Equationally Fully Abstract Models of PCF [1]

Allen Stoughton

Computer Science and Artificial Intelligence
School of Cognitive and Computing Sciences
University of Sussex
Falmer, Brighton BN1 9QH, England

1 Introduction

In Plotkin's applied typed lambda calculus PCF [Plo] it is natural to consider one term *operationally less defined* than another iff whenever the first term converges to a constant in a ground context, then the second term converges to the same constant in that context. Two terms are considered *operationally equivalent* iff each is less defined than the other, i.e., they have the same behaviour in all ground contexts. Terms are thus equivalent when they are interchangeable in complete programs. See [Mey] and [Sto] for detailed discussions of these concepts.

Over a decade ago, Robin Milner showed the existence of a unique order-extensional model of PCF that is *inequationally fully abstract* in the sense that one term is operationally less defined than another exactly when the meaning of the first is less than that of the second in the model [Mil]. (Models that consist of functions are called extensional; when in addition these functions are ordered pointwise, the models are called order-extensional.) Milner constructed this model using term model techniques, and considerable effort has been expended in attempts to synthesize his model in a more natural or semantic way; see [BerCurLév] for a survey of this work.

In practice, term equivalence is probably of greater interest than term ordering, and this suggests that one consider models that are *equationally fully abstract* in the sense that two terms are operationally equivalent exactly when they are mapped to the same semantic value. Milner's inequationally fully abstract model is clearly equationally fully abstract, and it is natural to ask whether there exist equationally fully abstract models that are not inequationally fully abstract. The purpose of this paper is to answer this question in the affirmative, and to begin the study of the category **E** of extensional, equationally fully abstract models and structure-preserving functions.

The paper's main results are as follows:

(i) **E** is a pre-ordering with arbitrary products and coproducts and whose initial and terminal objects are not isomorphic.

(ii) All objects of **E** are strongly algebraic (SFP) and all isolated elements of these models are definable by terms.

(iii) There is a morphism from an object $\mathcal{A}$ to an object $\mathcal{B}$ of **E** iff $\mathcal{B}$ relates at least as many pairs of terms as does $\mathcal{A}$ (i.e., if the meaning of M is less than that of N in $\mathcal{A}$, then the meaning of M is less than that of N in $\mathcal{B}$).

[1]Appears in *Fifth International Conference on the Mathematical Foundations of Programming Semantics*, Lecture Notes in Computer Science, vol. 442, pp. 271–283, Springer-Verlag, 1990.

(iv) Objects of **E** that relate the same pairs of terms are isomorphic.

(v) The initial object of **E** is also initial in the category of (not necessarily extensional) equationally fully abstract models.

(vi) The terminal object of **E** is order-extensional and inequationally fully abstract, i.e., is Milner's original model.

2 Preliminaries

The reader is assumed to be familiar with such standard domain-theoretic concepts as complete partial orders (cpo's), continuous functions, and ω-algebraic, strongly algebraic and consistently complete cpo's.

A function $f: P \to Q$ over posets is an *order-embedding* iff for all $p_1, p_2 \in P$, $p_1 \sqsubseteq p_2$ iff $f\,p_1 \sqsubseteq f\,p_2$.

In the sequel we will make essential use of Berry's category of dI-domains and stable functions, the definitions of which we now review. A *dI-domain* P is an ω-algebraic, consistently complete cpo such that

(i) $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$, for all $x, y, z \in P$ such that $\{y, z\}$ is consistent; and

(ii) for all isolated $p \in P$, $\{\, p' \in P \mid p' \sqsubseteq p \,\}$ is finite.

A function $f: P \to Q$ between dI-domains is *stable* iff it is continuous and for all $p \in P$ and $q \in Q$ such that $q \sqsubseteq f\,p$, there exists a least $p' \in P$ such that $p' \sqsubseteq p$ and $q \sqsubseteq f\,p'$. Given dI-domains P and Q, the poset $P \underset{s}{\to} Q$ consists of the set of all stable functions from P to Q, with the *stable ordering*: $f \sqsubseteq g$ iff

(i) $f\,p \sqsubseteq g\,p$, for all $p \in P$; and

(ii) for all $p, p' \in P$ and $q \in Q$, if $q \sqsubseteq f\,p$, $p' \sqsubseteq p$ and $q \sqsubseteq g\,p'$ then $q \sqsubseteq f\,p'$.

In [Ber], it is shown that the collection of dI-domains is closed under $\underset{s}{\to}$, and that the category of dI-domains and stable functions, ordered with the stable ordering, is a cpo-enriched cartesian closed category.

To see that the stable ordering is finer than the pointwise ordering, define functions $f, g: N_\perp \to N_\perp$ by

$$f\,x = \begin{cases} \perp & \text{if } x = \perp, \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

and $g\,x = 0$. Then f is less than g in the pointwise ordering, but not in the stable ordering.

3 Fully Abstract Models of Programming Languages

In this section, we recall—very briefly—the definitions and results from [Sto] that will be required in the sequel. A gentle introduction to this material can be found in this reference.

The reader is assumed to be familiar with many-sorted signatures Σ over sets of sorts S, as well as algebras over such signatures. Signatures are assumed to contain distinguished constants Ω_s at each sort s, which intuitively stand for divergence. We use uppercase script letters ($\mathcal{A}$, $\mathcal{B}$, etc.) to denote algebras and the corresponding italic letters (A, B, etc.) to stand for their carriers. We write $\mathcal{T}_\Sigma$ (or just $\mathcal{T}$) for the initial (term) algebra, so that T_s is the set of terms of sort s. Given an algebra $\mathcal{A}$ and a term t of sort s, $[\![t]\!]_\mathcal{A}$ (or just $[\![t]\!]$) is the meaning of t in A_s, i.e., the image of t under the unique homomorphism from $\mathcal{T}$ to $\mathcal{A}$. An algebra is *reachable* iff all of its elements are denotable (definable) by terms. A pre-ordering over an algebra is *substitutive* iff it is respected by all of the operations of that algebra. Substitutive equivalence relations are called *congruences*, as usual. A pre-ordering over an algebra in which the Ω constants are least elements at all sorts is referred to as Ω-*least*. The congruence over $\mathcal{T}$ that is induced by an algebra $\mathcal{A}$ is called $\approx_{\mathcal{A}}$: two terms are congruent when they are mapped to the same element of A. When we say that $c[v_1, \ldots, v_n]$ is a *derived operator* of type $s_1 \times \cdots \times s_n \to s'$, this means that c is a context of sort s' over context variables v_i of sort s_i. We write $c_{\mathcal{A}}$ for the corresponding *derived operation* over an algebra $\mathcal{A}$.

Familiarity with *ordered algebras*, i.e., algebras whose carriers are S-indexed families of posets with least elements denoted by the Ω constants, and whose operations are monotone functions, is also assumed. Such an algebra is called *complete* when its carrier is a cpo and operations are continuous, and a homomorphism over complete ordered algebras is called *continuous* when it is continuous on the underlying cpo's. Two complete ordered algebras are *order-isomorphic* iff there exists a continuous homomorphism from one to the other that is a surjective order-embedding on the underlying cpo's. In any full subcategory of the category of complete ordered algebras and continuous homomorphisms, objects are isomorphic exactly when they are order-isomorphic. We write $\mathcal{OT}_\Sigma$ (or just $\mathcal{OT}$) for the initial ordered algebra, which consists of $\mathcal{T}$ with the "Ω-match" ordering: one term is less than another when the second can be formed by replacing occurrences of Ω in the first by terms. A complete ordered algebra is called *inductively reachable* iff all of its elements can be reached by the following transfinite process: start with the denotable elements, and close under lub's of directed sets. Complete ordered algebras whose carriers are ω-algebraic and whose isolated elements are all denotable are thus inductively reachable, but the converse is false. The Ω-least substitutive pre-ordering over $\mathcal{T}$ that is induced by an ordered algebra $\mathcal{A}$ is called $\preceq_{\mathcal{A}}$: one term is less than another when the meaning of the first is less than that of the second in A.

If $P \subseteq S$, $\mathcal{A}$ is an algebra and R is a pre-ordering over $A|P$ then R^c, the *contextualization* of R, is the relation over A defined by: $a \, R^c_s \, a'$ iff $c\langle a\rangle \, R_p \, c\langle a'\rangle$, for all derived operators $c[v]$ of type $s \to p$, $p \in P$.

Lemma 3.1 *If $P \subseteq S$, $\mathcal{A}$ is a reachable algebra and R is a pre-ordering (respectively, equivalence relation) over $A|P$ then R^c is the greatest substitutive pre-ordering (respectively, congruence) over $\mathcal{A}$ whose restriction to P is included in R.*

Proof. See lemmas 2.2.25 and 2.2.29 of [Sto]. $\square$

Let $\approx$ be a congruence over $\mathcal{T}$ and $\mathcal{A}$ be an algebra. Then $\mathcal{A}$ is $\approx$-*equationally correct* iff $\approx_{\mathcal{A}} \subseteq \approx$, and $\approx$-*equationally fully abstract* iff $\approx_{\mathcal{A}} = \approx$.

Let $\preceq$ be an Ω-least substitutive pre-ordering over $\mathcal{T}$ and $\mathcal{A}$ be an ordered algebra. Then $\mathcal{A}$ is $\preceq$-*inequationally correct* iff $\preceq_{\mathcal{A}} \subseteq \preceq$, and $\preceq$-*inequationally fully abstract* iff $\preceq_{\mathcal{A}} = \preceq$.

Let $\approx$ be a congruence over $\mathcal{T}$ and $\mathcal{A}$ be an algebra. Then $\mathcal{A}$ is $\approx$-*contextually correct* iff for all derived operators $c_1[v_1, \ldots, v_n]$ and $c_2[v_1, \ldots, v_n]$ of type $s_1 \times \cdots \times s_n \to s'$,

$$\text{if } c_{1\mathcal{A}} = c_{2\mathcal{A}} \text{ then for all } t_i \in T_{s_i}, 1 \le i \le n,\ c_1\langle t_1, \ldots, t_n\rangle \approx_{s'} c_2\langle t_1, \ldots, t_n\rangle,$$

and $\mathcal{A}$ is $\approx$-*contextually fully abstract* iff for all derived operators $c_1[v_1, \ldots, v_n]$ and $c_2[v_1, \ldots, v_n]$ of type $s_1 \times \cdots \times s_n \to s'$,

$$c_{1\mathcal{A}} = c_{2\mathcal{A}} \text{ iff for all } t_i \in T_{s_i}, 1 \le i \le n,\ c_1\langle t_1, \ldots, t_n\rangle \approx_{s'} c_2\langle t_1, \ldots, t_n\rangle.$$

Theorem 3.2 *Suppose $\mathcal{A}$ is an inductively reachable complete ordered algebra and $\approx$ is a congruence over $\mathcal{T}$. Then $\mathcal{A}$ is $\approx$-fully abstract iff $\mathcal{A}$ is $\approx$-contextually fully abstract.*

Proof. See theorem 5.3.1 of [Sto]. $\square$

A *family of least fixed point constraints* Φ is an S-indexed family of sets such that for all $s \in S$, $\Phi_s \subseteq T_s \times \mathcal{P}T_s$, and for all $\langle t, T' \rangle \in \Phi_s$, T' is a directed set in OT_s. We write $t \equiv \bigsqcup T'$ instead of $\langle t, T' \rangle$ for elements of Φ_s.

A family of least fixed point constraints Φ is *closed* iff for all $\sigma \in \Sigma$ of type $s_1 \times \cdots \times s_n \rightarrow s'$, if $t_i \equiv \bigsqcup T'_i \in \Phi_{s_i}$, $1 \leq i \leq n$, and T'' is a cofinal subset of $\sigma(T'_1 \times \cdots \times T'_n)$ then $\sigma\langle t_1, \ldots, t_n \rangle \equiv \bigsqcup T'' \in \Phi_{s'}$. We write $\overline{\Phi}$ for the *closure* of Φ, i.e., the least closed family of least fixed point constraints containing Φ.

A complete ordered algebra $\mathcal{A}$ *satisfies* Φ iff for all $t \equiv \bigsqcup T' \in \Phi_s$, $s \in S$, $[\![t]\!] = \bigsqcup \{ [\![t']\!] \mid t' \in T' \}$. An Ω-least substitutive pre-ordering $\preceq$ over $\mathcal{T}$ *satisfies* Φ iff for all $t \equiv \bigsqcup T' \in \Phi_s$, $s \in S$, t is a lub of T' in $\langle T_s, \preceq_s \rangle$.

Lemma 3.3 *Let Φ be a family of least fixed point constraints and $\mathcal{A}$ be a complete ordered algebra. If $\mathcal{A}$ satisfies Φ, then $\mathcal{A}$ satisfies $\overline{\Phi}$.*

Proof. See lemma 3.2.7 of [Sto]. $\square$

Lemma 3.4 *Let $\mathcal{A}$ be a complete ordered algebra that satisfies Φ, and $P \subseteq S$. Define a pre-ordering $\preceq$ over $T|P$ by: $t_1 \preceq_p t_2$ iff $[\![t_1]\!] \sqsubseteq_p [\![t_2]\!]$. Then $\preceq^c$ is an Ω-least substitutive pre-ordering over $\mathcal{T}$ that satisfies $\overline{\Phi}$.*

Proof. See the proofs of lemma 4.1.1 and theorem 7.1.1 of [Sto]. $\square$

Theorem 3.5 *Suppose Φ is a closed family of least fixed point constraints and $\preceq$ is an Ω-least substitutive pre-ordering over $\mathcal{T}$ that satisfies Φ. There exists an inductively reachable, $\preceq$-inequationally fully abstract, complete ordered algebra $\mathcal{I}(\preceq, \Phi)$ satisfying Φ, such that if $\mathcal{A}$ is a complete ordered algebra satisfying Φ with the property that $\preceq \subseteq \preceq_{\mathcal{A}}$, then there is a unique continuous homomorphism $h{:}\, \mathcal{I}(\preceq, \Phi) \rightarrow \mathcal{A}$.*

Proof. See theorem 5.1.3 and corollary 5.1.6 of [Sto]. $\square$

4 Syntax and Semantics of PCF

In this section, we collect together the various definitions and theorems about the syntax and semantics of PCF that we require in the sequel. For technical simplicity, we have chosen to work with a combinatory logic version of PCF with a single ground type ι, whose intended interpretation is the natural numbers. From the viewpoint of the conditional operations, zero is interpreted as false and non-zero as true.

We begin by defining the syntax of PCF, i.e., its signature. The sorts of this signature consists of PCF's types. The set of *sorts* S is least such that

(i) $\iota \in S$, and

(ii) $s_1 \rightarrow s_2 \in S$ if $s_1 \in S$ and $s_2 \in S$.

Define ι^n, for $n \in \omega$, by: $\iota^0 = \iota$ and $\iota^{n+1} = \iota \rightarrow \iota^n$. The *signature* Σ over S has the following operators:

(i) Ω_s of type s,
(ii) K_{s_1,s_2} of type $(s_1 \rightarrow s_2 \rightarrow s_1)$,
(iii) S_{s_1,s_2,s_3} of type $((s_1 \rightarrow s_2 \rightarrow s_3) \rightarrow (s_1 \rightarrow s_2) \rightarrow s_1 \rightarrow s_3)$,
(iv) Y_s of type $((s \rightarrow s) \rightarrow s)$,
(v) n of type ι, for $n \in \omega$,
(vi) *Succ* and *Pred* of type $(\iota \rightarrow \iota)$,
(vii) *If*$_s$ of type $(\iota \rightarrow s \rightarrow s \rightarrow s)$, and
(viii) $\cdot_{s_1,s_2}$ of type $(s_1 \rightarrow s_2) \times s_1 \rightarrow s_2$,

where the compound sorts are parenthesized in order to avoid confusion. Thus $\cdot$ (application) is a binary operator, and all of the other operators are nullary. In keeping with standard practice, we usually abbreviate $M \cdot N$ to $M\,N$, and let application associate to the left.

Next, we define several combinators that will be required below. We confuse use and mention for these combinators: given a combinator C, we also write C for its denotation in any model that may be at hand.

For $s \in S$, we write I_s for the term $S_{s,s\rightarrow s,s}\,K_{s,s\rightarrow s}\,K_{s,s}$ of sort $s \rightarrow s$. I will be the identity operation in all models. For $s \in S$, define approximations Y_s^n to Y_s of sort $(s \rightarrow s) \rightarrow s$ by

$$Y_s^0 = \Omega_{(s\rightarrow s)\rightarrow s}, \qquad Y_s^{n+1} = S_{s\rightarrow s,s,s}\,I_{s\rightarrow s}\,Y_s^n,$$

so that Y_s^n is an ω-chain in $OT_{(s\rightarrow s)\rightarrow s}$. For all $n \in \omega$ and $s \in S$, define syntactic projections Ψ_s^n of sort $s \rightarrow s$ by

$$\Psi_\iota^n = Y_{\iota\rightarrow\iota}^n\,F, \qquad \Psi_{s_1\rightarrow s_2}^n = \lambda x.\,\lambda y.\,(\Psi_{s_2}^n(x(\Psi_{s_1}^n\,y))),$$

where F of sort $(\iota \rightarrow \iota) \rightarrow \iota \rightarrow \iota$ is

$$\lambda x.\,\lambda y.\,(\mathit{If}\;y\,(\mathit{Succ}(x(\mathit{Pred}\;y)))\,0).$$

Expanding the abstractions, one can see that the Ψ_s^n form an ω-chain in $OT_{s\rightarrow s}$. Let the equality test Eq of sort $\iota \rightarrow \iota \rightarrow \iota$ be

$$Y(\lambda z.\,\lambda x.\,\lambda y.(\mathit{If}\;x\,(\mathit{If}\;y\,(z(\mathit{Pred}\;x)(\mathit{Pred}\;y))\,0)\,(\mathit{If}\;y\,0\,1))).$$

Eq yields 1 for true and 0 for false. Define glb operators *Inf*$_s$ of sort $s \rightarrow s \rightarrow s$ by

$$\begin{aligned} \mathit{Inf}_\iota &= \lambda x.\,\lambda y.\,(\mathit{If}\;(Eq\;x\;y)\;x\;\Omega), \\ \mathit{Inf}_{s_1\rightarrow s_2} &= \lambda x.\,\lambda y.\,\lambda z.\,(\mathit{Inf}_{s_2}(x\;z)(y\;z)). \end{aligned}$$

For $n \in \omega$, define operators And_n of sort ι^n by: $And_0 = 1$ and

$$And_{n+1} = \lambda x.\,\lambda y_1.\,\ldots\,\lambda y_n.\,(\mathit{If}\;x\,(And_n\,y_1\;\cdots\;y_n)\,0).$$

Define step operators St_n of sort $\iota \rightarrow \iota$, for $n \in \omega$, by

$$St_n = \lambda x.\,(\mathit{If}\;(Eq\;n\;x)\,1\,\Omega).$$

St_n yields true (1) if its argument is n, and diverges otherwise. Define alternative identify operators I'_s of sort $s \rightarrow s$ by

$$I'_\iota = Y_{\iota\rightarrow\iota}\, F, \qquad I'_{s_1\rightarrow s_2} = \lambda x.\, \lambda y.\, (I'_{s_2}(x(I'_{s_1}\, y))).$$

I' will be identical to I in some models.

A *model* $\mathcal{A}$ of PCF is a complete ordered algebra such that the following conditions hold:

(i) A_ι is the flat cpo

$$\begin{tikzcd} 0_\mathcal{A} & 1_\mathcal{A} & 2_\mathcal{A} & \cdots \\ & \bot_\iota \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & & \end{tikzcd} ;$$

(ii) For all $s_1, s_2 \in S$, $a_1 \in A_{s_1}$ and $a_2 \in A_{s_2}$, $K_{s_1,s_2}\, a_1\, a_2 = a_1$;

(iii) For all $s_1, s_2, s_3 \in S$, $a_1 \in A_{s_1\rightarrow s_2\rightarrow s_3}$, $a_2 \in A_{s_1\rightarrow s_2}$ and $a_3 \in A_{s_1}$, $S_{s_1,s_2,s_3}\, a_1\, a_2\, a_3 = a_1\, a_3\, (a_2\, a_3)$;

(iv) For all $s \in S$, $Y_s = \bigsqcup_{n\in\omega} Y_s^n$;

(v) For all $a \in A_\iota$, $Succ\, a$ is equal to $\bot_\iota$, if $a = \bot_\iota$, and is equal to $a+1$, if $a \in \omega$;

(vi) For all $a \in A_\iota$, $Pred\, a$ is equal to $\bot_\iota$, if $a = \bot_\iota$, is equal to 0, if $a = 0$, and is equal to $a - 1$, if $a \in N - \{0\}$.

(vii) For all $s \in S$, $a_1 \in A_\iota$, and $a_2, a_3 \in A_s$, $If_s\, a_1\, a_2\, a_3$ is equal to $\bot_s$, if $a_1 = \bot_\iota$, is equal to a_2, if $a_1 \in N - \{0\}$, and is equal to a_3, if $a_1 = 0$.

A model $\mathcal{A}$ is *extensional* iff for all $a_1, a_2 \in A_{s_1\rightarrow s_2}$, if $a_1\, a = a_2\, a$, for all $a \in A_{s_1}$, then $a_1 = a_2$, and *order-extensional* iff for all $a_1, a_2 \in A_{s_1\rightarrow s_2}$, if $a_1\, a \sqsubseteq_{s_2} a_2\, a$, for all $a \in A_{s_1}$, then $a_1 \sqsubseteq_{s_1\rightarrow s_2} a_2$. Finally, *morphisms* between models are simply continuous homomorphisms between the complete ordered algebras.

Application is left-strict in all models $\mathcal{A}$ since $\bot_{s_1\rightarrow s_2} \sqsubseteq_{s_1\rightarrow s_2} K_{s_2,s_1}\, \bot_{s_2}$, and thus $\bot_{s_1\rightarrow s_2}\, a \sqsubseteq_{s_2} K_{s_2,s_1}\, \bot_{s_2}\, a = \bot_{s_2}$, for all $a \in A_{s_1}$.

The following theorem introduces the *stable function model*, which features prominently below [Ber][BerCurLév].

Theorem 4.1 (Berry) *There is a unique model* $\mathcal{A}$ *constructed from the category of dI-domains and stable functions in the natural way, i.e., such that* $A_\iota = N_\bot$, $A_{s_1\rightarrow s_2} = A_{s_1} \xrightarrow[s]{} A_{s_2}$, $a_1 \cdot a_2 = a_1\, a_2$, *and* $n_\mathcal{A} = n$. $\mathcal{A}$ *is extensional but not order-extensional.*

The following theorem is proved by making use of an operational semantics for PCF; see theorem 3.1 of [Plo].

Theorem 4.2 (Plotkin) *For all models* $\mathcal{A}$ *and* $\mathcal{B}$ *and terms* M *of sort* ι, $[\![M]\!]_\mathcal{A} = [\![M]\!]_\mathcal{B}$.

This theorem allows us to define the meaning $[\![M]\!] \in N_\bot$ of a term M of sort ι to be $[\![M]\!]_\mathcal{A}$, for an arbitrary model $\mathcal{A}$.

We now define notions of program ordering and equivalence for PCF. Define a pre-ordering $\precsim$ over $T|\{\iota\}$ by: $M \precsim_\iota N$ iff $[\![M]\!] \sqsubseteq [\![N]\!]$, and let $\approx$ be the equivalence relation over $T|\{\iota\}$ induced by $\precsim$. Then, $\precsim^c$ is an Ω-least substitutive pre-ordering over $\mathcal{T}$, $\approx^c$ is a congruence over $\mathcal{T}$, and $\precsim^c$ induces $\approx^c$.

Specializing the notions of the previous section, we say that a model is

(i) *inequationally correct* iff it is $\precsim^c$-*inequationally correct*;

(ii) *inequationally fully abstract* iff it is $\precsim^c$-*inequationally fully abstract*;

(iii) *equationally correct* iff it is $\approx^c$-*equationally correct*;

(iv) *equationally fully abstract* iff it is $\approx^c$-*equationally fully abstract*;

(v) *contextually correct* iff it is $\approx^c$-*contextually correct*; and

(vi) *contextually fully abstract* iff it is $\approx^c$-*contextually fully abstract*.

It is not hard to show that all models are inequationally, equationally and contextually correct. Clearly inequational full abstraction implies equational full abstraction, but the converse, as we shall see, is false. The stable function model is not even equationally fully abstract [Ber][BerCurLév].

Finally, we recall Milner's important result concerning the order-extensional nature of $\precsim^c$ and the extensional nature of $\approx^c$; see lemma 4.1.11 of [Cur].

Theorem 4.3 (Milner) (i) $\precsim^c_\iota = \precsim_\iota$ *and* $\approx^c_\iota = \approx_\iota$.

(ii) *For all* $M_1, M_2 \in T_{s_1 \to s_2}$, $M_1 \precsim^c_{s_1 \to s_2} M_2$ *iff for all* $N \in T_{s_1}$, $M_1\, N \precsim^c_{s_2} M_2\, N$.

(iii) *For all* $M_1, M_2 \in T_{s_1 \to s_2}$, $M_1 \approx^c_{s_1 \to s_2} M_2$ *iff for all* $N \in T_{s_1}$, $M_1\, N \approx^c_{s_2} M_2\, N$.

From theorem 4.3 (i), we know that for all terms M of sort ι, either $M \approx^c_\iota \Omega$ or $M \approx^c_\iota n$, for some $n \in \omega$.

5 Equationally Fully Abstract Models

This section consists of the paper's main results, concerning the category **E** of extensional, equationally fully abstract models and their morphisms. To begin with, we introduce our main technical device. Let Φ be the family of least fixed point constraints such that

$$\Phi_{(s \to s) \to s} = \{ Y_s \equiv \bigsqcup \{ Y^n_s \mid n \in \omega \} \},$$

for all $s \in S$, and $\Phi_s = \emptyset$, whenever s does not have the form $(s' \to s') \to s'$. A *least fixed point ordering* $\preceq$ is an Ω-least substitutive pre-ordering over $\mathcal{T}$ that induces $\approx^c$ and satisfies $\overline{\Phi}$. We write **L** for the set of all least fixed point orderings, ordered by inclusion.

By lemma 3.3, all models satisfy $\overline{\Phi}$. Lemma 3.4 allows us to conclude that $\precsim^c$ is an element of **L**.

Lemma 5.1 *For all least fixed point orderings* $\preceq$ *and terms* M, N *of sort* ι, $M \preceq_\iota N$ *iff either* $M \approx^c_\iota \Omega$ *or* $M \approx^c_\iota N$. *Thus, all least fixed point orderings agree at sort* ι.

Proof. Suppose that $\preceq \in \mathbf{L}$ and $m \preceq_\iota n$, for $m, n \in \omega$. Define a term M of sort $\iota \to \iota$ which yields n when applied to m and m when applied to n. Then $n \approx^c_\iota M\, m \preceq_\iota M\, n \approx^c_\iota m$, showing that $n \preceq_\iota m$, and thus $m \approx^c_\iota n$. The rest follows easily. □

Lemma 5.2 *Let* $\mathcal{A}$ *be an extensional model and* $P = \{\iota, \iota \to \iota\}$. *Define a pre-ordering* $\preceq$ *over* $T|P$ *by:* $M \preceq_p N$ *iff* $[\![M]\!] \sqsubseteq_p [\![N]\!]$. *Then* $\preceq^c$ *is a least fixed point ordering.*

Proof. By lemma 3.4, all that remains to be shown is that $\preceq^c \cap \succeq^c = \approx^c$. Clearly, $\preceq^c \subseteq \precsim^c$, and thus $\preceq^c \cap \succeq^c \subseteq \approx^c$. For the opposite inclusion, suppose that $M_1 \approx^c_s M_2$, and let $c[v]$ be a derived operator of type $s \to (\iota \to \iota)$. We must show that $[\![c\langle M_1\rangle]\!] = [\![c\langle M_2\rangle]\!]$, and since $\mathcal{A}$ is extensional and all elements of A_ι are denotable, it suffices to show that $[\![c\langle M_1\rangle\, N]\!] = [\![c\langle M_2\rangle\, N]\!]$, for all terms N of sort ι. But this follows from the assumption that $M_1 \approx^c_s M_2$. □

Theorem 5.3 **L** *is a nontrivial complete lattice whose greatest element is* $\precapprox^c$.

Proof. We have already observed that $\precapprox^c \in \mathbf{L}$. To see that **L** is nontrivial, let $\mathcal{A}$ be the stable function model, and define $\preceq$ as in the statement of lemma 5.2. The lemma then allows us to conclude that $\preceq^c \in \mathbf{L}$. To see that $\precapprox^c$ and $\preceq^c$ are distinct, define terms M, N of sort $\iota \to \iota$ by $M = \lambda x. (\mathit{If}\, x\, 0\, 0)$ and $N = \lambda x. 0$. Then $M \precapprox^c_{\iota\to\iota} N$ by theorem 4.3 (ii), but $M \not\preceq^c_{\iota\to\iota} N$ since M is not less than N in $A_{\iota\to\iota}$.

Showing that **L** is closed under arbitrary nonempty intersections is straightforward, and it remains to show that $\precapprox^c$ is the greatest element of **L**. Suppose that $\preceq \in \mathbf{L}$, $M \preceq_s N$ and let $c[v]$ be a derived operator of type $s \to \iota$. Then $c\langle M\rangle \preceq_\iota c\langle N\rangle$, and thus $c\langle M\rangle \precapprox_\iota c\langle N\rangle$ by lemma 5.1. But then $M \precapprox^c_s N$, as required. □

We write $\preceq_0$ for the least element of **L**.

Theorem 5.4 *For each least fixed point ordering* $\preceq$, *there is an inductively reachable,* $\preceq$-*inequationally fully abstract model* $\mathcal{M}(\preceq)$, *such that for all models* $\mathcal{A}$ *with the property that* $\preceq \subseteq \preceq_{\mathcal{A}}$, *there is a unique morphism from* $\mathcal{M}(\preceq)$ *to* $\mathcal{A}$. *In particular,* $\mathcal{M}(\preceq)$ *is initial in the category of* $\preceq$-*inequationally fully abstract models and their morphisms.*

Proof. By theorem 3.5, we know all that is necessary about $\mathcal{M}(\preceq)$ except conditions (i)–(iii) and (v)–(vii) of the definition of model. Condition (i) holds since the denotable elements are ordered properly (lemma 5.1) and $\mathcal{M}(\preceq)$ is inductively reachable. The remaining conditions can be expressed by sets of equations (pairs of derived operators), and these equations hold in $\mathcal{M}(\preceq)$ since it is contextually fully abstract (theorem 3.2) and all models are contextually correct. □

$\mathcal{M}(\preceq)$ is uniquely specified, up to order-isomorphism.

A model $\mathcal{A}$ is *syntactically strongly algebraic* (or *syntactically SFP*) iff the following conditions hold:

(i) $\Psi^n_s(\Psi^n_s\, a) = \Psi^n_s\, a$, for all $a \in A_s$, $n \in \omega$ and $s \in S$;

(ii) $a = \bigsqcup_{n\in\omega}(\Psi^n_s\, a)$, for all $a \in A_s$ and $s \in S$; and

(iii) $\{\, \Psi^n_s\, a \mid a \in A_s \,\}$ is finite, for all $n \in \omega$ and $s \in S$.

The carrier of any syntactically SFP model is clearly SFP. Furthermore, if such a model is inductively reachable then $\Psi^n_s\, a$ is isolated and thus denotable, for all $a \in A_s$ and $n \in \omega$.

Lemma 5.5 (Milner) (i) *Extensional models are syntactically SFP.*

(ii) *For all models* $\mathcal{A}$ *and* $a_1, a_2 \in A_\iota$, $\mathit{Inf}_\iota\, a_1\, a_2$ *is the glb of* a_1 *and* a_2. *If* $\mathcal{A}$ *is order-extensional, then for all* $s \in S$ *and* $a_1, a_2 \in A_s$, $\mathit{Inf}_s\, a_1\, a_2$ *is the glb of* a_1 *and* a_2.

(iii) *The carriers of order-extensional models are Scott domains, i.e., consistently complete,* ω-*algebraic cpo's.*

Proof. (i) and (ii) are straightforward inductions on S. For (iii), each A_s is ω-algebraic, by part (i). For consistent completeness, it suffices to show that each consistent pair a_1, a_2 of isolated elements of A_s has a lub. Let $n \in \omega$ be such that $\Psi^n\, a_i = a_i$, for $i = 1, 2$, and $X = \{\, \Psi^n\, a \mid a \sqsupseteq_s \{a_1, a_2\}\,\}$. Then X is nonempty and finite, and thus has a glb z, by part (ii). But z is easily seen to be the lub of a_1 and a_2. □

Lemma 5.5 tells us, in particular, that the stable function model is syntactically SFP.

Theorem 5.6 *Inductively reachable, equationally fully abstract models are syntactically SFP and extensional. If, in addition, a model is inequationally fully abstract, then it is order-extensional.*

Proof. Let $\mathcal{A}$ be such a model. Condition (i) of the definition of syntactic strong algebraicity holds, since $\mathcal{A}$ is contextually fully abstract and (i) holds in, e.g., the stable function model, which is contextually correct. Expanding the identifier abstractions, one can see that $I'_s \equiv \bigsqcup \{ \Psi^n_s \mid n \in \omega \} \in \overline{\Phi}_{s \to s}$, for all $s \in S$. Since $\mathcal{A}$ is equationally fully abstract, we have that $I'_s = I_s$, and thus that $I'_s\, a = a$, for all $a \in A_s$ and $s \in S$. Thus condition (ii) holds.

For condition (iii), we prove by induction on $\mathcal{A}$ that for all $a \in A_s$, $s \in S$, and $n \in \omega$, there is a term M of sort s such that $\Psi^n_s\, a = [\![\Psi^n_s\, M]\!]$. This is obvious for denotable elements. Suppose that it is true for the elements of a directed set D. Then

$$\Psi^n_s \bigsqcup D = \bigsqcup \{ \Psi^n_s\, d \mid d \in D \} = \bigsqcup \{ [\![\Psi^n_s\, N]\!] \mid N \in T' \},$$

for a set of terms T'. But $\{ [\![\Psi^n_s\, N]\!] \mid N \in T' \}$ is finite (since it is finite in, e.g., the stable function model) and thus contains its own lub, which is some $[\![\Psi^n_s\, N]\!]$, thus completing the induction. Then, $\{ \Psi^n_s\, a \mid a \in A_s \}$ is equal to $\{ [\![\Psi^n_s\, M]\!] \mid M \in T \}$, and thus is finite by the above reasoning.

For the extensionality of $\mathcal{A}$, suppose that $a_1, a_2 \in A_{s_1 \to s_2}$ and $a_1\, a' = a_2\, a'$, for all $a' \in A_{s_1}$. To show that $a_1 = a_2$, it suffices to show that $\Psi^n_{s_1 \to s_2}\, a_1 = \Psi^n_{s_1 \to s_2}\, a_2$, for all $n \in \omega$. From the above induction, we know that $\Psi^n_{s_1 \to s_2}\, a_1$ and $\Psi^n_{s_1 \to s_2}\, a_2$ are denotable. Furthermore, for all denotable $a' \in A_{s_1}$,

$$(\Psi^n_{s_1 \to s_2}\, a_1)\, a' = \Psi^n_{s_2}(a_1(\Psi^n_{s_1}\, a')) = \Psi^n_{s_2}(a_2(\Psi^n_{s_1}\, a')) = (\Psi^n_{s_1 \to s_2}\, a_2)\, a'.$$

Thus, by the obvious semantic restatement of theorem 4.3 (iii), $\Psi^n_{s_1 \to s_2}\, a_1 = \Psi^n_{s_1 \to s_2}\, a_2$, as required.

Order-extensionality under the additional hypothesis that $\mathcal{A}$ is inequationally fully abstract follows similarly, using theorem 4.3 (ii). $\square$

Theorem 5.7 (Milner/Berry) *Extensional, equationally fully abstract models are syntactically SFP and inductively reachable.*

Proof. Adapted from theorem 3.6.18 of [Ber]. Let $\mathcal{A}$ be such a model, which is syntactically SFP by lemma 5.5. Clearly, all elements of A_ι are denotable. Suppose that $s = s_1 \to \cdots \to s_n \to \iota$, for $n \geq 1$, is such that all isolated elements of each A_{s_i} are denotable. Suppose, toward a contradiction, that there is a non-denotable isolated element a of A_s. Let $n \in \omega$ be such that $\Psi^n\, a = a$. Define a pre-ordering $\leq$ over A_s by: $a \leq a'$ iff $a\, a_1 \cdots a_n \sqsubseteq_\iota a'\, a_1 \cdots a_n$, for all $a_i \in A_{s_i}$. Let X be the set of all denotable elements of $\{ \Psi^n\, a' \mid a' \in A_s \}$, $X^+ = \{ x \in X \mid a \leq x \}$ and $X^- = X - X^+$.

Let $\delta_1, \ldots, \delta_p$ be the elements of X^-; here $p \geq 1$, since $\perp \in X^-$. Then, for all $1 \leq i \leq p$, there exist isolated $w^i_j \in A_{s_j}$ and $z_i \in \omega$ such that $a\, w^i_1 \cdots w^i_n = z_i$ and $\delta_i\, w^i_1 \cdots w^i_n \neq z_i$. Let W^i_j be terms denoting the w^i_j, and let Q of sort $s \to \iota$ be

$$\lambda x.\, (And_p(St_{z_1}\, (x\, W^1_1 \cdots W^1_n)) \cdots (St_{z_p}\, (x\, W^p_1 \cdots W^p_n))).$$

There are now two cases to consider:

(X^+ is nonempty) Suppose that x_1 and x_2 are elements of X^+ that are denoted by terms X_1 and X_2, respectively. Let $X_3 = \Psi^n(Inf\, X_1\, X_2)$ and x_3 be the meaning of X_3. A bit of work then shows that x_3 is a $\leq$-lower bound of $x_1 = \Psi^n\, x_1$ and $x_2 = \Psi^n\, x_2$, and that $a = \Psi^n\, a \leq x_3$, i.e., $x_3 \in X^+$. Thus we can conclude that there is a $\leq$-least element γ of X^+. There exist isolated

$u_i \in A_{s_i}$ and $v \in \omega$ such that $a\, u_1 \cdots u_n = \bot$ and $\gamma\, u_1 \cdots u_n = v$. Let U_i be terms denoting the u_i, and define terms M_1 and M_2 of sort $s \to \iota$ by

$$\begin{aligned} M_1 &= \lambda x.\,(Q(\Psi^n\, x)), \\ M_2 &= \lambda x.\,(And_2(Q(\Psi^n\, x))(St_v\,(\Psi^n\, x\, U_1 \cdots U_n))). \end{aligned}$$

Then the meaning of M_1 applied to a is 1, whereas the meaning of M_2 applied to a is $\bot$. On the other hand, we can use theorem 4.3 (iii) to show that $M_1 \approx^c_{s\to\iota} M_2$. But this contradicts the equational full abstraction of $\mathcal{A}$.

(X^+ is empty) Similar to the nonempty case, with M_1 defined as before and $M_2 = \Omega$. □

Since all objects of **E** are inductively reachable (theorem 5.7), it follows that **E** is a pre-ordering.

Lemma 5.8 *If $\mathcal{A}$ is an equationally fully abstract model then $\preceq_{\mathcal{A}}$ is a least fixed point ordering.*

Proof. Immediate from lemma 3.3. □

Theorem 5.9 *If $\mathcal{A}$ is an extensional, equationally fully abstract model then it is order-isomorphic to $\mathcal{M}(\preceq_{\mathcal{A}})$.*

Proof. Let $\mathcal{B} = \mathcal{M}(\preceq_{\mathcal{A}})$ and i be the unique continuous homomorphism from $\mathcal{B}$ to $\mathcal{A}$. By theorem 5.7, $\mathcal{A}$ is inductively reachable, and thus it suffices to show that i is an order-embedding. Suppose that $i_s\, b_1 \sqsubseteq_s i_s\, b_2$. Then, for all $n \in \omega$,

$$i_s(\Psi^n\, b_1) = \Psi^n(i_s\, b_1) \sqsubseteq_s \Psi^n(i_s\, b_2) = i_s(\Psi^n\, b_2).$$

But $\Psi^n\, b_1$ and $\Psi^n\, b_2$ are denotable, and thus $\Psi^n\, b_1 \sqsubseteq_s \Psi^n\, b_2$. Thus $b_1 \sqsubseteq_s b_2$, since $\mathcal{B}$ is syntactically SFP. □

Proposition 5.10 *Suppose $\mathcal{A}$ and $\mathcal{B}$ are extensional, equationally fully abstract models. If $\preceq_{\mathcal{A}} \subseteq \preceq_{\mathcal{B}}$, then there is a unique morphism from $\mathcal{A}$ to $\mathcal{B}$. If there is a morphism from $\mathcal{A}$ to $\mathcal{B}$, then $\preceq_{\mathcal{A}} \subseteq \preceq_{\mathcal{B}}$.*

Proof. The first part follows from theorems 5.9 and 5.4, and the second part is obvious. □

Corollary 5.11 **E** *and* **L** *are equivalent categories.*

Proof. Immediate from theorems 5.4, 5.6 and 5.9 and proposition 5.10. □

From the above results, we know that $\mathcal{M}(\preceq_0)$ and $\mathcal{M}(\precsim^c)$ are the initial and terminal objects, respectively, of **E**. It is easy to see that $\mathcal{M}(\preceq_0)$ is also initial in the category of (not necessarily extensional) equationally fully abstract models and their morphisms. $\mathcal{M}(\precsim^c)$ is the only object of **E** that is order-extensional, since models that are order-extensional, SFP and whose isolated elements are all denotable are easily seen to be inequationally fully abstract. Another fact about $\mathcal{M}(\precsim^c)$ is that its carrier is consistently complete; it is unknown whether there are other objects of **E** with consistently complete carriers. Another obvious open question is whether $\mathcal{M}(\preceq_0)$ and $\mathcal{M}(\precsim^c)$ are the only objects of **E**.

Acknowledgments

Conversations with Albert Meyer and Gordon Plotkin stimulated my attempts to show that equational and inequational full abstraction were distinct for PCF.

References

[Ber] G. Berry. *Modèles complètement adéquats et stables des lambda-calculs typés.* Thèse de Doctorat d'Etat, Université Paris VII, 1979.

[BerCurLév] G. Berry, P.-L. Curien and J.-J. Lévy. Full abstraction for sequential languages: the state of the art. In M. Nivat and J. Reynolds (editors), *Algebraic Methods in Semantics*, Cambridge University Press, 1985.

[Cur] P.-L. Curien. *Categorical combinators, sequential algorithms and functional programming.* Research Notes in Theoretical Computer Science, Pitman/Wiley, 1986.

[Mey] A. Meyer and S. Cosmadakis. Semantical paradigms: notes for an invited lecture. *Proc. 3rd LICS*, 1988.

[Mil] R. Milner. Fully abstract models of typed λ-calculi. *Theoretical Computer Science* 4, 1977.

[Plo] G. Plotkin. LCF considered as a programming language. *Theoretical Computer Science* 5, 1977.

[Sto] A. Stoughton. *Fully Abstract Models of Programming Languages.* Research Notes in Theoretical Computer Science, Pitman/Wiley, 1988.