \_] \cdot \mathtt{ret}\, M \to [\mathtt{produce}\,\mathtt{ret}\ \_] \cdot M \\
C \cdot \mathtt{rec}\, x_\sigma.M \to C \cdot M[x_\sigma := \mathtt{rec}\, x_\sigma.M] & &
\end{array}
$$

$$
\frac{}{[\mathtt{produce}\,\mathtt{ret}\ \_] \cdot \underline{*} \downarrow a}\ (a \in \mathbb{Q} \cap [0,1)) \qquad \frac{}{C \cdot M \downarrow 0} \qquad \frac{}{C \cdot \mathtt{abort}_{\mathtt{F}\tau} \downarrow a}\ (a \in \mathbb{Q} \cap [0,1))
$$

$$
\frac{C' \cdot M' \downarrow a}{C \cdot M \downarrow a}\ (\text{if } C \cdot M \to C' \cdot M') \qquad \frac{C \cdot M \downarrow a \quad C \cdot N \downarrow b}{C \cdot M \oplus N \downarrow (a+b)/2} \qquad \frac{C \cdot M \downarrow a \quad C \cdot N \downarrow a}{C \cdot M \otimes N \downarrow a}
$$

$$
\frac{[\_] \cdot M \downarrow b \quad C \cdot \underline{*} \downarrow a}{C \cdot \bigcirc_{>b} M \downarrow a} \qquad \frac{C \cdot \mathtt{ifz}\ M\ N\ P \downarrow a}{C \cdot \mathtt{pifz}\ M\ N\ P \downarrow a} \qquad \frac{C \cdot N \downarrow a \quad C \cdot P \downarrow a}{C \cdot \mathtt{pifz}\ M\ N\ P \downarrow a}
$$

Figure 3: Operational semantics

We will freely reuse the notations $\precsim_{\overline{\sigma}}$, for the similarly defined notions on the related languages CBPV(D, P) + **pifz**, CBPV(D, P) + $\bigcirc$, and CBPV(D, P) + **pifz** + $\bigcirc$. If there is any need to make the language precise, we will mention it explicitly.

We end this section with a few elementary lemmata, which will come in handy later on, and which should help the reader train with the way the operational semantics works.

Lemma 4.5 *If $C \cdot M \downarrow a$ is derivable and $b \in \mathbb{Q}$ is such that $0 \leq b \leq a$, then $C \cdot M \downarrow b$ is also derivable, whether in CBPV(D, P), CBPV(D, P) + **pifz**, CBPV(D, P) + $\bigcirc$, or CBPV(D, P) + **pifz** + $\bigcirc$.*

Proof. Easy induction on the rules of Figure 3. In the case of a derivation of the form $C \cdot M \oplus N \downarrow a$, where $a = (a_1 + a_2)/2$, from $C \cdot M \downarrow a_1$ and $C \cdot N \downarrow a_2$, we write b as $(b_1 + b_2)/2$ where b_1 and b_2 are rational and between 0 and a_1, resp. a_2. (E.g., we let $b_1 = \min(a_1, 2b)$ and $b_2 = 2b - b_1 = \max(2b - a_1, 0)$.) By induction hypothesis we can derive $C \cdot M \downarrow b_1$ and $C \cdot N \downarrow b_2$, so we can derive $C \cdot M \oplus N \downarrow (b_1 + b_2)/2 = b$. □

Lemma 4.6 *If $C \cdot M \to C' \cdot M'$, then $Pr(C \cdot M\downarrow) \geq Pr(C' \cdot M'\downarrow)$.*

Proof. Whenever we can derive $C' \cdot M' \downarrow a$, we can derive $C \cdot M \downarrow a$ by the leftmost rule of the next-to-last row of Figure 3. □

Lemma 4.7 *Let $C' = E_1 \cdots E_n$ be a sequence of elementary contexts, of type $\overline{\sigma} \vdash \overline{\tau}$. For every context $C : \overline{\tau} \vdash \mathtt{FVunit}$, for every term $N : \overline{\sigma}$, $Pr(C \cdot C'[N]{\downarrow}) = Pr(CC' \cdot N{\downarrow})$.*

Proof. By the redex discovery rule, $C \cdot C'[N] \rightarrow^* CC' \cdot N$, so $\Pr(C \cdot C'[N]{\downarrow}) \geq \Pr(CC' \cdot N{\downarrow})$ by Lemma 4.6. Conversely, if $C \cdot C'[N]{\downarrow}a$ is derivable, then we show that $CC' \cdot N{\downarrow}a$ is derivable by induction on n. If $n = 0$, this is clear. Otherwise, there are only two rules that allow us to derive $C \cdot C'[N] \downarrow a$. In the case of the first of these rules (the middle rule of the first of the three rows of rules), $a = 0$, and we can derive $CC' \cdot N \downarrow a$ by the same rule. In the case of the other rule, $C \cdot C'[N] \downarrow a$ was derived from a shorter derivation of $CE_1 \cdot C''[N] \downarrow a$, where $C'' = E_2 \cdots E_n$, using the redex discovery rule $C \cdot C'[N] = C \cdot E_1[C''[N]] \rightarrow CE_1 \cdot C''[N]$. By induction hypothesis, $CE_1C'' \cdot N$ is derivable, namely $CC' \cdot N$ is derivable. □

Lemma 4.8 *Let $C' = E_1 \cdots E_n$ be a sequence of elementary contexts. If $C \cdot M \rightarrow^* CC' \cdot N$ then $Pr(C \cdot M{\downarrow}) \geq Pr(C \cdot C'[N]{\downarrow})$.*

Proof. $\Pr(C \cdot M{\downarrow}) \geq \Pr(CC' \cdot N{\downarrow}) = \Pr(C \cdot C'[N]{\downarrow})$, by Lemma 4.6 and Lemma 4.7. □

For short, let us write $\Pr(M{\downarrow})$ for $\Pr([\_] \cdot M{\downarrow})$.

Lemma 4.9 *Let C be any context of type $\overline{\sigma} \vdash \mathtt{FVunit}$. For every term $M : \overline{\sigma}$, $Pr(C[M]{\downarrow}) = Pr(C \cdot M{\downarrow})$.*

Proof. Let us write C as E_0C' where E_0 is an initial context and $C' = E_1E_2 \cdots E_n$ is a sequence of elementary contexts. We first show that $\Pr([\_] \cdot C[M]{\downarrow}) = \Pr(E_0 \cdot C'[M]{\downarrow})$. Once this is done, Lemma 4.7 states that $\Pr(E_0 \cdot C'[M]{\downarrow}) = \Pr(E_0C' \cdot M{\downarrow}) = \Pr(C \cdot M{\downarrow})$, and that will finish the proof.

We assume $E_0 \neq [\_]$, otherwise the claim is trivial. Then $[\_] \cdot C[M] \rightarrow^* E_0 \cdot C'[M]$. Indeed, $[\_] \cdot C[M] \rightarrow [\mathtt{produce}\,\_] \cdot C'[M]$ if $E_0 = [\mathtt{produce}\,\_]$, and $[\_] \cdot C[M] \rightarrow [\mathtt{produce}\,\_] \cdot \mathtt{ret}\,C'[M] \rightarrow [\mathtt{produce}\,\mathtt{ret}\,\_] \cdot C'[M]$ if $E_0 = [\mathtt{produce}\,\mathtt{ret}\,\_]$. By Lemma 4.6, $\Pr([\_] \cdot C[M]{\downarrow}) \geq \Pr(E_0 \cdot C'[M]{\downarrow})$.

In the converse direction, assume that $[\_] \cdot C[M] \downarrow a$ is derivable. If $a = 0$, then $E_0 \cdot C'[M] \downarrow a$ is also derivable. Otherwise, if $E_0 = [\mathtt{produce}\,\_]$, then the only remaining possible derivation is obtained from a smaller derivation of $[\mathtt{produce}\,\_] \cdot C'[M] \downarrow a$, so $E_0 \cdot C'[M] \downarrow a$ is again derivable. If $a \neq 0$ and $E_0 = [\mathtt{produce}\,\mathtt{ret}\,\_]$, then we can only have derived $[\_] \cdot C[M] \downarrow a$ from a smaller derivation of $[\mathtt{produce}\,\_] \cdot \mathtt{ret}\,C'[M] \downarrow a$, and then from another derivation of $[\mathtt{produce}\,\mathtt{ret}\,\_] \cdot C'[M] \downarrow a$, namely $E_0 \cdot C'[M] \downarrow a$. Since that holds for every a, $\Pr([\_] \cdot C[M]{\downarrow}) \leq \Pr(E_0 \cdot C'[M]{\downarrow})$. □

5 Soundness

We let the *rank* of a type be 0 for a value type that is not of the form $\mathbf{V}\sigma$, 1/2 for types of the form $\mathbf{V}\sigma$, and 1 for computation types. This will play a key role in our soundness proof, for the following reason: for every elementary or initial context $E : \overline{\sigma} \vdash \overline{\tau}$, the rank of $\overline{\sigma}$ is less than or equal to the rank of $\overline{\tau}$. Hence if $C = E_0 E_1 E_2 \cdots E_n$ is of type $\overline{\sigma} \vdash \overline{\tau}$, and E_i is of type $\overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$, then every $\overline{\sigma}_i$ has rank between those of $\overline{\sigma}$ and $\overline{\tau}$.

Beyond its role as a technical aide, the concept of rank is profitably interpreted from the point of view of the type and effect discipline [21]. While the separation between value types and computation types exhibits two kinds of effects, ranks refine this further by distinguishing between rank 0 value types, where the only effect is recursion, from rank 1/2 value types, where probabilistic choice is also allowed. Rank 1 types further allow for non-deterministic choice effects. With that viewpoint, one might be puzzled by the fact that the rank 0 types $\mathbf{U}\underline{\tau}$ are able to encapsulate arbitrary rank 1 types. However, the typical inhabitants of types $\mathbf{U}\underline{\tau}$ are *thunks* $\mathbf{thunk}\, M$, which do *not* execute, hence do not produce any side effect, unless being forced to, using the $\mathbf{force}$ operation, yielding again a value of the rank 1 type $\underline{\tau}$.

We will also need to define the semantics of contexts $C : \overline{\sigma} \vdash \mathbf{FVunit}$ so that $[\![C[M]]\!]\,\rho = [\![C]\!]\,\rho([\![M]\!]\,\rho)$ for every $M : \overline{\sigma}$ and for every environment ρ. $[\![E_0 E_1 E_2 \cdots E_n]\!]\,\rho$ is the composition of $[\![E_0]\!]\,\rho$, $[\![E_1]\!]\,\rho$, $[\![E_2]\!]\,\rho$, $\ldots$, $[\![E_n]\!]\,\rho$, where:

- $[\![[\_N]]\!]\,\rho$ maps f to $f([\![N]\!]\,\rho)$,
- $[\![[\_ \;\mathbf{to}\; x_\sigma \;\mathbf{in}\; N]]\!]\,\rho = (V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^*$,
- $[\![[\mathbf{force}\,\_]]\!]\,\rho$ is the identity map,
- $[\![[\mathbf{succ}\,\_]]\!]\,\rho$ maps $\bot$ to $\bot$ and otherwise adds one,
- $[\![[\mathbf{pred}\,\_]]\!]\,\rho$ maps $\bot$ to $\bot$ and otherwise subtracts one,
- $[\![[\mathbf{ifz}\,\_\; N\; P]]\!]\,\rho$ maps 0 to $[\![N]\!]\,\rho$, every non-zero number to $[\![P]\!]\,\rho$ and $\bot$ to $\bot$,
- $[\![[\_; N]]\!]\,\rho$ maps $\top$ to $[\![N]\!]\,\rho$, and $\bot$ to $\bot$,
- $[\![[\pi_1\_]]\!]\,\rho$ is first projection,
- $[\![[\pi_2\_]]\!]\,\rho$ is second projection,
- $[\![[\mathbf{do}\, x_\sigma \leftarrow \_; N]]\!]\,\rho = (V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^\dagger$,
- $[\![[\mathbf{produce}\,\_]]\!]\,\rho = \eta^{\mathcal{Q}}$, and
- $[\![[\mathbf{produce}\,\mathbf{ret}\,\_]]\!]\,\rho$ maps V to $\eta^{\mathcal{Q}}(\delta_V)$.

Proposition 5.1 (Soundness) *Let $C : \overline{\sigma} \vdash \mathbf{FVunit}$, $M : \overline{\sigma}$, where $\overline{\sigma}$ is a value or computation type, and let $\rho \in Env$. In CBPV$(\mathtt{D},\mathtt{P})$, in CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz}$, in CBPV$(\mathtt{D},\mathtt{P}) + \bigcirc$, and in CBPV$(\mathtt{D},\mathtt{P}) + \mathbf{pifz} + \bigcirc$:*

1. *For every $a \in \mathbb{Q} \cap [0, 1)$, if $C \cdot M \downarrow a$ is derivable, then either $[\![C[M]]\!]\,\rho = \bot$ and $a = 0$, or $[\![C[M]]\!]\,\rho \neq \bot$ and for every $\nu \in [\![C[M]]\!]\,\rho$, $a \ll \nu(\{\top\})$.*

2. *If* $[\![C[M]]\!]\,\rho = \bot$ *then* $Pr(C \cdot M\!\downarrow) = 0$*, otherwise for every* $\nu \in [\![C[M]]\!]\,\rho$*,* $\nu(\{\top\}) \geq Pr(C \cdot M\!\downarrow)$*.*

Proof. Item 2 is an easy consequence of item 1, which we prove by induction on the derivation.

In the case of the first rule ($[\mathbf{produce}\,\mathbf{ret}\,\_] \cdot \underline{*} \downarrow a$), $C[M] = \mathbf{produce}\,\mathbf{ret}\,\underline{*}$, and $[\![C[M]]\!] \neq \bot$. For every $\nu \in [\![C[M]]\!]\,\rho = \eta^{\mathcal{Q}}(\delta_\top)$, we have $\nu \geq \delta_\top$, so $\nu(\{\top\}) \geq 1$, and certainly $a \ll 1$ for every $a \in \mathbb{Q} \cap [0, 1)$.

The case of the second rule $C \cdot M \downarrow 0$ is obvious.

The case of the leftmost rule of the next row follows from the observation that if $C \cdot M \to C' \cdot M'$, then $[\![C[M]]\!]\,\rho = [\![C'[M']]\!]\,\rho$. We use the standard substitution lemma $[\![M]\!]\,(\rho[x_\sigma \mapsto [\![N]\!]\,\rho]) = [\![M[x_\sigma := N]]\!]\,\rho$ in the case of β-reduction ($C[\_N] \cdot \lambda x_\sigma.M \to C \cdot M[x_\sigma := N]$): the value of the left-hand side is $[\![C]\!]\,\rho([\![M]\!]\,(\rho[x_\sigma \mapsto [\![N]\!]\,\rho]))$, and the value of the right-hand side is $[\![C]\!]\,\rho([\![M[x_\sigma := N]]\!]\,\rho))$. In the case of $C[\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N] \cdot \mathbf{produce}\,M \to C \cdot N[x_\sigma := M]$, we also use the fact that $(V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma := V])^*(\eta^{\mathcal{Q}}([\![M]\!]\,\rho)) = [\![N]\!]\,\rho[x_\sigma \mapsto [\![M]\!]\,\rho]$ (Proposition 4.2, item 2). In the case of $C[\mathbf{do}\,x_\sigma \leftarrow \_; N] \cdot \mathbf{ret}\,M \to C \cdot N[x_\sigma := M]$, we use the equality $f^\dagger(\delta_x) = f(x)$ and the substitution lemma.

By our observation on ranks, if $C\colon \mathbf{F}\sigma \vdash \mathbf{FVunit}$, where $C = E_0 E_1 E_2 \cdots E_n$ and $E_i\colon \overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$ for each i, then all the types $\overline{\sigma}_i$ are computation types (rank 1). In that case, E_i can only be of one of the two forms $[\_N]$, $[\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]$. (Further inspection would reveal that the first case is impossible, but we will not need that yet.) We now observe that in each case, $[\![E_i]\!]\,\rho$ maps top to top: in the case of $[\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]$, this is by Proposition 4.2, item 3. It follows that $[\![C]\!]\,\rho$ also maps top to top, whence $[\![C[\mathbf{abort}_{\mathbf{F}\sigma}]]\!]\,\rho = [\![C]\!]\,\rho([\![\mathbf{abort}_{\mathbf{F}\sigma}]\!]\,\rho) = [\![C]\!]\,\rho(\emptyset) = \emptyset$. As a consequence, $[\![C[\mathbf{abort}_{\mathbf{F}\sigma}]]\!]\,\rho \neq \bot$, and the claim that for every $\nu \in [\![C[\mathbf{abort}_{\mathbf{F}\sigma}]]\!]\,\rho$, $\nu(\{\top\}) \geq \Pr(C \cdot \mathbf{abort}\!\downarrow)$ is vacuously true: the rule that derives $C \cdot \mathbf{abort}_{\mathbf{F}\sigma} \!\downarrow\! a$ for every $a \in \mathbb{Q} \cap [0, 1)$ is sound.

Similarly, and still assuming $C\colon \mathbf{F}\sigma \vdash \mathbf{FVunit}$, for each i, $[\![E_i]\!]\,\rho$ preserves binary infima. When $E_i = [\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]$, this is because the function $(V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^*$ maps binary infima to binary infima by Proposition 4.2, item 3. When $E_i = [\_N]$, $[\![[\_N]]\!]\,\rho$ maps every f to $f([\![N]\!]\,\rho)$, and therefore preserves binary infima by Lemma 4.3, item 2. It follows that $[\![C]\!]\,\rho$ preserves binary infima. We apply this to the rightmost rule of the middle row (if $C \cdot M \downarrow a$ and $C \cdot N \downarrow a$ then $C \cdot M \otimes N \downarrow a$). We have $[\![C[M \otimes N]]\!]\,\rho = [\![C]\!]\,\rho([\![M]\!]\,\rho \wedge [\![N]\!]\,\rho) = [\![C]\!]\,\rho([\![M]\!]\,\rho) \wedge [\![C]\!]\,\rho([\![N]\!]\,\rho) = [\![C[M]]\!]\,\rho \wedge [\![C[N]]\!]\,\rho$.

In particular, if $[\![C[M \otimes N]]\!]\,\rho = \bot$, and since $a \wedge b = \bot$ implies $a = \bot$ or $b = \bot$ in any space of the form $\mathcal{Q}^\top_\bot(X)$, then $[\![C[M]]\!]\,\rho$ or $[\![C[N]]\!]\,\rho$ is equal to $\bot$. By symmetry, let us assume that $[\![C[M]]\!]\,\rho = \bot$. By induction hypothesis, the only value of a such that $C \cdot M \!\downarrow\! a$ is derivable is $a = 0$. There are only two rules that can end a derivation of $C \cdot M \otimes N \downarrow a$, and they both require $a = 0$.

If $[\![C[M \otimes N]]\!]\,\rho \neq \bot$, then $[\![C[M]]\!]\,\rho \neq \bot$ and $[\![C[N]]\!]\,\rho \neq \bot$, so by induction hypothesis, for every ν in $[\![C[M]]\!]\,\rho$, and for every ν in $[\![C[N]]\!]\,\rho$, $a \ll \nu(\{\top\})$. Hence this holds for every $\nu \in [\![C[M \otimes N]]\!]\,\rho = [\![C[M]]\!]\,\rho \wedge [\![C[N]]\!]\,\rho = [\![C[M]]\!]\,\rho \cup [\![C[N]]\!]\,\rho$.

Let us deal with the last of the CBPV(D, P) rules (middle rule, middle row of Figure 3): we have deduced $C \cdot M \oplus N \downarrow (a+b)/2$ from $C \cdot M \downarrow a$ and $C \cdot N \downarrow b$, hence by induction hypothesis: (a) either $[\![C[M]]\!]\,\rho = \bot$ and $a = 0$, or for every $\nu \in [\![C[M]]\!]\,\rho$, $a \ll \nu(\{\top\})$; and (b) either $[\![C[N]]\!]\,\rho = \bot$ and $b = 0$, or for every $\nu \in [\![C[N]]\!]\,\rho$, $b \ll \nu(\{\top\})$. In that case $C = E_0 E_1 E_2 \cdots E_n$ has type $\mathbf{V}\sigma \vdash \mathbf{FVunit}$ for some value type σ, and every intermediate type $\overline{\sigma}_i$ must therefore have rank 1/2 or 1. The only eligible elementary contexts $E_i : \overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$ $(1 \leq i \leq n)$ are of the form $[\_N]$, $[\_\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]$, or $[\mathbf{do}\, x_\sigma \leftarrow \_; N]$. In each case, the rank of $\overline{\sigma}_i$ is equal to that of $\overline{\sigma}_{i+1}$. Since $\overline{\sigma}_{n+1} = \mathbf{FVunit}$ has rank 1 and $\overline{\sigma}_0 = \mathbf{V}\sigma$ has rank 1/2, E_0 cannot be $[\_] : \mathbf{FVunit} \vdash \mathbf{FVunit}$. It cannot be $[\mathbf{produce}\,\mathbf{ret}\,\_] : \mathbf{unit} \vdash \mathbf{FVunit}$ either since $\mathbf{unit}$ has rank 0. Hence E_0 is equal to $[\mathbf{produce}\,\_] : \mathbf{Vunit} \vdash \mathbf{FVunit}$, and every E_i $(1 \leq i \leq n)$ is of the form $[\mathbf{do}\, x_\sigma \leftarrow \_; N]$. We note that $[\![[\mathbf{do}\, x_\sigma \leftarrow \_; N]]\!]\,\rho = (V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma \mapsto V])^\dagger$ is a linear map, i.e., preserves sums and scalar multiplication. Indeed the formula $f^\dagger(\nu)(V) = \int_{x \in X} f(x)(V) d\nu$ is linear in ν. It follows that $[\![E_1 E_2 \cdots E_n]\!]\,\rho$ is also linear, so $[\![E_1 E_2 \cdots E_n[M \oplus N]]\!]\,\rho = [\![E_1 E_2 \cdots E_n]\!]\,\rho(\frac{1}{2}([\![M]\!]\,\rho + [\![N]\!]\,\rho)) = \frac{1}{2}(\nu_1 + \nu_2)$, where $\nu_1 = [\![E_1 E_2 \cdots E_n[M]]\!]\,\rho$ and $\nu_2 = [\![E_1 E_2 \cdots E_n[N]]\!]\,\rho$. Note that $[\![C[M]]\!]\,\rho = \eta^{\mathcal{Q}}(\nu_1) = \uparrow\nu_1$, and similarly $[\![C[N]]\!]\,\rho = \uparrow\nu_2$, and that those values are different from $\bot$. Similarly, $[\![C[M \oplus N]]\!]\,\rho = \uparrow(\frac{1}{2}(\nu_1 + \nu_2))$ is different from $\bot$. Since $\nu_1 \in [\![C[M]]\!]\,\rho$, we obtain that $a \ll \nu_1(\{\top\})$ by (a). Similarly, $b \ll \nu_2(\{\top\})$. Using the fact that, for all $s, t \in [0,1]$, $s \ll t$ if and only if $s = 0$ or $s < t$, $(a+b)/2 \ll \frac{1}{2}(\nu_1(\{\top\}) + \nu_2(\{\top\}))$. For every $\nu \in [\![C[M \oplus N]]\!]\,\rho = \uparrow(\frac{1}{2}(\nu_1 + \nu_2))$, and we therefore obtain that $(a+b)/2 \ll \nu(\{\top\})$.

We turn to the rules of the bottom row, which are specific to the extensions of CBPV(D, P) with $\mathbf{pifz}$, or $\bigcirc$, or both. For the first one, by induction hypothesis either $[\![M]\!]\,\rho = \bot$ and then $b = 0$, or else $b \ll \mu(\{\top\})$ for every $\mu \in [\![M]\!]\,\rho$. The first case is impossible since it is a requirement of the syntax of $\bigcirc_{>b} M$ that b be non-zero. This implies that $[\![\bigcirc_{>b} M]\!]\,\rho = \top$. It follows that $[\![C[\bigcirc_{>b} M]]\!]\,\rho = [\![C]\!]\,\rho([\![\bigcirc_{>b} M]\!]\,\rho) = [\![C]\!]\,\rho(\top) = [\![C[\underline{*}]]\!]\,\rho$. By induction hypothesis again, either $[\![C[\underline{*}]]\!]\,\rho = \bot$ and $a = 0$, or $a \ll \nu(\{\top\})$ for every ν in $[\![C[\underline{*}]]\!]\,\rho$. Hence either $[\![C[\bigcirc_{>b} M]]\!]\,\rho = \bot$ and $a = 0$, or $a \ll \nu(\{\top\})$ for every ν in $[\![C[\bigcirc_{>b} M]]\!]\,\rho$.

For the last two, we note that, in all three cases on $[\![M]\!]\,\rho$ (equal to $\bot$, to 0, or other), $[\![C[\mathbf{pifz}\ M\ N\ P]]\!]\,\rho$ is equal to one of the terms $[\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho$ or $[\![C[N \owedge P]]\!]\,\rho$, and is larger than or equal to the other one. In other words, $[\![C[\mathbf{pifz}\ M\ N\ P]]\!]\,\rho = \max([\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho, [\![C[N \owedge P]]\!]\,\rho)$. If that is equal to $\bot$, then both terms $[\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho$ and $[\![C[N \owedge P]]\!]\,\rho$ are equal to $\bot$, so by induction hypothesis the only derivations of $C \cdot \mathbf{ifz}\ M\ N\ P \downarrow a$ and $C \cdot N \owedge P \downarrow a$ are such that $a = 0$. Hence the only derivations of $C \cdot \mathbf{pifz}\ M\ N\ P \downarrow a$ are such that $a = 0$, using any of the three possible rules. If $[\![C[\mathbf{pifz}\ M\ N\ P]]\!]\,\rho \neq \bot$, then let us assume that $C \cdot \mathbf{pifz}\ M\ N\ P \downarrow a$ by any of the last two rules. If $a = 0$, then certainly $a \ll \nu(\{\top\})$ for every $\nu \in [\![C[\mathbf{pifz}\ M\ N\ P]]\!]\,\rho$. Otherwise, by induction hypothesis we have $[\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho \neq \bot$ and $a \ll \nu(\{\top\})$ for every $\nu \in [\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho$, or $[\![C[N \owedge P]]\!]\,\rho \neq \bot$ and $a \ll \nu(\{\top\})$ for every $\nu \in [\![C[N \owedge P]]\!]\,\rho$. Since $[\![C[\mathbf{pifz}\ M\ N\ P]]\!]\,\rho = \max([\![C[\mathbf{ifz}\ M\ N\ P]]\!]\,\rho, [\![C[N \owedge P]]\!]\,\rho)$, and max means smallest with respect to inclusion (for non-bottom elements), in particular $a \ll \nu(\{\top\})$ for every $\nu \in [\![C[\mathtt{pifz}\ M\ N\ P]]\!]\,\rho$. $\Box$

6 Adequacy

Adequacy is proved through the use of a suitable logical relation $(R_{\overline{\sigma}})_{\overline{\sigma}\text{ type}}$, where $R_{\overline{\sigma}}$ relates ground terms of type $\overline{\sigma}$ with elements of $[\![\overline{\sigma}]\!]$. (A term is *ground* if and only if it has no free variable. We define *ground* contexts similarly.) Again we work in CBPV$(\mathtt{D},\mathtt{P})$ or any of its extensions with **pifz** or $\bigcirc$ or both, without further mention.

Defining $R_{\overline{\sigma}}$ necessitates that we also define auxiliary relations $R_\sigma^\perp$ between ground contexts $C\colon \mathbf{V}\sigma \vdash \mathbf{FVunit}$ (resp., R_σ^* between ground contexts $C\colon \mathbf{F}\sigma \vdash \mathbf{FVunit}$) and continuous maps $h\colon [\![\sigma]\!] \to [0,1]$. This pattern is similar to the technique of $\top\top$-lifting, and particularly to Katsumata's $\top\top$-logical predicates [15]. We write "for all $C\ R_\sigma^\perp\ h$" instead of "for every ground context $C\colon \mathbf{V}\sigma \vdash \mathbf{FVunit}$ and for every continuous map $h\colon [\![\sigma]\!] \to [0,1]$ such that $C\ R_\sigma^\perp\ h$", $C\ R_\sigma^*\ h$ instead of "for every ground context $C\colon \mathbf{F}\sigma \vdash \mathbf{FVunit}$ and for every continuous map $h\colon [\![\sigma]\!] \to [0,1]$ such that $C\ R_\sigma^*\ h$", and $M\ R_\sigma\ a$ instead of "for every ground term $M\colon \sigma$ and for every $a \in [\![\sigma]\!]$ such that $M\ R_\sigma\ a$". We define:

- $M\ R_{\mathbf{U}\underline{\tau}}\ h$ iff $\mathbf{force}\,M\ R_{\underline{\tau}}\ h$;
- $M\ R_{\mathbf{unit}}\ \top$ if $\underline{*} \precsim_{\mathbf{unit}} M$, and $M\ R_{\mathbf{unit}}\ \bot$ always;
- $M\ R_{\mathbf{int}}\ n$ if $\underline{n} \precsim_{\mathbf{int}} M$, and $M\ R_{\mathbf{int}}\ \bot$ always;
- $M\ R_{\sigma\times\tau}\ (V_1, V_2)$ if and only if $\pi_1 M\ R_\sigma\ V_1$ and $\pi_2 M\ R_\tau\ V_2$;
- $M\ R_{\mathbf{V}\sigma}\ \nu$ if and only if $\Pr(C\cdot M{\downarrow}) \geq \int_{x\in[\![\sigma]\!]} h(x)d\nu$ for all $C\ R_\sigma^\perp\ h$;
- $C\ R_\sigma^\perp\ h$ if and only if $\Pr(C\cdot \mathbf{ret}\,M{\downarrow}) \geq h(V)$ for all $M\ R_\sigma\ V$;
- $M\ R_{\mathbf{F}\sigma}\ Q$ if and only if for all $C\ R_\sigma^*\ h$, $\Pr(C\cdot M{\downarrow}) \geq h^*(Q)$; here h is any continuous map from $[\![\sigma]\!]$ to the continuous complete lattice $[0,1]$, so h^* makes sense: $h^*(\bot) = 0$, and if $Q \neq \bot$, then $h^*(Q) = \bigwedge_{a\in Q} h(a)$—which is equal to 1 if $Q = \emptyset$;
- $C\ R_\sigma^*\ h$ if and only if $\Pr(C\cdot \mathbf{produce}\,M{\downarrow}) \geq h(V)$ for all $M\ R_\sigma\ V$;
- $M\ R_{\sigma\to\underline{\tau}}\ f$ if and only if $MN\ R_{\underline{\tau}}\ f(V)$ for all $N\ R_\sigma\ V$.

Lemma 6.1 *For all ground terms $M, N\colon \overline{\sigma}$, if $M \precsim_{\overline{\sigma}} N$ and $M\ R_{\overline{\sigma}}\ V$ then $N\ R_{\overline{\sigma}}\ V$.*

Proof. By induction on $\overline{\sigma}$. If $\overline{\sigma} = \mathbf{U}\underline{\tau}$, then $M\ R_{\overline{\sigma}}\ V$ means that $\mathbf{force}\,M\ R_{\underline{\tau}}\ V$. For every ground context $C\colon \underline{\tau} \vdash \mathbf{FVunit}$, $\Pr(C\cdot \mathbf{force}\,M{\downarrow}) = \Pr(C[\mathbf{force}\,\_]\cdot M{\downarrow})$ and $\Pr(C\cdot \mathbf{force}\,N{\downarrow}) = \Pr(C[\mathbf{force}\,\_]\cdot N{\downarrow})$ by Lemma 4.7. Since $M \precsim_{\mathbf{U}\underline{\tau}} N$, $\Pr(C[\mathbf{force}\,\_]\cdot M{\downarrow}) \leq \Pr(C[\mathbf{force}\,\_]\cdot N{\downarrow})$, so $\Pr(C\cdot \mathbf{force}\,M{\downarrow}) \leq \Pr(C\cdot \mathbf{force}\,N{\downarrow})$. It follows that $\mathbf{force}\,M \precsim_{\underline{\tau}} \mathbf{force}\,N$. By induction hypothesis, $\mathbf{force}\,N\ R_{\underline{\tau}}\ V$, whence $N\ R_{\mathbf{U}\underline{\tau}}\ V$.

If $\overline{\sigma} = \mathtt{unit}$, then $M\ R_{\overline{\sigma}}\ V$ means that $V = \bot$, or that $V = \top$ and $V \precsim_{\mathtt{unit}} M$. In the first case, $N\ R_{\overline{\sigma}}\ V$ holds vacuously. In the second case, $V \precsim_{\mathtt{unit}} M \precsim_{\mathtt{unit}} N$, so $N\ R_{\overline{\sigma}}\ V$ again. The case $\overline{\sigma} = \mathtt{int}$ is dealt with similarly—in the second case, $V = n \in \mathbb{N}$ and $\underline{*}$ has to be replaced by $\underline{n}$.

If $\overline{\sigma} = \sigma \times \tau$, then $M\ R_{\overline{\sigma}}\ V$ means that $\pi_1 M\ R_\sigma\ V_1$ and $\pi_2 M\ R_\tau\ V_2$, where $V = (V_1, V_2)$. We note that for every ground context $C\colon \sigma \to \mathtt{FVunit}$, $\Pr(C \cdot \pi_1 M{\downarrow}) = \Pr(C[\pi_1 \_] \cdot M{\downarrow})$ by Lemma 4.7. In turn, $\Pr(C[\pi_1 \_] \cdot M{\downarrow}) \leq \Pr(C[\pi_1 \_] \cdot N{\downarrow}) = \Pr(C \cdot \pi_1 N{\downarrow})$ since $M \precsim_{\sigma\times\tau}$ and using Lemma 4.7 again. Therefore $\pi_1 M \precsim_\sigma \pi_1 N$. By induction hypothesis, $\pi_1 N\ R_\sigma\ V_1$. Similarly, $\pi_2 N\ R_\tau\ V_2$, so $N\ R_{\sigma\times\tau}\ (V_1, V_2) = V$.

If $\overline{\sigma} = \mathbf{V}\sigma$, then $M\ R_{\overline{\sigma}}\ V$ means that $V = \nu$ for some $\nu \in \mathbf{V}_{\leq 1}([\![\sigma]\!])$, and that $\Pr(C \cdot M{\downarrow}) \geq \int_{x \in [\![\sigma]\!]} h(x) d\nu$ for all $C\ R_\sigma^\perp\ h$. For all such C and h, $\Pr(C \cdot N{\downarrow})$ is even larger, so $N\ R_{\overline{\sigma}}\ V$.

If $\overline{\sigma} = \mathbf{F}\sigma$, then $M\ R_{\overline{\sigma}}\ V$ means that for all $C\ R_\sigma^*\ h$, $\Pr(C \cdot M{\downarrow}) \geq h^*(V)$. Then $\Pr(C \cdot N{\downarrow})$ is even larger, so $N\ R_{\overline{\sigma}}\ V$.

If $\overline{\sigma} = \sigma \to \underline{\tau}$, then $M\ R_{\overline{\sigma}}\ V$ means that V is some function $f \in [[\![\sigma]\!] \to [\![\underline{\tau}]\!]]$, and that for all $P\ R_\sigma\ V'$, $MP\ R_{\underline{\tau}}\ f(V')$. For every ground context $C\colon \underline{\tau} \vdash \mathtt{FVunit}$, $\Pr(C \cdot NP{\downarrow}) = \Pr(C[\_P] \cdot N{\downarrow}) \geq \Pr(C[\_P] \cdot M{\downarrow}) = \Pr(C \cdot MP{\downarrow})$, by Lemma 4.7, the assumption $M \precsim_{\sigma\to\underline{\tau}} N$, and Lemma 4.7 again. Hence $MP \precsim_{\underline{\tau}} NP$. By induction hypothesis, $NP\ R_{\underline{\tau}}\ f(V')$. It follows that $N\ R_{\sigma\to\underline{\tau}}\ f = V$. ☐

For each type $\overline{\sigma}$, and every ground term $M\colon \overline{\sigma}$, let us write $M\ R_{\overline{\sigma}}$ for the set of values $a \in [\![\overline{\sigma}]\!]$ such that $M\ R_{\overline{\sigma}}\ a$.

Lemma 6.2 *For every type $\overline{\sigma}$, for every ground term $M\colon \overline{\sigma}$, $M\ R_{\overline{\sigma}}$ is Scott-closed and contains $\bot$.*

Proof. This is an easy induction on types. Only the cases $\overline{\sigma} = \mathbf{V}\sigma$ and $\overline{\sigma} = \mathbf{F}\sigma$ need some care. In the case $\overline{\sigma} = \mathbf{V}\sigma$, $M\ R_{\mathbf{V}\sigma}$ is Scott-closed because integration is Scott-continuous in the valuation. Explicitly, it is upwards-closed, and for every directed family $(\nu_i)_{i\in I}$ in $M\ R_{\mathbf{V}\sigma}$, with supremum ν, for all $C\ R_\sigma^\perp\ h$, $\Pr(C \cdot M{\downarrow}) \geq \int_{x\in[\![\sigma]\!]} h(x) d\nu_i$ for every $i \in I$, so $\Pr(C \cdot M{\downarrow}) \geq \sup_{i\in I} \int_{x\in[\![\sigma]\!]} h(x) d\nu_i = \int_{x\in[\![\sigma]\!]} h(x) d\nu$. In order to show that $M\ R_{\mathbf{V}\sigma}$ contains $\bot$ (the zero valuation), we must show that $\Pr(C \cdot M{\downarrow}) \geq \int_{x\in[\![\sigma]\!]} h(x) d0 = 0$ for all $C\ R_\sigma^\perp\ h$, and that is trivial.

In the case $\overline{\sigma} = \mathbf{F}\sigma$, let us fix C and h so that $C\ R_\sigma^*\ h$. Since h^* is continuous by Proposition 4.2, item 2, $\{Q \in \mathcal{Q}_\perp^\top([\![\sigma]\!]) \mid h^*(Q) > r\} = (h^*)^{-1}((r, \infty])$ is open for every $r \in \mathbb{R}_+$. By taking complements, the set $F_{C,h} = \{Q \in \mathcal{Q}_\perp^\top([\![\sigma]\!]) \mid h^*(Q) \leq \Pr(C \cdot M{\downarrow})\}$ is closed. Hence $M\ R_{\mathbf{F}\sigma} = \bigcap_{C R_\sigma^* h} F_{C,h}$ is closed in $\mathcal{Q}_\perp^\top([\![\sigma]\!])$. Finally, $M\ R_{\mathbf{F}\sigma}$ contains $\bot$ because h^* is strict, hence $h^*(\bot) = 0$. ☐

Let us say that a term M *has x_σ as sole free variable* if and only if the set of free variables of M is included in $\{x_\sigma\}$, namely if M is ground or if the only free variable of M is x_σ. In that case, for every ground term N, $M[x_\sigma := N]$ is ground.

Corollary 6.3 *Let $M : \sigma$ have x_σ as sole free variable, let f be a Scott-continuous map from $[\![\sigma]\!]$ to $[\![\sigma]\!]$, and assume that for all $N \; R_\sigma \; V$, $M[x_\sigma := N] \; R_\sigma \; f(V)$. Then $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; \mathrm{lfp}\, f$.*

Proof. We show that $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; f^n(\bot)$ for every $n \in \mathbb{N}$. Since $\mathtt{rec}\, x_\sigma.M \; R_\sigma$ contains $\bot$ by Lemma 6.2, this is true when $n = 0$. If $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; f^n(\bot)$, then $M[x_\sigma := \mathtt{rec}\, x_\sigma.M] \; R_\sigma \; f^{n+1}(\bot)$ by assumption. We now use the fact that for every ground context $C : \sigma \to \mathtt{FVunit}$, $C \cdot \mathtt{rec}\, x_\sigma.M \to C \cdot M[x_\sigma := \mathtt{rec}\, x_\sigma.M]$, hence $\Pr(C \cdot \mathtt{rec}\, x_\sigma.M{\downarrow}) \geq \Pr(C \cdot M[x_\sigma := \mathtt{rec}\, x_\sigma.M]{\downarrow})$, by Lemma 4.6. Using Lemma 6.1, we obtain that $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; f^{n+1}(\bot)$.

Since $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; f^n(\bot)$ for every $n \in \mathbb{N}$ and since $\mathtt{rec}\, x_\sigma.M \; R_\sigma$ is Scott-closed (Lemma 6.2), $\mathtt{rec}\, x_\sigma.M \; R_\sigma \; \mathrm{lfp}\, f$. ☐

Lemma 6.4 *Let σ be a value type. For all $M \; R_\sigma \; V$, $\mathtt{ret}\, M \; R_{\mathtt{V}\sigma} \; \delta_V$.*

Proof. Let C be a ground context of type $\mathtt{V}\sigma \vdash \mathtt{FVunit}$, h be a continuous map from $[\![\sigma]\!]$ to $[0,1]$, and assume that $C \; R_\sigma^\perp \; h$. By definition of $R_\sigma^\perp$, and since $M \; R_\sigma \; V$, $\Pr(C \cdot \mathtt{ret}\, M{\downarrow}) \geq h(V)$, and $h(V) = \int_{x \in [\![\sigma]\!]} h(x) d\delta_V$. ☐

Lemma 6.5 *Let σ and τ be two value types. Let $N : \mathtt{V}\tau$ be a term with x_σ as sole free variable, $f \in [[\![\sigma]\!] \to [\![\mathtt{V}\tau]\!]]$, and assume that for all $P \; R_\sigma \; V$, $N[x_\sigma := P] \; R_{\mathtt{V}\tau} \; f(V)$. For all $M \; R_{\mathtt{V}\sigma} \; \nu$, $\mathtt{do}\, x_\sigma \leftarrow M; N \; R_{\mathtt{V}\tau} \; f^\dagger(\nu)$.*

Proof. Let $C : \mathtt{V}\tau \to \mathtt{FVunit}$ be a ground context, and h be a Scott-continuous map from $[\![\tau]\!]$ to $[0,1]$ such that $C \; R_\tau^\perp \; h$. We wish to show that $\Pr(C \cdot \mathtt{do}\, x_\sigma \leftarrow M; N{\downarrow}) \geq \int_{y \in [\![\tau]\!]} h(y) df^\dagger(\nu)$, namely that $\Pr(C \cdot \mathtt{do}\, x_\sigma \leftarrow M; N{\downarrow}) \geq \int_{x \in [\![\sigma]\!]} (\int_{y \in [\![\tau]\!]} h(y) df(x)) d\nu$, using (1).

We first show that $C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \; R_\sigma^\perp \; g$, where $g(x) = \int_{y \in [\![\tau]\!]} h(y) df(x)$ for every $x \in [\![\sigma]\!]$. That reduces to showing that $\Pr(C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \cdot \mathtt{ret}\, P{\downarrow}) \geq g(x)$ for all $P \; R_\sigma \; x$. Now $C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \cdot \mathtt{ret}\, P \to C \cdot N[x_\sigma := P]$, so $\Pr(C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \cdot \mathtt{ret}\, P{\downarrow}) \geq \Pr(C \cdot N[x_\sigma := P]{\downarrow})$, by Lemma 4.6, and $\Pr(C \cdot N[x_\sigma := P]{\downarrow}) \geq g(x) = \int_{y \in [\![\tau]\!]} h(y) df(x)$ because $C \; R_\tau^\perp \; h$ and $N[x_\sigma := P] \; R_{\mathtt{V}\sigma} \; f(x)$ for all $P \; R_\sigma \; x$.

Using this together with the fact that $M \; R_{\mathtt{V}\sigma} \; \nu$, $\Pr(C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \cdot M{\downarrow}) \geq \int_{x \in [\![\sigma]\!]} g(x) d\nu$. Since $C \cdot (\mathtt{do}\, x_\sigma \leftarrow M; N) \to C[\mathtt{do}\, x_\sigma \leftarrow \_; N] \cdot M$, by Lemma 4.6, $\Pr(C \cdot \mathtt{do}\, x_\sigma \leftarrow M; N{\downarrow}) \geq \int_{x \in [\![\sigma]\!]} g(x) d\nu$. ☐

Lemma 6.6 *Let σ be a value type. For all $M \; R_\sigma \; V$, $\mathtt{produce}\, M \; R_{\mathtt{F}\sigma} \; \eta^{\mathcal{Q}}(V)$.*

Proof. Let $Q = \eta^{\mathcal{Q}}(V)$. Let C be a ground context of type $\mathtt{F}\sigma \vdash \mathtt{FVunit}$, h be a continuous map from $[\![\sigma]\!]$ to $[0,1]$, and assume that $C \; R_\sigma^* \; h$. By definition of R_σ^*, $\Pr(C \cdot \mathtt{produce}\, M{\downarrow}) \geq h(V)$. Since $V \in Q$, $h(V) \geq \bigwedge_{x \in Q} h(x) = h^*(Q)$, so $\mathtt{produce}\, M \; R_{\mathtt{F}\sigma} \; Q$. ☐

Lemma 6.7 *Let σ, τ be two value types. Let $N : \mathtt{F}\tau$ be a term with x_σ as sole free variable, $f \in [[\![\sigma]\!] \to [\![\mathtt{F}\tau]\!]]$, and assume that for all $P \; R_\sigma \; V$, $N[x_\sigma := P] \; R_{\mathtt{F}\tau} \; f(V)$. For all $M \; R_{\mathtt{F}\sigma} \; Q$, $M \; \mathtt{to}\; x_\sigma \; \mathtt{in}\; N \; R_{\mathtt{F}\tau} \; f^*(Q)$.*

Proof. Let $C\colon \mathbf{F}\tau \vdash \mathtt{FVunit}$ be a ground context, and h be a Scott-continuous map from $[\![\tau]\!]$ to $[0,1]$ such that $C\ R^*_\tau\ h$. We wish to show that $\Pr(C \cdot M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N\!\downarrow) \geq h^*(f^*(Q))$. Using Proposition 4.2, we will show the equivalent claim that $\Pr(C \cdot M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N\!\downarrow) \geq (h^* \circ f)^*(Q)$.

We first show that $C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N]\ R^*_\sigma\ h^* \circ f$. For all $P\ R_\sigma\ V$, we aim to show that $\Pr(C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot \mathtt{produce}\, P\!\downarrow) \geq h^*(f(V))$. Since $N[x_\sigma := P]\ R_{\mathbf{F}\tau}\ f(V)$ and $C\ R^*_\tau\ h$, $\Pr(C \cdot N[x_\sigma := P]\!\downarrow) \geq h^*(f(V))$. Since $C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot \mathtt{produce}\, P \to C \cdot N[x_\sigma := P]$, by Lemma 4.6 $\Pr(C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot \mathtt{produce}\, P\!\downarrow) \geq h^*(f(V))$, as desired.

Knowing that $C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N]\ R^*_\sigma\ h^* \circ f$, and using $M\ R_{\mathbf{F}\sigma}\ Q$, we obtain that $\Pr(C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot M\!\downarrow) \geq (h^* \circ f)^*(Q)$. Since $C \cdot M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N \to C[\_\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N] \cdot M$, by Lemma 4.6 $\Pr(C \cdot M\ \mathtt{to}\ x_\sigma\ \mathtt{in}\ N\!\downarrow) \geq (h^* \circ f)^*(Q)$. □

We write $\chi_U\colon X \to \mathbb{S}$ for the characteristic map of an open subset U of a space X.

Lemma 6.8 *1.* $[\mathtt{produce}\ \_]\ R^\perp_{\mathtt{unit}}\ \chi_{\{\top\}}$*;*

2. $[\_]\ R^*_{\mathtt{Vunit}}\ (\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\}))$.

Proof. 1. Let $M\ R_{\mathtt{unit}}\ V$. It suffices to show that $\Pr([\mathtt{produce}\ \_] \cdot \mathtt{ret}\, M\!\downarrow) \geq \chi_{\{\top\}}(V)$. If $V = \perp$, then the right-hand side is 0, and the inequality is clear. Otherwise, we claim that the left-hand side is (greater than or) equal to 1. We have $[\mathtt{produce}\ \_] \cdot \mathtt{ret}\, M \to [\mathtt{produce}\, \mathtt{ret}\ \_] \cdot M$, so $\Pr([\mathtt{produce}\ \_] \cdot \mathtt{ret}\, M\!\downarrow) \geq \Pr([\mathtt{produce}\, \mathtt{ret}\ \_] \cdot M\!\downarrow)$ by Lemma 4.6. Since $M\ R_{\mathtt{unit}}\ \top$, $\Pr([\mathtt{produce}\, \mathtt{ret}\ \_] \cdot M\!\downarrow) \geq \Pr([\mathtt{produce}\, \mathtt{ret}\ \_] \cdot \underline{*}\!\downarrow)$, and $\Pr([\mathtt{produce}\, \mathtt{ret}\ \_] \cdot \underline{*}\!\downarrow) = 1$ since we can deduce $[\mathtt{produce}\, \mathtt{ret}\ \_] \cdot \underline{*} \downarrow a$ for every $a \in \mathbb{Q} \cap [0,1)$.

2. Let $M\ R_{\mathtt{Vunit}}\ \nu$. It suffices to show that $\Pr([\_] \cdot \mathtt{produce}\, M\!\downarrow) \geq \nu(\{\top\})$. Since $[\mathtt{produce}\ \_]\ R^\perp_{\mathtt{unit}}\ \chi_{\{\top\}}$ by item 1, $\Pr([\mathtt{produce}\ \_] \cdot M\!\downarrow) \geq \int_{x \in [\![\mathtt{unit}]\!]} \chi_{\{\top\}}(x)\, d\nu = \nu(\{\top\})$. We use Lemma 4.6 together with $[\_] \cdot \mathtt{produce}\, M \to [\mathtt{produce}\ \_] \cdot M$ and we obtain the desired inequality. □

A *substitution* $\theta = [x_1 := N_1, \cdots, x_n := N_n]$ is a map of finite domain $\operatorname{dom}\theta = \{x_1, \cdots, x_n\}$ from pairwise distinct variables x_i to ground terms N_i of the same type as x_i. We omit the definition of (parallel) substitution application $M\theta$. The case $M[x_\sigma := N]$ is the special case $n = 1$. We note that $M[x_1 := N_1, \cdots, x_n := N_n][x := N] = M[x_1 := N_1, \cdots, x_n := N_n, x := N]$ when x is distinct from $x_1, \ldots, x_n$, and not free in $N_1, \ldots, N_n$. Also, if $\operatorname{dom}\theta$ contains all the free variables of M, then $M\theta$ is ground.

We define the relation $R^\bullet$ between substitutions and environments by $\theta\ R^\bullet\ \rho$ if and only if for every $x_\sigma \in \operatorname{dom}\theta$, $x_\sigma\theta\ R_\sigma\ \rho(x_\sigma)$.

Proposition 6.9 *For every type $\overline{\sigma}$, for every term $M\colon \overline{\sigma}$ of CBPV*(D, P) *or any of its extensions with* $\mathtt{pifz}$ *or* $\bigcirc$ *or both, for every substitution θ whose domain contains all the free variables of M, for every environment ρ, if $\theta\ R^\bullet\ \rho$ then $M\theta\ R_{\overline{\sigma}}\ [\![M]\!]\rho$.*

Proof. By induction on M. This is the assumption $\theta\ R^\bullet\ \rho$ when M is a variable.

In the case of λ-abstractions $\lambda x_\sigma.M\colon \sigma \to \underline{\tau}$, let us write θ as $[x_1 := N_1, \cdots, x_n := N_n]$, and assume by α-renaming that x_σ is different from every x_i and free in no N_i. For all $N\ R_\sigma\ V$, we define θ' as $[x_1 := N_1, \cdots, x_n := N_n, x_\sigma := N]$ and we observe that $\theta'\ R^\bullet\ \rho[x_\sigma \mapsto V]$, so by induction hypothesis $M\theta'\ R_{\underline{\tau}}\ [\![M]\!]\,\rho[x_\sigma \mapsto V]$. Hence $M\theta[x_\sigma := N]\ R_{\underline{\tau}}\ [\![M]\!]\,\rho[x_\sigma \mapsto V]$. By Lemma 4.6 and Lemma 6.1, using the fact that $C \cdot (\lambda x_\sigma.M\theta)N \to C[\_N] \cdot \lambda x_\sigma.M\theta \to C \cdot M\theta[x_\sigma := N]$ for all ground contexts $C\colon \underline{\tau} \vdash \texttt{FVunit}$, we obtain that $(\lambda x_\sigma.M\theta)N\ R_{\underline{\tau}}\ [\![M]\!]\,\rho[x_\sigma \mapsto V]$. Since that holds for all $N\ R_\sigma\ V$, $(\lambda x_\sigma.M)\theta = \lambda x_\sigma.M\theta\ R_{\sigma\to\underline{\tau}}\ [\![\lambda x_\sigma.M]\!]\,\rho$.

The case of applications is by definition of $R_{\sigma\to\underline{\tau}}$.

For terms of the form $\texttt{produce}\,M\colon \texttt{F}\sigma$, by assumption $M\theta\ R_\sigma\ [\![M]\!]\,\rho$. By Lemma 6.6, $\texttt{produce}\,M\theta\ R_{\texttt{F}\sigma}\ \eta^{\mathcal{Q}}([\![M]\!]\,\rho) = [\![\texttt{produce}\,M]\!]\,\rho$.

For terms of the form $M\ \texttt{to}\ x_\sigma\ \texttt{in}\ N$ where $M\colon \texttt{F}\sigma$ and $N\colon \texttt{F}\tau$, as for λ-abstractions we write θ as $[x_1 := N_1, \cdots, x_n := N_n]$, and we assume by that x_σ is different from every x_i and free in no N_i. By induction hypothesis $M\theta\ R_{\texttt{F}\sigma}\ [\![M]\!]\,\rho$, and for all $P\ R_\sigma\ V$, $N\theta'\ R_{\texttt{F}\tau}\ [\![N]\!]\,\rho[x_\sigma := V]$ where $\theta' = [x_1 := N_1, \cdots, x_n := N_n, x_\sigma := P]$. As for λ-abstractions, the latter means that $N\theta[x_\sigma := P]\ R_{\texttt{F}\tau}\ [\![N]\!]\,\rho[x_\sigma := V]$. Letting f be the map $V \in [\![\sigma]\!] \mapsto [\![N]\!]\,\rho[x_\sigma := V]$, therefore, $N\theta[x_\sigma := P]\ R_{\texttt{F}\tau}\ f(V)$ for all $P\ R_\sigma\ V$. By Lemma 6.7, $(M\ \texttt{to}\ x_\sigma\ \texttt{in}\ N)\theta = M\theta\ \texttt{to}\ x_\sigma\ \texttt{in}\ N\theta\ R_{\texttt{F}\tau}\ f^*([\![M]\!]\,\rho) = [\![M\ \texttt{to}\ x_\sigma\ \texttt{in}\ N]\!]\,\rho$.

For terms $\texttt{thunk}\,M\colon \texttt{U}\underline{\tau}$, by induction hypothesis $M\theta\ R_{\underline{\tau}}\ [\![M]\!]\,\rho$. For every ground context $C\colon \underline{\tau} \vdash \texttt{FVunit}$, $C \cdot \texttt{force}\,\texttt{thunk}\,M\theta \to C[\texttt{force}\,\_] \cdot \texttt{thunk}\,M\theta \to C \cdot M\theta$, so by Lemma 4.6 and Lemma 6.1, $\texttt{force}\,\texttt{thunk}\,M\ R_{\underline{\tau}}\ [\![M]\!]\,\rho$. By definition of $R_{\texttt{U}\underline{\tau}}$, $\texttt{thunk}\,M\theta\ R_{\texttt{U}\underline{\tau}}\ [\![M]\!]\,\rho = [\![\texttt{thunk}\,M]\!]\,\rho$.

The case of terms of the form $\texttt{force}\,M\colon \underline{\tau}$ is by definition of $R_{\texttt{U}\underline{\tau}}$.

In the case of $\underline{*}$, we have $\underline{*}\ R_{\texttt{unit}}\ \top$ by definition. Similarly, $\underline{n}\ R_{\texttt{int}}\ n$.

For terms $\texttt{succ}\,M$ with $M\colon \texttt{int}$, by induction hypothesis $M\theta\ R_{\texttt{int}}\ [\![M]\!]\,\rho$. If $[\![M]\!]\,\rho = \bot$, then $\texttt{succ}\,M\theta\ R_{\texttt{int}}\ \bot = [\![\texttt{succ}\,M]\!]\,\rho$. Otherwise, let $n = [\![M]\!]\,\rho \in \mathbb{Z}$. By definition, $\Pr(C \cdot M\theta\downarrow) \geq \Pr(C \cdot \underline{n}\downarrow)$ for every ground context $C\colon \texttt{int} \vdash \texttt{FVunit}$. Replacing C by $C[\texttt{succ}\,\_]$, $\Pr(C[\texttt{succ}\,\_] \cdot M\theta\downarrow) \geq \Pr(C[\texttt{succ}\,\_] \cdot \underline{n}\downarrow)$. Since $C \cdot \texttt{succ}\,M\theta \to C[\texttt{succ}\,\_] \cdot M$ and since $C[\texttt{succ}\,\_] \cdot \underline{n} \to C \cdot \underline{n+1}$, using Lemma 4.6 we obtain $\Pr(C \cdot \texttt{succ}\,M\theta\downarrow) \geq \Pr(C[\texttt{succ}\,\_] \cdot M\downarrow) \geq \Pr(C[\texttt{succ}\,\_] \cdot \underline{n}\downarrow) \geq \Pr(C \cdot \underline{n+1}\downarrow)$. This shows that $\texttt{succ}\,M\theta\ R_{\texttt{int}}\ \underline{n+1} = [\![\texttt{succ}\,M]\!]\,\rho$. The case of terms $\texttt{pred}\,M$ is similar.

For terms $\texttt{ifz}\ M\ N\ P\colon \overline{\sigma}$, by induction hypothesis $M\theta\ R_{\texttt{int}}\ [\![M]\!]\,\rho$, $N\theta\ R_{\overline{\sigma}}\ [\![N]\!]\,\rho$, and $P\theta\ R_{\overline{\sigma}}\ [\![P]\!]\,\rho$. If $[\![M]\!]\,\rho = \bot$, then $(\texttt{ifz}\ M\ N\ P)\theta\ R_{\overline{\sigma}}\ \bot = [\![\texttt{ifz}\ M\ N\ P]\!]\,\rho$, by Lemma 6.2. Otherwise, let $n = [\![M]\!]\,\rho \in \mathbb{Z}$. Since $M\theta\ R_{\texttt{int}}\ [\![M]\!]\,\rho$, $\Pr(C \cdot M\theta\downarrow) \geq \Pr(C \cdot \underline{n}\downarrow)$ for every ground context $C\colon \texttt{int} \vdash \texttt{FVunit}$. In particular, for every ground context $C\colon \overline{\sigma} \vdash \texttt{FVunit}$, $\Pr(C[\texttt{ifz}\ \_\ N\theta\ P\theta] \cdot M\theta\downarrow) \geq \Pr(C[\texttt{ifz}\ \_\ N\theta\ P\theta] \cdot \underline{n}\downarrow)$. Using Lemma 4.7, it follows that $\Pr(C \cdot \texttt{ifz}\ M\theta\ N\theta\ P\theta\downarrow) \geq \Pr(C[\texttt{ifz}\ \_\ N\theta\ P\theta] \cdot \underline{n}\downarrow)$. Since $C[\texttt{ifz}\ \_\ N\theta\ P\theta] \cdot \underline{n}$ reduces to $C \cdot N\theta$ if $n = 0$, and to $C \cdot P\theta$ if $n \neq 0$, by Lemma 4.6, $\Pr(C \cdot \texttt{ifz}\ M\theta\ N\theta\ P\theta\downarrow)$ is larger than or equal to $\Pr(C \cdot N\theta\downarrow)$ if $n = 0$, and to $\Pr(C \cdot P\theta\downarrow)$ otherwise. By Lemma 6.1, $\texttt{ifz}\ M\theta\ N\theta\ P\theta\ R_{\overline{\sigma}}\ [\![N]\!]\,\rho$ if $n = 0$, and $\texttt{ifz}\ M\theta\ N\theta\ P\theta\ R_{\overline{\sigma}}\ [\![P]\!]\,\rho$ if $n \neq 0$. In any case, $(\texttt{ifz}\ M\ N\ P)\theta = \texttt{ifz}\ M\theta\ N\theta\ P\theta\ R_{\overline{\sigma}}\ [\![\texttt{ifz}\ M\ N\ P]\!]\,\rho$.

The case of terms $M; N\colon \overline{\sigma}$ is similar. By induction hypothesis, $M\theta\ R_{\texttt{unit}}$

$\llbracket M \rrbracket \rho$ and $N\theta \; R_{\overline{\sigma}} \; \llbracket N \rrbracket \rho$. If $\llbracket M \rrbracket \rho = \bot$, then $\llbracket M; N \rrbracket \rho = \bot$, so $(M;N)\theta \; R_{\overline{\sigma}}$ $\llbracket M; N \rrbracket \rho$ by Lemma 6.2. Otherwise, $\llbracket M \rrbracket \rho = \top$, so $M\theta \; R_{\mathtt{unit}} \; \top$, meaning that $\Pr(C \cdot M\theta\downarrow) \geq \Pr(C \cdot \underline{*}\downarrow)$ for every ground context $C \colon \mathtt{unit} \vdash \mathtt{FVunit}$. In particular, for every ground context $C \colon \overline{\sigma} \vdash \mathtt{FVunit}$, $\Pr(C[\_; N\theta] \cdot M\theta\downarrow) \geq$ $\Pr(C[\_; N\theta] \cdot \underline{*}\downarrow)$. By Lemma 4.7, $\Pr(C \cdot M\theta; N\theta\downarrow) = \Pr(C[\_; N\theta] \cdot M\theta\downarrow)$, and by Lemma 4.6, $\Pr(C[\_; N\theta] \cdot \underline{*}\downarrow) \geq \Pr(C \cdot N\theta\downarrow)$, using the rule $C[\_; N\theta] \cdot \underline{*} \to C \cdot N\theta$. Hence $\Pr(C \cdot M\theta; N\theta\downarrow) \geq \Pr(C \cdot N\theta\downarrow)$. By Lemma 6.1, $(M;N)\theta = M\theta; N\theta \; R_{\overline{\sigma}}$ $\llbracket N \rrbracket \rho = \llbracket M; N \rrbracket \rho$.

The case of terms $\pi_1 M$ and $\pi_2 M$ follows from the definition of $R_{\sigma \times \tau}$.

For terms $\langle M, N \rangle \colon \sigma \times \tau$, by induction hypothesis $M\theta \; R_\sigma \; \llbracket M \rrbracket \rho$ and $N\theta \; R_\tau$ $\llbracket N \rrbracket \rho$. For every ground context $C \colon \sigma \to \mathtt{FVunit}$, $C \cdot \pi_1 \langle M\theta, N\theta \rangle \to C[\pi_1 \_] \cdot$ $\langle M\theta, N\theta \rangle \to C \cdot M\theta$, so by Lemma 4.6 and Lemma 6.1, $\pi_1 \langle M, N \rangle \theta = \pi_1 \langle M\theta,$ $N\theta \rangle \; R_\sigma \; \llbracket M \rrbracket \rho$. Similarly, $\pi_2 \langle M, N \rangle \theta \; R_\tau \; \llbracket N \rrbracket \rho$. By definition of $R_{\sigma \times \tau}$, it follows that $\langle M, N \rangle \theta \; R_{\sigma \times \tau} \; \llbracket \langle M, N \rangle \rrbracket \rho$.

For terms $\mathtt{ret}\, M \colon \mathtt{V}\tau$, by induction hypothesis $M\theta \; R_\tau \; \llbracket M \rrbracket \rho$, so $\mathtt{ret}\, M\theta \; R_{\mathtt{V}\tau}$ $\delta_{\llbracket M \rrbracket \rho} = \llbracket \mathtt{ret}\, M \rrbracket \rho$ by Lemma 6.4.

For terms $\mathtt{do}\, x_\sigma \leftarrow M; N$ where $M \colon \mathtt{V}\sigma$ and $N \colon \mathtt{V}\tau$, as for λ-abstractions we write θ as $[x_1 := N_1, \cdots, x_n := N_n]$, and we assume that x_σ is different from every x_i and free in no N_i. By induction hypothesis $M\theta \; R_{\mathtt{V}\sigma} \; \llbracket M \rrbracket \rho$, and for all $P \; R_\sigma \; V$, $N\theta' \; R_{\mathtt{V}\tau} \; \llbracket N \rrbracket \rho[x_\sigma := V]$ where $\theta' = [x_1 := N_1, \cdots, x_n :=$ $N_n, x_\sigma := P]$. As for λ-abstractions, the latter means that $N\theta[x_\sigma := P] \; R_{\mathtt{V}\tau}$ $\llbracket N \rrbracket \rho[x_\sigma := V]$. Letting f be the map $V \in \llbracket \sigma \rrbracket \mapsto \llbracket N \rrbracket \rho[x_\sigma := V]$, therefore, $N\theta[x_\sigma := P] \; R_{\mathtt{V}\tau} \; f(V)$ for all $P \; R_\sigma \; V$. By Lemma 6.5, $(\mathtt{do}\, x_\sigma \leftarrow M; N)\theta =$ $\mathtt{do}\, x_\sigma \leftarrow M\theta; (N\theta) \; R_{\mathtt{V}\tau} \; f^\dagger(\llbracket M \rrbracket \rho) = \llbracket \mathtt{do}\, x_\sigma \leftarrow M; N \rrbracket \rho$.

For terms $M \oplus N \colon \mathtt{V}\tau$, by induction hypothesis $M\theta \; R_\tau \; \llbracket M \rrbracket \rho$ and $N\theta \; R_\tau$ $\llbracket N \rrbracket \rho$. For all $C \; R_\tau^\perp \; h$, $\Pr(C \cdot M\theta\downarrow) \geq \int_{x \in \llbracket \tau \rrbracket} h(x) d \llbracket M \rrbracket \rho$, and $\Pr(C \cdot N\theta\downarrow) \geq$ $\int_{x \in \llbracket \tau \rrbracket} h(x) d \llbracket N \rrbracket \rho$. For all a and b, if we can deduce $C \cdot M\theta \downarrow a$ and $C \cdot N\theta \downarrow b$, then we can deduce $C \cdot (M \oplus N)\theta \downarrow (a+b)/2$. Therefore $\Pr(C \cdot (M \oplus N)\theta\downarrow) \geq$ $\frac{1}{2}(\Pr(C \cdot M\theta\downarrow) + \Pr(C \cdot N\theta\downarrow)) \geq \frac{1}{2}(\int_{x \in \llbracket \tau \rrbracket} h(x) d \llbracket M \rrbracket \rho + \int_{x \in \llbracket \tau \rrbracket} h(x) d \llbracket N \rrbracket \rho) =$ $\int_{x \in \llbracket \tau \rrbracket} h(x) d \llbracket M \oplus N \rrbracket \rho$. Hence $(M \oplus N)\theta \; R_\tau \; \llbracket M \oplus N \rrbracket \rho$.

The case of terms $M \otimes N \colon \mathtt{F}\tau$ is similar, using the fact that $\Pr(C \cdot (M \otimes$ $N)\theta\downarrow) \geq \min(\Pr(C \cdot M\theta\downarrow), \Pr(C \cdot N\theta\downarrow))$ instead. The latter follows from the fact that if we can deduce both $C \cdot M\theta \downarrow a$ and $C \cdot N\theta \downarrow a$, then we can deduce $C \cdot (M \otimes N)\theta \downarrow a$. By induction hypothesis, $M\theta \; R_{\mathtt{F}\tau} \; \llbracket M \rrbracket \rho$ and $N\theta \; R_{\mathtt{F}\tau} \; \llbracket N \rrbracket \rho$. For all $C \; R_\tau^* \; h$, $\Pr(C \cdot M\theta\downarrow) \geq h^*(\llbracket M \rrbracket \rho)$ and $\Pr(C \cdot N\theta\downarrow) \geq h^*(\llbracket N \rrbracket \rho)$, so $\Pr(C \cdot (M \otimes N)\theta\downarrow) \geq \min(h^*(\llbracket M \rrbracket \rho), h^*(\llbracket N \rrbracket \rho)) = h^*(\llbracket M \rrbracket \rho) \wedge h^*(\llbracket N \rrbracket \rho) =$ $h^*(\llbracket M \rrbracket \rho \wedge \llbracket N \rrbracket \rho)$ (because h^* preserves binary infima, see Proposition 4.2, item 3) $= h^*(\llbracket M \otimes N \rrbracket \rho)$. Hence $(M \otimes N)\theta \; R_{\mathtt{F}\tau} \; \llbracket M \otimes N \rrbracket \rho$.

For $\mathtt{abort}_{\mathtt{F}\tau} \colon \mathtt{F}\tau$, we show that $\mathtt{abort}_{\mathtt{F}\tau} \; R_{\mathtt{F}\tau} \; \llbracket \mathtt{abort}_{\mathtt{F}\tau} \rrbracket \rho = \emptyset \; (\neq \bot)$ by showing that for all $C \; R_\tau^* \; h$, $\Pr(C \cdot \mathtt{abort}_{\mathtt{F}\tau}\downarrow) \geq h^*(\emptyset)$. Indeed, by the rule $C \cdot \mathtt{abort}_{\mathtt{F}\tau} \downarrow a \; (a \in \mathbb{Q} \cap [0,1))$, $\Pr(C \cdot \mathtt{abort}_{\mathtt{F}\tau}\downarrow) = 1$.

For $\mathtt{rec}\, x_\sigma.M$ where $M \colon \sigma$, as for λ-abstractions, let us write θ as $[x_1 :=$ $N_1, \cdots, x_n := N_n]$, and assume by α-renaming that x_σ is different from every x_i and free in no N_i. For all $N \; R_\sigma \; V$, we define θ' as $[x_1 := N_1, \cdots, x_n :=$ $N_n, x_\sigma := N]$ and we observe that $\theta' \; R^\bullet \; \rho[x_\sigma \mapsto V]$, so by induction hypothesis

$M\theta' \; R_\sigma \; [\![M]\!]\, \rho[x_\sigma \mapsto V]$. Let $f(V) = [\![M]\!]\, \rho[x_\sigma \mapsto V]$. We have just shown that $M\theta[x_\sigma := N] \; R_\sigma \; f(V)$ for all $N \; R_\sigma \; V$. By Corollary 6.3, $(\mathbf{rec}\, x_\sigma.M)\theta = \mathbf{rec}\, x_\sigma.(M\theta) \; R_\sigma \; \mathrm{lfp}(f) = [\![\mathbf{rec}\, x_\sigma.M]\!]\, \rho$.

We finish with the constructions involving $\bigcirc$ or **pifz**. For $\bigcirc_{>b}M$ where $M\colon \mathbf{FVunit}$, by induction hypothesis $M\theta \; R_{\mathbf{FVunit}} \; [\![M]\!]\, \rho$. Using Lemma 6.8, item 2, we obtain that $\Pr([\_] \cdot M\theta{\downarrow}) \geq (\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\}))^*([\![M]\!]\, \rho)$. If $[\![M]\!]\, \rho = \bot$, then $[\![\bigcirc_{>b}M]\!]\, \rho = \bot$, so $\bigcirc_{>b}M\theta \; R_{\mathbf{unit}} \; [\![\bigcirc_{>b}M]\!]\, \rho$, trivially. Otherwise, $[\![M]\!]\, \rho$ is a compact saturated subset of $\mathbf{V}_{\leq 1}\mathbb{S}$. If $b \not\ll \nu(\{\top\})$ for some $\nu \in [\![M]\!]\, \rho$, then again $[\![\bigcirc_{>b}M]\!]\, \rho = \bot$, so $\bigcirc_{>b}M\theta \; R_{\mathbf{unit}} \; [\![\bigcirc_{>b}M]\!]\, \rho$ is again trivial. Finally, if $b \ll \nu(\{\top\})$ for every $\nu \in [\![M]\!]\, \rho$, then we verify that $b \ll (\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\}))^*([\![M]\!]\, \rho)$: if $[\![M]\!]\, \rho \neq \emptyset$, $(\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\}))^*([\![M]\!]\, \rho) = \min_{\nu \in [\![M]\!]\rho} \nu(\{\top\})$, so b is way-below that value; while if $[\![M]\!]\, \rho = \emptyset$, then $(\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\}))^*([\![M]\!]\, \rho) = 1$, and $b \ll 1$ because the $\bigcirc_{>b}$ operator requires $b < 1$. It follows that $b \ll \Pr([\_] \cdot M\theta{\downarrow})$, so there is a number a such that $b \leq a$ and $[\_] \cdot M \downarrow a$ is derivable. By Lemma 4.5, $[\_] \cdot M \downarrow b$ is derivable. For every ground context $C\colon \mathbf{unit} \vdash \mathbf{FVunit}$, for every a such that $C \cdot \underline{*} \downarrow a$ is derivable, the leftmost rule of the bottom row of Figure 3 allows us to derive $C \cdot \bigcirc_{>b}M \downarrow a$, so $\Pr(C \cdot \bigcirc_{>b}M{\downarrow}) \geq \Pr(C \cdot \underline{*}{\downarrow})$. It follows that $\bigcirc_{>b}M \; R_{\mathbf{unit}} \; \top = [\![\bigcirc_{>b}M]\!]\, \rho$.

Finally, for terms of the form $\mathbf{pifz}\; M \; N \; P$, where $M\colon \mathbf{int}$ and $N, P\colon \mathbf{F}\tau$, we wish to show that $(\mathbf{pifz}\; M \; N \; P)\theta \; R_{\mathbf{F}\tau} \; [\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho$. This means showing that, for all $C \; R^*_\tau \; h$, $\Pr(C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta{\downarrow}) \geq h^*([\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho)$.

If $[\![M]\!]\, \rho = \bot$, then $[\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho = [\![N]\!]\, \rho \wedge [\![P]\!]\, \rho$. In that case, we note that $\Pr(C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta{\downarrow})$ is larger than or equal to $\min(\Pr(C \cdot N\theta{\downarrow}), \Pr(C \cdot P\theta{\downarrow}))$: for every $a \in \mathbb{Q} \cap [0, 1)$ way-below $\min(\Pr(C \cdot N\theta{\downarrow}), \Pr(C \cdot P\theta{\downarrow}))$, we can derive $C \cdot N\theta \downarrow b$ for some $b \geq a$, and $C \cdot P\theta \downarrow c$ for some $c \geq a$; then, by Lemma 4.5, we can derive $C \cdot N\theta{\downarrow}a$ and $C \cdot P\theta{\downarrow}a$, hence $C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta{\downarrow}a$. By induction hypothesis, $N\theta \; R_{\mathbf{F}\tau} \; [\![N]\!]\, \rho$, so $\Pr(C \cdot N\theta{\downarrow}) \geq h^*([\![N]\!]\, \rho)$, and similarly $\Pr(C \cdot P\theta{\downarrow}) \geq h^*([\![P]\!]\, \rho)$. Therefore $\Pr(C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta{\downarrow}) \geq \min(h^*([\![N]\!]\, \rho), h^*([\![P]\!]\, \rho)) = h^*([\![N]\!]\, \rho \wedge [\![P]\!]\, \rho) = h^*([\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho)$, since h^* preserves binary infima (Proposition 4.2, item 3).

If $[\![M]\!]\, \rho \neq \bot$, then $[\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho = [\![\mathbf{ifz}\; M \; N \; P]\!]\, \rho$. We have already seen that $\mathbf{ifz}\; M\theta \; N\theta \; P\theta \; R_{\mathbf{F}\tau} \; [\![\mathbf{ifz}\; M \; N \; P]\!]\, \rho$, so $\Pr(C \cdot \mathbf{ifz}\; M\theta \; N\theta \; P\theta{\downarrow}) \geq h^*([\![\mathbf{ifz}\; M \; N \; P]\!]\, \rho) = h^*([\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho)$. For every $a \in \mathbb{Q} \cap [0, 1)$, if we can derive $C \cdot \mathbf{ifz}\; M\theta \; N\theta \; P\theta \downarrow a$, then we can also derive $C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta \downarrow a$, so $\Pr(C \cdot \mathbf{pifz}\; M\theta \; N\theta \; P\theta{\downarrow}) \geq \Pr(C \cdot \mathbf{ifz}\; M\theta \; N\theta \; P\theta{\downarrow})$, and that is larger than or equal to $h^*([\![\mathbf{pifz}\; M \; N \; P]\!]\, \rho)$. $\square$

Given a ground term (or context) M, $[\![M]\!]\, \rho$ does not depend on ρ, and we will simply write $[\![M]\!]$ in this case.

Proposition 6.10 (Adequacy) *In any of the languages $CBPV(\mathtt{D}, \mathtt{P})$, $CBPV(\mathtt{D}, \mathtt{P}) + \mathbf{pifz}$, $CBPV(\mathtt{D}, \mathtt{P}) + \bigcirc$, and $CBPV(\mathtt{D}, \mathtt{P}) + \mathbf{pifz} + \bigcirc$, for every ground term $M\colon \mathbf{FVunit}$,*

$$Pr(M{\downarrow}) = h^*([\![M]\!]),$$

where h is the map $\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\})$.

Explicitly: either $[\![M]\!] = \bot$ and $Pr(M{\downarrow}) = 0$, or $[\![M]\!] = \emptyset$ and $Pr(M{\downarrow}) = 1$, or $[\![M]\!] \neq \bot, \emptyset$ and $Pr(M{\downarrow}) = \min_{\nu \in [\![M]\!]} \nu(\{\top\})$.

Proof. By Proposition 6.9 applied to $\theta = []$, $M\ R_{\mathtt{FVunit}}\ [\![M]\!]$. By Lemma 6.8, item 2, $[\_]\ R^*_{\mathtt{Vunit}}\ h$, so $\Pr([\_] \cdot M{\downarrow}) \geq h^*([\![M]\!])$. The converse inequality is by soundness (Proposition 5.1, item 2). $\Box$

7 Consequences of Adequacy

Definition 7.1 *The* applicative preorder $\precsim^{app}_\tau$ *between ground CBPV*$(\mathtt{D},\mathtt{P})$ *terms of value type* τ *is defined by* $M \precsim^{app}_\tau N$ *if and only if for every ground term* $Q\colon \tau \to \mathtt{FVunit}$*,* $Pr(QM{\downarrow}) \leq Pr(QN{\downarrow})$*.*

While the applicative preorder is only defined at *value* types, one can extend it fairly trivially to computation types by letting $M \precsim^{app}_{\underline{\tau}} N$ if and only if $\mathtt{thunk}\, M \precsim^{app}_{\mathtt{U}\underline{\tau}} \mathtt{thunk}\, N$.

As for $\precsim_{\overline{\sigma}}$ (Definition 4.4), we will freely reuse the notations $\precsim^{app}_\tau$ for all the variants of CBPV$(\mathtt{D},\mathtt{P})$ considered in this paper, with or without $\bigcirc$ and $\mathtt{pifz}$. Any result that does not mention the language considered holds for all four: this will notably be the case in the current section.

Lemma 7.2 *For all ground terms* $M, N\colon \sigma \to \underline{\tau}$ *such that* $M \precsim_{\sigma\to\underline{\tau}} N$*, for every ground term* $P\colon \sigma$*,* $MP \precsim_{\underline{\tau}} NP$*.*

Proof. We must show that for every ground evaluation context $C\colon \underline{\tau} \vdash \mathtt{FVunit}$, $\Pr(C \cdot MP{\downarrow}) \leq \Pr(C \cdot NP{\downarrow})$. By Lemma 4.7, $\Pr(C \cdot MP{\downarrow}) = \Pr(C[\_P] \cdot M{\downarrow})$. Similarly, $\Pr(C \cdot NP{\downarrow}) = \Pr(C[\_P] \cdot N{\downarrow})$. Since $M \precsim_{\sigma\to\underline{\tau}} N$, $\Pr(C[\_P] \cdot M{\downarrow}) \leq \Pr(C[\_P] \cdot N{\downarrow})$, and we conclude. $\Box$

We reuse the logical relation of Section 6.

The following is sometimes called *Milner's Context Lemma* in the setting of PCF, and we will prove it by using a variant of an argument due to A. Jung [20, Theorem 8.1].

Theorem 7.3 (Contextual=applicative) *For every value type* τ*, the contextual preorder* $\precsim_\tau$ *and the applicative preorder* $\precsim^{app}_\tau$ *on ground CBPV*$(\mathtt{D},\mathtt{P})$ *terms of type* τ *are the same relation.*

Proof. Let M, N be two ground terms of type τ. If $M \precsim^{app}_\tau N$, then consider a ground evaluation context $C\colon \tau \vdash \mathtt{FVunit}$. By Lemma 4.9, $\Pr(C[M]{\downarrow})$, which is equal to $\Pr([\_] \cdot C[M]{\downarrow})$ by definition, is equal to $\Pr(C \cdot M{\downarrow})$. By adequacy (Proposition 6.10), $\Pr(C[M]{\downarrow}) = h^*([\![C[M]]\!])$ where h is the map $\nu \in \mathbf{V}_{\leq 1}\mathbb{S} \mapsto \nu(\{\top\})$. Let $Q = \lambda x_\tau.C[x_\tau]$, where x_τ is a fresh variable of type τ. Then $[\![C[M]]\!] = [\![QM]\!]$. By adequacy again, $\Pr(QM{\downarrow}) = h^*([\![QM]\!])$, so $\Pr(C[M]{\downarrow}) = \Pr(QM{\downarrow})$. Similarly, $\Pr(C[N]{\downarrow}) = \Pr(QN{\downarrow})$. Since $M \precsim^{app}_\tau N$, the former is less than or equal to the latter, so $M \precsim_\tau N$.

Conversely, let us assume $M \precsim_\tau N$. Consider a ground term $Q\colon \tau \to \mathtt{FVunit}$. By Proposition 6.9 with $\theta = []$, $M\ R_\tau\ [\![M]\!]$. By Lemma 6.1, since $M \precsim_\tau N$, we also have $N\ R_\tau\ [\![M]\!]$. By Proposition 6.9 again, $Q\ R_{\tau\to\mathtt{FVunit}}\ [\![Q]\!]$. Hence $QN\ R_{\mathtt{FVunit}}\ [\![QM]\!]$. By Lemma 6.8, $[\_]\ R^*_{\mathtt{Vunit}}\ h$, where h is as above. Using the definition of $R_{\mathtt{FVunit}}$, $\Pr(QN\downarrow) = \Pr([\_] \cdot QN\downarrow) \geq h^*(\llbracket QM \rrbracket)$. The latter is equal to $\Pr(QM\downarrow)$ by adequacy (Proposition 6.10). We have shown $\Pr(QM\downarrow) \leq \Pr(QN\downarrow)$, where Q is arbitrary, hence $M \precsim^{app}_{\tau} N$. □

Corollary 7.4 *For every computation type $\underline{\tau}$, the contextual preorder $\precsim_{\underline{\tau}}$ and the applicative preorder $\precsim^{app}_{\underline{\tau}}$ on ground CBPV*$(\mathtt{D},\mathtt{P})$ *terms of type $\underline{\tau}$ are the same relation.*

Proof. We claim that $M \precsim_{\underline{\tau}} N$ if and only if $\mathbf{thunk}\, M \precsim_{\mathbf{U}\underline{\tau}} \mathbf{thunk}\, N$. The result will then follow from Theorem 7.3, since $\mathbf{thunk}\, M \precsim_{\mathbf{U}\underline{\tau}} \mathbf{thunk}\, N$ is equivalent to $\mathbf{thunk}\, M \precsim^{app}_{\mathbf{U}\underline{\tau}} \mathbf{thunk}\, N$, hence to $M \precsim^{app}_{\underline{\tau}} N$, by definition.

If $M \precsim_{\underline{\tau}} N$, let C be any ground evaluation context of type $\mathbf{U}\underline{\tau} \vdash \mathbf{FVunit}$. Let us write C as $E_0 E_1 E_2 \cdots E_n$, where $E_i \colon \overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$, $\overline{\sigma}_{n+1} = \mathbf{U}\underline{\tau}$ and $\overline{\sigma}_0 = \mathbf{FVunit}$. Since $\mathbf{U}\underline{\tau}$ is not $\mathbf{unit}$, $\mathbf{Vunit}$, or $\mathbf{FVunit}$, n must be at least 1. The only elementary context E_n of type $\mathbf{U}\underline{\tau} \vdash \overline{\sigma}_n$ is $[\mathbf{force}\,\_]$. Let $C' = E_0 E_1 E_2 \cdots E_{n-1}$. Then $\Pr(C \cdot \mathbf{thunk}\, M\downarrow) = \Pr(C'[\mathbf{force}\,\_] \cdot \mathbf{thunk}\, M\downarrow) = \Pr(C'[\mathbf{force}\,\mathbf{thunk}\, M]\downarrow)$ (by Lemma 4.9) $= h^*(\llbracket C'[\mathbf{force}\,\mathbf{thunk}\, M] \rrbracket)$ (by adequacy, where h is given in Proposition 6.10) $= h^*(\llbracket C'[M] \rrbracket)$ (because $\mathbf{force}$ and $\mathbf{thunk}$ are both interpreted as identity maps) $= \Pr(C'[M]\downarrow) = \Pr(C' \cdot M\downarrow)$. Similarly, $\Pr(C \cdot \mathbf{thunk}\, N\downarrow) = \Pr(C' \cdot N\downarrow)$. Since $M \precsim_{\underline{\tau}} N$, the former is less than or equal to the latter. This allows us to conclude that $\mathbf{thunk}\, M \precsim_{\mathbf{U}\underline{\tau}} \mathbf{thunk}\, N$.

Conversely, we assume that $\mathbf{thunk}\, M \precsim_{\mathbf{U}\underline{\tau}} \mathbf{thunk}\, N$, and we consider an arbitrary ground evaluation context $C \colon \underline{\tau} \vdash \mathbf{FVunit}$. Then $C[\mathbf{force}\,\_]$ is a ground evaluation context of type $\mathbf{U}\underline{\tau} \vdash \mathbf{FVunit}$, so $\Pr(C[\mathbf{force}\,\_] \cdot \mathbf{thunk}\, M\downarrow) \leq \Pr(C[\mathbf{force}\,\_] \cdot \mathbf{thunk}\, N\downarrow)$. As above, we have $\Pr(C[\mathbf{force}\,\_] \cdot \mathbf{thunk}\, M\downarrow) = h^*(\llbracket C[\mathbf{force}\,\mathbf{thunk}\, M] \rrbracket) = h^*(\llbracket C[M] \rrbracket) = \Pr(C \cdot M\downarrow)$, and $\Pr(C[\mathbf{force}\,\_] \cdot \mathbf{thunk}\, N\downarrow) = \Pr(C \cdot N\downarrow)$, and the former is less than or equal to the latter. □

The following proposition is a form of extensionality: two abstractions are related by $\precsim_{\sigma \to \underline{\tau}}$ if and only if applying them to the same ground terms yield related results.

Proposition 7.5 *Let $M, N \colon \underline{\tau}$ be two terms with x_σ as sole free variable. Then $\lambda x_\sigma.M \precsim_{\sigma \to \underline{\tau}} \lambda x_\sigma.N$ if and only if for every ground term $P \colon \sigma$, $M[x_\sigma := P] \precsim_{\underline{\tau}} N[x_\sigma := P]$.*

Proof. If $\lambda x_\sigma.M \precsim_{\sigma \to \underline{\tau}} \lambda x_\sigma.N$, then $(\lambda x_\sigma.M)P \precsim_{\underline{\tau}} (\lambda x_\sigma.N)P$ for every ground term $P \colon \sigma$, by Lemma 7.2. Hence for every ground evaluation context $C \colon \tau \vdash \mathbf{FVunit}$, $\Pr(C \cdot (\lambda x_\sigma.M)P\downarrow) \leq \Pr(C \cdot (\lambda x_\sigma.N)P\downarrow)$. Using Lemma 4.9, we obtain $\Pr(C[(\lambda x_\sigma.M)P]\downarrow) \leq \Pr(C[(\lambda x_\sigma.N)P]\downarrow)$. By adequacy (Proposition 6.10), $\Pr(C[(\lambda x_\sigma.M)P]\downarrow) = h^*(\llbracket C[(\lambda x_\sigma.M)P] \rrbracket)$, where $h(\nu) = \nu(\{\top\})$. That is equal to $h^*(\llbracket C[M[x_\sigma := P]] \rrbracket)$, hence to $\Pr(C[M[x_\sigma := P]]\downarrow) = \Pr(C \cdot M[x_\sigma := P]\downarrow)$. Similarly, $\Pr(C[(\lambda x_\sigma.N)P]\downarrow) = \Pr(C \cdot N[x_\sigma := P]\downarrow)$, so $\Pr(C \cdot M[x_\sigma := P]\downarrow) \leq \Pr(C \cdot N[x_\sigma := P]\downarrow)$. Since C is arbitrary, $M[x_\sigma := P] \precsim_{\underline{\tau}} N[x_\sigma := P]$.

Conversely, assume that $M[x_\sigma := P] \precsim_\tau N[x_\sigma := P]$ for every ground term $P \colon \sigma$. We wish to show that for every ground evaluation context $C \colon (\sigma \to \underline{\tau}) \vdash \mathbf{FVunit}$, $\Pr(C \cdot \lambda x_\sigma.M\downarrow) \leq \Pr(C \cdot \lambda x_\sigma.N\downarrow)$. Let us write C as $E_0 E_1 E_2 \cdots E_n$, where each E_i is of type $\overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$, $\overline{\sigma}_0 = \mathtt{\textbf{FVunit}}$ and $\overline{\sigma}_{n+1} = \sigma \to \underline{\tau}$. We cannot have $n = 0$, since $\sigma \to \underline{\tau}$ is none of the types $\mathtt{\textbf{unit}}$, $\mathtt{\textbf{Vunit}}$, $\mathtt{\textbf{FVunit}}$. By inspection of the possible shape of the elementary context E_n, we see that it must be of the form $[\_P]$ for some (ground) term $P\colon \sigma$. Let $C' = E_0 E_1 E_2 \cdots E_{n-1} : \underline{\tau} \to \mathtt{\textbf{FVunit}}$. Using Lemma 4.9 and adequacy as above, $\Pr(C \cdot \lambda x_\sigma.M{\downarrow}) = \Pr(C' \cdot M[x_\sigma := P]{\downarrow})$, and similarly with N instead of M. We have $\Pr(C' \cdot M[x_\sigma := P]{\downarrow}) \leq \Pr(C' \cdot N[x_\sigma := P]{\downarrow})$ since $M[x_\sigma := P] \precsim_{\underline{\tau}} N[x_\sigma := P]$, so $\Pr(C \cdot \lambda x_\sigma.M{\downarrow}) \leq \Pr(C \cdot \lambda x_\sigma.N{\downarrow})$. $\square$

A final, expected, consequence of adequacy is the following.

Proposition 7.6 *For every value type τ, for every two ground terms $M, N\colon \tau$, if $[\![M]\!] \leq [\![N]\!]$ then $M \precsim_\tau N$.*

Proof. For every ground term $Q\colon \tau \to \mathtt{\textbf{FVunit}}$, $[\![QM]\!] = [\![Q]\!]\,([\![M]\!]) \leq [\![Q]\!]\,([\![N]\!])$, hence $h^*([\![QM]\!]) \leq h^*([\![QN]\!])$ for every continuous map $h\colon \mathbf{V}_{\leq 1}\mathbb{S} \to [0,1]$. By adequacy (Proposition 6.10), $\Pr(QM{\downarrow}) = h^*([\![QM]\!])$, and $\Pr(QN{\downarrow}) = h^*([\![QN]\!])$ where h is the map $\nu \mapsto \nu(\{\top\})$. Therefore $\Pr(QM{\downarrow}) \leq \Pr(QN{\downarrow})$. $\square$

The converse implication, if it holds, is full abstraction.

8 The Failure of Full Abstraction

We will show that CBPV($\mathtt{D}$, $\mathtt{P}$) is not fully abstract, for two reasons. One is the expected lack of a parallel if operator, just as in PCF [19]. The other is the lack of a statistical termination tester, as in [11].

Our main tool is a variant on our previous logical relations $(S_{\overline{\sigma}})_{\overline{\sigma}\text{ type}}$. This time, $S_{\overline{\sigma}}$ will be an I-ary relation, for some non-empty set I, between semantical values—namely, $S_{\overline{\sigma}} \subseteq [\![\overline{\sigma}]\!]^I$. The construction is parameterized by a finite family $\mathcal{J}$ of subsets of I, and two I-ary relations $\triangleright, \trianglerighteq \subseteq [0,1]^I$. Again we will also define auxiliary relations $S^\perp_\sigma$, and S^*_σ, which are certain sets of I-tuples of Scott-continuous maps from $[\![\sigma]\!]$ to $[0,1]$. We write $\vec{a}$ for $(a_i)_{i\in I}$, and similarly with $\vec{\nu}$, $\vec{Q}$, etc. For every $\vec{a} \in [0,1]^I$ and every subset J of I, we write $\vec{a}_{|J}$ for the vector obtained from $\vec{a}$ by replacing every element a_i, $i \in J$, by 0; namely, $a_{|J\ i}$ is equal to 0 if $i \in J$, to a_i otherwise. We require the following:

- $I \in \mathcal{J}$, $\mathcal{J}$ is closed under binary unions, and is well-founded: every filtered family $(J_k)_{k\in K}$ in $\mathcal{J}$ has a least element J_{k_1}, $k_1 \in K$.
- $\triangleright$ is non-empty, closed under directed suprema, convex (notably, if $(a_i)_{i\in I}$ and $(b_i)_{i\in I}$ are in $\triangleright$ then so is $((a_i + b_i)/2)_{i\in I}$), and is $\mathcal{J}$*-lower*, meaning that for every $\vec{a} \in \triangleright$, for every $J \in \mathcal{J}$, $\vec{a}_{|J}$ is in $\triangleright$;
- $\trianglerighteq$ is closed under directed suprema, under pairwise minima (if $(a_i)_{i\in I}$ and $(b_i)_{i\in I}$ are in $\trianglerighteq$ then so is $(\min(a_i + b_i))_{i\in I}$), contains the all one vector $\vec{1}$, and is $\mathcal{J}$-lower.

We define the following.

- $\vec{a} \in S_{\mathtt{U}\underline{\tau}}$ iff $\vec{a} \in S_\tau$;
- $\vec{a} \in S_{\mathtt{unit}}$ (resp., $S_{\mathtt{int}}$) iff: the set $J = \{i \in I \mid a_i = \bot\}$ is in $\mathcal{J}$ and the components a_i, $i \in I \smallsetminus J$, are all equal;
- $\vec{a} \in S_{\sigma\times\tau}$, where $a_i = (b_i, c_i)$ for every $i \in I$, iff $\vec{b} \in S_\sigma$ and $\vec{c} \in S_\tau$;
- $\vec{\nu} \in S_{\mathtt{V}\sigma}$ iff for all $\vec{h} \in S_\sigma^\perp$, $\left(\int_{x\in[\![\sigma]\!]} h_i(x)d\nu_i\right)_{i\in I} \in \triangleright$;
- $\vec{h} \in S_\sigma^\perp$ iff for all $\vec{a} \in S_\sigma$, $(h_i(a_i))_{i\in I} \in \triangleright$;
- $\vec{Q} \in S_{\mathtt{F}\sigma}$ iff for all $\vec{h} \in S_\sigma^*$, $({h_i}^*(Q_i))_{i\in I} \in \trianglerighteq$;
- $\vec{h} \in S_\sigma^*$ iff for all $\vec{a} \in S_\sigma$, $(h_i(a_i))_{i\in I} \in \trianglerighteq$;
- $\vec{f} \in S_{\sigma\to\underline{\tau}}$ iff for all $\vec{a} \in S_\sigma$, $(f_i(a_i))_{i\in I} \in S_{\underline{\tau}}$.

For every I-indexed tuple $\vec{\rho}$ of environments, finally, $\vec{\rho} \in S_*$ if and only if for every variable x_σ, $(\rho_i(x_\sigma))_{i\in I} \in S_\sigma$.

Lemma 8.1 *1. For every $\vec{\rho} \in S_*$, for every CBPV($\mathtt{D},\mathtt{P}$) term $M : \tau$, $([\![M]\!]\,\rho_i)_{i\in I}$ is in S_τ.*

*2. The same remains true for all CBPV($\mathtt{D},\mathtt{P}$) + **pifz** terms if $\mathcal{J} \subseteq \{\emptyset, I\}$.*

Proof. We first show: (a) $S_{\overline{\sigma}}$ is closed under directed suprema taken in $[\![\overline{\sigma}]\!]^I$, and contains $\vec{\bot} = (\bot)_{i\in I}$. This is by induction on the type $\overline{\sigma}$. Most cases are trivial. We deal with the remaining ones:

- When $\overline{\sigma} = \mathtt{unit}$ or $\overline{\sigma} = \mathtt{int}$, $\vec{\bot}$ is in $S_{\overline{\sigma}}$, because $I \in \mathcal{J}$. We must show that the supremum $\vec{a}$ of every directed family $(\vec{a}_k)_{k\in K}$ in $S_{\overline{\sigma}}$ is in $S_{\overline{\sigma}}$. Let $J_k = \{i \in I \mid a_{ki} = \bot\}$ for each $k \in K$, and $J = \{i \in I \mid a_i = \bot\}$. Define $k \sqsubseteq k'$ if and only if $\vec{a}_k \leq \vec{a}_{k'}$. Then $k \sqsubseteq k'$ implies $J_k \supseteq J_{k'}$, so $(J_k)_{k\in K}$ is a filtered family. Since $\mathcal{J}$ is well-founded, there is an index $k_1 \in K$ such that $J_k = J_{k_1}$ for every $k \sqsupseteq k_1$. Then, for every $i \in I$, $a_i = \sup_{k\sqsupseteq k_1} a_{ki}$ is equal to $\bot$ if $i \in J$, and is different from $\bot$ otherwise. In particular, $J = J_{k_1}$. Letting b_k be the common value of the terms a_{ki}, $i \in I \smallsetminus J_k = I \smallsetminus J$, for each $k \sqsupseteq k_1$, we have $a_i = \sup_{k\sqsupseteq k_1} b_k$ for every $i \in I \smallsetminus J$, and all these values are equal. Therefore $\vec{a}$ is in $S_{\overline{\sigma}}$.
- When $\overline{\sigma} = \mathtt{V}\sigma$, $\vec{\bot}$ is the tuple consisting of zero valuations only, and for every $\vec{h} \in S_\sigma^\perp$, $\left(\int_{x\in[\![\sigma]\!]} h_i(x)d0\right)_{i\in I} = \vec{0}$ is in $\triangleright$ (since $\triangleright$ is $\mathcal{J}$-lower and $I \in \mathcal{J}$), so $\vec{\bot} \in S_{\overline{\sigma}}$. In order to show closure under directed suprema, let $(\vec{\nu}_j)_{j\in J}$ be a directed family in $S_{\overline{\sigma}}$, with $\vec{\nu}_j = (\nu_{ji})_{i\in I}$. Its supremum is $\vec{\nu} = (\nu_i)_{i\in I}$ where $\nu_i = \sup_{j\in J} \nu_{ji}$. For every $\vec{h} \in S_\sigma^\perp$, $\left(\int_{x\in[\![\sigma]\!]} h_i(x)d\nu_i\right)_{i\in I} = \left(\sup_j \int_{x\in[\![\sigma]\!]} h_i(x)d\nu_{ji}\right)_{i\in I}$, since integration is Scott-continuous in the valuation. That is a directed supremum of values in $\triangleright$, hence is in $\triangleright$. It follows that $\vec{\nu}$ is in $S_{\mathtt{V}\sigma}$.

- When $\overline{\sigma} = \mathtt{F}\sigma$, $\vec{\bot}$ is in $S_{\mathtt{F}\sigma}$ because, for every $\vec{h} \in S^*_\sigma$, $({h_i}^*(\bot))_{i\in I}$ is equal to $\vec{0}$ (since ${h_i}^*$ is strict), and that is in $\trianglerighteq$: $\vec{0} = \vec{1}_{|I}$, which is in $\trianglerighteq$ because $\trianglerighteq$ is $\mathcal{J}$-lower and $I \in \mathcal{J}$. As far as closure under directed suprema is concerned, let $(\vec{Q}_j)_{j\in J}$ be a directed family in $S_{\overline{\sigma}}$, where $\vec{Q}_j = (Q_{ji})_{i\in I}$. Let us write its supremum as $\vec{Q} = (Q_i)_{i\in I}$. For every $h \in S^*_\sigma$, $({h_i}^*(Q_i))_{i\in I}$ is the supremum of the family of tuples $({h_i}^*(Q_{ji}))_{i\in I}$, $j \in J$, since ${h_i}^*$ is Scott-continuous (Proposition 4.2, item 2), and all those tuples are in $\trianglerighteq$. Since the latter is closed under directed suprema, $({h_i}^*(Q_i))_{i\in I}$ is in $\trianglerighteq$, so $\vec{Q}$ is in $S_{\mathtt{F}\sigma}$.

Next, we claim that: (b) for every $\vec{\nu} \in S_{\mathtt{V}\sigma}$ and for every $\vec{f} \in S_{\sigma\to\mathtt{V}\tau}$, $(f_i^\dagger(\nu_i))_{i\in I}$ is in $S_{\mathtt{V}\tau}$. To this end, let $\vec{h} \in S^\bot_\tau$. Our goal is to show that $\left(\int_{y\in[\![\tau]\!]} h_i(y) df_i^\dagger(\nu_i)\right)_{i\in I}$ is in $\triangleright$. Using (1), this boils down to showing that $\left(\int_{x\in[\![\sigma]\!]} h'_i(x) d\nu_i\right)_{i\in I}$ is in $\triangleright$, where h'_i is the map $x \mapsto \int_{y\in[\![\tau]\!]} h_i(y) df_i(x)$. We note that $\vec{h}' = (h'_i)_{i\in I}$ is in $S^\bot_\sigma$: for every $\vec{a} \in S_\sigma$, $(f_i(a_i))_{i\in I}$ is in $S_{\mathtt{V}\tau}$ (by definition of $S_{\sigma\to\mathtt{V}\tau}$); by the definition of $S_{\mathtt{V}\tau}$, and using the fact that $\vec{h} \in S^\bot_\tau$, $\left(\int_{y\in[\![\tau]\!]} h_i(y) df_i(a_i)\right)_{i\in I}$ is in $\triangleright$, in other words $(h'_i(a_i))_{i\in I}$ is in $\triangleright$. Since $(\vec{h}'_i)_{i\in I} \in S^\bot_\sigma$ and $\vec{\nu} \in S_{\mathtt{V}\sigma}$, the claim follows.

We also claim that: (c) for every $\vec{Q} \in S_{\mathtt{F}\sigma}$ and for every $\vec{f} \in S_{\sigma\to\mathtt{F}\tau}$, $({f_i}^*(Q_i))_{i\in I}$ is in $S_{\mathtt{F}\tau}$. Let $\vec{h} \in S^*_\tau$. We wish to show that $({h_i}^*({f_i}^*(Q_i)))_{i\in I}$ is in $\trianglerighteq$. Using Proposition 4.2, item 4, this amounts to showing that $(({h_i}^* \circ f_i)^*(Q_i))_{i\in I}$ is in $\trianglerighteq$. We note that $({h_i}^* \circ f_i)_{i\in I}$ is in $S^\bot_\sigma$: for every $\vec{a} \in S_\sigma$, $(f_i(a_i))_{i\in I}$ is in $S_{\mathtt{F}\tau}$, and $\vec{h}$ is in S^*_τ, so $({h_i}^*(f_i(a_i)))_{i\in I}$ is in $\trianglerighteq$. Since $\vec{Q} \in S_{\mathtt{F}\sigma}$, and using the definition of $S_{\mathtt{F}\sigma}$, $(({h_i}^* \circ f_i)^*(Q_i))_{i\in I}$ is in $\trianglerighteq$.

Finally, for every vector $\vec{a}$ in $[\![\overline{\sigma}]\!]^I$, and for every subset J of I, we define $\vec{a}_{|J}$ as the vector obtained from $\vec{a}$ by replacing each component a_i with $i \in J$ by $\bot$. We claim that: (d) for every $\vec{a} \in S_{\overline{\sigma}}$, for every $J \in \mathcal{J}$, $\vec{a}_{|J}$ is in $S_{\overline{\sigma}}$. This is by induction on $\overline{\sigma}$. For types $\overline{\sigma}$ of the form $\sigma \times \tau$, $\mathtt{U}\underline{\tau}$, and $\sigma \to \underline{\tau}$, we simply call the induction hypothesis. When $\overline{\sigma}$ is **unit** or **int**, let $J' = \{i \in I \mid a_i = \bot\}$, and $J'' = \{i \in I \mid a_{|J\,i} = \bot\}$. We have $J'' = J' \cup J$, and $J' \in \mathcal{J}$ by induction hypothesis. Since $\mathcal{J}$ is closed under binary unions, J'' is in $\mathcal{J}$. Moreover, all the components $a_{|J\,i}$ with $i \in I \smallsetminus J''$ are equal to a_i, and they are all equal. Therefore $\vec{a}_{|J}$ is in $S_{\overline{\sigma}}$. When $\overline{\sigma} = \mathtt{V}\sigma$, let $\vec{\nu} \in S_{\mathtt{V}\sigma}$. For every $\vec{h} \in S^\bot_\sigma$, $\vec{b} = \left(\int_{x\in[\![\sigma]\!]} h_i(x) d\nu_i\right)_{i\in I}$ is in $\triangleright$. The vector $\left(\int_{x\in[\![\sigma]\!]} h_i(x) d\nu_{|J\,i}\right)_{i\in I}$ is equal to $\vec{b}_{|J}$, hence is in $\triangleright$ as well, since $\triangleright$ is $\mathcal{J}$-lower. When $\overline{\sigma} = \mathtt{F}\sigma$, let $\vec{Q} \in S_{\mathtt{F}\sigma}$. For every $\vec{h} \in S^*_\sigma$, $({h_i}^*(Q_i))_{i\in I}$ is in $\trianglerighteq$. Since each function ${h_i}^*$ is strict, for every $i \in J$, ${h_i}^*(Q_{|J\,i}) = \bot$. For every $i \in I \smallsetminus J$, ${h_i}^*(Q_{|J\,i}) = {h_i}^*(Q_i)$. Therefore $({h_i}^*(Q_{|J\,i}))_{i\in I}$ is equal to $\vec{a}_{|J}$ where $\vec{a} = ({h_i}^*(Q_i))_{i\in I}$, and that is in $\trianglerighteq$ by assumption and the fact that $\trianglerighteq$ is $\mathcal{J}$-lower. Hence $\vec{Q}_{|J}$ is in $S_{\mathtt{F}\sigma}$.

1. We now prove the lemma by induction on M. For variables, this follows from the assumption that $\vec{\rho} \in S_*$. The case of constants $\underline{*}$ and $\underline{n}$ is clear. The case of λ-abstractions and of applications is immediate from the definition of $S_{\sigma\to\underline{\tau}}$. Similarly, the case of terms $\pi_1 M$, $\pi_2 M$ and $\langle M, N\rangle$ are immediate from

the definition of $S_{\sigma\times\tau}$. For terms of the form $\mathtt{thunk}\, M$, with $M\colon \underline{\tau}$, or terms of the form $\mathtt{force}\, M$, with $M\colon \mathtt{U}\underline{\tau}$, the claim is trivial.

For terms of the form $\mathtt{produce}\, M$, with $M\colon \sigma$, by induction hypothesis $(\llbracket M\rrbracket\,\rho_i)_{i\in I}$ is in S_σ. In order to show that $(\llbracket \mathtt{produce}\, M\rrbracket\,\rho_i)_{i\in I} = (\eta^{\mathcal{Q}}(\llbracket M\rrbracket\,\rho_i))_{i\in I}$ is in $S_{\mathtt{F}\sigma}$, we fix $\vec{h} \in S^*_\sigma$, and we check that $({h_i}^*(\eta^{\mathcal{Q}}(\llbracket M\rrbracket\,\rho_i)))_{i\in I}$ is in $\trianglerighteq$. Since ${h_i}^*(\eta^{\mathcal{Q}}(\llbracket M\rrbracket\,\rho_i)) = h_i(\llbracket M\rrbracket\,\rho_i)$ (Proposition 4.2, item 2), this follows from the definition of S^*_σ.

For terms of the form $M\;\mathtt{to}\;x_\sigma\;\mathtt{in}\;N$, with $M\colon \mathtt{F}\sigma$ and $N\colon \mathtt{F}\tau$, we must show that $(\llbracket M\;\mathtt{to}\;x_\sigma\;\mathtt{in}\;N\rrbracket\,\rho_i)_{i\in I}$ is in $\llbracket \mathtt{F}\tau\rrbracket$. Since $\llbracket M\;\mathtt{to}\;x_\sigma\;\mathtt{in}\;N\rrbracket\,\rho_i = {f_i}^*(\llbracket M\rrbracket\,\rho_i)$, where $f_i(V) = \llbracket N\rrbracket\,\rho_i[x_\sigma \mapsto V]$, we will obtain this as a consequence of (c) if we can show that $(f_i)_{i\in I}$ is in $S_{\sigma\to\mathtt{F}\tau}$. For every $\vec{a} \in S_\sigma$, $(\rho_i[x_\sigma\mapsto a_i])_{i\in I}$ is in S_*, so $(f_i(a_i))_{i\in I} = (\llbracket N\rrbracket\,\rho_i[x_\sigma\mapsto a_i])_{i\in I}$ is indeed in $S_{\sigma\to\mathtt{F}\tau}$.

For terms of the form $\mathtt{ret}\, M$, where $M\colon \tau$, we must show that for every $\vec{h} \in S^\perp_\tau$, $\left(\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket \mathtt{ret}\, M\rrbracket\,\rho_i\right)_{i\in I}$ is in $\triangleright$. Since $\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket \mathtt{ret}\, M\rrbracket\,\rho_i = \int_{x\in\llbracket\tau\rrbracket} h_i(x) d\delta_{\llbracket M\rrbracket\rho_i} = h_i(\llbracket M\rrbracket\,\rho_i)$, this follows from the fact that $\vec{h} \in S^\perp_\tau$ and the definition of $S^\perp_\tau$.

For terms of the form $\mathtt{do}\, x_\sigma \leftarrow M; N$, with $M\colon \mathtt{V}\sigma$ and $N\colon \mathtt{V}\tau$, we wish to show that $(\llbracket \mathtt{do}\, x_\sigma \leftarrow M; N\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{V}\tau}$, namely that $(f_i^\dagger(\llbracket N\rrbracket\,\rho_i))_{i\in I}$ is in $S_{\mathtt{V}\tau}$, where $f_i(V) = \llbracket N\rrbracket\,\rho_i[x_\sigma\mapsto V]$. As in the case of $\mathtt{to}$ terms, $(f_i)_{i\in I}$ is in $S_{\sigma\to\mathtt{V}\tau}$, and $(\llbracket N\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{V}\sigma}$, so the claim is proved by applying (b).

For terms of the form $\mathtt{succ}\, M$, with $M\colon \mathtt{int}$, by induction hypothesis $(\llbracket M\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{int}}$. Let $J = \{i\in I \mid \llbracket M\rrbracket\,\rho_i = \bot\}$, and $n\in\mathbb{Z}$ be the common value of $\llbracket M\rrbracket\,\rho_i$, $i\in I\smallsetminus J$ (or an arbitrary element of $\mathbb{Z}$ if $I = J$). Then J is also equal to $\{i\in I \mid \llbracket \mathtt{succ}\, M\rrbracket\,\rho_i = \bot\}$, which is therefore in $\mathcal{J}$. Moreover, $n+1$ is the common value of $\llbracket \mathtt{succ}\, M\rrbracket\,\rho_i$, $i\in I\smallsetminus J$. We reason similarly for terms of the form $\mathtt{pred}\, M$.

For terms of the form $\mathtt{ifz}\;M\;N\;P$, where $M\colon \mathtt{int}$ and $N, P\colon \overline{\sigma}$, by hypothesis, in particular, $(\llbracket M\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{int}}$. Let $J = \{i\in I \mid \llbracket M\rrbracket\,\rho_i = \bot\}$, and n be the common value of $\llbracket M\rrbracket\,\rho_i$, $i\in I\smallsetminus J$ (or any element of $\mathbb{Z}$ if $J = I$). $(\llbracket \mathtt{ifz}\;M\;N\;P\rrbracket\,\rho_i)_{i\in I}$ is equal to $\vec{a}_{|J}$, where $\vec{a} = (\llbracket N\rrbracket\,\rho_i)_{i\in I}$ if $n = 0$ and $\vec{a} = (\llbracket P\rrbracket\,\rho_i)_{i\in I}$ if $n\neq 0$. The latter is in $S_{\overline{\sigma}}$ by induction hypothesis, so the former is in $S_{\overline{\sigma}}$, too, by (d).

For terms of the form $M; N$, with $M\colon \mathtt{unit}$ and $N\colon \overline{\sigma}$, $(\llbracket M\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{unit}}$ by induction hypothesis. Let $J = \{i\in I \mid \llbracket M\rrbracket\,\rho_i = \bot\}$. $(\llbracket M; N\rrbracket)_{i\in I}$ is equal to $\vec{a}_{|J}$ where $\vec{a} = (\llbracket N\rrbracket\,\rho_i)_{i\in I}$, which is in $S_{\overline{\sigma}}$ by induction hypothesis and (d).

For terms of the form $M\oplus N$, with $M, N\colon \mathtt{V}\tau$, we wish to show that the tuple $(\llbracket M\oplus N\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{V}\tau}$. Let $\vec{h} \in S^\perp_\tau$. By induction hypothesis, the tuples $\left(\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket M\rrbracket\,\rho_i\right)_{i\in I}$ and $\left(\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket N\rrbracket\,\rho_i\right)_{i\in I}$ are in $\triangleright$. Since $\triangleright$ is convex, $\left(\frac{1}{2}\left(\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket M\rrbracket\,\rho_i + \int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket N\rrbracket\,\rho_i\right)\right)_{i\in I}$ is also in $\triangleright$, and that is just $\left(\int_{x\in\llbracket\tau\rrbracket} h_i(x) d\,\llbracket M\oplus N\rrbracket\,\rho_i\right)_{i\in I}$.

For terms of the form $M \owedge N$, with $M, N\colon \mathtt{F}\tau$, we wish to show that the tuple $(\llbracket M \owedge N\rrbracket\,\rho_i)_{i\in I}$ is in $S_{\mathtt{F}\tau}$. Let $\vec{h} \in S^*_\tau$. By induction hypothesis, $({h_i}^*(\llbracket M\rrbracket\,\rho_i))_{i\in I}$ and $({h_i}^*(\llbracket N\rrbracket\,\rho_i))_{i\in I}$ are in $\trianglerighteq$. Since $\trianglerighteq$ is closed under pairwise minima, and ${h_i}^*$ commutes with pairwise infima (Proposition 4.2, item 3), $({h_i}^*(\llbracket M \owedge N\rrbracket\,\rho_i))_{i\in I}$

is also in $\trianglerighteq$, showing the claim.

For $\mathbf{abort}_{\mathtt{F}\tau}$, we consider an arbitrary vector $\vec{h} \in S^*_\tau$, and we must show that $({h_i}^*(\emptyset))_{i\in I}$ is in $\trianglerighteq$. By Proposition 4.2, item 3, ${h_i}^*(\emptyset)$ is the top element, $\vec{1}$, of $[0,1]$, and the claim follows from the fact that $\vec{1} \in \trianglerighteq$.

For terms of the form $\mathbf{rec}\, x_\sigma.M$, let f_i be the map defined by $f_i(V) = [\![M]\!]\,\rho_i[x_\sigma \mapsto V]$. For every $\vec{a} \in S_\sigma$, $(\rho_i[x_\sigma \mapsto a_i])_{i\in I}$ is in S_*, hence by induction hypothesis $(f_i(a_i))_{i\in I}$ is in S_σ. Let us write $(f_i(a_i))_{i\in I}$ as $\vec{f}(\vec{a})$. By (a), $\vec{\bot} = (\bot)_{i\in I}$ is in S_σ, and therefore $\vec{f}(\vec{\bot})$, $\vec{f}(\vec{f}(\vec{\bot}))$, …, are all in S_σ. By the other part of (a), $\sup_{n\in\mathbb{N}} (\vec{f})^n(\vec{a})$ in in S_σ as well. That tuple is just $(\mathrm{lfp}(f_i))_{i\in I}$, namely $([\![\mathbf{rec}\, x_\sigma.M]\!]\,\rho_i)_{i\in I}$.

2. In the case of terms of the form $\mathbf{pifz}\ M\ N\ P$, of type $\overline{\sigma}$, and assuming $\mathcal{J} \subseteq \{\emptyset, I\}$, the induction hypothesis $([\![M]\!]\,\rho_i)_{i\in I} \in S_{\mathtt{int}}$ implies that all the values $[\![M]\!]\,\rho_i$ are the same: letting $J = \{i \in I \mid [\![M]\!]\,\rho_i = \bot\}$, either $J = I$ and they are all equal to $\bot$, or $J = \emptyset$ and they are all equal by definition of $S_{\mathtt{int}}$. Hence $([\![\mathbf{pifz}\, M\ N\ P]\!]\,\rho_i)_{i\in I}$ is equal to $([\![N]\!]\,\rho_i)_{i\in I}$, to $([\![P]\!]\,\rho_i)_{i\in I}$, or to $([\![M \owedge N]\!]\,\rho_i)_{i\in I}$, and they are all in $S_{\overline{\sigma}}$. ☐

8.1 The Need for Parallel If

In this section, we let $I = \{1,2,3\}$, $\mathcal{J} = \{\emptyset, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, $\triangleright$ be arbitrary (e.g., the whole of $[0,1]^3$), and $\trianglerighteq = \{(0,0,0), (0,1,0), (1,0,0), (1,1,1)\}$. The latter is the smallest possible set that satisfies the constraints required of $\trianglerighteq$, and is the graph of the infimum function $\wedge\colon \{0,1\}^2 \to \{0,1\}$.

A triple (n_1, n_2, n_3) in $\mathbb{Z}^3_\bot$ is in $S_{\mathtt{int}}$ if and only if $\{i \mid n_i = \bot\}$ is empty, equal to $\{1,3\}$ or $\{2,3\}$, or to $\{1,2,3\}$, and all the non-bottom components are equal. Those are the triples (n,n,n), $(\bot, n, \bot)$, $(n, \bot, \bot)$ and $(\bot,\bot,\bot)$ (with $n \neq \bot$).

Lemma 8.2 *The triples (h_1, h_2, h_3) in $S^*_{\mathtt{int}}$ are the triples of characteristic maps $(\chi_{U_1}, \chi_{U_2}, \chi_{U_3})$ of open subsets U_1, U_2, U_3 of $\mathbb{Z}_\bot$ of one of the following forms:*

1. *$U_1 = U_2 = U_3 = \mathbb{Z}_\bot$;*
2. *$U_1 = U_2 = U_3 = \{n\}$ for some $n \in \mathbb{Z}$;*
3. *$U_1 = U_3 = \emptyset$, U_2 arbitrary;*
4. *$U_2 = U_3 = \emptyset$, U_1 arbitrary.*

Proof. A triple of Scott-continuous maps (h_1, h_2, h_3) is in $S^*_{\mathtt{int}}$ if and only if for all $(n_1, n_2, n_3) \in S_{\mathtt{int}}$, $(h_1(n_1), h_2(n_2), h_3(n_3)) \in \trianglerighteq$. We claim that this is equivalent to: $(*)$ h_1, h_2, h_3 take their values in $\{0,1\}$ and for all $n_1, n_2, n_3 \in \mathbb{Z}_\bot$ such that $n_3 = n_1 \wedge n_2$, $h_3(n_3) = h_2(n_1) \wedge h_2(n_2)$. In one direction, if $(h_1, h_2, h_3) \in S^*_{\mathtt{int}}$, then since $(n,n,n) \in S_{\mathtt{int}}$ for every $n \in \mathbb{Z}$, $(h_1(n), h_2(n), h_3(n))$ is in $\trianglerighteq$ for every $n \in \mathbb{Z}$, in particular h_1, h_2, h_3 take their values in $\{0,1\}$. Also, for all $n_1, n_2, n_3 \in \mathbb{Z}_\perp$ such that $n_3 = n_1 \wedge n_2$, $h_3(n_3) = h_2(n_1) \wedge h_2(n_2)$. Indeed, the triples (n_1, n_2, n_3) such that $n_3 = n_1 \wedge n_2$ are of the form (n, n, n), or $(\perp, n, \perp)$, or $(n, \perp, \perp)$, or $(\perp, \perp, \perp)$, with $n \in \mathbb{Z}$, hence are exactly the triples in $S_{\mathtt{int}}$. Then $(h_1(n_1), h_2(n_2), h_3(n_3))$ is in $\trianglerighteq$, hence $h_3(n_3) = h_2(n_1) \wedge h_2(n_2)$ since $\trianglerighteq$ is the graph of $\wedge$ on $\{0, 1\}$. In the other direction, let us assume $(*)$. For all $(n_1, n_2, n_3) \in S_{\mathtt{int}}$, we have just seen that $n_3 = n_1 \wedge n_2$, so $(h_1(n_1), h_2(n_2), h_3(n_3))$ is in the graph of $\wedge$ on $\{0, 1\}$. It follows that (h_1, h_2, h_3) is in $S^*_{\mathtt{int}}$.

Equivalently, $(*)$ means that h_1, h_2, h_3 are the characteristic maps χ_{U_1}, χ_{U_2}, χ_{U_3} of open subsets U_1, U_2, U_3 of $\mathbb{Z}_\perp$ such that: $(**)$ for all $n_1, n_2, n_3 \in \mathbb{Z}_\perp$ such that $n_3 = n_1 \wedge n_2$, $n_3 \in U_3$ if and only if $n_1 \in U_1$ and $n_2 \in U_2$. Clearly, any of the cases 1–4 implies $(**)$.

Let us assume that $(**)$ holds. By taking $n_1 = n_2 = n_3$, we obtain that $U_3 = U_1 \cap U_2$. If U_1 is empty, then U_3 is empty and we are in case 3. If U_2 is empty, then U_3 is empty and we are in case 4. Henceforth, let us assume that U_1 and U_2 are non-empty. If $\perp \in U_1$, then pick any $n_2 \in U_2$: we can then take $n_3 = \perp$, so $\perp$ is in U_3 by $(**)$; this implies that $U_3 = \mathbb{Z}_\perp$, hence also $U_1 = U_2 = \mathbb{Z}_\perp$, since $U_3 = U_1 \cap U_2$; hence we are in case 1. We reason similarly if $\perp$ is in U_2. It remains to examine the cases where U_1 and U_2 are non-empty subsets of $\mathbb{Z}$. If there are two distinct elements $n_1 \in U_1$ and $n_2 \in U_2$, then $n_3 = n_1 \wedge n_2$ is equal to $\perp$ and must be in U_3 by $(**)$, so $U_3 = \mathbb{Z}_\perp$, and again $U_1 = U_2 = \mathbb{Z}_\perp$, meaning that we are in case 1. Otherwise, $U_1 = U_2 = \{n\}$ for some $n \in \mathbb{Z}$, then $U_3 = \{n\}$ as well, and we are in case 2. $\Box$

Lemma 8.3 *For every ground CBPV*(D, P) *term* $P \colon \mathtt{int} \to \mathtt{int} \to \mathtt{Fint}$ *such that* $[\![P]\!](\perp)(0) = [\![P]\!](0)(\perp) = \{0\}$, *the equality* $[\![P]\!](\perp)(\perp) = \{0\}$ *holds.*

Proof. Let $Q \in [\![\mathtt{Fint}]\!]$ be such that $(\{0\}, \{0\}, Q)$ is in $S_{\mathtt{Fint}}$. Consider any triple $(\chi_{U_1}, \chi_{U_2}, \chi_{U_3}) \in S^*_{\mathtt{int}}$, as given in Lemma 8.2. By definition, and recalling that $\trianglerighteq$ is the graph of the infimum map, ${\chi_{U_3}}^*(Q) = {\chi_{U_1}}^*(\{0\}) \wedge {\chi_{U_2}}^*(\{0\}) = \chi_{U_1}(0) \wedge \chi_{U_2}(0)$. If Q were empty, then ${\chi_{U_3}}^*(Q)$ would be equal to 1, so $\chi_{U_1}(0)$ and $\chi_{U_2}(0)$ would be equal to 1, and that is contradicted by the case 1 triple $U_1 = U_2 = U_3 = \mathbb{Z}_\perp$ for example. By considering the case 2 triple $U_1 = U_2 = U_3 = \{0\}$, we obtain that ${\chi_{\{0\}}}^*(Q) = 1$, namely that $Q \subseteq \{0\}$. Therefore the only $Q \in [\![\mathtt{Fint}]\!]$ such that $(\{0\}, \{0\}, Q) \in S_{\mathtt{Fint}}$ is $\{0\}$. (One can also check that $(\{0\}, \{0\}, \{0\})$ is indeed in $S_{\mathtt{Fint}}$, but that will not be needed.)

By Lemma 8.1, item 1, for all $(m_1, m_2, m_3) \in S_{\mathtt{int}}$ and $(n_1, n_2, n_3) \in S_{\mathtt{int}}$, the triple $([\![P]\!](m_1)(n_1), [\![P]\!](m_2)(n_2), [\![P]\!](m_3)(n_3))$ is in $S_{\mathtt{Fint}}$. The triples $(0, \perp, \perp)$ and $(\perp, 0, \perp)$ are in $S_{\mathtt{int}}$. Hence $([\![P]\!](0)(\perp), [\![P]\!](\perp)(0), [\![P]\!](\perp)(\perp))$ is in $S_{\mathtt{Fint}}$. Explicitly, $(\{0\}, \{0\}, [\![P]\!](\perp)(\perp))$ is in $S_{\mathtt{Fint}}$. We have just seen that this implies $[\![P]\!](\perp)(\perp) = \{0\}$. $\Box$

We introduce the following abbreviations.

- Ω_σ denotes $\mathbf{rec}\, x_\sigma . x_\sigma$ for every value type σ. We have $[\![\Omega_\sigma]\!] = \perp$.
- $\Omega_{\underline{\tau}}$ denotes $\mathbf{force}\, \Omega_{\mathbf{U}\underline{\tau}}$, for every computation type $\underline{\tau}$. We have $[\![\Omega_{\underline{\tau}}]\!] = \perp$.

- For all $M\colon \mathbf{Fint}$ and $N\colon \mathbf{Funit}$, $M == \underline{0} \mathbin{\&} N$ abbreviates M **to** $x_{\mathtt{int}}$ **in ifz** $x_{\mathtt{int}}\ N\ \Omega_{\mathtt{Funit}}$, where $x_{\mathtt{int}}$ is not free in N. $[\![M == \underline{0} \mathbin{\&} N]\!]\,\rho$ is equal to $[\![N]\!]\,\rho$ if $[\![M]\!]\,\rho = \{0\}$, to $\emptyset$ if $[\![M]\!]\,\rho = \emptyset$, and to $\bot$ in all other cases.

- Similarly, $M == \underline{1} \mathbin{\&} N$ abbreviates M **to** $x_{\mathtt{int}}$ **in ifz** (**pred** $x_{\mathtt{int}}$) $N\ \Omega_{\mathtt{Funit}}$, so that $[\![M == \underline{1} \mathbin{\&} N]\!]\,\rho$ is equal to $[\![N]\!]\,\rho$ if $[\![M]\!]\,\rho = \{1\}$, to $\emptyset$ if $[\![M]\!]\,\rho = \emptyset$, and to $\bot$ in all other cases.

- Finally, for all $M, N\colon \mathbf{Funit}$, let $M \mathbin{\&} N$ abbreviate M **to** $x_{\mathtt{int}}$ **in** N, where $x_{\mathtt{int}}$ is not free in N, so that $[\![M \mathbin{\&} N]\!]\,\rho$ is equal to $[\![N]\!]\,\rho$ if $[\![M]\!]\,\rho = \{\top\}$ or if $[\![M]\!]\,\rho = \mathbb{S}$, to $\emptyset$ if $[\![M]\!]\,\rho = \emptyset$ and to $\bot$ if $[\![M]\!]\,\rho = \bot$.

We let & associate to the right, so $A \mathbin{\&} B \mathbin{\&} C$ means $A \mathbin{\&} (B \mathbin{\&} C)$.

Proposition 8.4 *For every term $P\colon \mathtt{U}(\mathtt{int} \to \mathtt{int} \to \mathtt{Fint})$, let:*

$$M(P) = \mathbf{force}\,P(\Omega_{\mathtt{int}})(\underline{0}) == \underline{0} \mathbin{\&} \mathbf{force}\,P(\underline{0})(\Omega_{\mathtt{int}}) == \underline{0} \mathbin{\&} \mathbf{produce}\,\underline{*}$$
$$N(P) = M(P) \mathbin{\&} \mathbf{force}\,P(\Omega_{\mathtt{int}})(\Omega_{\mathtt{int}}) == \underline{0} \mathbin{\&} \mathbf{produce}\,\underline{*},$$

We also define M as $\lambda g.M(g)$, and N as $\lambda g.N(g)$, where g has type $\mathtt{U}(\mathtt{int} \to \mathtt{int} \to \mathtt{Fint})$.

In CBPV(D, P), $M \precsim_{\mathtt{U}(\mathtt{int}\to\mathtt{int}\to\mathtt{Fint})\to\mathtt{Funit}} N$, but $[\![M]\!] \not\leq [\![N]\!]$.

Proof. $[\![M]\!]$ applied to any Scott-continuous map $G\colon \mathbb{Z}_\bot \to \mathbb{Z}_\bot \to \mathcal{Q}^\top_\bot(\mathbb{Z}_\bot)$ returns:

- $\{\top\}$ if $G(\bot)(0) = G(0)(\bot) = \{0\}$;
- $\emptyset$ if $G(\bot)(0) = \emptyset$ or if $G(\bot)(0) = \{0\}$ and $G(0)(\bot) = \emptyset$;
- and $\bot$ in all other cases.

Then $[\![N]\!]$ applied to G returns:

- $\{\top\}$ if $[\![M]\!]\,(G) = \{\top\}$ and $G(\bot)(\bot) = \{0\}$;
- $\emptyset$ if $[\![M]\!]\,(G) = \{\top\}$ and $G(\bot)(\bot) = \emptyset$;
- $\emptyset$ if $[\![M]\!]\,(G) = \emptyset$;
- $\bot$ in all other cases.

In particular, $[\![M]\!] \not\leq [\![N]\!]$: defining G to be the parallel or map ($G(0)(n) = G(n)(0) = \{0\}$ for every $n \in \mathbb{Z}_\bot$, $G(1)(1) = \{1\}$, $G(m)(n) = \bot$ for all $m, n \in \mathbb{Z}_\bot \smallsetminus \{0\}$ such that $(m, n) \neq (1, 1)$), $[\![M]\!]\,(G) = \{\top\}$, but $[\![N]\!]\,(G) = \bot$. Note, by the way, that the argument would also work with other choices of map G, for example $G(0)(n) = G(n)(0) = \{0\}$ for every $n \in \mathbb{Z}_\bot$, and $G(m)(n) = \bot$ in all other cases.

For every ground CBPV(D, P) term $P\colon \mathtt{int} \to \mathtt{int} \to \mathtt{Fint}$, $[\![M(P)]\!] = \{\top\}$ if and only if $[\![P]\!]\,(\bot)(0) = [\![P]\!]\,(0)(\bot) = \{0\}$, and if so, $[\![P]\!]\,(\bot)(\bot) =$

$\{0\}$ by Lemma 8.3. Taking $G = [\![P]\!]$, it follows that the second case of the definition of $[\![N]\!]\,(G)$ does not occur, so $[\![N(P)]\!] = [\![N]\!]\,(G)$ is equal to $\{\top\}$ if $[\![M(P)]\!] = \{\top\}$ (and then $G(\bot)(\bot) = \{0\}$ is automatic), to $\emptyset$ if $[\![M(P)]\!] = \emptyset$, and to $\bot$ in all other cases. Hence $[\![N(P)]\!] = [\![M(P)]\!]$. Since in particular $[\![M(P)]\!] \leq [\![N(P)]\!]$, by Proposition 7.6, $M(P) \precsim_{\texttt{Funit}} N(P)$. Since P is arbitrary, $M \precsim_{\texttt{U(int}\to\texttt{int}\to\texttt{Fint)}\to\texttt{Funit}} N$ by Proposition 7.5. $\square$

8.2 The Need for Statistical Termination Testers

We turn to justify the need for a $\bigcirc$ operator, following similar ideas as in [11, Proposition 8.5].

Here we let $I = \{1, 2\}$, $\mathcal{J} = \{\emptyset, I\}$, $\rhd = \{(a_1, a_2) \in [0,1]^2 \mid a_1 + 1 \geq 2a_2\}$, and $\unrhd = \{(a_1, a_2) \in [0,1]^2 \mid a_1 \geq a_2\}$.

In that case, $(h_1, h_2) \in S^{\bot}_{\texttt{unit}}$ if and only if for every $b \in \mathbb{S}$, $h_1(b) + 1 \geq 2h_2(b)$. Letting $\alpha_i = h_i(\bot)$ and $\beta_i = h_i(\top)$, $i \in \{1, 2\}$, $(h_1, h_2) \in S^{\bot}_{\texttt{unit}}$ if and only if:

$$\alpha_1 + 1 \geq 2\alpha_2 \tag{2}$$
$$\beta_1 + 1 \geq 2\beta_2 \tag{3}$$
$$1 \geq \beta_1 \geq \alpha_1 \geq 0 \tag{4}$$
$$1 \geq \beta_2 \geq \alpha_2 \geq 0. \tag{5}$$

This defines a (bounded) polytope of $\mathbb{R}^4$, and we claim that its vertices are:

α_1	β_1	α_2	β_2
0	0	0	0
0	0	0	1/2
0	0	1/2	1/2
0	1	0	0
0	1	0	1
0	1	1/2	1/2
0	1	1/2	1
1	1	0	0
1	1	0	1
1	1	1	1

(6)

We check that those points satisfy all the given inequalities. Conversely, let $(\alpha_1, \beta_1, \alpha_2, \beta_2)$ satisfy (2)–(5). Because it satisfies (4), (α_1, β_1) is a linear convex combination $a(0,0) + b(0,1) + c(1,1)$, where $a, b, c \geq 0$ and $a + b + c = 1$, and the remaining inequalities become $c + 1 \geq 2\alpha_2$, $b + c + 1 \geq 2\beta_2$, $1 \geq \beta_2 \geq \alpha_2 \geq 0$, whose solutions in (α_2, β_2) are the convex combinations of $(0, 0)$, $(0, (b+c+1)/2)$, $((c+1)/2, (c+1)/2)$, and $((c+1)/2, (b+c+1)/2)$ (as a two-dimensional picture will show), say $a'(0, 0) + b'(0, (b + c + 1)/2) + c'((c + 1)/2, (c + 1)/2) + d'((c + 1)/2, (b + c + 1)/2)$, with $a', b', c', d' \geq 0$ and $a' + b' + c' + d' = 1$. Since the latter is affine in a, b and c, it follows that the solutions of (2)–(5) are all of the form a times $(0, 0).(a'(0, 0) + b'(0, 1/2) + c'(1/2, 1/2) + d'(1/2, 1/2))$, plus b times $(0, 1).(a'(0, 0) + b'(0, 1) + c'(1/2, 1/2) + d'(1/2, 1))$, plus c times

$(1,1).(a'(0,0)+b'(0,1)+c'(1,1)+d'(1,1))$ (where . denotes concatenation of tuples, i.e., $(x,y).(z,t)=(x,y,z,t)$), hence a a convex combination of the 10 tuples of the above table.

Lemma 8.5 *For all $a_1, a_2 \in [0,1]$, $(a_1\delta_\top, a_2\delta_\top) \in S_{\texttt{Vunit}}$ if and only if $a_1 + 1 \geq 2a_2$.*

Proof. We have $(a_1\delta_\top, a_2\delta_\top)\ S_{\texttt{Vunit}}$ if and only if for all $(h_1,h_2) \in S^\perp_{\texttt{unit}}$, $a_1h_1(\top)+1 \geq 2a_2h_2(\top)$. Writing h_1 and h_2 as above, the domain of variation of $(\alpha_1,\beta_1,\alpha_2,\beta_2)$ is the convex hull of the 10 points in (6), and we must check that $a_1\beta_1+1 \geq 2a_2\beta_2$ for all those 4-tuples. The domain of variation of the pairs (β_1,β_2) alone is the convex hull of $(0,0)$, $(0,1/2)$, $(1,0)$, $(1,1)$ (and $(1,1/2)$, which is already a convex combination of the others). By linearity, it is equivalent to check $a_1\beta_1+1 \geq 2a_2\beta_2$ for just those four values of (β_1,β_2). Therefore $(a_1\delta_\top, a_2\delta_\top)\ S_{\texttt{Vunit}}$ if and only if $1 \geq 0$, $1 \geq a_2$, $a_1+1 \geq 0$, and $a_1+1 \geq 2a_2$. Since the first three are always true, only the last one remains. ☐

Lemma 8.6 *Let $\nu_1,\nu_2 \in [\![\texttt{Vunit}]\!]$. If $(\nu_1,\nu_2) \in S_{\texttt{Vunit}}$ then $\nu_1 + \delta_\top \geq 2\nu_2$.*

Proof. For every $(h_1,h_2) \in S^\perp_{\texttt{unit}}$, $\int_{x\in\mathbb{S}} h_1(x)d\nu_1 + 1 \geq \int_{x\in\mathbb{S}} h_2(x)d\nu_2$. Considering the case where $h_1\colon \bot \mapsto \alpha_1, \top \mapsto \beta_1$ and $h_2\colon \bot \mapsto \alpha_2, \top \mapsto \beta_2$ are given by the data of the 5th row of (6), we obtain $\nu_1(\{\top\})+1 \geq 2\nu_2(\{\top\})$. Considering the last row instead, we obtain $\nu_1(\{\bot,\top\})+1 \geq 2\nu_2(\{\bot,\top\})$. The inequality $\nu_1(\emptyset)+\delta_\top(\emptyset) \geq 2\nu_2(\emptyset)$ is obvious. ☐

Lemma 8.7 *Let k be any Scott-continuous map from $\mathbf{V}_{\leq 1}\mathbb{S}$ to $[0,1]$. Then $(k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top), k) \in S^*_{\texttt{Vunit}}$.*

Proof. It suffices to verify that for all $(\nu_1,\nu_2) \in S_{\texttt{Vunit}}$, $(k(\frac{1}{2}\nu_1 + \frac{1}{2}\delta_\top), k(\nu_2))$ is in $\trianglerighteq$, namely that $k(\frac{1}{2}\nu_1 + \frac{1}{2}\delta_\top) \geq k(\nu_2)$. By Lemma 8.6, $\frac{1}{2}\nu_1 + \frac{1}{2}\delta_\top \geq \nu_2$, and we conclude since k, being Scott-continuous, is monotonic. ☐

Proposition 8.8 *Let:*

$$M = \lambda g.\,\mathbf{force}\,g(\Omega_{\texttt{Vunit}} \oplus \mathbf{ret}\,\underline{*}),$$
$$N = \lambda g.(\mathbf{force}\,g(\Omega_{\texttt{Vunit}}))\ \mathbf{to}\ y_{\texttt{Vunit}}\ \mathbf{in}\ \mathbf{produce}(y_{\texttt{Vunit}} \oplus \mathbf{ret}\,\underline{*}).$$

where g has type $\mathbf{U}(\mathbf{Vunit} \to \mathbf{FVunit})$.

*In CBPV$(\texttt{D},\texttt{P})$ and also in CBPV$(\texttt{D},\texttt{P})$+**pifz**, $M \precsim_{\mathbf{U}(\mathbf{Vunit}\to\mathbf{FVunit})\to\mathbf{FVunit}} N$, but $[\![M]\!] \not\leq [\![N]\!]$.*

Proof. Let P be any ground CBPV$(\texttt{D},\texttt{P})$ or CBPV$(\texttt{D},\texttt{P})$ + **pifz** term of type $\mathbf{U}(\mathbf{Vunit} \to \mathbf{FVunit})$, and:

$$M(P) = \mathbf{force}\,P(\Omega_{\texttt{Vunit}} \oplus \mathbf{ret}\,\underline{*})$$
$$N(P) = (\mathbf{force}\,P(\Omega_{\texttt{Vunit}}))\ \mathbf{to}\ y_{\texttt{Vunit}}\ \mathbf{in}\ \mathbf{produce}(y_{\texttt{Vunit}} \oplus \mathbf{ret}\,\underline{*}).$$

We have:

$$\llbracket M(P) \rrbracket = \llbracket P \rrbracket \left(\frac{1}{2}\delta_\top\right)$$
$$\llbracket N(P) \rrbracket = g^*(\llbracket P \rrbracket (0)),$$

where $g(\nu) = \uparrow(\frac{1}{2}\nu + \frac{1}{2}\delta_\top)$. By Lemma 8.5, $(0, \frac{1}{2}\delta_\top)$ is in $S_{\texttt{Vunit}}$. By Lemma 8.1 (item 2), $(\llbracket P \rrbracket, \llbracket P \rrbracket)$ is in $S_{\texttt{Vunit}\to\texttt{FVunit}}$, so $(\llbracket P \rrbracket (0), \llbracket P \rrbracket (\frac{1}{2}\delta_\top))$ is in $S_{\texttt{FVunit}}$. Using Lemma 8.7, for every Scott-continuous map $k\colon \llbracket \texttt{Vunit} \rrbracket \to [0,1]$, $(k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top), k) \in S^*_{\texttt{Vunit}}$, so $((k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top))^*(\llbracket P \rrbracket (0)), k^*(\llbracket P \rrbracket (\frac{1}{2}\delta_\top)))$ is in $\trianglerighteq$. In other words, $(k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top))^*(\llbracket P \rrbracket (0)) \geq k^*(\llbracket P \rrbracket (\frac{1}{2}\delta_\top))$.

Since $g = \eta^{\mathcal{Q}} \circ (\nu \mapsto \frac{1}{2}\nu + \frac{1}{2}\delta_\top)$, and using Proposition 4.2, item 2, $k^* \circ g = (k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top))$. It follows that $k^* \circ g^* = (k^* \circ g)^*$ (using Proposition 4.2, item 4) $= (k(\frac{1}{2}\_ + \frac{1}{2}\delta_\top))^*$. Hence our previous equality can be read, alternatively, as $k^*(g^*(\llbracket P \rrbracket (0))) \geq k^*(\llbracket P \rrbracket (\frac{1}{2}\delta_\top))$. In other words,

$$k^*(\llbracket N(P) \rrbracket) \geq k^*(\llbracket M(P) \rrbracket) \tag{7}$$

for every Scott-continuous map $k\colon \llbracket \texttt{Vunit} \rrbracket \to [0,1]$.

We claim that $M(P) \precsim_{\texttt{FVunit}} N(P)$. To this end, we let C be any ground evaluation context of type $\texttt{FVunit} \vdash \texttt{FVunit}$, and we aim to show that $\Pr(C \cdot M(P){\downarrow}) \leq \Pr(C \cdot N(P){\downarrow})$. By adequacy (Proposition 6.10) and Lemma 4.9, this means showing that $h^*(\llbracket C \rrbracket (\llbracket M(P) \rrbracket)) \leq h^*(\llbracket C \rrbracket (\llbracket N(P) \rrbracket))$, where $h(\nu) = \nu(\{\top\})$.

Let us write C as $E_0 E_1 E_2 \cdots E_n$, where $E_i\colon \overline{\sigma}_{i+1} \vdash \overline{\sigma}_i$, $\overline{\sigma}_{n+1} = \overline{\sigma}_0 = \texttt{FVunit}$. All the types $\overline{\sigma}_i$ have rank 1, namely, are computation types. It follows that $E_0 = [\_]$, and that the elementary contexts E_i, $1 \leq i \leq n$ are of the form $[\_\ \texttt{to}\ x_\tau\ \texttt{in}\ N]$ or $[\_N]$. However, $\overline{\sigma}_{n+1}$ is an $\texttt{F}$-type (i.e., of the form $\texttt{F}\tau$ for some value type τ), and that implies that E_n must be of the form $[\_\ \texttt{to}\ x_\tau\ \texttt{in}\ N]$ and $\overline{\sigma}_n$ must be an $\texttt{F}$-type again. Then E_{n-1} must again be of the form $[\_\ \texttt{to}\ x_\tau\ \texttt{in}\ N]$ and $\overline{\sigma}_{n-1}$ must be an $\texttt{F}$-type, and so on: the elementary contexts E_i, $1 \leq i \leq n$, are all of the form $[\_\ \texttt{to}\ x_\tau\ \texttt{in}\ N]$, and $\overline{\sigma}_i = \texttt{F}\tau_i$ for some value type τ_i, with $\tau_{n+1} = \tau_1 = \texttt{Vunit}$. In particular, $\llbracket E_i \rrbracket = {f_i}^*$ for some Scott-continuous map $f_i\colon \llbracket \texttt{V}\tau_{i+1} \rrbracket \to \llbracket \texttt{V}\tau_i \rrbracket$. It follows that $\llbracket C \rrbracket = {f_1}^* \circ {f_2}^* \circ \cdots \circ {f_n}^*$. If $n \neq 0$, then applying Proposition 4.2, item 4, repeatedly, we obtain that $\llbracket C \rrbracket = f^*$ for some Scott-continuous map $f\colon \llbracket \texttt{Vunit} \rrbracket \to \llbracket \texttt{FVunit} \rrbracket$; applying it one more time, $h^* \circ \llbracket C \rrbracket = (h^* \circ f)^*$. If $n = 0$, then $h^* \circ \llbracket C \rrbracket = h^*$. In both cases, $h^* \circ \llbracket C \rrbracket$ is equal to k^* for some Scott-continuous map $k\colon \llbracket \texttt{Vunit} \rrbracket \to [0,1]$.

By (7), $h^*(\llbracket C \rrbracket (\llbracket N(P) \rrbracket)) \geq h^*(\llbracket C \rrbracket (\llbracket M(P) \rrbracket))$, and this is what we needed to show to establish $M(P) \precsim_{\texttt{FVunit}} N(P)$.

Since P is arbitrary, by Proposition 7.5, $M \precsim_{\texttt{U}(\texttt{Vunit}\to\texttt{FVunit})\to\texttt{FVunit}} N$.

For every $b \in (0,1)$, let $[> b]$ be the map that sends every $\nu \in \llbracket \texttt{Vunit} \rrbracket$ to $\uparrow\{\delta_\top\}$ if $\nu(\{\top\}) > b$, and to $\perp$ otherwise. This is is easily seen to be Scott-continuous. For $b < 1/2$ (e.g., $b = 1/4$),

$$\llbracket M \rrbracket ([> b]) = [> b]\left(\frac{1}{2}\delta_\top\right) = \uparrow\{\delta_\top\}$$
$$\llbracket N \rrbracket ([> b]) = g^*([> b](0)) = g^*(\perp) = \perp.$$

In particular, $[\![M]\!]([> b]) \not\leq [\![N]\!]([> b])$, so $[\![M]\!] \not\leq [\![N]\!]$. $\Box$

The function $[> b]$ is, of course, the semantics of $\bigcirc_{>b}$. As a consequence, it is not definable in PCBV($\mathtt{D}, \mathtt{P}$) and even CBPV($\mathtt{D}, \mathtt{P}$)+**pifz**, at least for $b < 1/2$. A similar argument would show that it is not definable for any $b \in (0, 1)$, replacing the definition of $\rhd$ by $\rhd = \{(a_1, a_2) \in [0, 1]^2 \mid aa_1 + 1 - a \geq a_2\}$, for any dyadic number $a \in (0, 1)$.

9 Full Abstraction

Full abstraction for CBPV($\mathtt{D}, \mathtt{P}$)+**pifz**+$\bigcirc$ will follow from a series of auxiliary results that show that the Scott topology on various dcpos coincides with some other, simpler topologies. Before we make that precise, let us say that our goal is that every type should be *describable*, in the following sense. For a Scott-open subset U of $[\![\overline{\sigma}]\!]$, where $\overline{\sigma}$ is a type, recall that $\chi_U \in [[\![\overline{\sigma}]\!] \to \mathbb{S}]$ is its characteristic map. We write $\tilde{\chi}_U$ for the map $[\![\mathbf{produce}\,\mathbf{ret}\,\_]\!] \circ \chi_U$, which maps every $x \in [\![\overline{\sigma}]\!]$ to $\{\delta_\top\}$ if $x \in U$, to $\bot$ otherwise.

Definition 9.1 *An element of $[\![\overline{\sigma}]\!]$, for a type $\overline{\sigma}$, is* definable *if and only if it is equal to $[\![M]\!]$ for some ground CBPV($\mathtt{D}, \mathtt{P}$) + **pifz** + $\bigcirc$ term $M : \overline{\sigma}$.*

A Scott-open subset U of $[\![\tau]\!]$, for a value type τ, is definable *if and only if $\tilde{\chi}_U = [\![M]\!]$ for some ground CBPV($\mathtt{D}, \mathtt{P}$) + **pifz** + $\bigcirc$ term $M : \tau \to \mathbf{FVunit}$.*

For a computation type $\underline{\tau}$, a Scott-open subset U of $[\![\underline{\tau}]\!]$ is definable *if and only if $\tilde{\chi}_U = [\![M]\!]$ for some ground CBPV($\mathtt{D}, \mathtt{P}$) + **pifz** + $\bigcirc$ term $M : U\underline{\tau} \to$ **FVunit**.*

A type $\overline{\sigma}$ is describable *if and only if $[\![\overline{\sigma}]\!]$ has a basis of definable elements and the Scott topology on $[\![\overline{\sigma}]\!]$ has a subbase of definable open subsets.*

As a first, easy example of a describable type, we have:

Lemma 9.2 **unit** *is describable.*

Proof. All the elements of $[\![\mathbf{unit}]\!] = \mathbb{S}$ are definable, since $[\![\Omega_{\mathbf{unit}}]\!] = \bot$ and $[\![\underline{*}]\!] = \top$. The function $P = \lambda x_{\mathbf{unit}}.(x_{\mathbf{unit}}; \mathbf{produce}\,\mathbf{ret}\,\underline{*})$ defines the open subset $\{\top\}$, which is by itself a subbase of the Scott topology. $\Box$

Lemma 9.3 **int** *is describable.*

Proof. All the elements of $[\![\mathbf{int}]\!] = \mathbb{Z}_\bot$ are definable: $[\![\Omega_{\mathbf{int}}]\!] = \bot$, $[\![\underline{n}]\!] = n$. A subbase of the Scott topology consists of the sets $\{n\}$, $n \in \mathbb{Z}$, and they are definable by $\lambda x_{\mathbf{int}}.\mathbf{ifz}\ \underbrace{\mathbf{pred}(\mathbf{pred} \cdots (\mathbf{pred}}_{n \text{ times}} M))\ (\mathbf{produce}\,\mathbf{ret}\,\underline{*})\ \Omega_{\mathbf{FVunit}}$ if $n \geq 0$, and by $\lambda x_{\mathbf{int}}.\mathbf{ifz}\ \underbrace{\mathbf{succ}(\mathbf{succ} \cdots (\mathbf{succ}}_{n \text{ times}} M))\ (\mathbf{produce}\,\mathbf{ret}\,\underline{*})\ \Omega_{\mathbf{FVunit}}$ otherwise. $\Box$

We now consider more complex types. It will be useful to realize that every describable type has a base, not just a subbase, of definable open subsets.

Moreover this base, which is obtained as the collection of finite intersections of subbasic open sets, is closed under finite intersections. We call *strong base* any base that is closed under finite intersections.

Lemma 9.4 *For every describable type $\overline{\sigma}$, the Scott topology on $[\![\overline{\sigma}]\!]$ has a strong base of definable open subsets.*

Proof. For any two terms $M, N : \mathtt{FVunit}$, let $M \wedge N$ be the term M **to** $x_{\mathtt{Vunit}}$ **in** N, where $x_{\mathtt{Vunit}}$ is a fresh variable. For every environment ρ, $[\![M \wedge N]\!]\,\rho = h^*([\![M]\!]\,\rho)$ where $h(\nu) = [\![N]\!]\,\rho[x_{\mathtt{Vunit}} \mapsto \nu] = [\![N]\!]\,\rho$ (since $x_{\mathtt{V}\sigma}$ is not free in N). Since h^* is strict, if $[\![M]\!]\,\rho = \bot$, then $[\![M \wedge N]\!]\,\rho = \bot$. Otherwise, by Proposition 4.2, item 2, $h^*([\![M]\!]\,\rho) = \bigwedge_{\nu \in [\![M]\!]\rho} h(\nu)$. If $[\![M]\!]\,\rho \neq \emptyset$, in particular if $[\![M]\!] = \{\delta_\top\}$, this is equal to $[\![N]\!]\,\rho$.

We write $M_1 \wedge \cdots \wedge M_n$ for $M_1 \wedge (M_2 \wedge \cdots (M_n \wedge \mathtt{produce\,ret}\,\underline{*}) \cdots)$. This implements logical and, in the sense that if $[\![M_i]\!]\,\rho$ is either equal to $\{\delta_\top\}$ or to $\bot$ for every i, its denotation in any environment ρ is $\{\delta_\top\}$ if $[\![M_i]\!]\,\rho = \{\delta_\top\}$ for every i, and is $\bot$ if $[\![M_i]\!]\,\rho = \bot$ for some i.

Given finitely many open subsets $U_1, \ldots, U_n$ defined by terms $M_1, \cdots, M_n : \sigma \to \mathtt{FVunit}$ respectively (where $\sigma = \overline{\sigma}$ if $\overline{\sigma}$ is a value type, $\sigma = \mathtt{U}\overline{\sigma}$ if $\overline{\sigma}$ is a computation type), the term $\lambda x_\sigma.(M_1 x_\sigma) \wedge \cdots \wedge (M_n x_\sigma)$ then defines the intersection $U_1 \cap \cdots \cap U_n$. □

9.1 Product types

Lemma 9.5 *Let X, Y be two continuous dcpos. Let B_X be a basis of X, B_Y be a basis of Y, $\mathcal{S}_X$ be a subbase of the Scott topology on X, $\mathcal{S}_Y$ be a subbase of the Scott topology on Y. Then:*

- *The set $B_{X \times Y} = B_X \times B_Y$ is a basis of $X \times Y$.*
- *The set $\mathcal{S}_{X \times Y} = \{U \times V \mid U \in \mathcal{S}_X, V \in \mathcal{S}_Y\}$ is a subbase of the Scott topology on $X \times Y$.*

Proof. The second part follows from the fact that the Scott topology on a product of continuous dcpos is the product topology, because it is generated by sets of the form $\twoheaduparrow(x, y) = \twoheaduparrow x \times \twoheaduparrow y$. (This is not true of non-continuous dcpos.) □

Proposition 9.6 *For any two describable value types σ and τ, $\sigma \times \tau$ is describable.*

Proof. We use Lemma 9.5 with $X = [\![\sigma]\!]$, $Y = [\![\tau]\!]$. B_X (resp., B_Y) is the basis of definable elements of $[\![\sigma]\!]$ (resp., $[\![\tau]\!]$). $\mathcal{B}_X$ is the base of definable open subsets at type σ, obtained by Lemma 9.4, and similarly for $\mathcal{B}_Y$. The elements of $B_{X \times Y}$ are definable as $\langle M, N\rangle$, where $[\![M]\!] \in B_X$, $[\![N]\!] \in B_Y$, and the elements $U \times V$ of $\mathcal{B}_{X \times Y}$ are definable as $\lambda z_{\sigma \times \tau}.M(\pi_1 z) \wedge N(\pi_2 z)$, where U is defined by M and V is defined by N, and where $\wedge$ was defined in the course of the proof of Lemma 9.4. □

9.2 Function types

Semantically, at function types, the key result will be the following Proposition 9.10, which in particular says that the Scott topology on $[X \to Y]$ coincides with the topology of pointwise convergence, under certain assumptions.

A standard basis of $[X \to Y]$ is given by the *step functions* $\sup_{i=1}^m U_i \searrow b_i$, where each U_i is open in X, each b_i is in Y, and $U \searrow b$ denotes the map that maps every element of U to b, and all others to $\bot$. We show that this can be refined by requiring U_i to be taken from some given strong base $\mathcal{B}_X$ of the topology on X, and b_i to be taken from some basis B_Y of Y. We note that $\sup_{i=1}^m U_i \searrow b_i$ maps each point $x \in X$ to $\sup_{i \in I} b_i$, where $I = \{i \mid 1 \leq i \leq m, x \in U_i\}$. In general, $\sup_{i \in I} b_i$ will not be in B_Y. To avoid this problem, we require our step functions to be of a special form.

Definition 9.7 *Let X be a topological space, $\mathcal{B}_X$ be a strong base of the topology of X, Y be a continuous dcpo, and B_Y be a basis of Y. A $(\mathcal{B}_X, B_Y)$-*step function *is any step function of the form* $\sup_{I \subseteq \{1,\cdots,m\}} U_I \searrow y_I$ *where:*

1. *each U_I is in $\mathcal{B}_X$;*
2. *each y_I is in B_Y;*
3. *$U_\emptyset = X$ and $U_I \cap U_J = U_{I \cup J}$ for all $I, J \subseteq \{1, \cdots, m\}$;*
4. *for all $I \subseteq J$, $y_I \leq y_J$.*

We make a preliminary remark.

Lemma 9.8 *Given a continuous dcpo Z, and a family $B \subseteq Z$, in order to show that B is a basis of Z it is enough to show that for every $z \in Z$, every Scott-open neighborhood W of z contains a $d \in B$ such that $d \ll z$.*

Proof. If so, then the family $B_z = \{d \in B \mid d \ll z\}$ is non-empty (take $W = Z$) and directed (for any two $d_1, d_2 \in B_z$, take $W = \twoheaduparrow d_1 \cap \twoheaduparrow d_2$), and $\sup B_z = z$ (for every open neighborhood W of z, some element of B_z is in W so $\sup B_z \geq z$, and the converse inequality is obvious). ☐

A *core-compact* topological space X is one whose lattice of open subsets is a continuous dcpo. We write $\Subset$ for the way-below relation on that lattice. Every locally compact space is core-compact, with $U \Subset V$ if and only if $U \subseteq Q \subseteq V$ for some compact saturated set Q.

Lemma 9.9 *Let X be a core-compact space, $\mathcal{B}_X$ be a strong base of the topology of X, Y be a a continuous complete lattice, and B_Y be a basis of Y. Then $[X \to Y]$ is a continuous complete lattice, with a basis of $(\mathcal{B}_X, B_Y)$-step functions.*

Note: one could replace "continuous complete lattice" by "bc-domain" here, and the proof would only be slightly more complicated.

Proof. We apply Lemma 9.8 to $Z = [X \to Y]$. By Proposition 2 of [6], Z is a bounded complete continuous dcpo with a basis B_0 of step functions, and since it has a top, it is a continuous complete lattice. Let B_1 be the family of step functions of the form $\sup_{i=1}^m V_i \searrow y_i$ where each V_i is in $\mathcal{B}_X$. For every $f \in [X \to Y]$, and every Scott-open neighborhood W of f, there is an element $\sup_{i=1}^m U_i \searrow y_i$ of B_0, way-below f, and in W. Let us write U_i as a union $\bigcup_{j \in J_i} V_{ij}$ of elements of $\mathcal{B}_X$. The family of maps $\sup_{i=1}^m (\bigcup_{j \in F_i} V_{ij}) \searrow y_i$, where F_i ranges over the finite subsets of J_i for each i, is directed (since an upper bound of $\sup_{i=1}^m (\bigcup_{j \in F_i} V_{ij}) \searrow y_i$ and of $\sup_{i=1}^m (\bigcup_{j \in F'_i} V_{ij}) \searrow y_i$ is $\sup_{i=1}^m (\bigcup_{j \in F_i \cup F'_i} V_{ij}) \searrow y_i)$, and has $\sup_{i=1}^m U_i \searrow y_i$ as supremum (because for every $x \in X$, letting $I = \{i \mid x \in U_i\}$, there are indices $j_i \in J_i$ for each $i \in I$ such that $x \in V_{ij}$, hence $x \in F_i$ where $F_i = \{j_i\}$). Hence $\sup_{i=1}^m (\bigcup_{j \in F_i} V_{ij}) \searrow y_i$ is in W for some finite subsets F_i of J_i, $1 \leq i \leq m$. Now $\sup_{i=1}^m (\bigcup_{j \in F_i} V_{ij}) \searrow y_i$ is equal to $\sup_{i=1}^m \sup_{j \in F_i} V_{ij} \searrow y_i$, showing that it is in B_1. Moreover, $\sup_{i=1}^m (\bigcup_{j \in F_i} V_{ij}) \searrow y_i \leq \sup_{i=1}^m U_i \searrow y_i \ll f$. We can therefore apply our preliminary remark and conclude that B_1 is a basis of $[X \to Y]$.

Given any element $\sup_{i=1}^m U_i \searrow y_i$ of B_1, we can write it as $\sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow y_I$, where for each $I \subseteq \{1, \cdots, m\}$, $U_I = \bigcap_{i \in I} U_i$ and $y_I = \sup_{i \in I} y_i$. (In case Y were a bc-domain, the same argument would apply provided we only considered the subsets I such that U_I is non-empty.) Note that: (a) for all $I, J \subseteq \{1, \cdots, m\}$, $I \subseteq J$ implies $y_I \leq y_J$. Also: (b) $U_\emptyset = X$, for all $I, J \subseteq \{1, \cdots, m\}$, $U_I \cap U_J = U_{I \cup J}$, and each U_I is in $\mathcal{B}_X$ (because $\mathcal{B}_X$ is a strong base).

Let B_2 be the family of maps $\sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow y_I$, where U_I and y_I satisfy conditions (a) and (b) and, additionally, each y_I is in B_Y. For every $f \in [X \to Y]$, and every Scott-open neighborhood W of f, W contains an element $g = \sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow y_I$ of B_1 satisfying conditions (a) and (b) and way-below f.

Here is the idea of the rest of the proof. Enumerating the subsets I of $\{1, \cdots, m\}$ so that the cardinality of I never goes down, starting from the empty set, we replace y_I by an element z_I such that $z_I \ll y_I$ and $z_I \in B_Y$; at each step, we also replace y_J by $\sup(z_I, y_J)$ for all strict supersets J of I, so that (a) still holds. Since B_Y is a basis, for z_I large enough, the resulting function will be in W. We can also require that $z_J \leq z_I$ for all $J \subsetneq I$, since all those elements z_J have been chosen in previous steps so that $z_J \ll y_J$. At the end of the enumeration, we obtain a function $h = \sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow z_I$ of B_1 satisfying conditions (a) and (b), in W, below g hence way-below f, and such that $z_I \in B_Y$ and $z_I \ll y_I$ for every $I \in \{1, \cdots, m\}$. In particular, that element h is in B_2. Let us now prove that formally.

We claim that: ($*$) for every downwards-closed family $\mathcal{I}$ of $\mathbb{P}(\{1, \cdots, m\})$ (downwards-closed with respect to inclusion), there is an element h of the form $\sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow z_I$ in B_1 satisfying conditions (a) and (b), lying in W, such that $z_I \leq y_I$ for every $I \subseteq \{1, \cdots, m\}$ (in particular, $h \leq g$), and such that $z_I \in B_Y$ and $z_I \ll y_I$ for every $I \in \mathcal{I}$. This is proved by induction on the cardinality of $\mathcal{I}$. This is vacuous if $\mathcal{I}$ is empty. Hence consider a non-empty downwards-closed family $\mathcal{I}$ of $\mathbb{P}(\{1, \cdots, m\})$, let I_0 be a maximal element of $\mathcal{I}$, and let $\mathcal{I}' = \mathcal{I} \setminus \{I_0\}$. Notice that $\mathcal{I}'$ is again downwards-closed. Hence, by induction hypothesis, there an element $h = \sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow z_I$ of B_1 satisfying conditions (a) and (b), in W, such that $z_I \leq y_I$ for every $I \subseteq \{1, \cdots, m\}$, and such that $z_I \in B_Y$ and $z_I \ll y_I$ for every $I \in \mathcal{I}'$. Since B_Y is a basis, we can write y_{I_0} as the supremum of a directed family $(y'_j)_{j \in J}$ of elements of B_I. For each $j \in J$, let $h[y'_j] = \sup(\sup_{I \subseteq \{1,\cdots,m\}, I \neq I_0} U_I \searrow z_I, (U_{I_0} \searrow y'_j))$. One checks easily that $(h[y'_j])_{j \in J}$ is a directed family whose supremum is above h. Hence $h[y'_j]$ is in W for some $j \in J$. For every $I \subsetneq I_0$, $z_I \ll y_I \leq y_{I_0}$ (using (a)), so there is a $j_I \in J$ such that $z_I \leq y'_{j_I}$. By directedness, we can assume without loss of generality that j and all the indices j_I, $I \subsetneq I_0$, are equal. (Otherwise replace them by some $k \in J$ such that $y'_j \leq y'_k$ and $y'_{j_I} \leq y'_k$ for every $I \subsetneq I_0$.) For every $I \subseteq \{1, \cdots, m\}$, we define z'_I as z_I if I does not contain I_0, as y'_j if $I = I_0$, and as $\sup(z_I, y'_j)$ if I contains I_0 strictly. We have:

- For all $I \subseteq J \subseteq \{1, \cdots, m\}$, $z'_I \leq z'_J$. The key case is when $J = I_0$, which follows from the fact that $y'_j = z'_{I_0}$ was chosen larger than or equal to every z_I, $I \subsetneq I_0$, and that $z'_I = z_I$ in this case. When $I = I_0$ instead, $z'_I = y'_j \leq y_{I_0} \leq y_J$ (by (a)). The cases where I, J are both different from I_0 are easy verifications.

- Hence the function $h' = \sup_{I \subseteq \{1,\cdots,m\}} U_I \searrow z'_I$ satisfies (a), and trivially (b) as well.

- For every $I \subseteq \{1, \cdots, m\}$, $z'_I \leq y_I$. When $I = I_0$, this is because $z'_I = y'_j \leq y_{I_0}$. When $I \supsetneq I_0$, $z'_I = \sup(z_I, y'_j) \leq \sup(y_I, y_{I_0}) = y_I$, using (a).

- We have built h' so that it is in W.

- For every $I \in \mathcal{I}$, z'_I is in B_Y: when $I = I_0$, this is because $z'_{I_0} = y'_j$ is in B_Y; otherwise, since I_0 is maximal in $\mathcal{I}$, I cannot contain I_0, so $z'_I = z_I$, which is in B_Y because $I \in \mathcal{I}'$, using the induction hypothesis.

- For every $I \in \mathcal{I}$, $z'_I \ll y_I$: when $I = I_0$, this is because $z'_I = y'_j \ll y_{I_0}$; otherwise, $z'_i = z_I \ll y_I$ because $I \in \mathcal{I}'$, using the induction hypothesis.

This finishes to prove claim $(*)$. Applying this claim to the case where $\mathcal{I}$ is the whole of $\mathbb{P}(\{1, \cdots, m\})$, we obtain an element $h = \sup_{I \subseteq \{1,\cdots,m\}} U_I \searrow z_I$ of B_1 satisfying conditions (a) and (b), in W, below g hence way-below f, and such that $z_I \in B_Y$ and $z_I \ll y_I$ for every $I \in \{1, \cdots, m\}$. In particular, that element h is in B_2. By our preliminary remark, B_2 is a basis of $[X \to Y]$. $\square$

Proposition 9.10 *Let X be a continuous dcpo and Y be a bc-domain. Let B_X be a basis of X, $\mathcal{B}_X$ be a base of the Scott topology on X. Let B_Y be a basis of Y, and $\mathcal{S}_Y$ be a subbase of the Scott topology on Y. Then:*

- *The set $B_{[X \to Y]}$ of all $(\mathcal{B}_X, B_Y)$-step functions is a basis of $[X \to Y]$.*

- *The set $\mathcal{S}_{[X \to Y]}$ of all opens $[x \mapsto V]$, $x \in B_X$, $V \in \mathcal{S}_Y$, is a subbase of the Scott topology on $[X \to Y]$. We write $[x \mapsto V]$ for the open subset $\{f \in [X \to Y] \mid f(x) \in V\}$.*

Proof. The first part is Lemma 9.9. The second part is based on Lemma 5.16 of [9], which states that the subsets $[x \mapsto V]$, $x \in X$, V open in Y, form a subbase of the topology of $[X \to Y]$, as soon as X is a continuous poset and Y is a bc-domain. $\square$

We introduce the following abbreviations.

- For all $M : \mathtt{int}$, $N, P : \underline{\tau}$, and for every $n \in \mathbb{N}$, $\mathtt{pif}\ (M == \underline{n})\ N\ P$ denotes $\mathtt{pifz}\ \underbrace{\mathtt{pred}(\mathtt{pred} \cdots (\mathtt{pred}}_{n \text{ times}} M))\ N\ P$.
- Given terms $M : \mathtt{int}$ and $N_1, \ldots, N_n$ of type $\underline{\tau}$, $\mathtt{pswitch}\ M : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n$ abbreviates:

$$\begin{array}{l} \mathtt{pif}\ (M == \underline{n})\ N_n\ (\\ \quad \mathtt{pif}\ (M == \underline{n-1})\ N_{n-1}\ (\\ \quad \quad \cdots \\ \quad \quad \mathtt{pif}\ (M == \underline{2})\ N_2\ (\\ \quad \quad \quad \mathtt{pif}\ (M == \underline{1})\ N_1 \\ \quad \quad \quad \quad \mathtt{abort}_{\underline{\tau}}\quad))). \end{array}$$

  In particular, if $n = 0$, this is equal to $\mathtt{abort}_{\underline{\tau}}$.

- Given terms $M : \mathtt{unit}$ and $N : \mathtt{unit}$, $M \vee N : \mathtt{unit}$ is the term defined as $\bigcirc_{>1/2}(\mathtt{pifz}\ (M; \underline{0})\ (\mathtt{produce}\,\mathtt{ret}\,\underline{*})\ (\mathtt{produce}\,\mathtt{ret}\,N))$.
- Given a term $M : \mathtt{unit}$, $n \in \mathbb{N}$ and $i \in \mathbb{N}$ such that $1 \leq i \leq n$, $[M : i]$ is the term of type $\mathtt{Fint}$ defined as $\mathtt{pifz}\ (M; \underline{0})\ \mathtt{abort}_{\mathtt{Fint}}\ (\mathtt{produce}\, i)$.
- Given terms $M_1, \ldots, M_n$ of type $\mathtt{unit}$ and $N_1, \ldots, N_n$ of type $\underline{\tau}$, $\mathtt{pcase}\ M_1 \mapsto N_1 \mid \cdots \mid M_n \mapsto N_n$ abbreviates:

$$\begin{array}{l} ([M_1 : 1] \oslash \cdots \oslash [M_n : n])) \\ \quad \mathtt{to}\ y_{\mathtt{int}}\ \mathtt{in}\ \mathtt{pswitch}\ y_{\mathtt{int}} : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n. \end{array}$$

Lemma 9.11 *1. $[\![\mathtt{pif}\ (M == \underline{n})\ N\ P]\!]\,\rho$ is equal to $[\![N]\!]\,\rho$ if $[\![M]\!]\,\rho = n$, to $[\![P]\!]\,\rho$ if $[\![M]\!]\,\rho \neq n, \bot$ and to $[\![N]\!]\,\rho \wedge [\![P]\!]\,\rho$ if $[\![M]\!]\,\rho = \bot$;*

2. $[\![\mathtt{pswitch}\ M : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n]\!]\,\rho$ is equal to $[\![N_m]\!]\,\rho$ if $[\![M]\!]\,\rho$ is an element m of $\{1, \cdots, n\}$, to $\bigwedge_{i \in \{1,\cdots,n\}} [\![N_i]\!]\,\rho$ if $[\![M]\!]\,\rho = \bot$, and to $\top$ otherwise.

3. $[\![M \vee N]\!]\,\rho = \sup([\![M]\!]\,\rho, [\![N]\!]\,\rho)$.

4. $[\![[M : i]]\!]\,\rho$ is equal to $\emptyset$ if $[\![M]\!]\,\rho = \top$, to $\{i\}$ if $[\![M]\!]\,\rho = \bot$.

Proof. 1, 3 and 4 are clear. We prove item 2 by induction on n. If $n = 0$, then $[\![\mathtt{pswitch}\ M : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n]\!]\,\rho = [\![\mathtt{abort}_{\underline{\tau}}]\!]\,\rho$, which is the top element $\top$ of $[\![\underline{\tau}]\!]$, as an easy induction on $\underline{\tau}$ shows. Note that, in case $[\![M]\!]\,\rho = \bot$, this is also equal to $\bigwedge_{i \in \{1,\cdots,n\}} [\![N_i]\!]\,\rho$ since $n = 0$. If $n \geq 1$, then by item 1, $[\![\mathbf{pswitch}\, M : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n]\!]\, \rho$ is equal to $[\![N_n]\!]\, \rho$ if $[\![M]\!]\, \rho = n$, to $[\![\mathbf{pswitch}\, M : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n-1} \mapsto N_{n-1}]\!]\, \rho$ if $[\![M]\!]\, \rho \in \mathbb{Z} \setminus \{n\}$, and to their infimum if $[\![M]\!]\, \rho = \bot$. We then use the induction hypothesis to conclude. $\Box$

Lemma 9.12 *Let $M : \mathbf{F}\sigma$ and $N : \underline{\tau}$. Assume that $[\![M]\!]\, \rho$ is of the form $\uparrow\{V_1, \cdots, V_k\}$. Then $[\![M\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]\!]\, \rho = \bigwedge_{i=1}^{k} [\![N]\!]\, \rho[x_\sigma \mapsto V_i]$.*

Proof. By structural induction on $\underline{\tau}$. Let f be the map $V \in [\![\sigma]\!] \mapsto [\![N]\!]\, \rho[x_\sigma \mapsto V]$. If $\underline{\tau}$ is of the form $\mathbf{F}\tau$, then:

$$\begin{aligned}
[\![M\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]\!]\, \rho &= f^*(\uparrow\{V_1, \cdots, V_k\}) \\
&= \bigwedge_{i=1}^{k} f^*(\eta^{\mathcal{Q}}(V_i)) && \text{by Proposition 4.2, item 3} \\
&= \bigwedge_{i=1}^{k} f(V_i),
\end{aligned}$$

by Proposition 4.2, item 2.

If $\underline{\tau}$ is of the form $\lambda \to \underline{\tau}'$, then:

$$\begin{aligned}
[\![M\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N]\!]\, \rho &= [\![\lambda y_\lambda . M\ \mathbf{to}\ x_\sigma\ \mathbf{in}\ N y_\lambda]\!]\, \rho \\
&= (V \in [\![\lambda]\!] \mapsto \bigwedge_{i=1}^{k} f(V_i)(V)) && \text{by induction hypothesis} \\
&= \bigwedge_{i=1}^{k} f(V_i).
\end{aligned}$$

The last equality follows from the fact that finite infima of continuous functions are computed pointwise, by Lemma 4.3, item 2. $\Box$

Lemma 9.13 *$[\![\mathbf{pcase}\ M_1 \mapsto N_1 \mid \cdots \mid M_n \mapsto N_n]\!]\, \rho$ is equal to $\bigwedge_{i \in I} [\![N_i]\!]\, \rho$, where $I = \{i \in \{1, \cdots, n\} \mid [\![M_i]\!]\, \rho \neq \top\}$.*

Proof. By Lemma 9.11, item 4, $[\![[M_1 : 1] \oslash \cdots \oslash [M_n : n]]\!]\, \rho = \bigwedge_{i=1}^{n} [\![[M_i : i]]\!]\, \rho = \bigcup_{i=1}^{n} [\![[M_i : i]]\!]\, \rho = \bigcup_{i \in I} \{i\} = I = \uparrow I$. By Lemma 9.12, it then follows that $[\![\mathbf{pcase}\ M_1 \mapsto N_1 \mid \cdots \mid M_n \mapsto N_n]\!]\, \rho$ is equal to $\bigwedge_{i \in I} [\![P]\!]\, \rho[y_{\mathtt{int}} \mapsto i]$ where $P = \mathbf{pswitch}\, y_{\mathtt{int}} : \underline{1} \mapsto N_1 \mid \cdots \mid \underline{n} \mapsto N_n$, and by Lemma 9.11, item 2, this is equal to $\bigwedge_{i \in I} [\![N_i]\!]\, \rho$. $\Box$

It follows:

Proposition 9.14 *For every describable value type σ, for every describable computation type $\underline{\tau}$, the type $\sigma \to \underline{\tau}$ is describable.*

Proof. We use Proposition 9.10, with $X = [\![\sigma]\!]$, $Y = [\![\underline{\tau}]\!]$. B_X (resp., B_Y) is the basis of definable elements of $[\![\sigma]\!]$ (resp., $[\![\underline{\tau}]\!]$). $\mathcal{B}_X$ is the base of definable open subsets at type σ, obtained thanks to Lemma 9.4, and $\mathcal{S}_Y$ is the subbase of definable open subsets at type $\underline{\tau}$.

We first show that all the elements of $B_{[X \to Y]}$ are definable. This will imply that the definable elements at type $\sigma \to \underline{\tau}$ form a basis of $[\![\sigma \to \underline{\tau}]\!]$. We recall that such an element is a $(\mathcal{B}_X, B_Y)$-step function $f = \sup_{I \subseteq \{1, \cdots, m\}} U_I \searrow y_I$.

Let U_I be defined by ground terms $M_I \colon \sigma \to \mathtt{FVunit}$, i.e., $\tilde{\chi}_{U_I} = [\![M_I]\!]$, and let y_I be defined by ground terms $N_I \colon \underline{\tau}$. Let us pick a variable x_σ. For every subset I of $\{1, \cdots, m\}$, let $M_I^\perp(x_\sigma) = \bigvee_{J \subseteq \{1, \cdots, m\}, J \not\subseteq I} \bigcirc_{>1/2}(M_J x_\sigma)$. (If $I = \{1, \cdots, m\}$, the empty disjunction is $\Omega_{\mathtt{unit}}$.) For every environment ρ, and letting $a = \rho(x_\sigma)$, by Lemma 9.13, $[\![\mathtt{pcase}\ \{M_I^\perp(x_\sigma) \mapsto N_I \mid I \subseteq \{1, \cdots, m\}\}]\!]\ \rho$ is equal to the infimum of the values $[\![N_I]\!] = y_I$ over the subsets I of $\{1, \cdots, m\}$ such that $[\![M_I^\perp(x_\sigma)]\!]\ \rho \neq \top$, i.e., such that $a \notin \bigcup_{J \not\subseteq I} U_J$.

Let I_0 be the set of indices i between 1 and m such that $a \in U_{\{i\}}$. For every $J \subseteq \{1, \cdots, m\}$, $a \in U_J$ if and only if for every $i \in J$, a is in $U_{\{i\}}$, if and only if $J \subseteq I_0$. For every $I \subseteq \{1, \cdots, m\}$, $a \notin \bigcup_{J \not\subseteq I} U_J$ if and only if for every $J \not\subseteq I$, $a \notin U_J$, if and only if for every $J \subseteq \{1, \cdots, m\}$, $a \in U_J$ implies $J \subseteq I$ (by contraposition), if and only if for every $J \subseteq \{1, \cdots, m\}$, $J \subseteq I_0$ implies $J \subseteq I$, if and only if $I_0 \subseteq I$. Therefore $[\![\mathtt{pcase}\ \{M_I^\perp(x_\sigma) \mapsto N_I \mid I \subseteq \{1, \cdots, m\}\}]\!]\ \rho$ is equal to $\bigwedge_{I \supseteq I_0} y_I = y_{I_0} = f(a)$. It follows that f is definable as $\lambda x_\sigma.\mathtt{pcase}\ \{M_I^\perp(x_\sigma) \mapsto N_I \mid I \subseteq \{1, \cdots, m\}\}$.

Second, we show that all the elements of $\mathcal{S}_{[X \to Y]}$ are definable as ground terms of type $\mathtt{U}(\sigma \to \underline{\tau}) \to \mathtt{FVunit}$. Such an element is of the form $[x \mapsto V]$, where $x = [\![M]\!]$ for some ground term $M \colon \sigma$, and $V = [\![P]\!]$ for some ground term $P \colon \mathtt{U}\underline{\tau} \to \mathtt{FVunit}$. Then $[x \mapsto V]$ is definable as the ground term $\lambda f_{\mathtt{U}(\sigma \to \underline{\tau})}.P(\mathtt{thunk}(\mathtt{force}\ f_{\mathtt{U}(\sigma \to \underline{\tau})} M))$. $\square$

9.3 Valuation Types

We have already mentioned in Section 4 that, for every continuous dcpo, $\mathbf{V}_{\leq 1} X$ is a pointed continuous dcpo, and that its Scott topology coincides with the weak upwards topology [3]. The latter has a subbase of open sets of the form $[U > r]$, for every open subset U of X and $r \in \mathbb{R}_+ \setminus \{0\}$, where $[U > r] = \{\nu \in \mathbf{V}_{\leq 1} X \mid \nu(U) > r\}$. We can restrict r further so that $r < 1$, since otherwise $[U > r]$ is empty. Call a number *dyadic* if and only if it is of the form $a/2^k$, with $a, k \in \mathbb{N}$.

Proposition 9.15 *Let X be a pointed continuous dcpo. Let B_X be a basis of X, $\mathcal{B}_X$ be a base of the Scott topology on X. Then:*

- *The set $B_{\mathbf{V}_{\leq 1} X}$ of all simple probability valuations $\sum_{i=1}^n a_i \delta_{x_i}$, where each a_i is a dyadic number in $[0, 1]$, $\sum_{i=1}^n a_i \leq 1$, and each x_i is a point in B_X, is a basis of $\mathbf{V}_{\leq 1} X$.*
- *The set $\mathcal{S}_{\mathbf{V}_{\leq 1} X}$ of all opens $[U > r]$, where U is an element of $\mathcal{B}_X$, and r is a dyadic number in $(0, 1)$, is a subbase of the Scott topology on $\mathbf{V}_{\leq 1} X$.*

Proof. By a theorem of Jones [13, Theorem 5.2], the simple subprobability valuations form a basis of $\mathbf{V}_{\leq 1} X$. For every simple subprobability valuation $\nu = \sum_{i=1}^n a_i \delta_{x_i}$, one easily checks that the collection D_ν of simple subprobability valuations $\sum_{i=1}^n b_i \delta_{y_i}$ with b_i dyadic and way-below a_i in $[0,1]$, and $y_i \in B_X$ way-below x_i, is directed, and $\sup D_\nu = \nu$.

We check that every element of D_ν, as written above, is way-below ν. For convenience, we let $\mu = \sum_{i=1}^n b_i \delta_{y_i}$. Let $(\nu_k)_{k \in K}$ be a directed family in $\mathbf{V}_{\leq 1} X$ with a supremum above ν. We wish to show that there is a $k \in K$ such that for every open subset U of X, $\mu(U) \leq \nu_k(U)$. In order to do so, we show that for every subset J of $\{1, \cdots, n\}$, there is an index $k = k_J \in K$ such that for every open subset U of X such that $J = \{i \in \{1, \cdots, n\} \mid y_i \in U\}$, $\mu(U) \leq \nu_k(U)$. By directedness, there is a $k \in K$ such that $\nu_{k_J} \leq \nu_k$ for every such J, and this will show the claim.

Henceforth, let us fix $J \subseteq \{1, \cdots, n\}$. We have $\sum_{i \in J} b_i \ll \sum_{i \in J} a_i$ (because $b_i \ll a_i$ for each i, and recalling that $b_i \ll a_i$ iff $b_i = 0$ or $b_i < a_i$) $\leq \nu(\bigcup_{i \in J} \Uparrow y_i)$ (because $y_i \ll x_i$ for each i), so there is a $k \in K$ such that $\sum_{i \in J} b_i \leq \nu_k(\bigcup_{i \in J} \Uparrow y_i)$. For every open subset U with $J = \{i \in \{1, \cdots, n\} \mid y_i \in U\}$, $\mu(U) = \sum_{i \in J} b_i \leq \nu_k(\bigcup_{i \in J} \Uparrow y_i) \leq \nu_k(U)$, which finishes the proof.

It is standard domain theory that given a dcpo Z, a point $z \in Z$ that is the supremum of a directed family $(z_i)_{i \in I}$, where z_i is itself the supremum of a directed family D_i of points way-below z_i, then $\bigcup_{i \in I} D_i$ is directed and has z as supremum. In our case D_ν is included in $B_{\mathbf{V}_{\leq 1} X}$, showing that every continuous probability valuation is the supremum of a directed family of elements of $B_{\mathbf{V}_{\leq 1} X}$.

In order to show the second part of the proposition, we consider an arbitrary subbasic open set $[U > r]$ of the weak upwards (=Scott) topology, U open in X, $r \in (0,1)$. We write U as $\bigcup_{i \in I} U_i$, where each U_i is in $\mathcal{B}_X$, and r as the infimum of the numbers $r_n = \lceil 2^n r \rceil / 2^n$. Since $0 < r < 1$, r_n is in $(0,1)$ for n large enough. For every $\nu \in \mathbf{V}_{\leq 1} X$, $\nu(U) > r$ if and only if for some n large enough $\nu(U) > r_n$, if and only if for some n large enough and some finite subset A of I, $\nu(\bigcup_{i \in I} U_i) > r_n$. Hence $[U > r] = \bigcup_{A \text{ finite } \subseteq I, n / r_n < 1} [\bigcup_{i \in A} U_i > r_n]$, showing that $\mathcal{S}_{\mathbf{V}_{\leq 1} X}$ is a subbase of the weak upwards (=Scott) topology. $\Box$

Corollary 9.16 *For every describable value type σ, the type $\mathtt{V}\sigma$ is describable.*

Proof. Let $X = [\![\sigma]\!]$, B_X be the basis of definable elements of $[\![\sigma]\!]$, $\mathcal{B}_X$ be a strong base of definable open subsets at type σ guaranteed by Lemma 9.4, and let us use Proposition 9.15.

Although $\oplus$ is not associative, we can make sense of sums $M_1 \oplus M_2 \oplus \cdots \oplus M_{2^n}$ of 2^n terms of type $\mathtt{V}\sigma$: when $n = 0$, this is just M_1, otherwise this is $(M_1 \oplus \cdots \oplus M_{2^{n-1}}) \oplus (M_{2^{n-1}+1} \oplus \cdots \oplus M_{2^n})$. This way, $[\![M_1 \oplus M_2 \oplus \cdots \oplus M_{2^n}]\!] \rho$ is simply equal to $\frac{1}{2^n} \sum_{i=1}^{2^n} [\![M_i]\!] \rho$.

For every element $\nu = \sum_{i=1}^n a_i \delta_{x_i}$ in $B_{\mathbf{V}_{\leq 1} X}$, we can write each a_i ($1 \leq i \leq n$) as $k_i / 2^m$, where $k_i \in \mathbb{N}$ and with the same m for all values of i. Hence, and letting $k_0 = 2^m - \sum_{i=1}^n k_i$, ν can be written as a sum $\frac{1}{2^m} \sum_{i=1}^{2^m - k_0} \delta_{v_i} + \frac{1}{2^m} \sum_{i=2^m - k_0 + 1}^{2^m} 0$, where each v_i is in B_X. Since σ is describable, for each i ($1 \leq i \leq 2^m - k_0$) v_i is equal to $[\![M_i]\!]$ for some ground term $M_i \colon \sigma$ ($\bot$ is equal to $[\![\Omega_\sigma]\!]$). Also, 0 is equal to $[\![\Omega_{\mathtt{V}\sigma}]\!]$, so ν is definable as the sum of the $2^m - k_0$ terms $\mathtt{ret}\, M_i$, plus k_0 terms $\Omega_{\mathtt{V}\sigma}$.

Let $[U > r]$ be an element of $\mathcal{S}_{\mathbf{V}_{\leq 1}X}$, where $U = \bigcup_{i=1}^{m} U_i$, $U_i \in \mathcal{B}_X$, and r is a dyadic number in $(0,1)$. Each U_i is definable, that is, $\tilde{\chi}_{U_i} = [\![M_i]\!]$ for some ground term $M_i \colon \sigma \to \mathtt{FVunit}$. Let us fix a variable x_σ. For each i, let $M'(x_\sigma) = \bigcirc_{>1/2}(M_1 x_\sigma) \vee \cdots \vee \bigcirc_{>1/2}(M_m x_\sigma)$: $[\![M'(x_\sigma)]\!]\,\rho = \top$ if $\rho(x_\sigma) \in U$, $\perp$ otherwise. Then $[U > r]$ is definable by the term $\lambda y_{\mathtt{V}\sigma}.\bigcirc_{>r}$ $(\mathtt{produce}(\mathtt{do}\, x_\sigma \leftarrow y_{\mathtt{V}\sigma}; \mathtt{ret}\, M'(x_\sigma)))$. Indeed, letting $\nu = \rho(y_{\mathtt{V}\sigma})$,

$$\begin{aligned}
[\![\mathtt{do}\, x_\sigma \leftarrow y_{\mathtt{V}\sigma}; \mathtt{ret}\, M'(x_\sigma)]\!]\,\rho(\{\top\}) &= (a \in [\![\sigma]\!] \mapsto [\![\mathtt{ret}\, M'(x_\sigma)]\!]\,\rho[x_\sigma \mapsto a])^\dagger(\nu)(\{\top\}) \\
&= \int_{a \in [\![\sigma]\!]} [\![\mathtt{ret}\, M'(x_\sigma)]\!]\,\rho[x_\sigma \mapsto a](\{\top\}) d\nu \\
&= \int_{a \in [\![\sigma]\!]} \delta_{[\![M'(x_\sigma)]\!]\rho[x_\sigma \mapsto a]}(\{\top\}) d\nu \\
&= \int_{a \in [\![\sigma]\!]} \chi_U(a) d\nu = \nu(U),
\end{aligned}$$

so $[\![\bigcirc_{>r}(\mathtt{produce}(\mathtt{do}\, x_\sigma \leftarrow y_{\mathtt{V}\sigma}; \mathtt{ret}\, M'))]\!]\,\rho$ is equal to $\top$ if $r \ll \nu(U)$, $\perp$ otherwise. $\Box$

9.4 F Types

The *upper Vietoris topology* on $\mathcal{Q}^\top(X)$ (resp., $\mathcal{Q}^\top_\perp(X)$) has basic open sets $\Box U = \{Q \in \mathcal{Q}^\top(X) \mid Q \subseteq U\}$, where U ranges over the open subsets of X. The operator $\Box$ commutes with finite intersections and with directed suprema. Moreover, $\Box U$ is Scott-open if X is well-filtered.

Proposition 9.17 *Let X be a pointed, coherent, continuous dcpo. Let B_X be a basis of X, $\mathcal{S}_X$ be a subbase of the Scott topology on X. Then:*

- *The set $B_{\mathcal{Q}^\top_\perp X}$ consisting of $\perp$ plus the compact saturated sets of the form $\uparrow\{x_1, \cdots, x_n\}$, $n \in \mathbb{N}$, where each x_i is in B_X, is a basis of $\mathcal{Q}^\top_\perp(X)$.*
- *The set $\mathcal{S}_{\mathcal{Q}^\top_\perp X}$ of all opens $\Box U$, where U ranges over non-empty finite unions of elements of $\mathcal{S}_X$, plus the whole space $\mathcal{Q}^\top_\perp X$ itself, is a base of the Scott topology on $\mathcal{Q}^\top_\perp(X)$.*

Proof. By Proposition 4.2, item 1, $Q \ll Q'$ if and only if $Q = \perp$ or $Q' \subseteq \mathrm{int}(Q)$. Now $\mathrm{int}(Q)$ can be written as $\bigcup_{x \in Q \cap B_X} \twoheaduparrow x$, and since Q' is compact, if $Q' \subseteq \mathrm{int}(Q)$ then there are finitely many elements $x_1, \ldots, x_n$ of $Q \cap B_X$ such that $Q' \subseteq \bigcup_{i=1}^n \twoheaduparrow x_i = \mathrm{int}(\uparrow\{x_1, \cdots, x_n\})$. By Lemma 9.8, this shows the first part.

Let $\mathcal{U}$ be a Scott-open subset of $\mathcal{Q}^\top_\perp(X)$. If $\perp \in \mathcal{U}$, then $\mathcal{U}$ is the whole space, which is in $\mathcal{S}_{\mathcal{Q}^\top_\perp X}$. Otherwise, $\mathcal{U}$ is a Scott-open subset of $\mathcal{Q}^\top(X)$. By Proposition 4.1, item 1, $\mathcal{Q}^\top(X)$ is a continuous complete lattice, so $\mathcal{U}$ is a union of sets of the form $\twoheaduparrow Q$, where Q ranges over the elements of $\mathcal{U}$ belonging to any given basis, and $\twoheaduparrow$ is understood in $\mathcal{Q}^\top(X)$. Using the first part, we can take those elements Q of the form $\uparrow\{x_1, \cdots, x_n\}$, and then $\twoheaduparrow Q = \{Q \in \mathcal{Q}^\top(X) \mid Q' \subseteq \mathrm{int}(\uparrow\{x_1, \cdots, x_n\})\} = \Box\mathrm{int}(\uparrow\{x_1, \cdots, x_n\})$.

We can therefore write $\mathcal{U}$ as a union of sets $\Box U$, U open in X, and then we can write U as a union of finite intersections (taken in $\mathcal{Q}^\top(X)$) of elements of $\mathcal{S}_X$, hence as a directed union of finite unions of finite intersections of elements of $\mathcal{S}_X$, hence (by distributivity) as a directed union of finite intersections of finite unions of elements of $\mathcal{S}_X$. In $\mathcal{Q}^\top(X)$ (not $\mathcal{Q}^\top_\perp(X)$), $\Box$ commutes with directed unions and finite intersections (this would not hold for the empty intersection in $\mathcal{Q}^\top_\perp(X)$). The result follows. $\Box$

Corollary 9.18 *For every describable value type σ, $\mathbf{F}\sigma$ is a describable computation type.*

Proof. Let $X = [\![\sigma]\!]$, B_X be the basis of definable elements of $[\![\sigma]\!]$, and $\mathcal{S}_X$ be the subbase of definable open subsets at type σ, and let us use Proposition 9.17.

For every element $Q = \uparrow\{x_1, \cdots, x_n\}$ of $B_{\mathcal{Q}^\top_\perp X}$, where each x_i is in B_X, hence $x_i = [\![M_i]\!]$ for some ground term $M_i \colon \sigma$, the term $M = \mathtt{produce}\, M_1 \oslash \cdots \oslash \mathtt{produce}\, M_n$ ($\mathtt{abort}_{\mathbf{F}\sigma}$ if $n = 0$) defines Q, in the sense that $Q = [\![M]\!]$. The term $\Omega_{\mathbf{F}\sigma}$ defines $\perp$.

We deal with the second part. The whole space $[\![\mathbf{F}\sigma]\!]$ is definable as an open set by the term $\lambda x_{\mathbf{F}\sigma}.\mathtt{produce}\,\mathtt{ret}\,\underline{*}$. We consider the other elements $\Box U$ of $\mathcal{S}_{\mathcal{Q}^\top_\perp X}$. Let us write U as a finite union $U = \bigcup_{i=1}^m U_i$ of elements of $\mathcal{S}_X$, where U_i is defined by $M_i \colon \sigma \to \mathbf{FVunit}$ in the sense that $\tilde{\chi}_{U_i} = [\![M_i]\!]$. Then $\Box U$ is defined by $\lambda x_{\mathbf{F}\sigma}.x_{\mathbf{F}\sigma}$ $\mathtt{to}$ y_σ $\mathtt{in}$ $M(y_\sigma)$, where $M(y_\sigma) = (\bigcirc_{>1/2}(M_1 y_\sigma) \vee \cdots \vee \bigcirc_{>1/2}(M_m y_\sigma)); \mathtt{produce}\,\mathtt{ret}\,\underline{*}$. Indeed, for every environment ρ, letting $Q = \rho(x_{\mathbf{F}\sigma})$, if $Q = \perp$ then $[\![\lambda x_{\mathbf{F}\sigma}.x_{\mathbf{F}\sigma}\ \mathtt{to}\ y_\sigma\ \mathtt{in}\ M(y_\sigma)]\!]\,(\perp) = \perp$, matching the fact that Q is not in $\Box U$. Otherwise, using the fact that $[\![\bigcirc_{>1/2}(M_1 y_\sigma) \vee \cdots \vee \bigcirc_{>1/2}(M_m y_\sigma)]\!]\,\rho'$ is equal to $\top$ if $\rho'(y_\sigma) \in U$ and to $\perp$ otherwise, for every environment ρ', we obtain:

$$[\![x_{\mathbf{F}\sigma}\ \mathtt{to}\ y_\sigma\ \mathtt{in}\ M(y_\sigma)]\!]\,\rho = (\tilde{\chi}_U)^*(Q) = \bigwedge_{a \in Q} \tilde{\chi}_U(a),$$

by Proposition 4.2, item 2, and that is equal to $\{\delta_\top\}$ if $Q \subseteq U$, and to $\perp$ otherwise. $\Box$

9.5 Full Abstraction

By induction on types, using Lemma 9.2 ($\mathtt{unit}$), Lemma 9.3 ($\mathtt{int}$), Proposition 9.6 (product types), Proposition 9.14 (function types), Corollary 9.16 ($\mathbf{V}$ types), and Corollary 9.18 ($\mathbf{F}$ types), every type is describable (the case of $\mathbf{U}$ types is trivial).

Theorem 9.19 (Full abstraction) *CBPV*$(\mathtt{D}, \mathtt{P}) + \mathtt{pifz} + \bigcirc$ *is inequationally fully abstract. For every value type τ, for every two ground CBPV$(\mathtt{D}, \mathtt{P}) + \mathtt{pifz} + \bigcirc$ terms $M, N \colon \tau$, the following are equivalent:*

1. *$M \precsim^{app}_\tau N$;*
2. *$M \precsim_\tau N$;*

3. $[\![M]\!] \leq [\![N]\!]$.

Proof. The equivalence between 1 and 2 is Theorem 7.3. Item 3 implies item 1 by Proposition 7.6. In the converse direction, we assume that $[\![M]\!] \not\leq [\![N]\!]$ and we claim that there is a ground term $Q: \tau \to \mathbf{FVunit}$ such that $\Pr(QM\downarrow) \not\leq \Pr(QN\downarrow)$. Since $\leq$ is the specialization ordering of the Scott topology on $[\![\tau]\!]$, and the latter has a subbase of definable elements, there is a ground term $Q: \tau \to \mathbf{FVunit}$ such that $[\![M]\!] \in U$ and $[\![N]\!] \notin U$, where $\tilde{\chi}_U = [\![Q]\!]$. Hence $[\![QM]\!] = \tilde{\chi}_U([\![M]\!]) = \{\delta_\top\}$, while $[\![QN]\!] = \bot$. By adequacy (Proposition 6.10), and letting $h(\nu) = \nu(\{\top\})$, $\Pr(QM\downarrow) = h^*([\![QM]\!]) = 1$, while $\Pr(QN\downarrow) = 0$. $\square$

10 Conclusion and Open Problems

We started from the question of using call-by-push-value as a way of getting around our ignorance of the existence of a Cartesian-closed category of continuous dcpos that would be closed under the probabilistic powerdomain functor. This led us to define a pretty expressive call-by-push-value language with probabilistic choice and demonic non-determinism. We have gone so far as to show that it is inequationally fully abstract, once extended with parallel if **pifz** and statistical termination testers $\bigcirc$—and those are required for that.

One should note that both are implementable: **pifz** by standard dovetailing techniques, or more concretely by using threads, and $\bigcirc_{>b}M$ by guessing and checking a derivation of $[\_] \cdot M \downarrow b$, or more concretely by simulating all the execution traces of M and counting their probabilities. The latter can be done, concretely, by running M under a hypervisor that forks the process it emulates at each random binary choice $\oplus$: each subprocess that terminates after having gone through n random binary choices contributes $1/2^n$ to a global counter, and the hypervisor itself terminates when that counter exceeds b.

A few questions remain:

1. Is **pifz** definable in $\mathrm{CBPV}(\mathtt{D},\mathtt{P}) + \bigcirc$? Is $\mathrm{CBPV}(\mathtt{D},\mathtt{P}) + \bigcirc$ fully abstract? The results of Section 8.1 fail to answer those questions.

2. We have defined languages with an $\mathbf{abort}_{\mathbf{F}\sigma}$ operator, and where computation types are interpreted as continuous lattices. Would bc-domains be enough, namely, can we do without an $\mathbf{abort}_{\mathbf{F}\sigma}$ operator and still obtain a full abstraction result? Note that $\bigcirc_{>b}$ does not just estimate probabilities of termination, but also catches the exception raised by $\mathbf{abort}_{\mathbf{F}\sigma}$, hence serves more than one purpose.

3. Since the type $\mathbf{UF}\tau \to \mathbf{UF}\tau \to \mathbf{F}\tau$ is describable in $\mathrm{CBPV}(\mathtt{D},\mathtt{P}) + \bigcirc + \mathbf{pifz}$ for every value type τ, the binary supremum map on $[\![\mathbf{F}\tau]\!]$ is obtainable as a directed supremum of definable values. Whereas $\owedge$ implements demonic non-determinism, binary suprema implement *angelic* non-determinism. Is binary supremum itself definable?

References

[1] Samson Abramsky, Radha Jagadeesan, and Pasquale Malacaria. Full abstraction for PCF. *Information and Computation*, 163(2):409–470, 2000.

[2] Samson Abramsky and Achim Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Oxford University Press, 1994.

[3] Mauricio Alvarez-Manilla, Achim Jung, and Klaus Keimel. The probabilistic powerdomain for stably compact spaces. *Theoretical Computer Science*, 328(3):221–244, 2004.

[4] Thomas Ehrhard and Christine Tasson. Probabilistic call by push value. *Logical Methods in Computer Science*, 15(1), 2019. Also arXiv:1607.04690v4 [cs.LO], Aug. 2018.

[5] Thomas Ehrhard, Christine Tasson, and Michele Pagani. Probabilistic coherence spaces are fully abstract for probabilistic PCF. In Suresh Jagannathan and Peter Sewell, editors, *Proc. 41st Ann. ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '14)*, pages 309–320, 2014.

[6] Thomas Erker, Martín Hötzel Escardó, and Klaus Keimel. The way-below relation of function spaces over semantic domains. *Topology and Its Applications*, 89(1–2):61–74, 1998.

[7] Yuri L. Ershov. The bounded-complete hull of an α-space. *Theoretical Computer Science*, 175:3–13, 1997.

[8] Gerhard Gierz, Karl Heinrich Hofmann, Klaus Keimel, Jimmie D. Lawson, Michael Mislove, and Dana S. Scott. *Continuous Lattices and Domains*, volume 93 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2003.

[9] Jean Goubault-Larrecq. De Groot duality and models of choice: Angels, demons, and nature. *Mathematical Structures in Computer Science*, 20(2):169–237, April 2010.

[10] Jean Goubault-Larrecq. *Non-Hausdorff Topology and Domain Theory—Selected Topics in Point-Set Topology*, volume 22 of *New Mathematical Monographs*. Cambridge University Press, March 2013.

[11] Jean Goubault-Larrecq. Full abstraction for non-deterministic and probabilistic extensions of PCF I: the angelic cases. *Journal of Logic and Algebraic Methods in Programming*, 84(1):155–184, January 2015.

[12] J. Martin E. Hyland and Luke Ong. On full abstraction for PCF: I, II and III. *Information and Computation*, 163(2):285–408, 2000.

[13] Claire Jones. *Probabilistic Non-Determinism.* PhD thesis, University of Edinburgh, 1990. Technical Report ECS-LFCS-90-105.

[14] Achim Jung and Regina Tix. The troublesome probabilistic powerdomain. In A. Edalat, A. Jung, K. Keimel, and M. Kwiatkowska, editors, *Proc. 3rd Workshop on Computation and Approximation*, volume 13, pages 70–91. Elsevier, 1998. 23pp.

[15] Shin-Ya Katsumata. A semantic formulation of $\top\top$-lifting and logical predicates for computational metalanguage. In L. Ong, editor, *Proc. 19th Intl. Workshop CSL 2005, 14th Ann. Conf. of the EACSL*, pages 87–102. Springer Verlag LNCS 3634, 2005.

[16] Olaf Kirch. *Bereiche und Bewertungen.* Master's thesis, Technische Hochschule Darmstadt, June 1993.

[17] Paul Blain Levy. Call-by-Push-Value: A Subsuming Paradigm. In J.-Y. Girard, editor, *Typed Lambda Calculi and Applications*, pages 228–243. Springer Verlag LNCS 1581, 1999.

[18] Paul Blain Levy. *Call-by-Push-Value. A Functional/Imperative Synthesis.* Semantic Structures in Computation. Springer Verlag, 2003.

[19] Gordon D. Plotkin. LCF considered as a programming language. *Theoretical Computer Science*, 5(1):223–255, 1977.

[20] Thomas Streicher. *Domain-Theoretic Foundations of Functional Programming.* World Scientific, 2006.

[21] Jean-Pierre Talpin and Pierre Jouvelot. The type and effect discipline. *Information and Computation*, 111(2):245–296, 1994.

[22] Regina Tix. *Stetige Bewertungen auf topologischen Räumen.* Diplomarbeit, TH Darmstadt, June 1995.

[23] Matthijs Vákár, Ohad Kammar, and Sam Staton. A domain theory for statistical probabilistic programming. In *Proc. 46th ACM Symp. Principles of Programming Languages (POPL'19)*, 2019. arXiv:1811.04196 [cs.LO].