Step-Indexed Kripke Models over Recursive Worlds

Lars Birkedal
IT University of Copenhagen, Denmark
birkedal@itu.dk

Bernhard Reus
University of Sussex, UK
bernhard@sussex.ac.uk

Jan Schwinghammer
Saarland University, Germany
jan@ps.uni-saarland.de

Kristian Støvring
IT University of Copenhagen, Denmark
kss@itu.dk

Jacob Thamsborg
IT University of Copenhagen, Denmark
thamsborg@itu.dk

Hongseok Yang
Queen Mary University London, UK
hyang@dcs.qmul.ac.uk

Abstract

Over the last decade, there has been extensive research on modelling challenging features in programming languages and program logics, such as higher-order store and storable resource invariants. A recent line of work has identified a common solution to some of these challenges: Kripke models over worlds that are recursively defined in a category of metric spaces. In this paper, we broaden the scope of this technique from the original domain-theoretic setting to an elementary, operational one based on step indexing. The resulting method is widely applicable and leads to simple, succinct models of complicated language features, as we demonstrate in our semantics of Charguéraud and Pottier's type-and-capability system for an ML-like higher-order language. Moreover, the method provides a high-level understanding of the essence of recent approaches based on step indexing.

1. Introduction

Over the last decade, there has been extensive research on modelling challenging features in programming languages, type systems and program logics, such as higher-order store and storable resource invariants, where modelling involves constructing recursively defined structures [15, 23, 30, 33, 41, 42]. One of the main aims of this research has been to develop a method for building semantic models such that (1) the method is simple enough to be understood by the designers of a type system or a program logic (who might have only limited knowledge of domain theory) but (2) the method is powerful enough to resolve the issue of constructing recursive structures.

Unfortunately, existing methods do not fully achieve this aim. Methods based on classical domain theory provide techniques for constructing recursive structures, but they require non-trivial mathematical knowledge from users. Methods based on step indexing [2, 4, 6, 11, 12], on the other hand, do not require sophisticated mathematics from the users; usually, the prerequisite is just familiarity with standard operational semantics of programs. However, the step-indexed methods only partially address the issue of constructing recursive structures. They change the original recursive equations that solutions have to satisfy to easier approximate ones, and construct structures that satisfy the approximate equations. We point out that solving the original recursive equations is crucial in some applications, such as the semantics of various higher-order frame and anti-frame rules [44, 45]. Hence, in those applications, only domain-theoretic models, not step-indexed ones, have been developed.

In this paper, we propose a new method that brings together the benefits of both domain-theoretic and step-indexing methods. Our approach is based on a recent line of work where challenging features of programming languages and logics are modelled using a common solution: Kripke models over worlds that are recursively defined in a category of metric spaces [22, 44, 45]. This method transfers those worlds from the original domain-theoretic setup to an elementary, operational one based on step indexing.

Although our method does involve a modicum of metric space theory, it retains the flavour and simplicity of traditional step-indexed methods [2, 4, 6, 11, 12]. Unlike these step-indexed models, which only provide solutions to approximated versions of recursive equations, our approach provides solutions to the equations proper, i.e., we solve the equation up to isomorphism. In the paper, we demonstrate the benefits of our method by presenting the first semantic model of Charguéraud and Pottier's capability calculus [25]. This calculus is a substructural type system for a higher-order ML-like language with state, and imposes a nontrivial soundness issue, because a model needs to involve a recursively defined operation on a recursively-defined set of worlds. Our semantics justifies the typing rules of the calculus, and it also suggests a sound extension of the type system with a higher-order (deep) frame rule.[1]

Our method also provides a high-level understanding of the essence of step-indexed models. In particular, we show that the method can be specialized to Hobor et al.'s recent abstract description of step-indexed models [31], and explain the benefits of taking the metric viewpoint we suggest.

The remainder of the paper is organized as follows. In Section 2, we give an extensive introduction of our method, by developing a step-indexed Kripke model for ML references. In Section 3, we address the challenging problem of modelling Charguéraud and Pottier's capability type system, and show how our method gives rise to a step-indexed Kripke model of the calculus. Next, in Section 4, we consider the connection with the indirection theory

[1] We have also used the new method to give an elementary *operational* model for a program logic for reasoning about higher-order store; this yields an alternative soundness proof to the earlier non-trivial domain-theoretic one [44]. Please see Appendix D for this model.

of Hobor et al. [31], and point out what new insights our method brings to the work on step indexing. Finally, in Sections 5 and 6, we discuss related work and conclude the paper.

2. Introductory Example: ML References

In this section, we give an extensive introduction of our method, using a programming language with impredicative polymorphism and general ML-like references, i.e., an extension of the call-by-value polymorphic lambda calculus with higher-order store. We do not give the syntax of this language as it is standard but point out that we use v for values, e for expressions and τ for types, in particular $e[\tau]$ is application of a polymorphic term to a type.

First, we describe the general idea of interpreting the programming language with a Kripke-style possible-worlds model, where the set of worlds is recursively defined. Then, we review an existing model that realizes the idea in a domain-theoretic setting (based on an adequate denotational semantics of the language). Finally, we present a new step-indexed model (based purely on the operational semantics), and compare it with the domain-theoretic one.

A simple approach for modelling the polymorphic lambda calculus, without general references, is to interpret types as predicates (subsets) on some fixed set of values. To model the programming language of interest now, however, we need to extend this approach, because the language includes dynamic allocation of general references. Following earlier work on the semantics of dynamic allocation of simple integer cells [14, 33, 40, 47], we use an extension with Kripke-style possible worlds. In this extension, a type is interpreted as a predicate on values parameterized over worlds, and a world describes the type for each allocated location—a world $w \in W$ is a finite map from locations (modelled as natural numbers) to semantic types in T. The extension is described by the following recursive equations on the set W of worlds and the set T of semantic types:

$$\begin{array}{c} V \;=\; \text{set of values, including locations} \\ W \;=\; \mathbb{N} \rightharpoonup_{\mathit{fin}} T \qquad\qquad T \;=\; W \rightarrow_{mon} \mathit{Pred}(V) \end{array} \tag{1}$$

Note that in the equation for T, we impose a monotonicity requirement (with respect to an extension ordering of worlds). Intuitively, this requirement means that validity of semantic types is preserved in presence of a growing heap. The formal meaning of the monotonicity will be explained later in Section 2.2.

Once we are given the semantic domains W and T satisfying the above equations, we can interpret types as elements in T. In particular, the meaning of a reference type $\mathsf{ref}\,\tau$ can be defined roughly as

$$(\mathsf{ref}\,\tau)w = \{l \mid w(l) = \tau\},$$

i.e., for a world w, it is the set of locations l such that the semantic type recorded in the world at l is the same as τ.[2]

Observe that the natural model of types here is a *Kripke model over a recursively-defined set of worlds*. It is a Kripke model because the semantic types are parameterized over W. The problem is, of course, that for cardinality reasons there are no solutions to the above equations in the category of sets; unfolding the above equations we get $W = \mathbb{N} \rightharpoonup_{\mathit{fin}} (W \rightarrow_{mon} \mathit{Pred}(V))$ with W in a negative position, see also Ahmed [2].

To address this cardinality issue, existing methods based on step indexing, including the recent work by Hobor et al. [31], propose that we should give up solving the original recursive equations and instead solve approximate versions. As Hobor et al. show, solutions of the approximate equations are often sufficient for the applications of interest.

[2] In both of the concrete models to be presented next, the interpretation of reference types is actually more complicated and involves certain "approximate equality" relations on semantic types.

In this paper, we follow a different approach, which involves finding an appropriate simple category of metric spaces and solving the original recursive equations in the category. This approach has been developed in the setting of denotational semantics and domain theory. We show that the same approach can also be applied to operational semantics and step indexing. In the next subsections, we explain this point by giving a Kripke model of ML references, first using domain-theoretic methods, and then step indexing.

2.1 Review of Metric Spaces

Before describing our Kripke models, we review basic facts on the metric spaces, which will be used in the models. A **1-bounded ultrametric space** (X, d) is a metric space where the distance function $d : X \times X \to \mathbb{R}$ takes values in the closed interval $[0, 1]$ and satisfies the strong triangle inequality $d(x, y) \leq \max\{d(x, z), d(z, y)\}$. An (ultra-)metric space is **complete** if every Cauchy sequence has a limit. A function $f : X_1 \to X_2$ between metric spaces (X_1, d_1) and (X_2, d_2) is **non-expansive** if $d_2(f(x), f(y)) \leq d_1(x, y)$ for all $x, y \in X_1$. It is **contractive** if there exists some $\delta < 1$ such that $d_2(f(x), f(y)) \leq \delta \cdot d_1(x, y)$ for all $x, y \in X_1$.

The complete, 1-bounded, non-empty, ultrametric spaces and non-expansive functions between them form a Cartesian closed category $\mathbf{CBUlt}_{\mathrm{ne}}$. Products are given by the set-theoretic product where the distance is the maximum of the componentwise distances. The exponential $(X_1, d_1) \to (X_2, d_2)$ has the set of non-expansive functions from (X_1, d_1) to (X_2, d_2) as underlying set, and distance function: $d_{X_1 \to X_2}(f, g) = \sup\{d_2(f(x), g(x)) \mid x \in X_1\}$. For any set S and space $(X, d) \in \mathbf{CBUlt}_{\mathrm{ne}}$, the set of finite partial functions $S \rightharpoonup_{\mathit{fin}} X$ from S to X is again a complete, 1-bounded ultrametric space with distance function given by $d(f, g) = 1$, if the domains of f and g are not equal, and $d(f, g) = \max\{d(f(s), g(s)) \mid s \in \mathrm{dom}(f)\}$, if the domains of f and g are equal.

A functor $F : \mathbf{CBUlt}_{\mathrm{ne}}^{\mathrm{op}} \times \mathbf{CBUlt}_{\mathrm{ne}} \longrightarrow \mathbf{CBUlt}_{\mathrm{ne}}$ is **locally non-expansive** if $d(F(f, g), F(f', g')) \leq \max\{d(f, f'), d(g, g')\}$ for all non-expansive f, f', g, g'. It is **locally contractive** if there exists $\delta < 1$ such that $d(F(f, g), F(f', g')) \leq \delta \cdot \max\{d(f, f'), d(g, g')\}$ for all non-expansive f, f', g, g'. By multiplication of the distances of (X, d) with a non-negative shrinking factor $\delta < 1$, one obtains a new ultrametric space, $\delta \cdot (X, d) = (X, d')$ where $d'(x, y) = \delta \cdot d(x, y)$. By shrinking, a locally non-expansive functor F yields a locally contractive functor $(\delta \cdot F)(X_1, X_2) = \delta \cdot (F(X_1, X_2))$. For a less condensed introduction to ultrametric spaces we refer to [46].

It is well-known that one can solve recursive domain equations in $\mathbf{CBUlt}_{\mathrm{ne}}$ by an adaptation of the inverse-limit method from classical domain theory:

Theorem 2.1 (America-Rutten [9])**.** Let $F : \mathbf{CBUlt}_{\mathrm{ne}}^{\mathrm{op}} \times \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ be a locally contractive functor. Then there exists a unique (up to isomorphism) $(X, d) \in \mathbf{CBUlt}_{\mathrm{ne}}$ such that $(X, d) \cong F((X, d), (X, d))$.

All the metric spaces we consider satisfy the following property:

Definition 2.2. A metric space is *bisected* if all non-zero distances are of the form 2^{-n} for some natural number $n \geq 0$.

The following notation is convenient when working with bisected metric spaces: in such a space, $x \stackrel{n}{=} y$ means that $d(x, y) \leq 2^{-n}$. We use two facts on $\stackrel{n}{=}$. First, each relation $\stackrel{n}{=}$ is an equivalence relation because of the ultrametric inequality. We are therefore justified in referring to the relation $\stackrel{n}{=}$ as "n-equality." Second, the distance of a bisected metric space is bounded by 1. In other words, the relation $x \stackrel{0}{=} y$ always holds.

Proposition 2.3. Let (X_1, d_1) and (X_2, d_2) be bisected metric spaces. A function $f : X_1 \to X_2$ is non-expansive if and only if $x_1 \overset{n}{=} x_1' \Rightarrow f(x_1) \overset{n}{=} f(x_1')$ holds for all $x_1, x_1' \in X_1$ and all natural numbers $n \geq 0$.

2.2 General Recipe and Domain-Theoretic Model

We now follow the idea outlined earlier and reformulate the recursive equations (1) in $\mathbf{CBUlt}_{\mathrm{ne}}$ to find solutions within this category. Concretely, the proposal suggests to use the recipe below:

1. Define a set V with a structure. The structure can be a pre-order, or a uniform complete partial order, but does not have to be. Intuitively, V is a domain for semantic values.
2. Define an object $Pred(V)$ in $\mathbf{CBUlt}_{\mathrm{ne}}$. Elements in this object represent predicates on values.
3. Solve the recursive domain equation below in $\mathbf{CBUlt}_{\mathrm{ne}}$:
$$\hat{T} \;\cong\; \tfrac{1}{2} \cdot ((\mathbb{N} \rightharpoonup_{\mathit{fin}} \hat{T}) \to_{mon} Pred(V)) \,. \qquad (2)$$
4. Define T and W using $\hat{T}$:
$$W \;=\; N \rightharpoonup_{\mathit{fin}} \hat{T}, \qquad T \;=\; W \to_{mon} Pred(V). \qquad (3)$$

The function space in the equivalence in the third step consists of non-expansive and monotone functions, where monotonicity is imposed with respect to the following extension order on $\mathbb{N} \rightharpoonup_{\mathit{fin}} T$: For $w, w' \in \mathbb{N} \rightharpoonup_{\mathit{fin}} T$, we have $w \sqsubseteq w'$ iff the domain of w is included in the domain of w', and w and w' agree on the former. The $\frac{1}{2}$ is an example of a shrinking factor and, technically, ensures that the functor is locally contractive; it is a standard technique [9]. The equivalence is well-formed in $\mathbf{CBUlt}_{\mathrm{ne}}$, and it has a unique solution up to isomorphism by Theorem 2.1.

The recipe has been used by Birkedal, Støvring and Thamsborg [22], when they gave a relationally-parametric domain-theoretic model of a call-by-value language with impredicative polymorphism, general references and recursive types. They constructed the parameters V and $Pred(V)$ of the recipe using domain theory, choosing for V the cpo of values that is used in the standard "untyped" domain-theoretic interpretation of the language. This domain V comes with a family of projections $\pi_n : V \to V_\perp$ satisfying certain properties (so it becomes a uniform cpo). For the next parameter $Pred(V)$, Birkedal et al. used these projections to define $Pred(V)$ as the collection of *complete uniform* subsets of V. *Completeness* says that a subset P is closed under least upper bounds of chains, and *uniformity* that P is closed under all the projections (i.e., $\forall v \in P.\ \forall n > 0.\ \pi_n(v) \in P_\perp$). The set $Pred(V)$ can be viewed as a metric space in $\mathbf{CBUlt}_{\mathrm{ne}}$, by giving it an appropriate distance function along the lines of earlier work on interpreting recursive types and impredicative polymorphism [1, 7, 8, 24, 34].

Now, by simply following the recipe from the given ingredients (i.e. parameters V and $Pred(V)$) one obtains metric spaces T for semantic types and W for possible worlds, respectively. With this indexed semantic model of types, Birkedal et al. gave an interpretation of all the types of the programming language, and defined the typed meaning of expressions by proving the fundamental theorem of logical relations wrt. the untyped semantics of expressions. See [22] for a detailed treatment.[3]

[3] Notice that we use a small "trick" to construct the space of worlds W using Theorem 2.1. By solving the equation (2) we first obtain the space of semantic types, and we then define worlds in terms of semantic types. It is also possible to obtain W directly, as a solution of a recursive equation in a category of *pre-ordered* ultrametric spaces [21]. The latter technique is more general, but for this paper we do not need such pre-ordered spaces.

2.3 Step-Indexed Model

Our new insight is that the recipe presented in Section 2.2 is not tied to domain theory and denotational semantics, but it can also be used with operational semantics. In this case, the first parameter of the recipe is the set *Val* of closed syntactic values from the operational semantics. The second parameter is the set of predicates on step-approximated values. Precisely, it is the collection $UPred(\mathit{Val})$ of subsets of $\mathbb{N} \times \mathit{Val}$ that are downwards closed in the first step $(\mathbb{N})$ component:

$$UPred(\mathit{Val}) \;=\; \{p \subseteq \mathbb{N}\times \mathit{Val} \mid \forall (k, v) \in p. \forall j \leq k. (j, v) \in p\}.$$

We call $p \in UPred(\mathit{Val})$ a **uniform predicate** on *Val*.

The idea of considering predicates on step-approximated values is from step-indexed models [2, 6, 11, 12]. Here we go "a step further" and show that the collection $UPred(\mathit{Val})$ of such predicates can always be made into an object in $\mathbf{CBUlt}_{\mathrm{ne}}$. To do this, for $p \in UPred(\mathit{Val})$ and $k \in \mathbb{N}$, we use the notation $p_{[k]} = \{(m, v) \in p \mid m < k\}$, representing the k-th approximation of p. With this notation, we define a distance function d on $UPred(\mathit{Val})$, which measures "up-to-what-level" two predicates agree:

$$d(p, q) \;=\; \begin{cases} 2^{-\max\{k \,\mid\, p_{[k]} = q_{[k]}\}} & \text{if } p \neq q \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.4. $(UPred(\mathit{Val}), d)$ is a well-defined object in $\mathbf{CBUlt}_{\mathrm{ne}}$. In fact, the construction in $UPred(\mathit{Val})$ does not depend on our choice of *Val*, and can be applied to any set X, giving a metric space $UPred(X)$ in $\mathbf{CBUlt}_{\mathrm{ne}}$.

Note that because of this lemma, we can consider uniform predicates $p \in UPred(X)$ on any set X.

Hence, the recipe in Section 2.2 is applicable for *Val* and $UPred(\mathit{Val})$, and gives rise to semantic domains $\hat{T}$, W and T that satisfy the recursive equations in (2) and (3). Note that by working in $\mathbf{CBUlt}_{\mathrm{ne}}$, we have solved the desired equations, even for a setting based on operational semantics. In the rest of this section, we use these domains and model the programming language with impredicative polymorphism and ML references.

For concreteness, we consider a language as in Dreyer et al. [29], except that we do not consider recursive types and we split the context for type variables and term variables in two. Term judgments take the form

$$\Xi; \Gamma; \Sigma \;\vdash\; M : \tau$$

where Ξ is a context of type variables $\alpha_1, \ldots, \alpha_n$; Γ is a context of typed term variables $x_1 : \tau_1, \ldots, x_m : \tau_m$; and Σ is a context of typed locations $l_1 : \tau_1, \ldots, l_k : \tau_k$. Detailed typing judgments and operational semantics can be found in the online appendix to Dreyer et al.

Types in this language are interpreted similar to those used in existing step-indexed models [2], but one can exploit the fact that W and T are solutions to the recursive equations above. The semantics of types in context is defined as a non-expansive function

$$[\![\Xi \vdash \tau]\!] \;:\; T^{|\Xi|} \to T$$

in $\mathbf{CBUlt}_{\mathrm{ne}}$. The definition is shown in Figure 1. In the figure, we use η for environments for Ξ, i.e., elements in the product space $T^{|\Xi|}$ in $\mathbf{CBUlt}_{\mathrm{ne}}$. Notice that in the case for $[\![\Xi \vdash \mathsf{ref}\ \tau]\!]$, we use k-equality in the space T and that $\mathcal{E}[\![\Xi \vdash \tau]\!]$ generalizes $[\![\Xi \vdash \tau]\!]$ from values to expressions.

Lemma 2.5. $[\![\Xi \vdash \tau]\!]$ is well-defined. In particular,

- for all $\eta \in T^{|\Xi|}$, $[\![\Xi \vdash \tau]\!]_\eta$ is non-expansive and monotone; and
- $[\![\Xi \vdash \tau]\!]$ is a non-expansive map on η's.

In Figure 2 we define interpretations of contexts and the logical relation interpretation of well-typed expressions. Using those

$$\llbracket \Xi \vdash \tau \rrbracket_\eta : W \to_{mon} UPred(Val)$$

$$\llbracket \Xi \vdash 1 \rrbracket_\eta w = \{(k, ()) \mid k \in \mathbb{N}\}$$

$$\llbracket \Xi \vdash \mathsf{ref}\,\tau \rrbracket_\eta w = \{(k, l) \mid l \in \mathrm{dom}(w) \wedge w(l) \stackrel{k}{=} \llbracket \Xi \vdash \tau \rrbracket_\eta\}$$

$$\llbracket \Xi \vdash \alpha \rrbracket_\eta w = \eta(\alpha)(w)$$

$$\llbracket \Xi \vdash \forall\alpha.\tau \rrbracket_\eta w = \{(k, v) \mid \forall \tau' \in \mathit{SyntacticType}.\ \forall r \in T.\ \forall w' \sqsupseteq w.\ \forall i \leq k.\ (i, v[\tau']) \in \mathcal{E}\llbracket \Xi, \alpha \vdash \tau \rrbracket_{\eta[\alpha \mapsto r]} w'\}$$

$$\llbracket \Xi \vdash \tau \to \tau' \rrbracket_\eta w = \{(k, v) \mid \forall v' \in \mathit{Val}.\ \forall w' \sqsupseteq w.\ \forall i \leq k.\ (i, v') \in \llbracket \Xi \vdash \tau \rrbracket_\eta w' \Rightarrow (i, v\,v') \in \mathcal{E}\llbracket \Xi \vdash \tau' \rrbracket_\eta w'\}$$

$$\mathcal{E}\llbracket \Xi \vdash \tau \rrbracket_\eta w = \{(k, t) \mid \forall i \leq k.\ \forall h, h'.\ \forall e'.\ \big(h :_k w \wedge (t \mid h) \longmapsto^i (e' \mid h') \wedge (e', h') \text{ irreducible}\big) \Rightarrow \big(\exists w' \sqsupseteq w.\ h' :_{k-i} w' \ \wedge\ (k-i, e') \in \llbracket \Xi \vdash \tau \rrbracket_\eta w'\big)\}$$

$$h :_k w \iff \mathrm{dom}(h) = \mathrm{dom}(w) \ \wedge\ \forall i < k.\ \forall l \in \mathrm{dom}(w).\ (i, h(l)) \in w(l)(w)$$

(where $()$ is the unique element in the empty product, $\mathit{SyntacticType}$ is the set of syntactic types, *Exp* is the set of closed syntactic expressions, and $(t \mid h)$ is a configuration of an expression t and a heap h. A heap h is a finite function from locations to closed syntactic values.)

Figure 1. Interpretation of types

$$\llbracket \Xi \vdash \Gamma \rrbracket_\eta : W \to UPred(Val^{|\Gamma|})$$

$$\llbracket \Xi \vdash \emptyset \rrbracket_\eta w = \{(k, ()) \mid k \in \mathbb{N}\}$$

$$\llbracket \Xi \vdash \Gamma, x : \tau \rrbracket_\eta w = \{(k, \rho[x \mapsto v]) \mid (k, \rho) \in \llbracket \Gamma \rrbracket_\eta w \wedge (k, v) \in \llbracket \Xi \vdash \tau \rrbracket_\eta w\}$$

$$\llbracket \Sigma \rrbracket : UPred(W)$$

$$\llbracket \Sigma \rrbracket = \{(k, w) \mid \forall (l : \tau) \in \Sigma.\ (k, l) \in \llbracket \emptyset \vdash \mathsf{ref}\,\tau \rrbracket_{()} w\}$$

$$\Xi; \Gamma; \Sigma \vdash t :^{\log} \tau \iff \exists \alpha_1, \ldots, \alpha_n.\ \Xi = \alpha_1, \ldots, \alpha_n \ \wedge\ \forall \tau_1, \ldots, \tau_n.\ \forall k \geq 0.\ \forall \eta.\ \forall \rho.\ \forall w.\ \big(\eta \in T^{|\Xi|} \ \wedge\ (k, \rho) \in \llbracket \Xi \vdash \Gamma \rrbracket_\eta w \ \wedge\ (k, w) \in \llbracket \Sigma \rrbracket\big) \Rightarrow \big((k,\ (\rho(t))[\alpha_1{:=}\tau_1, \ldots, \alpha_n{:=}\tau_n]) \in \mathcal{E}\llbracket \Xi \vdash \tau \rrbracket_\eta w\big)$$

(where $()$ is the unique environment for the empty context, and both $(-)[\alpha_1{:=}\tau_1, \ldots, \alpha_n{:=}\tau_n]$ and $\rho(-)$ represent the applications of substitutions.)

Figure 2. Interpretation of contexts and well-typed expressions

definitions, we are ready to prove the main soundness result:

Theorem 2.6 (Fundamental Theorem of Logical Relations)**.** If $\Xi; \Gamma; \Sigma \vdash t : \tau$, then $\Xi; \Gamma; \Sigma \vdash t :^{\log} \tau$.

One oddity is worth explaining: there is no coherence between the syntactic types that we substitute for type variables and the corresponding semantic types in the environment; this is the case both for the interpretation of universal types and in the definition of the logical relation. The explanation is simply that the syntactic types in values and expressions do not influence the computation; indeed, we could equally well have worked with a language without type-decorations as, e.g., Ahmed [5] does.

We finally remark that it is not surprising that there is a connection between metric spaces and step-indexed models; this was already pointed out in [11]. The point is that it is useful not to forget this connection because it, e.g., allows us to define solutions to recursive world equations such as the ones in this section. (See also the discussion in Section 4.2.)

We do not present a formal relationship to existing models for this particular example, but rather show, in Section 4, how all the step-indexed models described via the indirection theory of Hobor et al. can be obtained by a specialization of our general approach. In Section 4.2, we will also highlight the advantages of using metric spaces. Next, however, we consider another more substantial application to illustrate our method.

3. Application: A Step-indexed Model of Capabilities

Reasoning about higher-order stateful programs is notoriously difficult, and often involves the need to track aliasing information. A particular line of work that has been proposed to this end are substructural type systems with regions, capabilities and singleton types [3, 25, 27]. In this section, we give a step-indexed model for a substantial fragment[4] of Charguéraud and Pottier's capability calculus [25]. Our model provides an alternative soundness proof to the translation and progress and preservation results in [25, 38], and allows for the analysis of soundness of extensions. We illustrate this latter point by proving sound an extension of the language with higher-order frame rules [19, 44], and establish an explicit connection with models of separation logic *qua* our model, which shows that capabilities can be understood semantically as separation logic predicates, i.e., as predicates on heaps.

We believe that this step-indexed model provides an interesting application of the metric point of view that has been emphasized in the previous section. The model construction takes advantage of the fact that the recursive world equation can be *solved* (up to isomorphism), rather than merely *approximated*: the higher-order frame rules are modelled with the help of a recursive operation on worlds, and this operation is defined using the metric structure.

3.1 A Calculus of Capabilities

In the following presentation, we keep close to the notation of Charguéraud and Pottier [25, 38]. Figures 3 and 4 give the syntax and operational semantics of the programming language that we consider. It is a standard call-by-value, higher-order language with general references, and polymorphic and recursive types. The only noteworthy point about the syntax is that expressions are restricted so that all sequencing is made explicit; this simplifies the presentation of the typing rules and semantics but is no real restriction. The term $\mu f.\lambda x.t$ stands for the recursive procedure f with body t and argument x. If f does not appear in t, we may simply write $\lambda x.t$.

The operational semantics is defined between configurations $(t \mid h)$ that consist of a (closed) expression t and a heap h. As in the previous section, a heap h is a finite map from locations to closed values. Also, we remind the reader of our notation $t[x{:=}v]$ that means the substitution of v for x in t. We use the notation $h\#h'$ to indicate that two heaps h and h' have disjoint domains, and we write $h \cdot h'$ for the union of two such heaps.

The types used in the system are given by the grammar in Figure 5. *Capabilities* C describe heap properties (much like the assertions of a Hoare-style program logic), *value types* τ classify values, and *memory types* θ (and the subset of computation types) describe properties of expressions and how their evaluation affects the heap. Because of the heap dependency, capabilities and memory

[4] We do not consider group regions.

Variables	$\xi ::= \alpha \mid \beta \mid \gamma \mid \sigma$
Capabilities	$C ::= C \otimes C \mid \emptyset \mid C * C \mid \{\sigma : \theta\} \mid \exists \sigma.C \mid \gamma \mid \mu\gamma.C \mid \forall \xi.C$
Value types	$\tau ::= \tau \otimes C \mid 0 \mid 1 \mid \mathsf{int} \mid \tau + \tau \mid \tau \times \tau \mid \chi \to \chi \mid [\sigma] \mid \alpha \mid \mu\alpha.\tau \mid \forall \xi.\tau$
Memory types	$\theta ::= \theta \otimes C \mid \tau \mid \theta + \theta \mid \theta \times \theta \mid \mathsf{ref}\, \theta \mid \theta * C \mid \exists \sigma.\theta \mid \beta \mid \mu\beta.\theta \mid \forall \xi.\theta$
Computation types	$\chi ::= \chi \otimes C \mid \tau \mid \chi * C \mid \exists \sigma.\chi$
Value environments	$\Delta ::= \Delta \otimes C \mid \varnothing \mid \Delta, x{:}\tau$
Linear environments	$\Gamma ::= \Gamma \otimes C \mid \varnothing \mid \Gamma, x{:}\chi \mid \Gamma * C$

Figure 5. Capabilities and types

$$v ::= x \mid () \mid \mathsf{inj}^i\, v \mid (v_1, v_2) \mid \mu f.\lambda x.t \mid l$$
$$t ::= v \mid (v\, t) \mid \mathsf{case}(v_1, v_2, v) \mid \mathsf{proj}^i\, v \mid \mathsf{ref}\, v \mid \mathsf{get}\, v \mid \mathsf{set}\, v$$

Figure 3. Syntax of values and expressions

$$\begin{array}{rll}
(\mu f.\lambda x.t)\, v \mid h \longmapsto t[f := \mu f.\lambda x.t,\ x := v] \mid h & \\
\mathsf{proj}^i(v_1, v_2) \mid h \longmapsto v_i \mid h & \text{for } i = 1, 2 \\
\mathsf{case}(v_1, v_2, \mathsf{inj}^i v) \mid h \longmapsto v_i\, v \mid h & \text{for } i = 1, 2 \\
\mathsf{ref}\, v \mid h \longmapsto l \mid h{\cdot}[l \mapsto v] & \text{if } l \notin \mathrm{dom}\, h \\
\mathsf{get}\, l \mid h \longmapsto h(l) \mid h & \text{if } l \in \mathrm{dom}\, h \\
\mathsf{set}\,(l, v) \mid h \longmapsto () \mid h[l := v] & \text{if } l \in \mathrm{dom}\, h \\
v\, t \mid h \longmapsto v\, t' \mid h' & \text{if } t \mid h \longmapsto t' \mid h'
\end{array}$$

Figure 4. Operational semantics

types are linear, and correspondingly there is a distinction between value type environments and the more general linear environments.

A *region* σ is a static name that represents a value, and $[\sigma]$ is a singleton type that contains only this particular value. Capabilities are formed from *singleton capabilities* $\{\sigma : \theta\}$ by separating conjunction and existential quantification over regions. We also include capability variables γ and permit recursively defined capabilities. A singleton capability $\{\sigma : \theta\}$ asserts that the value denoted by σ has type θ, and moreover it represents the ownership of both this value and the fragment of the heap described by θ. Thus, it is similar to the points-to predicate of separation logic: for example, the capability $\{\sigma : \mathsf{ref}\, \tau\}$ means that σ denotes the address of a reference cell, and that the "owned" part of the heap stores a value of type τ at this address. Apart from singleton types, the value types include base types (here an empty type 0, the unit type 1, and int) and are closed under products, sums, and universal quantification over singletons, types and capabilities. The memory types extend value types by a type of references, and by the possibility to $*$-conjoin a capability. Like the pre- and postconditions used in Hoare logic, the arrow types make explicit which part of the heap is accessed when a procedure is called. For instance, the type $\forall \sigma, \sigma'. [\sigma] * \{\sigma : \mathsf{ref}\, [\sigma']\} \to [\sigma'] * \{\sigma : \mathsf{ref}\, [\sigma']\}$ can be given to a procedure that dereferences its argument.

Recursive capabilities and types are subject to a syntactic restriction: C must be *formally contractive* in γ for $\mu\gamma.C$ to be well-formed. By this we mean that the recursion must go through one of the type constructors $+, \times, \to$ or ref, or through the right-hand side of $\otimes$. This restriction ensures that the capability $\mu\gamma.C$ is the unique solution of the capability equation $\gamma = C$. Corresponding restrictions apply to recursively defined types $\mu\alpha.\tau$ and $\mu\beta.\theta$. We omit the straightforward inductive definition of formal contractiveness.

One interesting aspect of the type system is that each of the syntactic categories is equipped with an *invariant extension* operation, $\cdot \otimes C$. Intuitively, this operation conjoins C to the domain and codomain of every arrow type that occurs within its left hand argument, which means that the capability C is preserved by all functions of this type. This intuition is made precise by regarding capabilities and types modulo the structural equivalence given in Figure 6. This equivalence subsumes the "distribution axioms" for $\otimes$ that are used to express generic higher-order frame rules [19]. The first two groups of equations, equivalences (4)–(11), state that both $*$ and the derived operation $\circ$ on capabilities satisfy the axioms of a monoid, and that $*$ and $\otimes$ are actions of these monoids. Equivalences (15)–(30) describe the action by $\otimes$ on types. In particular, (25) shows the key case of the invariant extension described informally above.[5] Finally, the equivalences (34)–(38) for *focusing* let us build and deconstruct the capabilities over complex types in terms of capabilities over more primitive types.

The system also uses a subtyping relation, and Figure 7 gives some of the subtyping axioms. The typing rules are shown in Figure 8. Due to the use of linear environments and computation types (which in general contain embedded capabilities), the typing judgement $\Gamma \Vdash t : \chi$ is similar to a Hoare triple where Γ serves as a precondition and χ as a postcondition. This view explains the rules SHALLOW-FRAME and DEEP-FRAME; as in separation logic, these rules can be used to add an invariant C to a specification. The difference between SHALLOW-FRAME and DEEP-FRAME is that the former adds C only on the top-level, whereas the latter also extends all arrow types nested inside Γ and χ, via $\cdot \otimes C$. As with the higher-order frame rules in separation logic, this is useful for reasoning about information hiding [19].

3.2 Upwards Closed Uniform Predicates and Worlds

The main idea of the model that we present next is that types (as well as type contexts and capabilities) are parameterized by invariants. Thus, in this case the worlds will be predicates that, like the syntactic capabilities of the calculus, describe properties of the heap that all computations must preserve.

Recall that the set $UPred(X)$ of uniform predicates on a set X is defined by

$$UPred(X) \;=\; \{p \subseteq \mathbb{N} \times X \mid \forall (k, v) \in p. \forall j \leq k. (j, v) \in p\}.$$

The interpretation of types and capabilities is based on a variation on these uniform predicates. Let $(A, \sqsubseteq)$ be a partially ordered set. An *upwards closed* uniform predicate p on A is a predicate in $UPred(A)$ that is also upward closed in the second argument, i.e. if $(k, a) \in p$ and $a \sqsubseteq b$ then $(k, b) \in p$. We write $UPred^{\uparrow}(A)$ for the set of all upwards closed uniform predicates on A, and define

$$p_{[k]} \;=\; \{(j, a) \in p \mid j < k\}.$$

[5] Note that (13) and (14) let us move capabilities between assumptions – a form of ownership transfer.

$$\textsc{Var}\ \frac{(x:\tau)\in\Delta}{\Delta\vdash x:\tau}\qquad \textsc{Unit}\ \frac{}{\Delta\vdash ():1}\qquad \textsc{Inj}\ \frac{\Delta\vdash v:\tau_i}{\Delta\vdash (\mathsf{inj}^i\ v):(\tau_1{+}\tau_2)}\qquad \textsc{Pair}\ \frac{\Delta\vdash v_1:\tau_1\qquad \Delta\vdash v_2:\tau_2}{\Delta\vdash (v_1,v_2):(\tau_1\times\tau_2)}\qquad \textsc{RecFun}\ \frac{\Delta,\, f:\chi_1\to\chi_2,\, x:\chi_1\Vdash t:\chi_2}{\Delta\vdash \mu f.\lambda x.t:\chi_1\to\chi_2}$$

$$\textsc{Val}\ \frac{\Delta\vdash v:\tau}{\Delta\Vdash v:\tau}\qquad \textsc{App}\ \frac{\Delta\vdash v:\chi_1\to\chi_2\qquad \Delta,\Gamma\Vdash t:\chi_1}{\Delta,\Gamma\Vdash (v\,t):\chi_2}\qquad \textsc{Proj-1}\ \frac{\Gamma\Vdash v:[\sigma]*\{\sigma:\tau_1\times\theta_2\}}{\Gamma\Vdash \mathsf{proj}^1\, v:\tau_1*\{\sigma:\tau_1\times\theta_2\}}\qquad \textsc{Proj-2}\ \frac{\Gamma\Vdash v:[\sigma]*\{\sigma:\theta_1\times\tau_2\}}{\Gamma\Vdash \mathsf{proj}^2\, v:\tau_2*\{\sigma:\theta_1\times\tau_2\}}$$

$$\textsc{Case}\ \frac{\begin{array}{c}\Delta\vdash v_1:(\exists\sigma_1.[\sigma_1]*\{\sigma:[\sigma_1]+0\}*\{\sigma_1:\theta_1\}*C)\to\chi\\ \Delta\vdash v_2:(\exists\sigma_2.[\sigma_2]*\{\sigma:0+[\sigma_2]\}*\{\sigma_2:\theta_2\}*C)\to\chi\\ \Delta,\Gamma\Vdash v:[\sigma]*\{\sigma:\theta_1+\theta_2\}*C\end{array}}{\Delta,\Gamma\Vdash \mathsf{case}(v_1,v_2,v):\chi}\qquad \forall\textsc{-Intro}\ \frac{\Delta\vdash v:\tau}{\Delta\vdash v:\forall\xi.\tau}\,\xi\notin\Delta\qquad \forall\textsc{-Elim-1}\ \frac{\Delta\vdash v:\forall\alpha.\tau}{\Delta\vdash v:\tau[\alpha:=\tau']}$$

$$\textsc{Ref}\ \frac{\Gamma\Vdash v:\tau}{\Gamma\Vdash \mathsf{ref}\, v:\exists\sigma.[\sigma]*\{\sigma:\mathsf{ref}\,\tau\}}\qquad \textsc{Get}\ \frac{\Gamma\Vdash v:[\sigma]*\{\sigma:\mathsf{ref}\,\tau\}}{\Gamma\Vdash \mathsf{get}\, v:\tau*\{\sigma:\mathsf{ref}\,\tau\}}\qquad \textsc{Set}\ \frac{\Gamma\Vdash v:([\sigma]\times\tau_2)*\{\sigma:\mathsf{ref}\,\tau_1\}}{\Gamma\Vdash \mathsf{set}\, v:1*\{\sigma:\mathsf{ref}\,\tau_2\}}$$

$$\textsc{Shallow-Frame}\ \frac{\Gamma\Vdash t:\chi}{\Gamma*C\Vdash t:\chi*C}\qquad \textsc{Deep-Frame}\ \frac{\Gamma\Vdash t:\chi}{(\Gamma\otimes C)*C\Vdash t:(\chi\otimes C)*C}\qquad \textsc{Sub}\ \frac{\Gamma\Vdash t:\chi_1\qquad \chi_1\le\chi_2}{\Gamma\Vdash t:\chi_2}$$

Figure 8. Typing of values and expressions

As in Section 2.3 on $UPred(V)$, this restricts p to pairs with first component less than k. Note that $p_{[k]}$ is again upwards closed and uniform, so it belongs to $UPred^{\uparrow}(A)$ as well. We equip $UPred^{\uparrow}(A)$ with the same distance function d as $UPred(A)$ in Section 2.3. This makes $(UPred^{\uparrow}(A), d)$ an object of $\mathbf{CBUlt}_{\mathrm{ne}}$.

In our model, we use $UPred^{\uparrow}(A)$ with the following concrete instances for the partial order $(A, \sqsubseteq)$:

- $(Heap, \sqsubseteq)$ where $h \sqsubseteq h'$ iff $h' = h \cdot h_0$ for some $h_0 \# h$,
- $(Val, \sqsubseteq)$ where $u \sqsubseteq v$ iff $u = v$,
- $(Val \times Heap, \sqsubseteq)$ where $(u, h) \sqsubseteq (v, h')$ iff $u = v$ and $h \sqsubseteq h'$.

We also use variants of the latter two instances where the set *Val* is replaced by the set of value substitutions, *Env*, and by the set of expressions, *Exp*.

On $UPred^{\uparrow}(Heap)$, ordered by subset inclusion, we have a complete Heyting BI algebra structure [17]. Meets and joins are given by set-theoretic intersections and unions, resp., and implication, separating conjunction and separating implication are given by

$$(k,h) \in p \to q \ \Leftrightarrow\ \forall j \le k.\ \forall h' \sqsupseteq h.\ (j,h') \in p \Rightarrow (j,h') \in q$$
$$(k,h) \in p_1 * p_2 \ \Leftrightarrow\ \exists h_1, h_2.\ h = h_1 \cdot h_2 \wedge (k, h_i) \in p_i$$
$$(k,h) \in p \mathrel{-\!\!*} q \ \Leftrightarrow\ \forall j \le k.\ \forall h' \# h.\ (j,h') \in p \Rightarrow (j, h \cdot h') \in q$$

The unit for $*$ is given by $I = \mathbb{N} \times Heap = \top$. Up to the natural number indexing, this is just the standard intuitionistic (in the sense that it is not "tight") model of separation logic [43].

Since the worlds are to represent invariants (for instance, describing the shape of data structures laid out in the heap) and since the language of Section 3.1 has general references (so these invariants talk about stored procedures and are themselves world-dependent), it is natural that worlds $w \in W$ must also double-act as functions $W \to UPred^{\uparrow}(Heap)$. Consequently, we solve in $\mathbf{CBUlt}_{\mathrm{ne}}$ the following recursive world equation:

$$W \ \cong\ \tfrac{1}{2} \cdot W \to UPred^{\uparrow}(Heap)\,. \tag{46}$$

Here, the function space is that of $\mathbf{CBUlt}_{\mathrm{ne}}$ and the $1/2$ denotes the scaling of the distance function on W. That W exists (and is uniquely determined up to isomorphism) follows from Theorem 2.1, applied to the locally contractive functor $F(X,Y) = \frac{1}{2} \cdot X \to UPred^{\uparrow}(Heap)$ on $\mathbf{CBUlt}_{\mathrm{ne}}$. Worlds are thus essentially *contractive* functions from worlds to $UPred^{\uparrow}(Heap)$, i.e. world dependent heap predicates. We define

$$Cap \ =\ \tfrac{1}{2} \cdot W \to UPred^{\uparrow}(Heap),$$

and write $\iota : Cap \to W$ for the isomorphism in (46), and ι^{-1} for its inverse. By ordering the elements of *Cap* pointwise,

$$p \le q \ \Leftrightarrow\ \forall w.\ p(w) \subseteq q(w),$$

we can lift the algebra structure on $UPred^{\uparrow}(Heap)$.

Lemma 3.1. With the above ordering and the pointwise lifting of the algebra operations on $UPred^{\uparrow}(Heap)$, the set *Cap* is a complete Heyting BI algebra.

The fact that *Cap* is a complete BI algebra immediately gives us a sound interpretation of $*$ on capabilities. (Moreover, it suggests that the syntax of capabilities could be extended with all the logical connectives of separation logic.) However, to interpret recursive capabilities we also need to know that the operations are non-expansive:

Lemma 3.2. The BI algebra operations on *Cap* are non-expansive functions, i.e., they are morphisms in $\mathbf{CBUlt}_{\mathrm{ne}}$:

$$\wedge, \vee, \to, *, \mathrel{-\!\!*} : Cap \times Cap \to Cap$$
$$\textstyle\bigwedge_I, \bigvee_I : (I \to Cap) \to Cap$$

(For the last two operations, the indexing set I is given the discrete metric, i.e., the distance of any two different elements is 1.)

Proof sketch. One can first show the corresponding property for the operations on $UPred^{\uparrow}(Heap)$ which is straightforward; the result then follows from the pointwise definition and the use of the sup-metric on *Cap*. To illustrate the non-expansiveness on $UPred^{\uparrow}(Heap)$, we consider the case of separating conjunction: It suffices to show that $p \overset{n}{=} p'$ and $q \overset{n}{=} q'$ implies $p * q \overset{n}{=} p' * q'$. By definition of the n-equality, $p * q \overset{n}{=} p' * q'$ is equivalent to $(j,h) \in p * q \ \Leftrightarrow\ (j,h) \in p' * q'$ for all $j < n$, which follows easily from the assumptions that $p \overset{n}{=} p'$ and $q \overset{n}{=} q'$. ☐

monoids

$$C_1 \circ C_2 \stackrel{def}{=} (C_1 \otimes C_2) * C_2 \quad (4)$$

$$(C_1 \circ C_2) \circ C_3 = C_1 \circ (C_2 \circ C_3) \quad (5)$$

$$C \circ \emptyset = C \quad (6)$$

$$(C_1 * C_2) * C_3 = C_1 * (C_2 * C_3) \quad (7)$$

$$C * \emptyset = C \quad (8)$$

$$C_1 * C_2 = C_2 * C_1 \quad (9)$$

monoid actions

$$(\cdot \otimes C_1) \otimes C_2 = \cdot \otimes (C_1 \circ C_2) \qquad \cdot \otimes \emptyset = \cdot \quad (10)$$

$$(\cdot * C_1) * C_2 = \cdot * (C_1 * C_2) \qquad \cdot * \emptyset = \cdot \quad (11)$$

action by $*$ on singleton

$$\{\sigma : \theta\} * C = \{\sigma : \theta * C\} \quad (12)$$

action by $*$ on linear environments

$$(\Gamma, x{:}\chi) * C = \Gamma, x{:}(\chi * C) \quad (13)$$

$$= (\Gamma * C), x{:}\chi \quad (14)$$

action by $\otimes$ on capabilities, types, and environments

$$(\cdot * \cdot) \otimes C = (\cdot \otimes C) * (\cdot \otimes C) \quad (15)$$

$$(\exists \sigma.\cdot) \otimes C = \exists \sigma.(\cdot \otimes C) \qquad \text{if } \sigma \notin \mathit{RegNames}(C) \quad (16)$$

$$\emptyset \otimes C = \emptyset \quad (17)$$

$$\{\sigma : \theta\} \otimes C = \{\sigma : \theta \otimes C\} \quad (18)$$

$$0 \otimes C = 0 \quad (19)$$

$$1 \otimes C = 1 \quad (20)$$

$$\mathsf{int} \otimes C = \mathsf{int} \quad (21)$$

$$(\theta_1 + \theta_2) \otimes C = (\theta_1 \otimes C) + (\theta_2 \otimes C) \quad (22)$$

$$(\theta_1 \times \theta_2) \otimes C = (\theta_1 \otimes C) \times (\theta_2 \otimes C) \quad (23)$$

$$(\forall \xi.\theta) \otimes C = \forall \xi.(\theta \otimes C) \qquad \text{if } \xi \notin \text{fv}\, C \quad (24)$$

$$(\chi_1 \to \chi_2) \otimes C = (\chi_1 \circ C) \to (\chi_2 \circ C) \quad (25)$$

$$[\sigma] \otimes C = [\sigma] \quad (26)$$

$$(\mathsf{ref}\, \theta) \otimes C = \mathsf{ref}\, (\theta \otimes C) \quad (27)$$

$$\varnothing \otimes C = \varnothing \quad (28)$$

$$(\Gamma, x{:}\chi) \otimes C = (\Gamma \otimes C), x{:}(\chi \otimes C) \quad (29)$$

$$(\Gamma * C_1) \otimes C_2 = (\Gamma \otimes C_2) * (C_1 \otimes C_2) \quad (30)$$

region abstraction

$$\exists \sigma_1.\exists \sigma_2.\cdot = \exists \sigma_2.\exists \sigma_1.\cdot \quad (31)$$

$$\cdot * (\exists \sigma.C) = \exists \sigma.(\cdot * C) \quad (32)$$

$$\{\sigma_1 : \exists \sigma_2.\theta\} = \exists \sigma_2.\{\sigma_1 : \theta\} \qquad \text{where } \sigma_1 \neq \sigma_2 \quad (33)$$

focusing

$$\{\sigma_1 : \mathsf{ref}\, \theta\} = \exists \sigma_2.\{\sigma_1 : \mathsf{ref}\, [\sigma_2]\} * \{\sigma_2 : \theta\} \quad (34)$$

$$\{\sigma : \theta_1 \times \theta_2\} = \exists \sigma_1.\{\sigma : [\sigma_1] \times \theta_2\} * \{\sigma_1 : \theta_1\} \quad (35)$$

$$\{\sigma : \theta_1 \times \theta_2\} = \exists \sigma_2.\{\sigma : \theta_1 \times [\sigma_2]\} * \{\sigma_2 : \theta_2\} \quad (36)$$

$$\{\sigma : \theta_1 + 0\} = \exists \sigma_1.\{\sigma : [\sigma_1] + 0\} * \{\sigma_1 : \theta_1\} \quad (37)$$

$$\{\sigma : 0 + \theta_2\} = \exists \sigma_2.\{\sigma : 0 + [\sigma_2]\} * \{\sigma_2 : \theta_2\} \quad (38)$$

recursion

$$\mu\gamma.C = C[\gamma{:=}\mu\gamma.C] \quad (39)$$

$$\mu\alpha.\tau = \tau[\alpha{:=}\mu\alpha.\tau] \quad (40)$$

$$\mu\beta.\theta = \theta[\beta{:=}\mu\beta.\theta] \quad (41)$$

Figure 6. Structural equivalence

(first-order) frame axiom

$$\chi_1 \to \chi_2 \leq (\chi_1 * C) \to (\chi_2 * C) \quad (42)$$

free

$$C_1 * C_2 \leq C_1 \quad (43)$$

singletons

$$\tau \leq \exists \sigma.[\sigma] * \{\sigma : \tau\} \quad (44)$$

$$[\sigma] * \{\sigma : \tau\} \leq \tau * \{\sigma : \tau\} \quad (45)$$

Figure 7. Some subtyping axioms

Next, we define a 'composition' operation on the worlds W. This operation plays a role similar to the ordering by extension in the case where worlds are finite maps from locations to semantic types (cf. Section 2). However, it is more involved than a simple extension of worlds; rather, it corresponds to the syntactic abbreviation $C_1 \circ C_2 = C_1 \otimes C_2 * C_2$ from Figure 6, of conjoining C_1 and C_2 and additionally applying an invariant extension $\cdot \otimes C_2$ to C_1. Formally, $\circ : W \times W \to W$ is a non-expansive operation that for all $p, r, w \in W$ satisfies

$$\iota^{-1}(p \circ r)(w) \;=\; \iota^{-1}(p)(r \circ w) \;*\; \iota^{-1}(r)(w) \;.$$

Using the metric-space setup, we can define this operation by an easy application of Banach's fixed point theorem, as in [44]. Observe that it is here where we exploit that we have obtained a proper solution to the world equation (46) in $\mathbf{CBUlt}_{\text{ne}}$.

We write *emp* for the image $\iota(\lambda w.I)$ of the BI unit under ι. Then it turns out that $\circ$ is associative and $p \circ \mathit{emp} = \mathit{emp} \circ p = p$ holds for all p, so $(W, \circ, \mathit{emp})$ is a monoid in $\mathbf{CBUlt}_{\text{ne}}$. Now let (X, d) be an arbitrary ultrametric space. Using the composition operator on worlds, we consider a semantic analogue of the invariant extension operation, $\otimes : X^{(\frac{1}{2}\cdot W)} \times W \to X^{(\frac{1}{2}\cdot W)}$ defined by

$$(f \otimes w_0)(w) \;=\; f(w_0 \circ w) \;.$$

The following proposition is a slight generalization of [44, Lemma 5], and summarizes the key properties of $\circ$ and $\otimes$. In the following, these properties are used to justify some of the equivalences given in Figure 6.

Proposition 3.3 (Monoid and monoid action)**.** Let (X, d) be an ultrametric space. Then $(W, \circ, \mathit{emp})$ is a monoid in $\mathbf{CBUlt}_{\text{ne}}$, and the operation $\otimes : X^{(\frac{1}{2}\cdot W)} \times W \to X^{(\frac{1}{2}\cdot W)}$ is a (non-expansive) action of the monoid W on the ultrametric space of non-expansive functions from $\frac{1}{2} \cdot W$ to X, i.e., $f \otimes \mathit{emp} = f$ and $(f \otimes w_1) \otimes w_2 = f \otimes (w_1 \circ w_2)$.

3.3 Semantic Domains and Interpretation

In this section we give the interpretation of the capabilities, types and environments of the type system. The semantic domain corresponding to each syntactic category is a set of (contractively world-dependent) upwards closed and uniform predicates:

$$\mathit{VT} \;=\; \tfrac{1}{2} \cdot W \;\to\; \mathit{UPred}^{\uparrow}(\mathit{Val})$$
$$\mathit{MT} \;=\; \tfrac{1}{2} \cdot W \;\to\; \mathit{UPred}^{\uparrow}(\mathit{Val} \times \mathit{Heap}) \;.$$

In particular, in each case there is an action of W by the operation $\otimes$, as described in Proposition 3.3. Note that $\mathit{Cap} = \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Heap})$ acts on itself, via the isomorphism ι between W and *Cap*. This operation plays a key role in explaining the higher-order frame (and also anti-frame) inference rules and the associated distribution axioms [44, 45]. Moreover, due to the shrinking factor $\delta = \frac{1}{2}$, this action is contractive in its right-hand side: for all $p, r \in \mathit{Cap}$, the assignment $r \mapsto p \otimes \iota(r)$ is a contractive endomap on *Cap*. This observation explains why the (syntactic) invariant extension can be assumed formally contractive in its second argument.

We also consider a further overloading of the separating conjunction. It is the below generalization $S * q$ to sets of the form $S \in \mathit{UPred}^{\uparrow}(A \times \mathit{Heap})$ and $q \in \mathit{UPred}^{\uparrow}(\mathit{Heap})$:

$$S * q = \{(k,(a, h \cdot h')) \mid (k,(a,h)) \in S \wedge (k,h') \in q \wedge h\#h'\}.$$

As for the separating conjunction on $\mathit{UPred}^{\uparrow}(\mathit{Heap})$, this operation can be lifted pointwise to give a non-expansive operation on $S \in \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(A \times \mathit{Heap})$ and $r \in \mathit{Cap}$,

$$(S * r)(w) = S(w) * r(w) \; . \tag{47}$$

This provides a second monoid action, with respect to the monoid structure given by the separating conjunction on *Cap*.

Proposition 3.4 (Monoid and monoid action). $(\mathit{Cap}, *, I)$ is a commutative monoid, and for any (pre-ordered) set A the operation in (47) is an action of this monoid on the space of non-expansive functions from $\frac{1}{2} \cdot W$ to $\mathit{UPred}^{\uparrow}(A \times \mathit{Heap})$, i.e., $S * I = S$ and $(S * p) * q = S * (p * q)$.

The interpretation of capabilities and types is given in Figure 9. This interpretation depends on an environment η, which maps region names $\sigma \in \mathit{RegName}$ to closed values $\eta(\sigma) \in \mathit{Val}$, capability variables γ to semantic capabilities $\eta(\gamma) \in \mathit{Cap}$, and type variables α and β to semantic types $\eta(\alpha) \in \mathit{VT}$ and $\eta(\beta) \in \mathit{MT}$. As indicated above, the semantics of capabilities is defined in terms of the BI structure on *Cap*. The semantics of memory types uses the action of *Cap* on *MT* described in (47). It also makes explicit the aliasing information contained in memory types: for instance, the two components of a pair of type $\theta_1 \times \theta_2$ cannot overlap in the heap (a similar exclusion of sharing holds for referenced cells). In the interpretation of a value type τ considered as memory type, $[\![\tau]\!]$ on the right-hand side refers to the value type interpretation. Note that the computation types χ form a subset of the memory types, and thus obtain their interpretation in *MT*.

Let *Env* denote the finite maps from variables to closed values. Duplicable (heap-independent) environments are interpreted as contractive maps from W to $\mathit{UPred}^{\uparrow}(\mathit{Env})$. Linear environments are modelled as contractive maps from W to $\mathit{UPred}^{\uparrow}(\mathit{Env} \times \mathit{Heap})$. Conceptually, each of the entries in a linear environment owns a part of the heap, disjoint from that of the other entries.

With the exception of arrow types, the semantics of value types deserves little explanation; in all cases, the world is simply passed through, and the index is decreased (whenever justified by the operational semantics) to ensure that type constructors become contractive. The definition of arrow types is more intricate, and uses the following extension of memory types from values to expressions.

Definition 3.5. Let $S \in \mathit{MT}$. Then the function $\mathcal{E}(S) : W \to \mathit{UPred}^{\uparrow}(\mathit{Exp} \times \mathit{Heap})$ is defined by $(k,(t,h)) \in \mathcal{E}(S)(w)$ iff

$$\forall j \leq k, t', h'.\ (t \mid h) \longmapsto^{j} (t' \mid h') \ \wedge\ (t' \mid h') \text{ irreducible} \\ \Rightarrow\ (k-j,(t',h')) \in S(w) * \iota^{-1}(w)(\mathit{emp}) \; .$$

Note that there is no scaling by $\frac{1}{2}$, i.e., $\mathcal{E}(S)$ is a non-expansive, but not a contractive, function of worlds. However, we do have a form of contractiveness on non-values:

Lemma 3.6. For all $S_1, S_2 \in \mathit{MT}$, expressions t and $h \in \mathit{Heap}$, if $w_1 \overset{n}{=} w_2$ in W, $S_1 \overset{n-1}{=} S_2$ and $t \notin \mathit{Val}$, then for all $k \leq n$,

$$(k,(t,h)) \in \mathcal{E}(S_1)(w_1) \ \Leftrightarrow\ (k,(t,h)) \in \mathcal{E}(S_2)(w_2) \; .$$

Proof. Let $w_1 \overset{n}{=} w_2$, and observe that this implies $S_1(w_1) \overset{m}{=} S_2(w_2)$ and $\iota^{-1}(w_1)(\mathit{emp}) \overset{m}{=} \iota^{-1}(w_2)(\mathit{emp})$ for any $m < n$. Now assume that $(k,(t,h)) \in \mathcal{E}(S_1)(w_1)$ for some $k \leq n$. We must show that $(k,(t,h)) \in \mathcal{E}(S_2)(w_2)$. For this, suppose that $(t \mid h) \longmapsto^{j} (t' \mid h')$ for some $j \leq k$ where $(t' \mid h')$ is irreducible. The assumption $(k,(t,h)) \in \mathcal{E}(S_1)(w_1)$ yields $(k-j,(t',h')) \in S_1(w_1) * \iota^{-1}(w_1)(\mathit{emp})$. In particular, $t' \in \mathit{Val}$ and therefore $t \neq t'$ by the assumption that $t \notin \mathit{Val}$. Thus we must have $j > 0$, and therefore $k - j < k \leq n$ which by the above observations means that $(k-j,(t',h')) \in S_2(w_2) * \iota^{-1}(w_2)(\mathit{emp})$.

The direction from right to left is symmetric. □

We now explain the ideas behind the definition of arrow types in Figure 9 in more detail. First, the basic idea of our Kripke style semantics is that invariants added by the context are collected in the worlds. Thus, for a procedure application we realize this idea by interpreting the current world as a predicate $\iota^{-1}(w)(\mathit{emp})$ on heaps, which is conjoined to the actual argument (computation) type $[\![\chi_1]\!]_\eta\,(w)$, as well as to the result (computation) type $[\![\chi_2]\!]_\eta\,(w)$ through the definition of $\mathcal{E}$. Second, by additionally conjoining r as an invariant we bake in the first-order frame property. Finally, the quantification over indices j less than k achieves that $[\![\chi_1 \to \chi_2]\!]_\eta\, w$ is in $\mathit{UPred}^{\uparrow}(\mathit{Val})$. There are two explanations why we require that j be *strictly* less than k in the definition of $[\![\chi_1 \to \chi_2]\!]$. Technically, the use of $\iota^{-1}(w)$ in the definition "undoes" the scaling by $\frac{1}{2}$, and the strictly smaller index is needed to ensure the non-expansiveness of $[\![\chi_1 \to \chi_2]\!]$ as a function $\frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Val})$. Moreover, the smaller index allows us to prove the typing rule for recursive functions, by induction on k. Intuitively, the use of $j < k$ for the arguments suffices since each procedure application consumes a step.

Proposition 3.7. The interpretation in Figure 9 is well-defined: all the $[\![\cdot]\!]$'s map into the declared sets, and the recursive definitions of capabilities and types have unique solutions.

Proof sketch. We equip the set of values with the discrete metric, and then obtain a complete 1-bounded ultrametric on environments:

$$d(\eta,\eta') \ = \ \sup_{\xi} d(\eta(\xi), \eta'(\xi)) \; . \tag{48}$$

We then show by simultaneous induction on C, τ, and θ, the following properties:

1. $[\![C]\!]_\eta\, w$, $[\![\tau]\!]_\eta\, w$, and $[\![\theta]\!]_\eta\, w$ are upwards closed and uniform predicates;
2. $[\![C]\!]_\eta\, w$, $[\![\tau]\!]_\eta\, w$, and $[\![\theta]\!]_\eta\, w$ are non-expansive functions of η (with respect to the distance in (48)) and w (with respect to the metric on $\frac{1}{2} \cdot W$);
3. if C is formally contractive in ξ then $[\![C]\!]_{\eta[\xi:=(\cdot)]}$ is contractive;
4. if θ is formally contractive in ξ then $[\![\theta]\!]_{\eta[\xi:=(\cdot)]}$ is contractive.

These properties can be verified by a straightforward (but tedious) simultaneous induction, for instance using Lemma 3.6 and the non-expansiveness of separating conjunction to show the non-expansiveness of arrow types. The interpretation of recursive types and capabilities relies on our restriction to formally contractive equations, so that they are uniquely defined from Banach's fixed point theorem by the above properties 3 and 4. □

This interpretation respects the structural equivalence, i.e., whenever C_1 and C_2 are equivalent capabilities then $[\![C_1]\!] = [\![C_2]\!]$ (and similarly for value and memory types). The proofs of these facts are easy consequences of the definition of $[\![C]\!]$ and Propositions 3.3 and 3.4, and are given in Appendix C.1. Moreover, the interpretation validates the subtyping axioms, i.e., whenever $\theta_1 \leq \theta_2$ then $[\![\theta_1]\!]_\eta\, w \subseteq [\![\theta_2]\!]_\eta\, w$ holds for all η and w. These proofs can be found in Appendix C.2.

Recall that we have two kinds of judgments, one for typing of values and the other for the typing of expressions:

$$\Delta \vdash v : \tau \qquad\qquad \Gamma \Vdash t : \chi$$

Capabilities, $[\![C]\!]_\eta : \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Heap})$

$$[\![C_1 \otimes C_2]\!]_\eta\, w = ([\![C_1]\!]_\eta \otimes \iota([\![C_2]\!]_\eta))w$$
$$[\![\emptyset]\!]_\eta\, w = \mathbb{N} \times \mathit{Heap}$$
$$[\![C_1 * C_2]\!]_\eta\, w = ([\![C_1]\!]_\eta * [\![C_2]\!]_\eta)w$$
$$[\![\{\sigma : \theta\}]\!]_\eta\, w = \{(k,h) \mid (k,(\eta(\sigma),h)) \in [\![\theta]\!]_\eta\, w\}$$
$$[\![\exists \sigma.C]\!]_\eta\, w = \textstyle\bigcup_{v \in \mathit{Val}} [\![C]\!]_{\eta[\sigma:=v]}\, w$$
$$[\![\gamma]\!]_\eta\, w = \eta(\gamma)(w)$$
$$[\![\mu\gamma.C]\!]_\eta\, w = \mathit{fix}(\lambda r.\ [\![C]\!]_{\eta[\gamma:=r]})w$$

Value types, $[\![\tau]\!]_\eta : \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Val})$

$$[\![\tau \otimes C]\!]_\eta\, w = ([\![\tau]\!]_\eta \otimes \iota([\![C]\!]_\eta))w$$
$$[\![0]\!]_\eta\, w = \emptyset$$
$$[\![1]\!]_\eta\, w = \mathbb{N} \times \{()\}$$
$$[\![\mathsf{int}]\!]_\eta\, w = \mathbb{N} \times \{\underline{n} \mid n \in \mathbb{Z}\}$$
$$[\![\tau_1 + \tau_2]\!]_\eta\, w = \{(k, \mathsf{inj}^i v) \mid k > 0 \Rightarrow (k-1, v) \in [\![\tau_i]\!]_\eta\, w\}$$
$$[\![\tau_1 \times \tau_2]\!]_\eta\, w = \{(k, (v_1, v_2)) \mid k > 0 \Rightarrow (k-1, v_i) \in [\![\tau_i]\!]_\eta\, w\}$$
$$[\![\chi_1 \to \chi_2]\!]_\eta\, w = \{(k,v) \mid \forall j < k.\ \forall r \in \mathit{Cap}.\ \forall (j,(v',h)) \in ([\![\chi_1]\!]_\eta * r)(w) * \iota^{-1}(w)(\mathit{emp}).\ (j{+}1, (v\,v', h)) \in \mathcal{E}([\![\chi_2]\!]_\eta * r)(w)\}$$
$$[\![[\sigma]]\!]_\eta\, w = \mathbb{N} \times \{\eta(\sigma)\}$$
$$[\![\alpha]\!]_\eta\, w = \eta(\alpha)(w)$$
$$[\![\mu\alpha.\tau]\!]_\eta\, w = \mathit{fix}(\lambda S.\ [\![\tau]\!]_{\eta[\alpha:=S]})w$$
$$[\![\forall\alpha.\tau]\!]_\eta\, w = \textstyle\bigcap_{a \in \mathit{VT}} [\![\tau]\!]_{\eta[\alpha:=a]}\, w$$

Memory types, $[\![\theta]\!]_\eta : \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Val} \times \mathit{Heap})$

$$[\![\theta \otimes C]\!]_\eta\, w = ([\![\theta]\!]_\eta \otimes \iota([\![C]\!]_\eta))\, w$$
$$[\![\tau]\!]_\eta\, w = \{(k,(v,h)) \mid h \in \mathit{Heap},\ (k,v) \in [\![\tau]\!]_\eta\, w\}$$
$$[\![\theta_1 + \theta_2]\!]_\eta\, w = \{(k, (\mathsf{inj}^i v, h)) \mid k{>}0 \Rightarrow (k-1, (v,h)) \in [\![\theta_i]\!]_\eta\, w\}$$
$$[\![\theta_1 \times \theta_2]\!]_\eta\, w = \{(k, (v_1,v_2), h_1{\cdot}h_2) \mid k{>}0 \Rightarrow (k-1, (v_i,h_i)) \in [\![\theta_i]\!]_\eta w\}$$
$$[\![\mathsf{ref}\,\theta]\!]_\eta\, w = \{(k, (l, h{\cdot}[l \mapsto v])) \mid k{>}0 \Rightarrow (k-1, (v,h)) \in [\![\theta]\!]_\eta w\}$$
$$[\![\theta * C]\!]_\eta\, w = ([\![\theta]\!]_\eta\, w) * ([\![C]\!]_\eta\, w)$$
$$[\![\exists\sigma.\theta]\!]_\eta\, w = \textstyle\bigcup_{v \in \mathit{Val}} [\![\theta]\!]_{\eta[\sigma:=v]}\, w$$
$$[\![\beta]\!]_\eta\, w = \eta(\beta)(w)$$
$$[\![\mu\beta.\theta]\!]_\eta\, w = \mathit{fix}(\lambda S.\ [\![\theta]\!]_{\eta[\beta:=S]})w$$

Duplicable environments, $[\![\theta]\!]_\eta : \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Env})$

$$[\![\Delta \otimes C]\!]_\eta\, w = ([\![\Delta]\!]_\eta \otimes \iota([\![C]\!]_\eta))w$$
$$[\![\varnothing]\!]_\eta\, w = \mathbb{N} \times \{[\,]\}$$
$$[\![\Delta, x{:}\tau]\!]_\eta\, w = \{(k, \rho[x \mapsto v]) \mid (k,\rho) \in [\![\Delta]\!]_\eta\, w \wedge (k,v) \in [\![\tau]\!]_\eta\, w\}$$

Linear environments, $[\![\theta]\!]_\eta : \frac{1}{2} \cdot W \to \mathit{UPred}^{\uparrow}(\mathit{Env} \times \mathit{Heap})$

$$[\![\Gamma \otimes C]\!]_\eta\, w = ([\![\Gamma]\!]_\eta \otimes \iota([\![C]\!]_\eta))w$$
$$[\![\varnothing]\!]_\eta\, w = \mathbb{N} \times (\{[\,]\} \times \mathit{Heap})$$
$$[\![\Gamma, x{:}\chi]\!]_\eta\, w = \{(k, (\rho[x \mapsto v], h \cdot h')) \mid (k,(\rho,h)) \in [\![\Gamma]\!]_\eta\, w \wedge (k,(v,h')) \in [\![\chi]\!]_\eta\, w\}$$
$$[\![\Gamma * C]\!]_\eta\, w = ([\![\Gamma]\!]_\eta\, w) * ([\![C]\!]_\eta\, w)$$

Figure 9. Interpretation

The semantics of a value judgement simply establishes truth with respect to all worlds w, all environments η and all $k \in \mathbb{N}$:

$$\models (\Delta \vdash v : \tau) \overset{\mathit{def}}{\iff} \forall\eta.\ \forall w \in W.\ \forall k \in \mathbb{N}.\ \forall (k,\rho) \in [\![\Delta]\!]_\eta\, w.\ (k, \rho(v)) \in [\![\tau]\!]_\eta\, w\ .$$

Here $\rho(v)$ means the application of the substitution ρ to v. The judgement for expressions mirrors the interpretation of the arrow case for value types, in that there is also a quantification over heap predicates $r \in \mathit{Cap}$:

$$\models (\Gamma \Vdash t : \chi) \overset{\mathit{def}}{\iff} \forall\eta.\ \forall w \in W.\ \forall k \in \mathbb{N}.\ \forall r \in \mathit{Cap}.\ \forall (k,(\rho,h)) \in ([\![\Gamma]\!]_\eta * r)w * \iota^{-1}(w)(\mathit{emp}).\ (k, (\rho(t), h)) \in \mathcal{E}([\![\chi]\!]_\eta * r)(w).$$

The universal quantifications allow us to have frame rules: the universal quantification over worlds w ensures the soundness of the deep frame rule, and the universal quantification over capabilities r validates the shallow frame rule.

We can now give the main result of this section, which expresses that the extension of the capability system with higher-order frame rules is sound. In particular, the below theorem implies type safety.

Theorem 3.8 (Soundness)**.** If $\Delta \vdash v : \tau$ then $\models (\Delta \vdash v : \tau)$, and if $\Gamma \Vdash t : \chi$ then $\models (\Gamma \Vdash t : \chi)$.

To prove the theorem, we show that each typing rule preserves the truth of judgements. These proofs are given in Appendix C.3.

3.4 Observations

We conclude this section with some remarks on the model.

Structural equivalence. In previous work, where Pottier first introduced the anti-frame rule [38], the syntactic types are considered modulo the structural equivalence. This means that they are not inductively defined, and consequently Pottier avoids inductive proofs on their syntax. In contrast, our interpretation is given by induction on the structure of types and capabilities, and only after having established the interpretation do we consider the structural equivalence (and prove that our interpretation respects it).

Unique solutions proof principle. In practice, one may have to show type equivalences that do not easily follow from the structural equivalence. The metric structure of our model suggests a proof principle for this, by the uniqueness of solutions of contractive type equations: if two types are solutions of a common contractive fixed point equation, then we can conclude that they are equal.

Additional subtyping axioms. Our model satisfies some additional subtyping axioms that have not been mentioned in the literature before. These refer, e.g. to the duplication of value capabilities. In particular, our model implies the soundness of the axiom

$$[\sigma] * \{\sigma : \tau\} \ \leq\ [\sigma] * \{\sigma : \tau\} * \{\sigma : \tau\}.$$

A possible explanation why these axioms have not been noted before may be that previous soundness proofs for capability type systems (e.g. by translation [25] or progress and preservation [38]) rest on invariants that are stronger than necessary.

Classical interpretation. The capability calculus of Crary et al. [27] has a memory deallocation construct, and satisfies a "complete collection" property. Essentially, if a program of type $\tau * \emptyset$ terminates, then it does so in an empty heap. After dropping the subtyping axiom $C_1 * C_2 \leq C_1$ and adding a deallocation construct to our calculus, it would also satisfy this property. Our approach is flexible enough so that this can be shown by modifying the semantics and using the "classical" interpretation of separation logic.

That is, the definition of worlds and capabilities would be based on $UPred(Heap)$ where *Heap* is discretely ordered, and where the BI structure is given by $*$ and $-\!\!*$ as above but with unit $I = \omega \times \{[]\}$. However, this complete collection property is not only destroyed by the axiom $C_1 * C_2 \leq C_1$ but also by the inclusion of an anti-frame rule (which we do not consider in this paper, though).

Aliasing. Even though our model is based on the operational semantics, it gives a semantic understanding of capabilities. Let θ be any memory type, and consider the recursively defined memory type $mlist = \mu\beta.\mathsf{ref}\ 1 + \theta \times \beta$ of mutable lists from [25]. In *loc. cit.* it is mentioned (without proof) that this is the type of mutable *non-aliased* lists, and our semantics shows very directly that this is indeed the case: From the semantics of memory types in Figure 9, we see (for k large enough) that $(k, (l_1, h)) \in [\![mlist]\!]$ just in case that for some $n < k$, heap h can be split up into $2n$ disjoint parts:

$$h = [l_1 \mapsto (v_1, l_2)] \cdot h_1 \cdot [l_2 \mapsto (v_2, l_3)] \cdot h_2 \cdot \dots \cdot [l_n \mapsto ()] \cdot h_n,$$

with $(k-i, (v_i, h_i)) \in [\![\theta]\!]$, for all $1 \leq i < n$. Thus, all list entries live in disjoint parts of the heap and all locations l_i must be distinct; in particular, $mlist$ cannot contain cyclic lists.

4. Specialization to Indirection Theory

Hobor, Dockins and Appel [31] present a general *theory of indirection* for giving set-theoretic models of recursively defined structures. Faced with a recursive equation, Hobor et al. provide an approximate solution: this is a set together with a pair of functions characterized by the two axioms of indirection theory that elegantly capture the approximative nature of the solution.

Our approach to recursive equations is different. We provide an exact solution, but in a category of metric spaces instead of the category of sets and functions. In this section we argue that our approach is more general in the sense that, for the same recursive equation, one may build the approximative solution of Hobor et al. from our solution.

Before starting, we point out that this specialization to indirection theory is not unconditional. The construction presented by Hobor et al. is parameterized over a set-theoretic functor F : **Set** $\to$ **Set**, and this functor must in a suitable sense have an extension to **CBUlt**$_{\text{ne}}$ in order for our approach to apply. Fortunately, this condition holds for functors on **Set** built with standard constructors. In return for requiring this extra condition, we can obtain an approximate solution that improves on the one constructed in Hobor et al.: the metric-space setup guarantees that all the predicates we consider are so-called *hereditary*.

We now sketch how the specialization to indirection theory proceeds. The full story, including proofs, can be found in Appendices A and B.

4.1 Indirection Theory

Assume that we are given a functor F : **Set** $\to$ **Set** and a non-empty set O. Let $2 = \{0, 1\}$ be the set of "truth values." Indirection theory begins from the desire to solve the equation

$$K \cong F(K \times O \to 2) \tag{49}$$

in **Set**, which is often impossible for cardinality reasons.[6] Instead, one obtains an approximate solution

$$K \underset{\mathsf{squash}}{\overset{\mathsf{unsquash}}{\rightleftarrows}} \mathbb{N} \times F(K \times O \to 2)$$

[6] Unlike Hobor et al. we do not parameterize over the set of truth values. The generalization, while probably technically feasible, does not appear necessary for applications.

consisting of a set K and functions squash and $\mathsf{unsquash}$ satisfying:

1. $\mathsf{squash}(\mathsf{unsquash}\ k) = k$.
2. $\mathsf{unsquash}(\mathsf{squash}(m, \nu)) = (m, F(\mathsf{approx}_m)(\nu))$.

Here $\mathsf{level} = \mathsf{fst} \circ \mathsf{unsquash} : K \to \mathbb{N}$, and the map approx_m : $(K \times O \to 2) \to (K \times O \to 2)$ is defined, for each $m \in \mathbb{N}$, by

$$\mathsf{approx}_m(\psi)(k, o) \;\; = \;\; (\psi(k, o) \wedge \mathsf{level}(k) < m).$$

The idea is that elements of K have "levels," and that the function approx_m transforms a predicate on K to one that only holds for elements of level less than m. Notice that squash is a left inverse of $\mathsf{unsquash}$, but in general not a right inverse: $\mathsf{unsquash}(\mathsf{squash}(m, \nu))$ is in some sense an approximation of (m, ν).

4.2 From Metric Spaces to Indirection Theory

Every set can be considered as a metric space by giving it the discrete metric d (i.e., $d(x, y) = 1$ if $x \neq y$). In this way, the category of non-empty sets can be viewed as a subcategory of **CBUlt**$_{\text{ne}}$. We now assume that the functor F : **Set** $\to$ **Set** considered above has a so-called *plain lift* $\hat{F}$: **CBUlt**$_{\text{ne}}$ $\to$ **CBUlt**$_{\text{ne}}$. This means that $\hat{F}$ is a locally non-expansive functor which agrees with F on non-empty sets (and functions between them), and also that $\hat{F}$ satisfies some technical conditions given in Appendix A. As noted above, plain lifts exist for all the standard constructors (see Proposition A.7). In particular we have plain lifts of the functors of all the examples of Hobor et al.[7]

From Theorem 2.1 and Lemma 2.4, we easily obtain:

Theorem 4.1. There is a non-empty, complete, 1-bounded ultrametric space X and an isomorphism

$$\Phi \; : \; X \;\; \cong \;\; \hat{F}\left(\tfrac{1}{2}\left(X \to UPred(O)\right)\right),$$

where the function space consists of non-expansive maps.

We now show that one can use such an isomorphism to construct an approximate solution in the sense of indirection theory.

We deviate from Hobor et al. by building a solution that features only so-called *hereditary* maps from $K \times O$ to 2. This is a direct consequence of the downwards closedness required of members of $UPred(O)$, since hereditary predicates are, intuitively, "closed under approximation" in the K component. As mentioned above, we regard this difference as an improvement. Indeed, Hobor et al. state a clear desire to consider hereditary predicates only (Section 5.3) and briefly mention an alternative, more complicated construction of approximate solutions that guarantees that all predicates are hereditary (Section 10). Here we obtain such a guarantee directly from the metric-space setup.

Theorem 4.2. Let F : **Set** $\to$ **Set** be a functor with a plain lift $\hat{F}$: **CBUlt**$_{\text{ne}}$ $\to$ **CBUlt**$_{\text{ne}}$. We can, from the isomorphism of Theorem 4.1, build a set K, a subset of *hereditary* maps $K \times O \to_{her} 2$ of the full function space $K \times O \to 2$ and two maps

$$K \underset{\mathsf{squash}}{\overset{\mathsf{unsquash}}{\rightleftarrows}} \mathbb{N} \times F(K \times O \to_{her} 2)$$

satisfying Hobor et al.'s requirements for an approximate solution (items 1 and 2 above).

Advantages of metric solution approach. Having proved that our metric-space approach specializes to the indirection theory, we now proceed to argue some advantages of our approach in general.

[7] With the possible exception of Example 2.7. The functor in that example is complex, and the presentation is a bit dense, so we are not sure whether the functor has a plain lift.

Firstly, although we do not think that the step-indexed version of our metric-space approach is more expressive than standard step-indexed models, we believe that our version provides a good framework for doing step-indexing with useful conceptual guidelines. This holds even if we disregard recursively defined worlds. Consider the interpretation of recursive types in Section 3. The idea of 'stepping one down' when interpreting recursive types seems natural to anyone familiar with step-indexed models. But coming up with the correct criteria on the interpretation function for this to work out properly, also with nested recursive types, is not so easy a priori. If, however, we employ the metric approach, including Banach's fixed-point theorem, then writing down the requirements as done in the section is straightforward. Another example is the $\otimes$ operator in the same section, which is constructed using Banach's fixed-point theorem. A similar construction could possibly be pushed through either with hand-built approximate worlds as employed by Ahmed et al. [4] or with the indirection theory of Hobor et al. [31]. But the precise course of action is much less immediate.

Secondly, in comparison with the indirection theory [31], our approach of solving recursive metric equations allows one to use a body of supporting theory on metric spaces and to construct a wider variety of possible worlds to be used in Kripke models. To illustrate this point, let us focus on the step-indexed model of ML references discussed in Section 2.3 and in Sections 2.1, 4.1 and 5 of [31]. In the model provided by indirection theory, types are arbitrary maps from worlds to values, modulo currying and nomenclature. But, as argued in [31, Section 5.1], we really want types that are both hereditary and monotone. In [31, Section 5.1], such types are elegantly identified using modal operators, but this does not change the problem that the types in a world may fail to meet these criteria. This is addressed in the last paragraph of [31, Section 10] where an alternative, and less straightforward, model with only hereditary types in the worlds is sketched. Alas, this means that one has to start the model construction all over again from scratch and it does not buy us monotonicity. On the other hand, to obtain hereditary types with the metric approach we just use the downwards-closure condition on $UPred(V)$, verify Lemma 2.4 and apply Theorem 2.1. And to work with monotone types, we can apply a slightly stronger existence result [21, Proposition 5.4] for *pre-ordered* metric spaces. By a similar argument one can extend the approach to mixed variance functors discussed in [31, Section 10]: Indeed, in unpublished work we have used mixed-variance functors to verify that the metric-space approach scales to the elaborate worlds of [4].

Finally, we think that it is advantageous that the metric approach applies both to models based on domain theory and to models based on operational semantics.

5. Related and Future Work

Relational reasoning. We have focused on unary reasoning in this paper, but the techniques developed here also apply to relational reasoning. Relational reasoning principles about programs with higher-order store, such as logical relations for reasoning about contextual equivalence of programs, have been developed both based on domain theory (e.g., [15, 22]), and on step-indexed models (e.g., [4]). For such relational reasoning, the worlds are typically more sophisticated than the worlds we have discussed so far. This is because for relational reasoning worlds need to describe situations in which programs are contextually equivalent even though they use local states in different ways. One of us (Thamsborg) has recently phrased the state-of-the-art world model from [4] as a recursive world equation over a domain-theoretic model. He did this to obtain more abstract proof principles for program equivalences, which does not involve reasoning about step indices. Alternatively, Dreyer et al. [29] have shown how to extend the relational step-indexed model [4] to a model of a modal logic for more abstract reasoning about program equivalences. The latter modal logic has been derived from the step-indexed model. Even with this development, it is still a challenge to develop relational step-indexed models of Hoare Type Theory [35] and its new developments. It would be interesting to see whether the step-indexed metric space approach can be used to address this challenge.

Formalization. An often mentioned advantage of the traditional step-indexed approach is that it lends itself well to formalization in theorem provers. Indeed, impressive formalization work has been carried out in, e.g., Coq [10].

Thus, one may wonder whether our proposed metric approach hinders formalizations. It does not. Following the treatment in [21], Varming et. al. have recently formalized the solutions of recursive metric-space equations in Coq [16] and the step-indexed model of ML references from Section 2.3.

Capabilities. In [3], Ahmed et al. presented a step-indexed model of a substructural type system, which is similar to the capability calculus considered in this paper. However, their model did not provide a satisfactory semantic analysis of capabilities. Ahmed et al. instrumented the operational semantics with abstract run-time entities corresponding to capabilities, and their model included those abstract entities, instead of giving a semantic analysis of what they really should denote. Moreover, they did not consider non-trivial combinations of capabilities such as $C_1 * C_2$ and did not include frame rules, etc. The step-indexed model in this paper does not alter the operational semantics, interprets capabilities including $C_1 * C_2$ and justifies (shallow and deep) frame rules.

We point out that an alternative semantic model of the basic capability system could be obtained by combining the functional translation of Charguéraud and Pottier [25] with a semantic model of their purely functional target calculus. The functional translation in [25] does not, however, include higher-order frame rules and it is not immediate how to include those rules.

To extend our semantics to group regions is future work. Note that group regions are non-trivial, since they might grow over time but types need to be invariant (monotone) with respect to this growth. Further extensions will address, for instance, frame rules for more general (parameterized) invariants on local state [39].

Other operational techniques. We briefly mention two techniques other than step indexing that can be used to define logical relations based on operational semantics. First, *syntactic minimal invariance* [18, 26] is based on operational counterparts of the projection functions one obtains from solutions to recursive domain equations. As far as we know, this technique has not been developed for languages with store. Second, *biorthogonality* [13, 32, 37] is based on syntactically defined closure operators on relations. Biorthogonality has been developed for a language with integer store [37], but not (without also using step indexing) for languages with general recursive types or higher-order store. Voullion and Melliès [49] give an axiomatic setup that incorporates both of these techniques (for a language without store).

As an alternative to logical relations, techniques based on *bisimulation* can be used to show contextual equivalences for languages with store [48]. However, such techniques do not seem helpful for modelling expressive type systems such as the one considered in Section 3.

6. Conclusion

In this paper, we have argued that recursive features of programming languages, type systems and program logics, such as higher-order store, can be naturally interpreted via Kripke models over worlds that are recursively defined in a category of metric spaces. Interestingly, this can be carried out not only denotationally but also using operational semantics. Our method combines the simplicity of existing step-indexed models with the accuracy of domain-theoretic approaches for recursive domain equations. Unlike other step-indexed models, our method uses solutions of the original recursive equations, not their approximated versions. The benefits of this technique have been demonstrated in our new semantics of Charguéraud and Pottier's type-and-capability system [25], where solving an original recursive equation over worlds played a crucial role in modelling a recursively defined operator on worlds.

Additionally, we have shown that our metric approach can be specialized to Hobor et al.'s recent proposal [31] and argued that the metric approach has some advantages.

Acknowledgments

We would like to thank François Pottier, Aquinas Hobor, Robert Dockins, Andrew W. Appel and Carsten Varming for helpful discussions and insightful comments. Yang and Reus acknowledge support from the EPSRC.

References

[1] M. Abadi and G. D. Plotkin. A per model of polymorphism and recursive types. In *Proceedings of LICS*, pages 355–365, 1990.

[2] A. Ahmed. *Semantics of Types for Mutable State*. PhD thesis, Princeton University, 2004.

[3] A. Ahmed, M. Fluet, and G. Morrisett. L3: A linear language with locations. *Fundam. Inf.*, 77(4):397–449, 2007.

[4] A. Ahmed, D. Dreyer, and A. Rossberg. State-dependent representation independence. In *Proceedings of POPL*, pages 340–353, 2009.

[5] A. J. Ahmed. Step-indexed syntactic logical relations for recursive and quantified types. In P. Sestoft, editor, *ESOP*, volume 3924 of *Lecture Notes in Computer Science*, pages 69–83. Springer, 2006. ISBN 3-540-33095-X.

[6] A. J. Ahmed, A. W. Appel, and R. Virga. A stratified semantics of general references. In *Proceedings of LICS*, pages 75–84, 2002.

[7] R. M. Amadio. Recursion over realizability structures. *Information and Computation*, 91(1):55–85, 1991.

[8] R. M. Amadio and P.-L. Curien. *Domains and Lambda-Calculi*. Cambridge University Press, 1998.

[9] P. America and J. J. M. M. Rutten. Solving reflexive domain equations in a category of complete metric spaces. *J. Comput. Syst. Sci.*, 39(3):343–375, 1989.

[10] A. Appel, R. Dockins, and A. Hobor. Mechanized semantic library. `http://msl.cs.princeton.edu/`, 2009.

[11] A. W. Appel and D. A. McAllester. An indexed model of recursive types for foundational proof-carrying code. *ACM Trans. Program. Lang. Syst.*, 23(5): 657–683, 2001.

[12] A. W. Appel, P. Melliès, C. D. Richards, and J. Vouillon. A very modal model of a modern, major, general type system. In *Proceedings of POPL*, pages 109–122, 2007.

[13] N. Benton and C.-K. Hur. Biorthogonality, step-indexing and compiler correctness. In *Proceedings of ICFP*, pages 97–108, 2009.

[14] N. Benton and B. Leperchey. Relational reasoning in a nominal semantics for storage. In *Proceedings of TLCA*, pages 86–101, 2005.

[15] N. Benton, L. Beringer, M. Hofmann, and A. Kennedy. Relational semantics for effect-based program transformations: Higher-order store. In *Proceedings of PPDP*, pages 301–312, 2009.

[16] N. Benton, A. Kennedy, C. Varming, and L. Birkedal. Formalizing domains, ultrametric spaces and semantics of programming languages. Manuscript. Available at `http://www.itu.dk/people /birkedal/papers/formalizing-semantics.pdf`, 2010.

[17] B. Biering, L. Birkedal, and N. Torp-Smith. Bi-hyperdoctrines, higher-order separation logic, and abstraction. *ACM Trans. Program. Lang. Syst.*, 29(5), 2007.

[18] L. Birkedal and R. W. Harper. Constructing interpretations of recursive types in an operational setting. *Information and Computation*, 155:3–63, 1999.

[19] L. Birkedal, N. Torp-Smith, and H. Yang. Semantics of separation-logic typing and higher-order frame rules for Algol-like languages. *LMCS*, 2(5:1), 2006.

[20] L. Birkedal, B. Reus, J. Schwinghammer, and H. Yang. A Simple Model of Separation Logic for Higher-order Store. In *Proceedings of ICALP*, pages 348–360, 2008.

[21] L. Birkedal, K. Støvring, and J. Thamsborg. The category-theoretic solution of recursive metric-space quations. Technical Report ITU-2009-119, IT University of Copenhagen, 2009.

[22] L. Birkedal, K. Støvring, and J. Thamsborg. Realizability semantics of parametric polymorphism, general references, and recursive types. In *Proceedings of FOSSACS*, pages 456–470, 2009.

[23] N. Bohr and L. Birkedal. Relational reasoning for recursive types and references. In *Proceedings of APLAS*, pages 79–96, 2006.

[24] F. Cardone. Relational semantics for recursive types and bounded quantification. In *Proceedings of ICALP*, pages 164–178, 1989.

[25] A. Charguéraud and F. Pottier. Functional translation of a calculus of capabilities. In *Proceedings of ICFP*, pages 213–224, 2008.

[26] K. Crary and R. Harper. Syntactic logical relations for polymorphic and recursive types. *Electronic Notes in Theoretical Computer Science*, 172:259–299, 2007.

[27] K. Crary, D. Walker, and G. Morrisett. Typed memory management in a calculus of capabilities. In *Proceedings of POPL*, pages 262–275, 1999.

[28] J. de Bakker and E. de Vink. *Control flow semantics*. MIT Press, 1996.

[29] D. Dreyer, G. Neis, A. Rossberg, and L. Birkedal. A relational modal logic for higher-order stateful ADTs. In *Proceedings of POPL*, pages 185–198, 2010.

[30] A. Hobor, A. Appel, and F. Nardelli. Oracle semantics for concurrent separation logic. In *Proceedings of ESOP*, pages 353–367, 2008.

[31] A. Hobor, R. Dockins, and A. Appel. A theory of indirection via approximation. In *Proceedings of POPL*, pages 171–184, 2010.

[32] P. Johann and J. Voigtländer. A family of syntactic logical relations for the semantics of haskell-like languages. *Informantion and Computation*, 207(2): 341–368, 2009.

[33] P. B. Levy. Possible world semantics for general storage in call-by-value. In *Proceedings of CSL*, pages 232–246, 2002.

[34] D. B. MacQueen, G. D. Plotkin, and R. Sethi. An ideal model for recursive polymorphic types. *Information and Control*, 71(1/2):95–130, 1986.

[35] A. Nanevski, G. Morrisett, and L. Birkedal. Polymorphism and separation in hoare type theory. In *Proceedings of ICFP*, pages 62–73, 2006.

[36] P. W. O'Hearn and D. J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, June 1999.

[37] A. M. Pitts and I. D. B. Stark. Operational reasoning for functions with local state. In A. D. Gordon and A. M. Pitts, editors, *Higher-Order Operational Techniques in Semantics*, Publications of the Newton Institute, pages 227–273. Cambridge University Press, 1998.

[38] F. Pottier. Hiding local state in direct style: a higher-order anti-frame rule. In *Proceedings of LICS*, pages 331–340, 2008.

[39] F. Pottier. Generalizing the higher-order frame and anti-frame rules. Unpublished, July 2009.

[40] U. S. Reddy and H. Yang. Correctness of data representations involving heap data structures. *Science of Computer Programming*, 50(1–3):129–160, March 2004.

[41] B. Reus and J. Schwinghammer. Separation logic for higher-order store. In *Proceedings of CSL*, pages 575–590, 2006.

[42] B. Reus and T. Streicher. Semantics and logic of object calculi. In *Proceedings of LICS*, pages 113–124, 2002.

[43] J. C. Reynolds. Separation logic: A logic for shared mutable data structures. In *Proceedings of LICS*, pages 55–74, 2002.

[44] J. Schwinghammer, L. Birkedal, B. Reus, and H. Yang. Nested Hoare triples and frame rules for higher-order store. In *Proceedings of CSL*, pages 440–454, 2009.

[45] J. Schwinghammer, H. Yang, L. Birkedal, F. Pottier, and B. Reus. A semantic foundation for hidden state. In *Proceedings of FOSSACS*, pages 2–17, 2010.

[46] M. B. Smyth. Topology. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*. Oxford University Press, 1992.

[47] I. Stark. Categorical models for local names. *LISP and Symbolic Computation*, 9(1):77–107, Feb. 1996.

[48] E. Sumii. A complete characterization of observational equivalence in polymorphic lambda-calculus with general references. In *Proceedings of CSL*, pages 455–469, 2009.

[49] J. Vouillon and P.-A. Melliès. Semantic types: a fresh look at the ideal model for types. In *Proceedings of POPL*, pages 52–63, 2004.

A. Specialization to Indirection Theory

Faced with a higher-order store recursive equation, Hobor, Dockins and Appel [31] provide an approximative solution. This is a section-retraction pair characterized by the two axioms of indirection theory that elegantly capture the approximative nature of the solution. Our approach is different, we solve the recursion proper in a certain category of metric spaces. In both cases, however, the solution provides a notion of worlds[8] to be used in Kripke models as exemplified amply in *loc.cit.* and in the previous section. In this section we shall argue that our approach is the more general in the sense that, for the same recursive equation, one may build the approximative solution of Hobor et al. from our solution – this is Theorem A.6. A consequence is that, somewhat indirectly, we have shown our method applicable to all examples considered by Hobor et al.

This specialization to indirection theory is not unconditional. The construction presented by Hobor et al. is parameterized over a set-theoretic functor $F : \mathbf{Set} \to \mathbf{Set}$ but our approach deals in metric-space equations phrased in terms of a locally non-expansive functor on $\mathbf{CBUlt}_{\mathrm{ne}}$. So we must have one of the latter corresponding to the former or, more precisely, we must have a *plain lift* of $F : \mathbf{Set} \to \mathbf{Set}$, as defined below, to apply the specialization. Fortunately, in many cases such a lift exists; indeed it always holds for functors on **Set** built with standard constructors as is made precise in Proposition A.7. In particular we have plain lifts of the functors of all the examples of Hobor et al.[9]

Definition A.1. A functor $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ is called *non-shrinking* if for any object X and any morphism $\varphi : X \to X$ of $\mathbf{CBUlt}_{\mathrm{ne}}$ and any $m > 0$ such that

$$\forall x, y \in X.\, x =_m y \Rightarrow \varphi(x) = \varphi(y)$$

we also have that

$$\forall x, y \in \hat{F}(X).\, x =_m y \Rightarrow \hat{F}(\varphi)(x) = \hat{F}(\varphi)(y).$$

Here $x =_m y$ is short for $d(x, y) \leq 2^{-m}$ where d is the distance on X. Intuitively, elements of $\hat{F}(X)$ contain components from X. If closeness of two elements of $\hat{F}(X)$ implies similar closeness between the components, then $\hat{F}$ is non-shrinking because $\hat{F}(\varphi)$ applies φ to all components. Note that the condition is required only to hold for $m > 0$; the case $m = 0$ comes down to preserving constant functions and that would preclude, e.g., constant functors.

Definition A.2. A metric space is *bisected* if any non-zero distance is of the form 2^{-m} for some $m \in \mathbb{N}$.

For bisected metric spaces we have the following proposition which is useful for showing maps non-expansive:

Proposition A.3. A map $\varphi : X \to X$ on a bisected metric space X is non-expansive if and only if we have

$$\forall m \in \mathbb{N}.\, \forall x, y \in X.\, x =_m y \Rightarrow \varphi(x) =_m \varphi(y).$$

Definition A.4. We say that a functor $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ is the *lift* of a functor $F : \mathbf{Set} \to \mathbf{Set}$ if the following diagram commutes

$$\begin{array}{ccc} \mathbf{CBUlt}_{\mathrm{ne}} & \xrightarrow{\hat{F}} & \mathbf{CBUlt}_{\mathrm{ne}} \\ {\scriptstyle U}\downarrow & & \downarrow{\scriptstyle U} \\ \mathbf{Set} & \xrightarrow[F]{} & \mathbf{Set}, \end{array}$$

where $U : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{Set}$ is the obvious forgetful functor. Furthermore, we say that a functor $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ is *plain* if it is non-shrinking, locally non-expansive and, on objects, preserves the property of being bisected.

Theorem A.5. Let $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ be a locally non-expansive functor and O a non-empty set. Then there is a non-empty, complete, 1-bounded ultrametric space X and an isomorphism

$$\Phi : X \cong \hat{F}\left(\tfrac{1}{2}\left(X \to_{ne} \mathit{UPred}(O)\right)\right).$$

Here we put a subscript ne on $\to$ and make it explicit that we are using the space of non-expansive functions.

This is an easy consequence of Theorem 2.1: $\hat{F}$ is assumed locally non-expansive and the functor $\frac{1}{2}((-) \to_{ne} \mathit{UPred}(O))$ is a locally contractive contravariant functor on $\mathbf{CBUlt}_{\mathrm{ne}}$ and so is the composite of the two.

Envision now a functor $F : \mathbf{Set} \to \mathbf{Set}$, a non-empty set O of values and a request for a solution to the recursive equation $K \cong F(K \times O \to 2)$. Indirection theory provides an approximative such, the above theorem another and the next theorem builds the former from the latter, thus demonstrating the generality of our approach.

We deviate from indirection theory as introduced by Hobor et al. on two counts: We do not parameterize over the set of truth values but stick to $2 = \{0, 1\}$; the generalization, while probably technically feasible, appears unmotivated. More importantly, we build a solution that features only *hereditary* maps from $K \times O$ to 2, see the definition below. This is a direct consequence of the uniformity required of members of $\mathit{UPred}(O)$, lifting the latter constraint would most likely remove the former too. But we regard it as a strength, not a shortcoming, as we really would like to stay hereditary all the way and now we know that 'unsquashing a knot' does not invalidate this wish – compare with the discussion in the last paragraph of [31, Section 10].

Theorem A.6. Let $F : \mathbf{Set} \to \mathbf{Set}$ be a functor with a plain lift $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$. We can, from the isomorphism of Theorem A.5, build a set K, a subset of *hereditary* maps $K \times O \to_{her} 2$ of the full function space $K \times O \to 2$ and two maps

$$K \underset{\mathsf{squash}}{\overset{\mathsf{unsquash}}{\rightleftarrows}} \mathbb{N} \times F(K \times O \to_{her} 2)$$

with the following three properties:

1. $\mathsf{squash} \circ \mathsf{unsquash} = 1_K$.
2. $(\mathsf{unsquash} \circ \mathsf{squash})(m, \nu) = (m, F(\mathsf{approx}_m)(\nu))$.
3. $\forall \psi \in K \times O \to 2.\, \psi \in K \times O \to_{her} 2 \Leftrightarrow \psi = \Box\, \psi$.

Here the $\mathsf{level} = \mathsf{fst} \circ \mathsf{unsquash} : K \to \mathbb{N}$ and the map $\mathsf{approx}_m : (K \times O \to_{her} 2) \to (K \times O \to_{her} 2)$ is defined, for each $m \in \mathbb{N}$, by

$$\mathsf{approx}_m(\psi)(k, o) = \psi(k, o) \wedge \mathsf{level}(k) < m.$$

And for $\psi \in K \times O \to 2$ we define $\Box\, \psi \in K \times O \to 2$ by

$$(\Box\, \psi)(k, o) = \forall l \in K.\, k\, \mathsf{A}^*\, l \Rightarrow \psi(l, o),$$

where A^* is the reflexive, transitive closure of the relation A on K defined, for any two $k, l \in K$, by

$$k\, \mathsf{A}\, l \Leftrightarrow \mathsf{unsquash}(k) = (m + 1, \nu) \wedge l = \mathsf{squash}(m, \nu).$$

Proposition A.7. There is a plain lift of any functor built from the identity, constant non-empty sets, products, sums and (possibly finite and partial) maps from a constant set.

[8] There is a conflict of nomenclature, what we call *worlds* are known as *knots* to Hobor et al. Their worlds are pairs of knots and values.

[9] With the possible exception of [31, Example 2.7.]. The functor in that example is complex and the presentation dense to it is hard to tell.

B. Specialization to Indirection Theory, Three Proofs

Proof of Proposition A.3. It is immediate that any non-expansive φ has the stated property. Assume, on the other hand, that we need to show φ non-expansive. Let $x, y \in X$, we must show that $d(\varphi(x), \varphi(y)) \leq d(x, y)$, where d is the metric on X. We may without loss of generality assume that $d(x, y) \neq 0$. But then there is $m \in \mathbb{N}$ with $d(x, y) = 2^{-m}$, in particular we have $d(x, y) \leq 2^{-m}$ which we usually write $x =_m y$. From the assumption we get that $\varphi(x) =_m \varphi(y)$, i.e., that $d(\varphi(x), \varphi(y)) \leq 2^{-m}$ and we are done. □

Proof of Theorem A.6. Let X and Φ be the result of applying Theorem A.5 to $\hat{F}$. Note initially that X must be bisected. This is by definition the case for $\mathit{UPred}(O)$ and hence any two elements of $X \to_{ne} \mathit{UPred}(O)$ have a distance that is the supremum of a nonempty subset of $\{0\} \cup \{2^{-m} \mid m \in \mathbb{N}\}$. But this set is closed under nonempty suprema and so $X \to_{ne} \mathit{UPred}(O)$ is bisected too. Both of the functors $\frac{1}{2}(-)$ and $\hat{F}$ preserve the property of being bisected, the former by construction and the latter by assumption. And so X, which is isomorphic to $\hat{F}\left(\frac{1}{2}(X \to_{ne} \mathit{UPred}(O))\right)$, must be bisected.

Without further ado, let us plunge into the construction. For every $m \in \mathbb{N}$ we know that $=_m$ is an equivalence relation on X, for $x \in X$ we denote by $[x]_m$ the equivalence class containing x. We let K be the sum of all but the first of the sets of equivalence classes:

$$K = \sum_{m \geq 1} X/ =_m$$

Furthermore we let $K \times O \to_{her} 2$ consist of the set-theoretic maps $\psi : K \times O \to 2$ such that for any $(m, [x]_m) \in K$, any $o \in O$ and any $0 < n < m$ we have

$$\psi((m, [x]_m), o) \Rightarrow \psi((n, [x]_n), o).$$

To build squash and $\mathsf{unsquash}$ we need auxiliary maps:

$$\tfrac{1}{2}(X \to_{ne} \mathit{UPred}(O)) \underset{B}{\overset{H}{\rightleftarrows}} K \times O \to_{her} 2$$

defined by

$$H(\varphi) = \lambda((m, [x]_m), o) \in K \times O.\ \varphi(x) \ni (m-1, o)$$

respectively by

$$B(\psi) = \lambda x \in X.\ \{(m, o) \mid \psi((m+1, [x]_{m+1}), o)\}.$$

These are well-defined. To verify this for H take $\varphi \in \frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$, $(m, [x]_m) \in K$ and $o \in O$. Notice initially that the choice of the representative x does not matter for if $x =_m y$ holds for two $x, y \in X$ we have $\varphi(x) =_m \varphi(y)$ too, in particular $(m-1, o) \in \varphi(x)$ if and only if $(m-1, o) \in \varphi(y)$. To prove $H(\varphi) \in K \times O \to_{her} 2$ we furthermore take $0 < n < m$ and assume that $H(\varphi)((m, [x]_m), o)$ holds, i.e., that $(m-1, o) \in \varphi(x)$. Proving $H(\varphi)((n, [x]_n), o)$ comes down to showing $(n-1, o) \in \varphi(x)$ which is true by uniformity of $\varphi(x)$.

To verify that B is well-defined we take $\psi \in K \times O \to_{her} 2$. First we take $x \in X$ and must prove $\{(m, o) \mid \psi((m+1, [x]_{m+1}), o)\}$ uniform. So assume that we have $n < m \in \mathbb{N}$ and $o \in O$ with $\psi((m+1, [x]_{m+1}), o)$, we immediately get $\psi((n+1, [x]_{n+1}), o)$. Second we take $x, y \in X$ with $x =_m y$ for some $m \in \mathbb{N}$, we must show that $B(\psi)(x) =_m B(\psi)(y)$, i.e., that for all $n < m \in \mathbb{N}$ and all $o \in O$ we have $\psi((n+1, [x]_{n+1}), o)$ iff $\psi((n+1, [y]_{n+1}), o)$ but this is immediate since $[x]_{n+1} = [y]_{n+1}$. Here we used Proposition A.3 to prove non-expansiveness of $B(\psi)$.

Going back and forth with H and B gets you nowhere. For $\psi \in K \times O \to_{her} 2$ we get that

$$\begin{aligned} H(B(\psi)) &= H(\lambda x.\ \{(m, o) \mid \psi((m+1, [x]_{m+1}), o)\}) \\ &= \lambda((m, [x]_m), o).\ \psi((m, [x]_m), o) \\ &= \psi \end{aligned}$$

and for $\varphi \in \frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$ we get

$$\begin{aligned} B(H(\varphi)) &= B(\lambda((m, [x]_m), o).\ \varphi(x) \ni (m-1, o)) \\ &= \lambda x.\ \{(m, o) \mid \varphi(x) \ni (m, o)\} \\ &= \varphi. \end{aligned}$$

Up until this point, the maps H and B have been merely set-theoretic and not morphisms in **CBUlt**$_{\mathrm{ne}}$, indeed, $K \times O \to_{her} 2$ is itself just a set. But now we equip it with the metric induced by the bijection with $\frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$, i.e., the distance between to elements is the distance between the images of these elements under application of B. With this metric we obviously get an object of **CBUlt**$_{\mathrm{ne}}$ and the maps H and B are morphisms of **CBUlt**$_{\mathrm{ne}}$, indeed, they are isomorphisms. We need this to be able to apply $\hat{F}$ to them.

Also we need, for each $m \in \mathbb{N}$, to define π_m on $\frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$ by pointwise application of the restriction map, i.e., for $\varphi \in \frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$ we define

$$\pi_m(\varphi)(x) = \varphi(x)|_m.$$

We should verify that this is a non-expansive map. It has been argued above that $\frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$ is bisected so by Proposition A.3 we take $\varphi_0, \varphi_1 \in \frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$, $n \in \mathbb{N}$, assume $\varphi_0 =_n \varphi_1$ and aim to prove $\pi_m(\varphi_0) =_n \pi_m(\varphi_1)$. We may without loss of generality assume $n > 0$. For $x \in X$ we get by assumption that $\varphi_0(x) =_{n-1} \varphi_1(x)$ which implies that $\varphi_0(x)|_m =_{n-1} \varphi_1(x)|_m$ too and we are done. Really we would like to talk about the maps $(\mathsf{approx}_m)_{m \in \mathbb{N}}$ on $K \times O \to_{her} 2$ but we cannot since squash and $\mathsf{unsquash}$ have not been defined yet; instead we deal in $(\pi_m)_{m \in \mathbb{N}}$ on $\frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$. We shall need and prove a close correspondence between the two below.

We are now ready to construct the promised set-theoretic maps squash and $\mathsf{unsquash}$. For $(m, [x]_m) \in K$ we define

$$\mathsf{unsquash}(m, [x]_m) = \left(m-1, (\hat{F}(H) \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)\right)$$

and for $(m, \nu) \in \mathbb{N} \times \hat{F}(K \times O \to_{her} 2)$ we set

$$\mathsf{squash}(m, \nu) = \left(m+1, [(\Phi^{-1} \circ \hat{F}(B))(\nu)]_{m+1}\right).$$

Our first aim is to verify that $\mathsf{unsquash}$ is indeed well-defined, i.e., that the choice of the representative x does not matter. For $x, y \in X$ with $x =_m y$ for some $m > 0$ we get $\Phi(x) =_m \Phi(y)$ too. For any two $\varphi_0, \varphi_1 \in \frac{1}{2}(X \to_{ne} \mathit{UPred}(O))$ we get that if $\varphi_0 =_m \varphi_1$ then for any $z \in X$ we have $\varphi_0(z) =_{m-1} \varphi_1(z)$. But then

$$\begin{aligned} \pi_{m-1}(\varphi_0)(z) &= \varphi_0(z)|_{m-1} \\ &= \varphi_1(z)|_{m-1} \\ &= \pi_{m-1}(\varphi_1)(z) \end{aligned}$$

so we have $\pi_{m-1}(\varphi_0) = \pi_{m-1}(\varphi_1)$. As $\hat{F}$ was assumed non-shrinking, we can now conclude that $\hat{F}(\pi_{m-1})(x) = \hat{F}(\pi_{m-1})(y)$ and we know that $\mathsf{unsquash}$ is well defined.

Before we go on, we need a quick comment on an easily overlooked issue. The maps squash and $\mathsf{unsquash}$ are both set-theoretic as desired but really they go between K and $\mathbb{N} \times U(\hat{F}(K \times O \to_{her} 2))$ where U : **CBUlt**$_{\mathrm{ne}}$ → **Set** is the forgetful functor. But we assumed $\hat{F}$ a lift of F so

$$U(\hat{F}(K \times O \to_{her} 2)) = F(U(K \times O \to_{her} 2))$$

and the latter is what we usually just write $F(K \times O \to_{her} 2)$. So the domain respectively codomain of squash and $\mathsf{unsquash}$ really are what they are supposed to be.

With the issues of well-definedness taken care of, we now pursue the promised equalities. For $(m, [x]_m) \in K$ we calculate as follows:

$$\begin{aligned}
&(\mathsf{squash} \circ \mathsf{unsquash})(m, [x]_m) \\
&\quad = \mathsf{squash}\left(m-1, (\hat{F}(H) \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)\right) \\
&\quad = (m, [(\Phi^{-1} \circ \hat{F}(B) \circ \hat{F}(H) \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)]_m) \\
&\quad = (m, [(\Phi^{-1} \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)]_m).
\end{aligned}$$

A bit of reasoning remains to show that this is indeed $(m, [x]_m)$. Notice first that we may rewrite

$$x = (\Phi^{-1} \circ \hat{F}(1_{\frac{1}{2}(X \to_{ne} UPred(O))}) \circ \Phi)(x).$$

This means that if we can prove

$$\pi_{m-1} =_m 1_{\frac{1}{2}(X \to_{ne} UPred(O))}$$

then we are done as $\hat{F}$ was assumed locally non-expansive. So take $\varphi \in \frac{1}{2}(X \to_{ne} UPred(O))$. For any $y \in X$ we get that

$$\pi_{m-1}(\varphi)(y) = \varphi(y)|_{m-1} =_{m-1} \varphi(y)$$

so in $X \to_{ne} UPred(O)$ we have $\pi_{n-1}(\varphi) =_{m-1} \varphi$ and we are done because of the shrinking factor.

For $(m, \nu) \in \mathbb{N} \times \hat{F}(K \times O \to_{her} 2)$ we get

$$\begin{aligned}
&(\mathsf{unsquash} \circ \mathsf{squash})(m, \nu) \\
&\quad = \mathsf{unsquash}\left(m+1, [(\Phi^{-1} \circ \hat{F}(B))(\nu)]_{m+1}\right) \\
&\quad = (m, (\hat{F}(H) \circ \hat{F}(\pi_m) \circ \Phi \circ \Phi^{-1} \circ \hat{F}(B))(\nu)) \\
&\quad = (m, (\hat{F}(H) \circ \hat{F}(\pi_m) \circ \hat{F}(B))(\nu)).
\end{aligned}$$

To finish this we need to look into the relationship between π_m and the map approx_m. Take $\psi \in K \times O \to_{her} 2$, we start from one end and get that

$$\begin{aligned}
&(\pi_m \circ B)(\psi) \\
&\quad = \pi_m(\lambda x.\ \{(n, o) \mid \psi((n+1, [x]_{n+1}), o)\}) \\
&\quad = \lambda x.\ \{(n, o) \mid \psi((n+1, [x]_{n+1}), o) \wedge n < m\} \\
&\quad = \lambda x.\ \{(n, o) \mid \mathsf{approx}_m(\psi)((n+1, [x]_{n+1}), o)\} \\
&\quad = (B \circ \mathsf{approx}_m)(\psi)
\end{aligned}$$

where we remember that $\mathsf{level}(n+1, [x]_{n+1})) = n$ since level is the composite of the first projection and $\mathsf{unsquash}$. Summing up we have proved that

$$\begin{aligned}
&(\mathsf{unsquash} \circ \mathsf{squash})(m, \nu) \\
&\qquad = (m, (F(H) \circ F(B) \circ F(\mathsf{approx}_m))(\nu)) \\
&\qquad = (m, F(\mathsf{approx}_m)(\nu))
\end{aligned}$$

as desired – again we applied that $\hat{F}$ is a lift of F.

We now consider the third property; we need to prove that the subset $K \times O \to_{her} 2$ of the full function space $K \times O \to 2$ coincides with the functions that are hereditary in the sense that they are fixed under application of $\Box$. Take initially $(m, [x]_m)$ and $(n, [y]_n)$ in K, we get that $(m, [x]_m)\ \mathsf{A}\ (n, [y]_n)$ holds iff we have

$$\begin{aligned}
&\mathsf{unsquash}(m, [x]_m) = (l+1, \nu) \wedge (n, [y]_n) = \mathsf{squash}(l, \nu) \\
&\quad \Leftrightarrow (m-1, (\hat{F}(H) \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)) = (l+1, \nu) \wedge \\
&\qquad (n, [y]_n) = (l+1, [(\Phi^{-1} \circ \hat{F}(B))(\nu)]_{l+1}) \\
&\quad \Leftrightarrow m = n+1 \wedge \\
&\qquad [y]_n = [(\Phi^{-1} \circ \hat{F}(B) \circ \hat{F}(H) \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)]_n \\
&\quad \Leftrightarrow m = n+1 \wedge [y]_n = [x]_n.
\end{aligned}$$

Here the last bi-implication is a consequence of the fact that $x =_m (\Phi^{-1} \circ \hat{F}(\pi_{m-1}) \circ \Phi)(x)$ by arguments used to prove $\mathsf{squash} \circ \mathsf{unsquash} = 1_K$ above. It is immediate from this that for the closure A^* of A we have

$$(m, [x]_m)\ \mathsf{A}^*\ (n, [y]_n) \iff m \geq n \wedge [y]_n = [x]_n.$$

We know by definition that for $\psi \in K \times O \to 2$ we have $\psi = \Box\,\psi$ iff for all $(m, [x]_m) \in K$ and all $o \in O$ we have

$$\psi((m, [x]_m), o) = (\Box\,\psi)((m, [x]_m), o).$$

But by our characterization of A^* we have that the right hand side again equals

$$\begin{aligned}
&\forall (n, [y]_n) \in K.\ (m, [x]_m)\ \mathsf{A}^*(n, [y]_n) \Rightarrow \psi((n, [y]_n), o) \\
&\qquad = \forall n \leq m.\ \psi((n, [x]_n), o).
\end{aligned}$$

From this it is immediate that $\psi = \Box\,\psi$ holds iff we have that $\psi \in K \times O \to_{her} 2$ and we are done. ☐

Proof of Proposition A.7. We shall consider only three of the cases.

Constant Non-empty Sets Let X be some fixed non-empty set. Let $F : \mathbf{Set} \to \mathbf{Set}$ be the constant functor mapping any set to X and any function to the identity map 1_X. We need to come up with a plain lift $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ of F. We naturally choose $\hat{F}$ to be the constant functor mapping any object of $\mathbf{CBUlt}_{\mathrm{ne}}$ to X equipped with the discrete metric d_1 and any morphism of $\mathbf{CBUlt}_{\mathrm{ne}}$ to the identity map 1_X. This easily constitutes a locally non-expansive functor $\hat{F} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ and obviously is a lift of F. For any $\varphi : (Y, d) \to (Z, e)$ whatsoever we get that for any $m > 0$ and any two $x, y \in \hat{F}(Y, d) = (X, d_1)$ with $x =_m y$ we have $x = y$, in particular we have that $\hat{F}(\varphi)(x) = 1_X(x) = 1_X(y) = \hat{F}(\varphi)(y)$. Hence $\hat{F}$ is non-shrinking. Finally note that since (X, d_1) is bisected we have that $\hat{F}$ maps all objects to bisected objects, in particular those that were bisected already.

Products Let us consider the case of products; we shall work with binary products only but the construction generalizes to any finite product. Take two functors $F, G : \mathbf{Set} \to \mathbf{Set}$ and define $H : \mathbf{Set} \to \mathbf{Set}$ by mapping a set X to the set $F(X) \times G(X)$ and a map $\varphi : X \to Y$ to $F(\varphi) \times G(\varphi) : F(X) \times G(X) \to F(Y) \times G(Y)$. Under the assumption that we have plain lifts $\hat{F}, \hat{G} : \mathbf{CBUlt}_{\mathrm{ne}} \to \mathbf{CBUlt}_{\mathrm{ne}}$ of F and G, we have to build a plain lift $\hat{H}$ of H.

For an object $(X, d) \in \mathbf{CBUlt}_{\mathrm{ne}}$ we write $(Y, e) = \hat{F}(X, d)$ and $(Z, f) = \hat{G}(X, d)$ and assign

$$\hat{H}(X, d) = (Y \times Z, e \times f),$$

where the product metric $e \times f$ on $Y \times Z$ is defined by $(e \times f)((y_0, z_0), (y_1, z_1)) = \max(e(y_0, y_1), f(z_0, z_1))$ for any two $(y_0, z_0), (y_1, z_1) \in Y \times Z$. For a morphism $\varphi : (X_0, d_0) \to (X_1, d_1) \in \mathbf{CBUlt}_{\mathrm{ne}}$ we write $\hat{F}(\varphi) = (Y_0, e_0) \to (Y_1, e_1)$ and $\hat{G}(\varphi) = (Z_0, f_0) \to (Z_1, f_1)$ and assign

$$\hat{H}(\varphi) = \hat{F}(\varphi) \times \hat{G}(\varphi) : Y_0 \times Z_0 \to Y_1 \times Z_1.$$

It is well known that this yields a well-defined and locally non-expansive functor $\hat{H} : \mathbf{CBUlt}_{\text{ne}} \to \mathbf{CBUlt}_{\text{ne}}$. For the action on objects, this is spelled out in Lemmas 1.24 and 1.28 of [28].

We now proceed to prove that the functor $\hat{H}$ is indeed a plain lift of H. First up is the property of being a lift, take an object (X, d) of $\mathbf{CBUlt}_{\text{ne}}$. We write $(Y, e) = \hat{F}(X, d)$ and $(Z, f) = \hat{G}(X, d)$ and get that

$$\begin{aligned} U(\hat{H}(X,d)) &= U(Y \times Z, e \times f) \\ &= Y \times Z \\ &= U(\hat{F}(X,d)) \times U(\hat{G}(X,d)) \\ &= F(U(X,d)) \times G(U(X,d)) \\ &= H(U(X,d)). \end{aligned}$$

For a morphism $\varphi : (X_0, d_0) \to (X_1, d_1) \in \mathbf{CBUlt}_{\text{ne}}$ we get the weirdly easy calculation $U(\hat{H}(\varphi)) = \hat{H}(\varphi) = \hat{F}(\varphi) \times \hat{G}(\varphi) = F(\varphi) \times G(\varphi) = H(\varphi)$ since the forgetful functor has no action on morphisms.

Next up is proof that $\hat{H}$ is non-shrinking. Take a morphism $\varphi : (X_0, d_0) \to (X_1, d_1) \in \mathbf{CBUlt}_{\text{ne}}$, we write $\hat{F}(\varphi) = (Y_0, e_0) \to (Y_1, e_1)$ and $\hat{G}(\varphi) = (Z_0, f_0) \to (Z_1, f_1)$. Assume that for some $m > 0$ we have that

$$\forall x, y \in X_0.\, x =_m y \Rightarrow \varphi(x) = \varphi(y).$$

Now take $(y_0, z_0), (y_1, z_1) \in Y_0 \times Z_0$ and assume that we have $(y_0, z_0) =_m (y_1, z_1)$. But then $y_0 =_m y_1$ and $z_0 =_m z_1$ by the definition of the metric $e_0 \times f_0$. And so we have

$$\begin{aligned} \hat{H}(\varphi)(y_0, z_0) &= \left(\hat{F}(\varphi) \times \hat{G}(\varphi)\right)(y_0, z_0) \\ &= \left(\hat{F}(\varphi)(y_0), \hat{G}(\varphi)(z_0)\right) \\ &= \left(\hat{F}(\varphi)(y_1), \hat{G}(\varphi)(z_1)\right) \\ &= \left(\hat{F}(\varphi) \times \hat{G}(\varphi)\right)(y_1, z_1) \\ &= \hat{H}(\varphi)(y_1, z_1) \end{aligned}$$

since both $\hat{F}$ and $\hat{G}$ were assumed non-shrinking. Finally we remark that $\hat{H}$ preserves the property of being bisected since that holds by assumption for $\hat{F}$ and $\hat{G}$ and because the product metric introduces no new distances.

Finite, Partial Maps from a Constant Set Now on to finite, partial maps from a constant set. Take a set X and a functor $F : \mathbf{Set} \to \mathbf{Set}$, define $G : \mathbf{Set} \to \mathbf{Set}$ by mapping a set Y to the set $X \rightharpoonup_{fin} F(Y)$ of partial maps with a finite domain. A map $\varphi : Y \to Z$ is mapped to $\lambda\psi : X \rightharpoonup_{fin} F(Y).\ F(\varphi) \circ \psi$. Under the assumption that we have a plain lift $\hat{F} : \mathbf{CBUlt}_{\text{ne}} \to \mathbf{CBUlt}_{\text{ne}}$ of F, we have to build a plain lift $\hat{G}$ of G.

For an object $(Y, d) \in \mathbf{CBUlt}_{\text{ne}}$ we write $(Z, e) = \hat{F}(Y, d)$ and assign

$$\hat{G}(Y, d) = (X \rightharpoonup_{fin} Z, e_{X \rightharpoonup_{fin}}),$$

where $e_{X \rightharpoonup_{fin}}(\psi_0, \psi_1)$ is $\max_{x \in \text{dom}(\varphi)} e(\psi_0(x), \psi_1(x))$ for any two $\psi_0, \psi_1 : X \rightharpoonup_{fin} Z$ with identical domain, otherwise the distance is 1. For a morphism $\varphi : (Y_0, d_0) \to (Y_1, d_1)$ in $\mathbf{CBUlt}_{\text{ne}}$ we write $\hat{F}(\varphi) : (Z_0, e_0) \to (Z_1, e_1)$ and employ that $\hat{F}$ is a lift of F to simply assign

$$\hat{G}(\varphi) = G(\varphi) : (X \rightharpoonup_{fin} Z_0) \to (X \rightharpoonup_{fin} Z_1).$$

It is easily verifiable – if not exactly well known – that this yields a well-defined and locally non-expansive functor $\hat{G} : \mathbf{CBUlt}_{\text{ne}} \to \mathbf{CBUlt}_{\text{ne}}$, a high level argument is given in the proof of Proposition 22 of [22].

We now proceed to prove that the functor $\hat{G}$ is a plain lift of G. First we verify that it is a lift, take an object (Y, d) of $\mathbf{CBUlt}_{\text{ne}}$. We write $(Z, e) = \hat{F}(Y, d)$ and get that

$$\begin{aligned} U(\hat{G}(Y,d)) &= U(X \rightharpoonup_{fin} Z, e_{X \rightharpoonup_{fin}}) \\ &= X \rightharpoonup_{fin} Z \\ &= X \rightharpoonup_{fin} U(\hat{F}(Y,d)) \\ &= X \rightharpoonup_{fin} F(U(Y,d)) \\ &= G(U(Y,d)). \end{aligned}$$

The case of morphisms holds by definition.

Next up is proof that $\hat{G}$ is non-shrinking. Take a morphism $\varphi : (Y_0, d_0) \to (Y_1, d_1) \in \mathbf{CBUlt}_{\text{ne}}$, we write $\hat{F}(\varphi) = (Z_0, e_0) \to (Z_1, e_1)$. Assume that for some $m > 0$ we have that

$$\forall x, y \in Y_0.\, x =_m y \Rightarrow \varphi(x) = \varphi(y).$$

Now take $\psi_0, \psi_1, \in X \rightharpoonup_{fin} Z_0$ and assume that we have $\psi_0 =_m \psi_1$. We have $\text{dom}(\psi_0) = \text{dom}(\psi_1)$ and furthermore know that for all $x \in \text{dom}(\psi_0)$ we have $\psi_0(x) =_m \psi_1(x)$. We obviously have $\text{dom}(\hat{G}(\varphi)(\psi_0)) = \text{dom}(\psi_0) = \text{dom}(\psi_1) = \text{dom}(\hat{G}(\varphi)(\psi_0))$ and for any x in this domain we get

$$\begin{aligned} \hat{G}(\varphi)(\psi_0)(x) &= G(\varphi)(\psi_0)(x) \\ &= (F(\varphi) \circ \psi_0)(x) \\ &= F(\varphi)(\psi_0(x)) \\ &= F(\varphi)(\psi_1(x)) \\ &= (F(\varphi) \circ \psi_1)(x) \\ &= G(\varphi)(\psi_1)(x) \\ &= \hat{G}(\varphi)(\psi_1)(x) \end{aligned}$$

Finally we remark that $\hat{G}$ preserves the property of being bisected since that holds by assumption for $\hat{F}$ and because we introduce no new distances by taking a maximum of finitely many existing distances. □

C. Proofs about Capabilities

The interpretation of types and capabilities satisfies standard substitution properties.

Lemma C.1. If η and η' agree on the free variables of τ, θ and C then $[\![\tau]\!]_\eta = [\![\tau]\!]_{\eta'}$, $[\![\theta]\!]_\eta = [\![\theta]\!]_{\eta'}$, and $[\![C]\!]_\eta = [\![C]\!]_{\eta'}$.

Lemma C.2. We have $[\![\tau[\alpha{:=}\tau']]\!]_\eta = [\![\tau]\!]_{\eta[\alpha := [\![\tau']\!]_\eta]}$, and analogous substitution properties hold for capabilities and memory types.

Lemma C.3. For all $S \in \mathit{MT}$ and $c \in \mathit{Cap}$,

$$(S \otimes \iota(c) * c)(w) * \iota^{-1}(w)(\mathit{emp}) = S(w') * \iota^{-1}(w')(\mathit{emp})$$

for $w' = \iota(c) \circ w$. Moreover, $\mathcal{E}(S \otimes \iota(c) * c) = \mathcal{E}(S) \otimes \iota(c)$.

Proof. Let $S \in \mathit{MT}$, $c \in \mathit{Cap}$, $w \in W$ and set $w' = \iota(c) \circ w$. By definition of $\circ$ we have

$$\begin{aligned} & S(w') * \iota^{-1}(w')(\mathit{emp}) \\ &\quad = S(\iota(c) \circ w) * \iota^{-1}(\iota(c) \circ w)(\mathit{emp}) \\ &\quad = (S \otimes \iota(c))(w) * c(w \circ \mathit{emp}) * \iota^{-1}(w)(\mathit{emp}) \\ &\quad = (S \otimes \iota(c))(w) * c(w) * \iota^{-1}(w)(\mathit{emp}) \\ &\quad = (S \otimes \iota(c) * c)(w) * \iota^{-1}(w)(\mathit{emp}) \end{aligned}$$

Since w above was chosen arbitrarily, the second statement, $\mathcal{E}(S \otimes \iota(c) * c) = \mathcal{E}(S) \otimes \iota(c)$, is an immediate consequence by the definition of $\mathcal{E}$ and $\otimes$. □

C.1 Structural Equivalence of Capabilities and Types

Capabilities and types are considered up to the structural equivalence given in Figure 6. In this subsection we check that our semantics of types respects this equivalence.

Note that the abbreviation defined in (4) gives a connective that is interpreted by the operation $\circ$ on W, up to the isomorphism between W and *Cap*. More precisely, by definition of $\circ$ we have

$$\begin{aligned}\iota^{-1}(\iota(c_1) \circ \iota(c_2))(w) &= \iota^{-1}(\iota(c_1))(\iota(c_2) \circ w) * \iota^{-1}(\iota(c_2))(w)) \\ &= (c_1 \otimes \iota(c_2))(w) * c_2(w) \\ &= (c_1 \otimes \iota(c_2) * c_2)(w)\end{aligned}$$

for all $c_1, c_2 \in \mathit{Cap}$ and all w, and thus

$$\iota [\![C_1 \circ C_2]\!] = \iota [\![C_1]\!] \circ \iota [\![C_2]\!] \ .$$

Hence, equations (5), (6) and (10) follow from Proposition 3.3. That (7)–(9) and (11) hold is a direct consequence of the interpretation of $*$ in terms of the commutative monoid structure on *Cap* and the associated monoid action (Proposition 3.4).

Next, we consider the action by $*$ on capabilities and contexts.

Lemma C.4 ($*$-distribution axiom for singleton capability)**.** The following equivalence holds with respect to the semantics:

$$\{\sigma : \theta\} * C = \{\sigma : \theta * C\} \tag{12}$$

Proof. We calculate as follows.

$$\begin{aligned}&[\![\{\sigma : \theta\} * C]\!]_\eta\, w \\ &= [\![\{\sigma : \theta\}]\!]_\eta\, w * [\![C]\!]_\eta\, w \\ &= \{(k, h) \mid (k, (\eta\sigma, h)) \in [\![\theta]\!]_\eta\, w\} * [\![C]\!]_\eta\, w \\ &= \{(k, h \cdot h') \mid (k, (\eta\sigma, h)) \in [\![\theta]\!]_\eta\, w \ \wedge\ (k, h') \in [\![C]\!]_\eta\, w\} \\ &= [\![\{\sigma : \theta * C\}]\!]_\eta\, w\end{aligned}$$

Since this holds for arbitrary η and w we have proved (12). ☐

Lemma C.5 ($*$-distribution axiom for linear environments)**.** The following equivalences holds with respect to the semantics:

$$(\Gamma, x{:}\chi) * C = \Gamma, x{:}(\chi * C) \tag{13}$$

$$(\Gamma, x{:}\chi) * C = (\Gamma * C), x{:}\chi \tag{14}$$

Proof. The equivalences (13) and (14) follow since all three environments have the same interpretation: $[\![(\Gamma, x{:}\chi) * C]\!]_\eta\, w$, $[\![\Gamma, x{:}(\chi * C)]\!]_\eta\, w$, and $[\![(\Gamma * C), x{:}\chi]\!]_\eta\, w$ consist of all those pairs $(k, (\rho, h))$ where we have

$$\begin{gathered}\rho = \rho_1[x \mapsto v] \\ h = h_1 \cdot h_2 \cdot h_3 \\ (k, (\rho_1, h_1)) \in [\![\Gamma]\!]_\eta\, w \\ (k, (v, h_2)) \in [\![\chi]\!]_\eta\, w \\ (k, h_3) \in [\![C]\!]_\eta\, w\end{gathered}$$

for some ρ_1, v and h_1, h_2, h_3 . ☐

We next consider the equivalences that describe the action by $\otimes$. The first group are the general equivalences (15) and (16) that apply to several syntactic categories. The first equation says that $\otimes$ distributes over $*$. Equation (16) states that $\otimes$ does not affect existential quantification over region names.

Lemma C.6 (General $\otimes$-distribution axioms)**.** The following equivalences hold with respect to the semantics:

$$(\cdot * \cdot) \otimes C = (\cdot \otimes C) * (\cdot \otimes C) \tag{15}$$

$$(\exists\sigma.\cdot) \otimes C = \exists\sigma.(\cdot \otimes C) \qquad \text{if } \sigma \notin \mathit{RegNames}(C) \tag{16}$$

Proof. In each case, we prove that the left hand side and right hand side have the same denotation. Equation (15) follows from the pointwise definition of $*$ with respect to worlds; we show this for the case of memory types:

$$\begin{aligned}[\![(\theta * C') \otimes C]\!]_\eta\, w &= ([\![\theta * C']\!]_\eta \otimes \iota([\![C]\!]_\eta))w \\ &= [\![\theta * C']\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= [\![\theta]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) * [\![C']\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= ([\![\theta \otimes C]\!]_\eta\, w) * ([\![C' \otimes C]\!]_\eta\, w) \\ &= [\![(\theta \otimes C) * (C' \otimes C)]\!]_\eta\, w\end{aligned}$$

Equation (16) follows from the interpretation of existential quantification. We show this again for the case of memory types:

$$\begin{aligned}[\![(\exists\sigma.\theta) \otimes C]\!]_\eta\, w &= [\![\exists\sigma.\theta]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= \bigcup\{[\![\theta]\!]_{\eta[\sigma:=v]}\, (\iota([\![C]\!]_\eta) \circ w) \mid v \in \mathit{Val}\} \\ &= \bigcup\{[\![\theta]\!]_{\eta[\sigma:=v]}\, (\iota([\![C]\!]_{\eta[\sigma:=v]}) \circ w) \mid v \in \mathit{Val}\} \\ &= \bigcup\{[\![\theta \otimes C]\!]_{\eta[\sigma:=v]}\, w \mid v \in \mathit{Val}\} \\ &= [\![\exists\sigma.(\theta \otimes C)]\!]_\eta\, w\end{aligned}$$

Here, the third equation uses the assumption $\sigma \notin \mathit{RegNames}(C)$, and thus that $[\![C]\!]_\eta$ does not depend on the value of η on σ. ☐

The next group of equivalences (17) and (18) describes the interaction of $\otimes$ with the remaining capabilities. Together with (10), (15), (16) and the unfolding of recursively defined capabilities, they cover all the cases.

Lemma C.7 ($\otimes$-distribution axiom for singleton capabilities)**.** The following equivalences hold:

$$\emptyset \otimes C = \emptyset \tag{17}$$

$$\{\sigma : \theta\} \otimes C = \{\sigma : \theta \otimes C\} \tag{18}$$

Proof. Equivalence (17) follows from the interpretation of $\emptyset$ as a constant function:

$$[\![\emptyset \otimes C]\!]_\eta\, w = [\![\emptyset]\!]_\eta\, (\iota\, [\![C]\!]_\eta \circ w) = \mathbb{N} \times \mathit{Heap} = [\![\emptyset]\!]_\eta\, w$$

For (18) we note that

$$\begin{aligned}&[\![\{\sigma : \theta\} \otimes C]\!]_\eta\, w \\ &= [\![\{\sigma : \theta\}]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= \{(k, h) \mid (k, (\eta(\sigma), h)) \in [\![\theta]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w)\} \\ &= \{(k, h) \mid (k, (\eta(\sigma), h)) \in [\![\theta \otimes C]\!]_\eta\, w\} \\ &= [\![\{\sigma : \theta \otimes C\}]\!]_\eta\, w\end{aligned}$$

Since this holds for arbitrary w, the equivalence of the left hand side and right hand side of (18) follows. ☐

Next, we consider the equivalences that describe the interaction between $\otimes$ and the value type constructors.

Lemma C.8 ($\otimes$-distribution axioms for value types)**.** The following equivalences hold:

$$0 \otimes C = 0 \qquad (19)$$

$$1 \otimes C = 1 \qquad (20)$$

$$\mathsf{int} \otimes C = \mathsf{int} \qquad (21)$$

$$(\tau_1 + \tau_2) \otimes C = (\tau_1 \otimes C) + (\tau_2 \otimes C) \qquad (22)$$

$$(\tau_1 \times \tau_2) \otimes C = (\tau_1 \otimes C) \times (\tau_2 \otimes C) \qquad (23)$$

$$(\forall \xi.\tau) \otimes C = \forall \xi.(\tau \otimes C) \qquad \xi \notin \mathrm{fv}\, C \qquad (24)$$

$$(\chi_1 \to \chi_2) \otimes C = (\chi_1 \circ C) \to (\chi_2 \circ C) \qquad (25)$$

$$[\sigma] \otimes C = [\sigma] \qquad (26)$$

Proof. Equations (19), (20), (21) and (26) follow since $[\![0]\!]_\eta$, $[\![1]\!]_\eta$, $[\![\mathsf{int}]\!]_\eta$ and $[\![[\sigma]]\!]_\eta$ are all constant functions. The equation (22) for sum types uses the pointwise definition of $[\![\tau_1 + \tau_2]\!]$:

$$\begin{aligned}[\![(\tau_1 + \tau_2) \otimes C]\!]_\eta\, w &= [\![\tau_1 + \tau_2]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= \{(k, \mathsf{inj}^i v) \mid (k, v) \in [\![\tau_i]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w)\} \\ &= \{(k, \mathsf{inj}^i v) \mid (k, v) \in [\![\tau_i \otimes C]\!]_\eta\, w\} \\ &= [\![(\tau_1 \otimes C) + (\tau_2 \otimes C)]\!]_\eta\, w\end{aligned}$$

Equation (23) is proved similarly. For (24) we consider the case of universal quantification over capabilities:

$$\begin{aligned}[\![(\forall \gamma.\tau) \otimes C]\!]_\eta\, w &= [\![\forall \gamma.\tau]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &= \bigcap_{c \in \mathit{Cap}} [\![\tau]\!]_{\eta[\gamma:=c]}\, (\iota([\![C]\!]_\eta) \circ w) \\ &= \bigcap_{c \in \mathit{Cap}} [\![\tau]\!]_{\eta[\gamma:=c]}\, (\iota([\![C]\!]_{\eta[\gamma:=c]}) \circ w) \\ &= \bigcap_{c \in \mathit{Cap}} [\![\tau \otimes C]\!]_{\eta[\gamma:=c]}\, w \\ &= [\![\forall \gamma.(\tau \otimes C)]\!]_\eta\, w\end{aligned}$$

Here, the third equality is by Lemma C.1 and assumption $\gamma \notin \mathrm{fv}\, C$.

The most interesting equivalence is the distribution axiom for function types, equation (25). However, the semantics of function types is set up such that this axiom can be proved fairly straightforwardly: first note that

$$[\![(\chi_1 \to \chi_2) \otimes C]\!]_\eta\, w = [\![\chi_1 \to \chi_2]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w)$$

Assume $(k, v) \in [\![(\chi_1 \to \chi_2) \otimes C]\!]_\eta\, w$. Thus, for all $j < k$, and for all $r' \in \mathit{Cap}$: if $w' = (\iota([\![C]\!]_\eta) \circ w$ then

$$\begin{aligned}&\forall (j, (v', h)) \in ([\![\chi_1]\!]_\eta\, w') * r'(w') * \iota^{-1}(w')(\mathit{emp}). \\ &\qquad (j{+}1, (v\, v', h)) \in \mathcal{E}([\![\chi_2]\!]_\eta * r')(w')\,. \qquad (50)\end{aligned}$$

We show that $(k, v) \in [\![(\chi_1 \circ C) \to (\chi_2 \circ C)]\!]_\eta\, w$. So let $j < k$, $r \in \mathit{Cap}$ and let

$$(j, (v', h)) \in [\![\chi_1 \circ C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\,. \qquad (51)$$

Since $\chi_1 \circ C$ abbreviates $(\chi_1 \otimes C) * C$ and

$$\begin{aligned}&[\![(\chi_1 \otimes C) * C]\!]_\eta\, w * \iota^{-1}(w)(\mathit{emp}) \\ &\qquad = ([\![\chi_1]\!]_\eta\, w') * \iota^{-1}(w')(\mathit{emp})\end{aligned}$$

by Lemma C.3, (51) is equivalent to

$$(j, (v', h)) \in [\![\chi_1]\!]_\eta\, w' * r(w) * \iota^{-1}(w')(\mathit{emp})\,.$$

Set $r'(w_0) = r(w)$, then (50) yields

$$(j{+}1, (v\, v', h)) \in \mathcal{E}([\![\chi_2]\!]_\eta * r')(w')$$

and with Lemma C.3 we can use

$$\begin{aligned}&([\![\chi_1]\!]_\eta\, w') * \iota^{-1}(w')(\mathit{emp}) * r'(w') \\ &\qquad = [\![(\chi_2 \otimes C) * C]\!]_\eta\, w * \iota^{-1}(w)(\mathit{emp}) * r(w)\end{aligned}$$

to conclude $\mathcal{E}([\![\chi_2]\!]_\eta * r')(w') = \mathcal{E}([\![\chi_2 \circ C]\!]_\eta * r)(w)$. Hence we have shown $(k, v) \in [\![(\chi_1 \circ C) \to (\chi_2 \circ C)]\!]_\eta\, w$. The other direction is analogous. ☐

Lemma C.9 ($\otimes$-distribution axioms for memory types)**.** The following equivalences hold:

$$(\theta_1 + \theta_2) \otimes C = (\theta_1 \otimes C) + (\theta_1 \otimes C) \qquad (22)$$

$$(\theta_1 \times \theta_2) \otimes C = (\theta_1 \otimes C) \times (\theta_1 \otimes C) \qquad (23)$$

$$(\mathsf{ref}\, \theta) \otimes C = \mathsf{ref}\, (\theta \otimes C) \qquad (27)$$

Moreover, the inclusion of value types into memory types commutes with $\cdot \otimes C$.

Proof. Equivalence (27) is an easy verification:

$$\begin{aligned}&[\![(\mathsf{ref}\, \theta) \otimes C]\!]_\eta\, w \\ &\quad = [\![\mathsf{ref}\, \theta]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &\quad = \{(k, (l, h \cdot [l \mapsto v])) \mid (k, (v, h)) \in [\![\theta]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w)\} \\ &\quad = \{(k, (l, h \cdot [l \mapsto v])) \mid (k, (v, h)) \in [\![\theta \otimes C]\!]_\eta\, w\} \\ &\quad = [\![\mathsf{ref}\, (\theta \otimes C)]\!]_\eta\, w\end{aligned}$$

Equivalences (22) and (23) are similar. Finally,

$$\begin{aligned}&[\![\tau \otimes C]\!]_\eta\, w \\ &\quad = [\![\tau]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w) \\ &\quad = \{(k, (v, h)) \mid h \in \mathit{Heap},\ (k, v) \in [\![\tau]\!]_\eta\, (\iota([\![C]\!]_\eta) \circ w)\} \\ &\quad = \{(k, (v, h)) \mid h \in \mathit{Heap},\ (k, v) \in [\![\tau \otimes C]\!]_\eta\, w\}\end{aligned}$$

shows that invariant extension commutes with the inclusion of value types τ into memory types. ☐

Lemma C.10 ($\otimes$-distribution axioms for environments)**.** The following equivalences hold:

$$\varnothing \otimes C = \varnothing \qquad (28)$$

$$(\Gamma, x{:}\chi) \otimes C = (\Gamma \otimes C), x{:}(\chi \otimes C) \qquad (29)$$

$$(\Gamma * C') \otimes C = (\Gamma \otimes C) * (C' \otimes C) \qquad (30)$$

Proof. Equation (28) follows since $[\![\varnothing]\!]$ is a constant function; equations (29) and (30) hold due to the pointwise interpretation. ☐

Lemma C.11 (Distribution axioms for region abstraction)**.** The following equivalences hold:

$$\exists \sigma_1.\exists \sigma_2.\cdot = \exists \sigma_2.\exists \sigma_1.\cdot \qquad (31)$$

$$\cdot * (\exists \sigma.C) = \exists \sigma.(\cdot * C) \qquad (32)$$

$$\{\sigma_1 : \exists \sigma_2.\theta\} = \exists \sigma_2.\{\sigma_1 : \theta\} \qquad \text{where } \sigma_1 \neq \sigma_2 \qquad (33)$$

Proof. Equation (31) follows from the semantics of existential quantification; we show this for the case of a capability C:

$$\begin{aligned}[\![\exists \sigma_1.\exists \sigma_2.C]\!]_\eta\, w &= \bigcup \{[\![C]\!]_{\eta[\sigma_1:=v_1, \sigma_2:=v_2]}\, w \mid v_1, v_2 \in \mathit{Val}\} \\ &= [\![\exists \sigma_2.\exists \sigma_1.C]\!]_\eta\, w\end{aligned}$$

Similarly, we verify (32) for a capability C_1 such that $\sigma \notin \mathit{RegNames}(C_1)$:

$$\begin{aligned}\llbracket C_1 * (\exists\sigma.C)\rrbracket_\eta\, w &= \llbracket C_1\rrbracket_\eta\, w * \bigcup\{\llbracket C\rrbracket_{\eta[\sigma:=v]} \mid v \in \mathit{Val}\}\\ &= \bigcup\{\llbracket C_1\rrbracket_{\eta[\sigma:=v]}\, w * \llbracket C\rrbracket_{\eta[\sigma:=v]} \mid v \in \mathit{Val}\}\\ &= \llbracket \exists\sigma.(C_1 * C)\rrbracket_\eta\, w\end{aligned}$$

Finally, we consider (33):

$$\begin{aligned}&\llbracket\{\sigma_1 : \exists\sigma_2.\theta\}\rrbracket_\eta\, w\\ &\quad= \{(k,h) \mid (k,(\eta\sigma_1,h)) \in \llbracket\exists\sigma_2.\theta\rrbracket_\eta\, w\}\\ &\quad= \{(k,h) \mid (k,(\eta\sigma_1,h)) \in \bigcup\{\llbracket\theta\rrbracket_{\eta[\sigma_2:=v]}\, w \mid v\in\mathit{Val}\}\ \}\\ &\quad= \bigcup\{(k,h) \mid v \in \mathit{Val},\ (k,(\eta[\sigma_2{:=}v](\sigma_1),h)) \in \llbracket\theta\rrbracket_{\eta[\sigma_2:=v]}\, w\}\\ &\quad= \bigcup\{\llbracket\{\sigma_1:\theta\}\rrbracket_{\eta[\sigma_2:=v]}\, w \mid v \in \mathit{Val}\}\\ &\quad= \llbracket\exists\sigma_2.\{\sigma_1:\theta\}\rrbracket_\eta\, w\end{aligned}$$

where the third step holds since we assumed $\sigma_1 \neq \sigma_2$. □

Lemma C.12 (Axioms for focusing)**.** The following equivalences hold:

$$\{\sigma_1 : \mathsf{ref}\,\theta\} = \exists\sigma_2.\{\sigma_1 : \mathsf{ref}\,[\sigma_2]\} * \{\sigma_2 : \theta\} \quad (\sigma_2 \notin \mathit{RegNames}(\sigma_1,\theta)) \tag{34}$$

$$\{\sigma : \theta_1\times\theta_2\} = \exists\sigma_1.\{\sigma : [\sigma_1]\times\theta_2\} * \{\sigma_1 : \theta_1\} \quad (\sigma_1 \notin \mathit{RegNames}(\sigma,\theta_1,\theta_2)) \tag{35}$$

$$\{\sigma : \theta_1\times\theta_2\} = \exists\sigma_2.\{\sigma : \theta_1\times[\sigma_2]\} * \{\sigma_2 : \theta_2\} \quad (\sigma_2 \notin \mathit{RegNames}(\sigma,\theta_1,\theta_2)) \tag{36}$$

$$\{\sigma : \theta_1 + 0\} = \exists\sigma_1.\{\sigma : [\sigma_1] + 0\} * \{\sigma_1 : \theta_1\} \quad (\sigma_1 \notin \mathit{RegNames}(\sigma,\theta_1)) \tag{37}$$

$$\{\sigma : 0 + \theta_2\} = \exists\sigma_2.\{\sigma : 0 + [\sigma_2]\} * \{\sigma_2 : \theta_2\} \quad (\sigma_2 \notin \mathit{RegNames}(\sigma,\theta_2)) \tag{38}$$

Proof. For equation (34) we can calculate as follows.

$$\begin{aligned}&\llbracket\exists\sigma_2.\{\sigma_1 : \mathsf{ref}\,[\sigma_2]\} * \{\sigma_2:\theta\}\rrbracket_\eta\, w\\ &\quad= \bigcup_v \llbracket\{\sigma_1 : \mathsf{ref}\,[\sigma_2]\}\rrbracket_{\eta[\sigma_2:=v]}\, w * \llbracket\{\sigma_2:\theta\}\rrbracket_{\eta[\sigma_2:=v]}\, w\\ &\quad= \bigcup_v\{(k,h_1) \mid (k,(\eta[\sigma_2{:=}v](\sigma_1),h_1)) \in \llbracket\mathsf{ref}\,[\sigma_2]\rrbracket_{\eta[\sigma_2:=v]}\, w\}\\ &\qquad\quad * \{(k,h_2) \mid (k,(v,h_2)) \in \llbracket\theta\rrbracket_{\eta[\sigma_2:=v]}\, w\}\\ &\quad= \bigcup_v\{(k,h_1'\cdot[\eta\sigma_1\mapsto v']) \mid (k,(v',h_1')) \in \llbracket[\sigma_2]\rrbracket_{\eta[\sigma_2:=v]}\, w\}\\ &\qquad\quad * \{(k,h_2) \mid (k,(v,h_2)) \in \llbracket\theta\rrbracket_\eta\, w\}\\ &\quad= \bigcup_v\{(k,[\eta\sigma_1{\mapsto}v']) \mid v'{=}v\} * \{(k,h_2) \mid (k,(v,h_2)) \in \llbracket\theta\rrbracket_\eta\, w\}\\ &\quad= \{(k,[\eta\sigma_1\mapsto v]\cdot h_2) \mid (k,(v,h_2)) \in \llbracket\theta\rrbracket_\eta\, w\}\\ &\quad= \{(k,h) \mid (k,(\eta\sigma_1,h)) \in \llbracket\mathsf{ref}\,\theta\rrbracket_\eta\, w\}\\ &\quad= \llbracket\{\sigma_1 : \mathsf{ref}\,\theta\}\rrbracket_\eta\, w\end{aligned}$$

For equation (35) we calculate similarly:

$$\begin{aligned}&\llbracket\exists\sigma_1.\{\sigma : [\sigma_1]\times\theta_2\} * \{\sigma_1:\theta_1\}\rrbracket_\eta\, w\\ &\quad= \bigcup_v\{(k,h_2) \mid (k,(\eta\sigma,h_2)) \in \llbracket[\sigma_1]\times\theta_2\rrbracket_{\eta[\sigma_1:=v]}\, w\}\\ &\qquad\quad * \{(k,h_1) \mid (k,(v,h_1)) \in \llbracket\theta_1\rrbracket_\eta\, w\}\\ &\quad= \bigcup_{v,\ \eta\sigma=(v,v')}\{(k,h_2) \mid (k,(v',h_2)) \in \llbracket\theta_2\rrbracket_{\eta[\sigma_1:=v]}\, w\}\\ &\qquad\quad * \{(k,h_1) \mid (k,(v,h_1)) \in \llbracket\theta_1\rrbracket_\eta\, w\}\\ &\quad= \{(k,h) \mid (k,(\eta\sigma,h)) \in \llbracket\theta_1\times\theta_2\rrbracket_\eta\, w\}\\ &\quad= \llbracket\{\sigma : \theta_1\times\theta_2\}\rrbracket_\eta\, w\end{aligned}$$

Equation (36) is shown analogously. Next, we consider (37).

$$\begin{aligned}&\llbracket\exists\sigma_1.\{\sigma : [\sigma_1]+0\} * \{\sigma_1:\theta_1\}\rrbracket_\eta\, w\\ &\quad= \bigcup_v\{(k,h_1) \mid (k,(\eta\sigma,h_1)) \in \llbracket[\sigma_1]+0\rrbracket_{\eta[\sigma_1:=v]}\, w\}\\ &\qquad\quad * \{(k,h_2) \mid (k,(v,h_2)) \in \llbracket\theta_1\rrbracket_\eta\, w\}\\ &\quad= \bigcup_{v,\ \eta\sigma=\mathsf{inj}^1 v}\{(k,h) \mid (k,(v,h)) \in \llbracket\theta_1\rrbracket_\eta\, w\}\\ &\quad= \{(k,h) \mid (k,(\eta\sigma,h)) \in \llbracket\theta_1+0\rrbracket_\eta\, w\}\\ &\quad= \llbracket\{\sigma : \theta_1+0\}\rrbracket_\eta\, w\end{aligned}$$

Equation (38) is analogous. □

Finally, the axioms (39)–(41) hold as a consequence of the substitution lemma C.2 and our use of equirecursive types.

C.2 Subtyping

This section gives the proofs of the subtyping axioms in Figure 7.

Lemma C.13 (Frame axiom)**.** The following subtyping axiom holds:

$$\chi_1 \to \chi_2 \le (\chi_1 * C) \to (\chi_2 * C) \tag{42}$$

Proof. We show that for any w and η, $\llbracket\chi_1\to\chi_2\rrbracket_\eta\, w$ is contained in $\llbracket(\chi_1 * C)\to(\chi_2 * C)\rrbracket_\eta\, w$. Assume $(k,v) \in \llbracket\chi_1\to\chi_2\rrbracket_\eta\, w$. Let $j<k$, $r \in \mathit{Cap}$, and let

$$(j,(v',h)) \in \llbracket\chi_1 * C\rrbracket_\eta\, w\ *\ r(w)\ *\ \iota^{-1}(w)(\mathit{emp})\ ,$$

or equivalently,

$$(j,(v',h)) \in \llbracket\chi_1\rrbracket_\eta\, w\ *\ (\llbracket C\rrbracket_\eta * r)(w)\ *\ \iota^{-1}(w)(\mathit{emp})\ .$$

Thus, from the assumption $(k,v) \in \llbracket\chi_1\to\chi_2\rrbracket_\eta\, w$ we obtain

$$(j{+}1,(v\,v',h)) \in \mathcal{E}(\llbracket\chi_2\rrbracket_\eta * \llbracket C\rrbracket_\eta * r)(w)\ .$$

By definition, this is just $(j{+}1,(v\,v',h)) \in \mathcal{E}(\llbracket\chi_2 * C\rrbracket_\eta * r)(w)$ and we have shown $(k,v) \in \llbracket(\chi_1 * C)\to(\chi_2 * C)\rrbracket_\eta\, w$. □

Lemma C.14 (Free)**.** The following subtyping axiom holds:

$$C_1 * C_2 \le C_1 \tag{43}$$

Proof. This axiom follows from the upwards closure of predicates in $\mathit{UPred}^{\uparrow}(\mathit{Heap})$. More precisely, if $(k,h) \in \llbracket C_1 * C_2\rrbracket_\eta\, w$ then h splits into $h = h_1\cdot h_2$ such that $(k,h_1) \in \llbracket C_1\rrbracket_\eta\, w$. Since $h_1 \sqsubseteq h$ we also have $(k,h) \in \llbracket C_1\rrbracket_\eta\, w$. □

Lemma C.15 (Singleton creation)**.** The following subtyping axiom holds:

$$\tau \le \exists\sigma.[\sigma] * \{\sigma : \tau\} \tag{44}$$

if σ is not free in τ.

Proof. We must show that for any w and η, if $(k,(v,h)) \in [\![\tau]\!]_\eta\, w$ then $(k,(v,h)) \in [\![\exists\sigma.[\sigma] * \{\sigma : \tau\}]\!]_\eta\, w$. Let $\eta' = \eta[\sigma{:=}v]$. By definition of the existential quantification over region names, it suffices to show that $(k,(v,h)) \in [\![[\sigma] * \{\sigma : \tau\}]\!]_{\eta'}\, w$. Since we have $\eta'(\sigma) = v$ it is clear that $(k,v) \in [\![[\sigma]]\!]_{\eta'}\, w$. The remaining proof obligation $(k,h) \in [\![\{\sigma : \tau\}]\!]_{\eta'}\, w$ follows since $[\![\tau]\!]_\eta = [\![\tau]\!]_{\eta'}$, due to the assumption that σ is not free in τ. ☐

Lemma C.16 (Singleton extraction)**.** The following subtyping axiom holds:

$$[\sigma] * \{\sigma : \tau\} \leq \tau * \{\sigma : \tau\} \tag{45}$$

Proof. We must show that for any w and η, if $[\![[\sigma] * \{\sigma : \tau\}]\!]_\eta\, w$ is contained in $[\![\tau * \{\sigma : \tau\}]\!]_\eta\, w$. So assume $(k,(v,h))$ is in the former set. By definition, this means $(k,v) \in [\![[\sigma]]\!]_\eta\, w$ and $(k,h) \in [\![\{\sigma : \tau\}]\!]_\eta\, w$. The first property gives $\eta\sigma = v$. But then the second property yields $(k,(v,h)) \in [\![\tau]\!]_\eta\, w$, and thus $(k,v) \in [\![\tau]\!]_\eta\, w$. Combining these facts, we get $(k,(v,h)) \in [\![\tau * \{\sigma : \tau\}]\!]_\eta\, w$. ☐

C.3 Value and expression typing judgements

Most of the typing rules for values are verified straightforwardly with respect to the step-indexed semantics.

Lemma C.17 (VAR)**.** Suppose $(x : \tau) \in \Delta$.
Then, for any η, $\eta \vDash (\Delta \vdash x : \tau)$.

Proof. Let $w \in W$, $k \in \mathbb{N}$ and $(k,\rho) \in [\![\Delta]\!]_\eta\, w$. Since $x{:}\tau$ in Δ we immediately obtain the required $(k,\rho(x)) \in [\![\tau]\!]_\eta\, w$ from the definition of $[\![\Delta]\!]$. ☐

Lemma C.18 (UNIT)**.** For any η, $\eta \vDash (\Delta \vdash () : 1)$.

Proof. Let $w \in W$, $k \in \mathbb{N}$ and $(k,\rho) \in [\![\Delta]\!]_\eta\, w$. We must show that $(k,\rho\,()) \in [\![1]\!]_\eta\, w$, which is immediate by the definition of $[\![1]\!]$. ☐

Lemma C.19 (INJ)**.** Suppose $\eta \vDash (\Delta \vdash v : \tau_i)$.
Then $\eta \vDash (\mathsf{inj}^i\, v : \tau_1{+}\tau_2)$.

Proof. Let $i = 1$ or $i = 2$. Let $w \in W$, $k \in \mathbb{N}$ and $(k,\rho) \in [\![\Delta]\!]_\eta\, w$. We must show that $(k,\rho(\mathsf{inj}^i\, v)) \in [\![\tau_1{+}\tau_2]\!]_\eta\, w$. Unfolding the assumption, we have $(k,\rho(v)) \in [\![\tau_i]\!]_\eta\, w$, and thus $(k{-}1,\rho(v)) \in [\![\tau_i]\!]_\eta\, w$ by the uniformity of $[\![\tau_i]\!]_\eta\, w$. Using $\rho(\mathsf{inj}^i\, v) = \mathsf{inj}^i\, \rho(v)$ and the definition of $[\![\tau_1{+}\tau_2]\!]$, we obtain $(k,\rho(\mathsf{inj}^i\, v)) \in [\![\tau_1{+}\tau_2]\!]_\eta\, w$. ☐

Lemma C.20 (PAIR)**.** Suppose $\eta \vDash (\Delta \vdash v_1 : \tau_1)$ and $\eta \vDash (\Delta \vdash v_2 : \tau_2)$. Then $\eta \vDash (\Delta \vdash (v_1,v_2) : (\tau_1 \times \tau_2))$.

Proof. Let $w \in W$, $k \in \mathbb{N}$ and $(k,\rho) \in [\![\Delta]\!]_\eta\, w$. We must show $(k,\rho(v_1,v_2)) \in [\![\tau_1{\times}\tau_2]\!]_\eta\, w$, i.e., $(k,(\rho(v_1),\rho(v_2))) \in [\![\tau_1{\times}\tau_2]\!]_\eta\, w$. By assumption, we have both $(k,\rho(v_1)) \in [\![\tau_1]\!]_\eta\, w$ and $(k,\rho(v_2)) \in [\![\tau_2]\!]_\eta\, w$, which by the uniformity of $[\![\tau_1]\!]_\eta\, w$ and $[\![\tau_2]\!]_\eta\, w$ and by the definition of $[\![\tau_1 \times \tau_2]\!]$ suffices. ☐

Lemma C.21 (RECFUN)**.** Suppose $\eta \vDash (\Delta,\, f : \chi_1 \to \chi_2,\, x : \chi_1 \Vdash t : \chi_2)$. Then $\eta \vDash (\Delta \vdash \mu f.\lambda x.t : \chi_1 \to \chi_2)$.

Proof. Let $w \in W$. We prove by induction on k:

$$\forall k \in \mathbb{N}.\ (k,\rho) \in [\![\Delta]\!]_\eta\, w \ \Rightarrow\ (k,\rho(\mu f.\lambda x.t)) \in [\![\chi_1 \to \chi_2]\!]_\eta\, w$$

In the case $k = 0$ there is nothing to show, since $(0,v) \in [\![\chi_1 \to \chi_2]\!]_\eta\, w$ holds for any value v by definition of $[\![\chi_1 \to \chi_2]\!]$. So suppose $k > 0$, let $(k,\rho) \in [\![\Delta]\!]_\eta\, w$, let $j < k$, let $r \in \mathit{Cap}$ and

$$(j,(v,h)) \in [\![\chi_1]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

We can assume that $f, x \notin \operatorname{dom}\rho$ and then have to show

$$(j{+}1,((\mu f.\lambda x.\rho\, t)\, v,h)) \in \mathcal{E}([\![\chi_2]\!]_\eta * r)(w)\ . \tag{52}$$

By the operational semantics,

$$\big((\mu f.\lambda x.\rho\, t)\, v \mid h\big) \longmapsto \big((\rho[f{:=}\mu f.\lambda x.\rho\, t, x{:=}v])(t) \mid h\big)\ . \tag{53}$$

By uniformity of $[\![\Delta]\!]_\eta\, w$, the induction hypothesis and uniformity of $[\![\chi_1 \to \chi_2]\!]_\eta\, w$ we have

$$(j,\mu f.\lambda x.\rho\, t) \in [\![\chi_1 \to \chi_2]\!]_\eta\, w$$

Thus, by the uniformity of $[\![\chi_1]\!]$, we obtain

$$(j,(\rho[f{:=}\mu f.\lambda x.\rho\, t, x{:=}v],h)) \in [\![\Delta, f{:}\chi_1 \to \chi_2, x{:}\chi_1]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Hence we have

$$\big(j,\big((\rho[f{:=}\mu f.\lambda x.\rho\, t, x{:=}v])(t),h\big)\big) \in \mathcal{E}([\![\chi_2]\!]_\eta * r)(w)\ , \tag{54}$$

by the assumption $\eta \vDash (\Delta,\, f : \chi_1 \to \chi_2,\, x : \chi_1 \Vdash t : \chi_2)$. From (54) and (53) we can conclude (52). ☐

Lemma C.22 ($\forall$-INTRO)**.** Suppose $\vDash (\Delta \vdash v : \tau)$ and α not free in Δ. Then $\vDash (\Delta \vdash v : \forall\alpha.\tau)$.

Lemma C.23 ($\forall$-ELIM 1)**.** Suppose $\vDash (\Delta \vdash v : \forall\alpha.\tau)$. Then, for any τ', we have that $\vDash (\Delta \vdash v : \tau[\alpha{:=}\tau'])$.

Lemma C.24 (VAL)**.** Suppose $\eta \vDash (\Delta \vdash v : \tau)$.
Then $\eta \vDash (\Delta \Vdash v : \tau)$.

Proof. Let $w \in W$, $k \in \mathbb{N}$, $r \in \mathit{Cap}$ and

$$(k,(\rho,h)) \in [\![\Delta]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Hence, $(k,h) \in r(w) * \iota^{-1}(w)(\mathit{emp})$ and $(k,\rho\, v) \in [\![\tau]\!]_\eta\, w$ by assumption $\eta \vDash (\Delta \vdash v : \tau)$. The latter yields $(k,(\rho\, v,[])) \in [\![\tau]\!]_\eta\, w$ in case τ is viewed as a computation type, and therefore $(k,(\rho\, v,h)) \in \mathcal{E}([\![\tau]\!]_\eta * r)(w)$ by definition of $\mathcal{E}$. ☐

Lemma C.25 (APP)**.** Suppose $\eta \vDash (\Delta \vdash v : \chi_1 \to \chi_2)$ and $\eta \vDash (\Delta,\Gamma \Vdash t : \chi_1)$. Then $\eta \vDash (\Delta,\Gamma \Vdash (v\, t) : \chi_2)$.

Proof. Let $w \in W$, $k \in \mathbb{N}$, and $r \in \mathit{Cap}$. Let

$$(k,(\rho,h)) \in [\![\Delta,\Gamma]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ ,$$

and let ρ_1 be the restriction of ρ to $\operatorname{dom}\Delta$. Thus, $(k,\rho_1) \in [\![\Delta]\!]_\eta\, w$. By the assumptions and using $\rho\, v = \rho_1\, v$ we obtain

$$(k,\rho\, v) \in [\![\chi_1 \to \chi_2]\!]_\eta\, w \tag{55}$$

$$(k,(\rho\, t,h)) \in \mathcal{E}([\![\chi_1]\!]_\eta * r)(w) \tag{56}$$

We must show

$$(k,((\rho\, v)\,(\rho\, t),h)) \in \mathcal{E}([\![\chi_2]\!]_\eta * r)(w)\ . \tag{57}$$

To this end, assume that $((\rho\, v)\,(\rho\, t) \mid h) \longmapsto^j (t' \mid h')$ for some $j \leq k$ and irreducible $(t' \mid h')$. By the determinacy of the operational semantics (up to the choice of location names), there exists $i \leq j$ such that this sequence decomposes into

$$((\rho\, v)\,(\rho\, t) \mid h) \longmapsto^i ((\rho\, v)\, t'' \mid h'') \longmapsto^{j-i} (t' \mid h')$$

where $(\rho\, t \mid h) \longmapsto^i (t'' \mid h'')$ and $(t'' \mid h'')$ is irreducible. By (56) and the uniformity of $[\![\chi_1]\!]_\eta$ we know

$$(k{-}i{-}1, (t'', h'')) \in [\![\chi_1]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

By (55) this yields $(k{-}i, ((\rho\, v)\, t'', h'')) \in \mathcal{E}([\![\chi_2]\!]_\eta * r)(w)$, and from $j - i \leq k - i$ we therefore have

$$(k{-}i{-}(j{-}i), (t', h')) \in [\![\chi_2]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

In summary, we have shown (57). ☐

Lemma C.26 (SHALLOW-FRAME)**.** Suppose $\eta \vDash (\Gamma \Vdash t : \chi)$. Then $\eta \vDash (\Gamma * C \Vdash t : \chi * C)$.

Proof. Let $w \in W$, $k \in \mathbb{N}$ and $r \in Cap$. Let

$$(k, (\rho, h)) \in [\![\Gamma * C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

This can be written equivalently as

$$(k, (\rho, h)) \in [\![\Gamma]\!]_\eta\, w * r'(w) * \iota^{-1}(w)(emp)\ ,$$

for $r' = [\![C]\!]_\eta * r$. The assumption $\eta \vDash (\Gamma \Vdash t : \chi)$ then yields

$$(k, (\rho\, t, h)) \in \mathcal{E}([\![\chi]\!]_\eta * r')(w)\ ,$$

and thus, by unfolding r',

$$(k, (\rho\, t, h)) \in \mathcal{E}([\![\chi * C]\!]_\eta * r)(w)\ .$$

In summary, we have shown $\eta \vDash (\Gamma * C \Vdash t : \chi * C)$. ☐

Lemma C.27 (DEEP-FRAME)**.** Suppose $\eta \vDash (\Gamma \Vdash t : \chi)$. Then $\eta \vDash (\Gamma \otimes C, C \Vdash t : (\chi \otimes C) * C)$.

Proof. A proof of this inference rule is given in an abstract setting in [45, Sect. 3]. Here we give a direct proof: Let $w \in W$, $k \in \mathbb{N}$ and $r \in Cap$. Let

$$(k, (\rho, h)) \in [\![(\Gamma \otimes C) * C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ ,$$

Note that this can be written equivalently as

$$(k, (\rho, h)) \in [\![\Gamma]\!]_\eta\, w' * r'(w') * \iota^{-1}(w')(emp)\ .$$

for $w' = \iota([\![C]\!]_\eta) \circ w$ and $r'(w_0) = r(w)$, by Lemma C.3. Then the assumption $\eta \vDash (\Gamma \Vdash t : \chi)$ yields

$$(k, (\rho\, t, h)) \in \mathcal{E}([\![\chi]\!]_\eta * r')(w')\ .$$

By the definition of w', r' and Lemma C.3,

$$\begin{aligned}(k, (\rho\, t, h)) &\in \mathcal{E}([\![\chi]\!]_\eta * r')(\iota([\![C]\!]_\eta) \circ w)\\ &= \mathcal{E}(([\![\chi]\!]_\eta * r') \otimes \iota([\![C]\!]_\eta) * [\![C]\!]_\eta)(w)\\ &= \mathcal{E}(([\![\chi \otimes C]\!]_\eta * [\![C]\!]_\eta * r' \otimes \iota([\![C]\!]_\eta))(w)\\ &= \mathcal{E}([\![\chi \otimes C * C]\!]_\eta * r)(w)\ .\end{aligned}$$

We have shown $\eta \vDash (\Gamma \otimes C, C \Vdash t : (\chi \otimes C) * C)$. ☐

Lemma C.28 (SUB)**.** Suppose $\eta \vDash (\Gamma \Vdash t : \chi_1)$ and $\chi_1 \leq \chi_2$. Then $\eta \vDash (\Gamma \Vdash t : \chi_2)$.

Proof. As shown in Section C.2, $\chi_1 \leq \chi_2$ implies $[\![\chi_1]\!]_\eta\, w \subseteq [\![\chi_2]\!]_\eta\, w$ for all η and w. This gives us the soundness of SUB. ☐

Lemma C.29 (PROJ-1)**.** Suppose $\eta \vDash (\Gamma \Vdash v : [\sigma] * \{\sigma : \tau_1 \times \theta_2\})$.
Then $\eta \vDash (\Gamma \Vdash \mathsf{proj}^1\, v : \tau_1 * \{\sigma : \tau_1 \times \theta_2\})$.

Proof. Let $k \in \mathbb{N}$ and $w \in W$. Let $r \in Cap$ and let

$$(k, (\rho, h)) \in [\![\Gamma]\!]_\eta\, w * r(w) * \iota^{-1}(w)(\mathsf{emp})\ .$$

By assumption,

$$(k, (\rho(v), h) \in \mathcal{E}([\![[\sigma] * \{\sigma : \tau_1 \times \theta_2\}]\!]_\eta * r)(w)\ .$$

Since $\rho(v)$ is a value and therefore $(\rho(v)h)$ is irreducible, this means by definition that h splits into $h = h' \cdot h''$ and that

$$\begin{aligned}&\eta(\sigma) = \rho(v)\\ &(k, (\rho(v), h')) \in [\![\tau_1 \times \theta_2]\!]_\eta\, w\\ &(k, h'') \in r(w) * \iota^{-1}(w)(emp)\end{aligned}$$

Thus there exist $v_1, v_2 \in \mathit{Val}$ such that $\rho(v) = (v_1, v_2)$ and $(k{-}1, v_1) \in [\![\tau_1]\!]_\eta\, w$ and $(k{-}1, (v_2, h')) \in [\![\theta_2]\!]_\eta\, w$. By definition of the operational semantics, $(\mathsf{proj}^1(\rho v) \mid h) \longmapsto (v_1 \mid h)$, and by the above considerations, $(k{-}1, (v_1, h' \cdot h''))$ is in

$$[\![\tau_1 * \{\sigma : \tau_1 \times \theta_2\}]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

Thus, $(k, (\mathsf{proj}^1 v', h)) \in \mathcal{E}([\![\tau_1 * \{\sigma : \tau_1 \times \theta_2\}]\!]_\eta * r)(w)$, and we have shown $\eta \vDash (\Gamma \Vdash \mathsf{proj}^1\, v : \tau_1 * \{\sigma : \tau_1 \times \theta_2\})$. ☐

The case of PROJ-2 is analogous to Lemma C.29.

Lemma C.30 (CASE)**.** Suppose
$\eta \vDash (\Delta \vdash v_1 : (\exists \sigma_1.[\sigma_1] * \{\sigma : [\sigma_1] + 0\} * \{\sigma_1 : \theta_1\} * C) \to \chi)$,
$\eta \vDash (\Delta \vdash v_2 : (\exists \sigma_2.[\sigma_2] * \{\sigma : 0 + [\sigma_2]\} * \{\sigma_2 : \theta_2\} * C) \to \chi)$,
$\eta \vDash (\Delta, \Gamma \Vdash v : [\sigma] * \{\sigma : \theta_1 + \theta_2\} * C)$.
Then $\eta \vDash (\Delta, \Gamma \Vdash \mathsf{case}(v_1, v_2, v) : \chi)$.

Proof. Let $k \in \mathbb{N}$ and $w \in W$. Let $r \in Cap$ and let

$$(k, (\rho, h)) \in [\![\Delta, \Gamma]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

Since the restriction ρ_1 of ρ to the domain of Δ satisfies $(k, \rho_1) \in [\![\Delta]\!]_\eta\, w$, the assumptions give the following properties:

$$\begin{aligned}&(k, \rho(v_1)) \in [\![(\exists \sigma_1.[\sigma_1]{*}\{\sigma : [\sigma_1] + 0\}{*}\{\sigma_1 : \theta_1\}{*}C) \to \chi]\!]_\eta\, w\\ &(k, \rho(v_2)) \in [\![(\exists \sigma_2.[\sigma_2]{*}\{\sigma : 0 + [\sigma_2]\}{*}\{\sigma_2 : \theta_2\}{*}C) \to \chi]\!]_\eta\, w\\ &(k, \rho(v)) \in [\![[\sigma]]\!]_\eta\, w\\ &(k, h) \in [\![\{\sigma : \theta_1 + \theta_2\} * C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\end{aligned}$$

Unfolding the definitions, we obtain a splitting $h = h' \cdot h''$ such that

$$\begin{aligned}&(k, (\eta(\sigma), h')) \in [\![\theta_1 + \theta_2]\!]_\eta\, w\\ &(k, h'') \in [\![C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\end{aligned}$$

and thus $\rho(v) = \eta(\sigma) = \mathsf{inj}{i}v''$ for some $i = 1$ or $i = 2$ and some v'' such that

$$(k{-}1, (v'', h')) \in [\![\theta_i]\!]_\eta\, w$$

Let us assume $i = 1$; the other case is analogous. Further, let us write η_1 for $\eta[\sigma_1 := v'']$. Then, assuming $\sigma_1 \notin \mathit{RegNames}(C)$ and using uniformity, we have

$$\begin{aligned}&(k{-}1, v'') \in [\![[\sigma_1]]\!]_{\eta_1}\, w\\ &(k{-}1, []) \in [\![\{\sigma : [\sigma_1] + 0\}]\!]_{\eta_1}\, w\\ &(k{-}1, h') \in [\![\{\sigma_1 : \theta_1\}]\!]_{\eta_1}\, w\\ &(k{-}1, h'') \in [\![C]\!]_{\eta_1}\, w * r(w) * \iota^{-1}(w)(emp)\end{aligned}$$

Thus, we have $(k{-}1, (v'', h))$ in

$$[\![\exists \sigma_1.[\sigma_1] * \{\sigma : [\sigma_1] + 0\} * \{\sigma_1 : \theta_1\} * C]\!]_\eta\, w * r(w) * \iota^{-1}(w)(emp)\ .$$

By the above considerations for v_1 we obtain

$$(k-1, (\rho(v_1)\, v'', h)) \in \mathcal{E}(\llbracket\chi\rrbracket_\eta * r)(w)\ .$$

Since $(\rho(\mathsf{case}(v_1, v_2, v)) \,|\, h) \longmapsto (\rho(v_1)\, v'' \,|\, h)$ by the operational semantics, this gives

$$(k, (\rho(\mathsf{case}(v_1, v_2, v)), h)) \in \mathcal{E}(\llbracket\chi\rrbracket_\eta * r)(w)\ .$$

In summary, we have shown $\eta \vDash (\Delta, \Gamma \Vdash \mathsf{case}(v_1, v_2, v) : \chi)$. ☐

Lemma C.31 (REF)**.** Suppose $\eta \vDash (\Gamma \Vdash v : \tau)$. Then $\eta \vDash (\Gamma \Vdash \mathsf{ref}\, v : \exists\sigma.[\sigma] * \{\sigma : \mathsf{ref}\,\tau\})$.

Proof. Let $k \in \mathbb{N}$ and $w \in W$, $r \in \mathit{Cap}$ and

$$(k, (\rho, h)) \in \llbracket\Gamma\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Thus, the assumption $\eta \vDash (\Gamma \Vdash v : \tau)$ yields $(k, (\rho\, v, h)) \in \mathcal{E}(\llbracket\tau\rrbracket_\eta * r)(w)$, and therefore

$$(k, (\rho\, v, h)) \in \llbracket\tau\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Thus, $(k, \rho\, v) \in \llbracket\tau\rrbracket_\eta\, w$ and $(k, h) \in r(w) * \iota^{-1}(w)(\mathit{emp})$. By uniformity, also $(k-2, \rho\, v) \in \llbracket\tau\rrbracket_\eta\, w$. By definition of the operational semantics,

$$(\mathsf{ref}\,(\rho\, v) \,|\, h) \longmapsto (l \,|\, h \cdot [l \mapsto (\rho\, v)])$$

for $l \notin \mathrm{dom}\, h$. If we write η_1 for $\eta[\sigma := l]$ then we have

$$(k-1, l) \in \llbracket[\sigma]\rrbracket_{\eta_1}\, w$$
$$(k-1, (l, [l \mapsto (\rho\, v)])) \in \llbracket\mathsf{ref}\,\tau\rrbracket_{\eta_1}\, w$$

and thus also $(k-1, [l \mapsto (\rho\, v)]) \in \llbracket\{\sigma : \mathsf{ref}\,\tau\}\rrbracket_{\eta_1}\, w$. In summary, we have shown that $(k-1, (l, h \cdot [l \mapsto (\rho\, v)]))$ is in

$$\llbracket\exists\sigma.[\sigma] * \{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ ,$$

and thus $(k, (\mathsf{ref}\,(\rho\, v), h)) \in \mathcal{E}(\llbracket\exists\sigma.[\sigma] * \{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta * r)(w)$, i.e., we have shown $\eta \vDash (\Gamma \Vdash \mathsf{ref}\, v : \exists\sigma.[\sigma] * \{\sigma : \mathsf{ref}\,\tau\})$. ☐

Lemma C.32 (GET)**.** Suppose $\eta \vDash (\Gamma \Vdash v : [\sigma] * \{\sigma : \mathsf{ref}\,\tau\})$. Then $\eta \vDash (\Gamma \Vdash \mathsf{get}\, v : \tau * \{\sigma : \mathsf{ref}\,\tau\})$.

Proof. Let $k \in \mathbb{N}$ and $w \in W$. Let $r \in \mathit{Cap}$ and

$$(k, (\rho, h)) \in \llbracket\Gamma\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

By the assumption $\eta \vDash (\Gamma \Vdash v : [\sigma] * \{\sigma : \mathsf{ref}\,\tau\})$, this means

$$(k, ((\rho\, v), h)) \in \mathcal{E}(\llbracket[\sigma] * \{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta * r)(w)$$

and therefore

$$(k, ((\rho\, v), h)) \in \llbracket[\sigma]*\{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Then h splits into $h = h' \cdot h''$ such that

$$\eta(\sigma) = \rho(v)$$
$$(k, h') \in \llbracket\{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta\, w$$
$$(k, h'') \in r(w) * \iota^{-1}(w)(\mathit{emp})$$

The second item means that h' is $[(\rho\, v) \mapsto v'] \cdot h_0$ for some value v' with $(k-1, v') \in \llbracket\tau\rrbracket_\eta\, w$, and therefore

$$(k-1, (v', h)) \in \llbracket\tau * \{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

From $(\mathsf{get}\,(\rho\, v) \,|\, h) \longmapsto (v' \,|\, h)$ we obtain

$$(k, (\mathsf{get}\,(\rho\, v), h)) \in \mathcal{E}(\llbracket\tau * \{\sigma : \mathsf{ref}\,\tau\}\rrbracket_\eta * r)(w)\ ,$$

hence $\eta \vDash (\Gamma \Vdash \mathsf{get}\, v : \tau * \{\sigma : \mathsf{ref}\,\tau\})$. ☐

Lemma C.33 (SET)**.** Suppose $\eta \vDash (\Gamma \Vdash v : ([\sigma] \times \tau_2) * \{\sigma : \mathsf{ref}\,\tau_1\})$. Then $\eta \vDash (\Gamma \Vdash \mathsf{set}\, v : 1 * \{\sigma : \mathsf{ref}\,\tau_2\})$.

Proof. Let $k \in \mathbb{N}$ and $w \in W$. Let $r \in \mathit{Cap}$ and

$$(k, (\rho, h)) \in \llbracket\Gamma\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

By the assumption $\eta \vDash (\Gamma \Vdash v : ([\sigma] \times \tau_2) * \{\sigma : \mathsf{ref}\,\tau_1\})$ this gives

$$(k, (\rho\, v, h)) \in \mathcal{E}(\llbracket([\sigma]\times\tau_2)*\{\sigma : \mathsf{ref}\,\tau_1\}\rrbracket_\eta * r)(w)$$

and therefore

$$(k, (\rho\, v, h)) \in \llbracket([\sigma]\times\tau_2)*\{\sigma : \mathsf{ref}\,\tau_1\}\rrbracket_\eta\, w*r(w)*\iota^{-1}(w)(\mathit{emp})\ .$$

Then h splits into $h = h' \cdot h''$ such that

$$(k, \rho\, v) \in \llbracket[\sigma] \times \tau_2\rrbracket_\eta\, w$$
$$(k, h') \in \llbracket\{\sigma : \mathsf{ref}\,\tau_1\}\rrbracket_\eta\, w$$
$$(k, h'') \in r(w) * \iota^{-1}(w)(\mathit{emp})$$

Thus $\rho(v)$ is of the form $v = (v_1, v_2)$, $\eta(\sigma) = v_1$ and h' is of the form $[v_1 \mapsto v_1'] \cdot h_0$, for some values v_1, v_1', v_2 with $(k-1, v_2) \in \llbracket\tau_2\rrbracket_\eta\, w$. In particular, $(k-1, [v_1 \mapsto v_2] \cdot h_0) \in \llbracket\{\sigma : \mathsf{ref}\,\tau_2\}\rrbracket_\eta\, w$ by the uniformity of $\llbracket\tau_2\rrbracket_\eta\, w$ and therefore

$$(k-1, ((), [v_1 \mapsto v_2] \cdot h'')) \in \llbracket 1 * \{\sigma : \mathsf{ref}\,\tau_2\}\rrbracket_\eta\, w * r(w) * \iota^{-1}(w)(\mathit{emp})\ .$$

Since $(\mathsf{set}\, v \,|\, h) \longmapsto (() \,|\, h[v_1 := v_2])$, and $h[v_1 := v_2]$ is just $[v_1 \mapsto v_2] \cdot h_0 \cdot h''$, this immediately yields

$$(k, (\mathsf{set}\, v, h)) \in \mathcal{E}(\llbracket 1 * \{\sigma : \mathsf{ref}\,\tau_2\}\rrbracket_\eta * r)(w)\ ,$$

and we have shown $\eta \vDash (\Gamma \Vdash \mathsf{set}\, v : 1 * \{\sigma : \mathsf{ref}\,\tau_2\})$. ☐

D. Application: Step-Indexed Model of Separation Logic for Nested Hoare Triples

In this appendix we present another new application of recursively-defined sets of Kripke worlds: a step-indexed model of separation logic for nested Hoare triples.

In recent work, Schwinghammer et al. [44] present a domain-theoretic model of a variant of separation logic for a language that allows code to be stored in the heap (a form of "higher-order store"). The model is used to prove soundness of rules for "recursion through the heap" as well as soundness of higher-order frame rules that take stored code into account. (Both kinds of rules will be explained in more detail below.) The model is based on the solution of a recursive world equation using complete uniform subsets of a domain, akin to the situation in Section 2.2.

In this section we present a new, *operational* model of the same logic, following the approach outlined in Section 2.3. We do this for three reasons: first, to substantiate the claim that the metric-space technique works for both domain-theoretic and step-indexed models, and second, to illustrate the use of obtaining a *solution* (rather than an approximation of a solution) of a recursive equation for "worlds," and three, to obtain a *simpler* model than the one in [44]. (We do not claim that the new model is sound for more inference rules than the one in [44].)

The development in the rest of this section mostly follows the one in [44]; we shall highlight some key differences. The reader is assumed to be familiar with basic properties of separation logic [43].

D.1 Programming language

Figure 10 presents the language we consider [44]. It deviates from the "standard" core programming language of separation logic [43] in two ways. First, stack variables are immutable: only heap cells can be updated. Second, commands are first-class values that can be stored in the heap: there is a new form of expression called a

Expressions:

$$e ::= x \mid `C` \mid n \mid e_1 + e_2 \mid \ldots \qquad (n \in \mathbb{Z})$$

Commands:

$$\begin{aligned} C ::= {} & [e_1] := e_2 \mid \mathsf{let}\ x = [e]\ \mathsf{in}\ C \mid \mathsf{eval}\ [e] \\ & \mid \mathsf{let}\ x = \mathsf{new}(e)\ \mathsf{in}\ C \mid \mathsf{free}\ e \\ & \mid \mathsf{skip} \mid C_1; C_2 \mid \mathsf{if}\ (e_1 = e_2)\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2 \end{aligned}$$

Figure 10. Programming language.

quoted command, written 'C', and a new command for evaluating stored commands, written eval $[e]$. Informally, if the value of e is an integer n, and if the current heap contains the quoted command 'C' at location n, then the command eval $[e]$ executes C as a subroutine.

We write $\mathrm{fv}(C)$ for the set of free variables of the command C, and similarly for expressions. Let V be the set of closed values of the language, and let H be the set of *heaps*, i.e., finite maps from integers to closed values:

$$V = \mathbb{Z} \cup \{`C` \mid \mathrm{fv}(C) = \emptyset\},$$
$$H = \mathbb{Z} \rightharpoonup_{fin} V.$$

For two heaps $h_1, h_2 \in H$ we write $h_1 \# h_2$ if they have disjoint domains and $h_1 \cdot h_2$ for their union if this is the case. An *environment* is a finite map η from variables to closed values. When C is a command satisfying that $\mathrm{fv}(C) \subseteq \eta$, we let $\eta(C)$ denote the result of applying η to C as a capture-avoiding substitution. Given an expression e and an environment η such that $\mathrm{fv}(e) \subseteq \mathrm{dom}(\eta)$, we define $[\![e]\!]_\eta \in V$ as follows. When e is a quoted command 'C' we let $[\![e]\!]_\eta = [\![`C`]\!]_\eta = \eta(C)$. When e is an arithmetic expression, $[\![e]\!]_\eta$ is defined in the expected way, *except* that arithmetic operations on quoted commands are, for definiteness, given the meaning 0. Thence we avoid the complications of introducing undefined expressions in a Hoare-style logic.[10]

A small-step operational semantics for the language is defined in Figure 11. A configuration (C, h) of the semantics consists of a closed command C and a heap h. An aborting configuration indicates a memory fault or a runtime "type error" due to confusion between integers and quoted commands.

Example D.1 (Iteration). The language does not include any high-level constructs for iteration. One can encode a "while" loop by means of "Landin's knot" in the heap:

$$\begin{aligned} \mathsf{while}\ [e] \neq 0\ \mathsf{do}\ C \stackrel{def}{=}\ & \mathsf{let}\ x = \mathsf{new}(`\mathsf{skip}`)\ \mathsf{in} \\ & ([x] := `\ \mathsf{let}\ y = [e]\ \mathsf{in} \\ & \qquad \mathsf{if}\ (y = 0)\ \mathsf{then\ free}\ x \\ & \qquad \mathsf{else}\ (C; \mathsf{eval}\ [x])`\,; \\ & \ \mathsf{eval}\ [x]) \end{aligned}$$

(Here $x, y \notin \mathrm{fv}(e, C)$.) With that abbreviation, the following rule is derivable in the logic we present below:

$$\frac{\Gamma \vdash \{\exists y.\, e \mapsto y * I(y) \wedge y \neq 0\} C \{\exists y.\, e \mapsto y * I(y)\}}{\Gamma \vdash \{\exists y.\, e \mapsto y * I(y)\} \mathsf{while}\ [e] \neq 0\ \mathsf{do}\ C \{e \mapsto 0 * I(0)\}}$$

[10] A more robust approach would be to introduce a simple type system that distinguishes integers from quoted commands; for simplicity we do not do so here.

D.2 Logic

The formulas of the logic [44] are called *assertions* and are generated by the grammar:

$$\begin{aligned} P, Q ::= {} & \mathsf{false} \mid \mathsf{true} \mid P \wedge Q \mid P \vee Q \mid P \Rightarrow Q \mid \\ & \forall x.P \mid \exists x.P \mid \mathsf{int}(e) \mid e_1 = e_2 \mid e_1 \leq e_2 \mid \\ & e_1 \mapsto e_2 \mid \mathsf{emp} \mid P * Q \mid P -\!\!* Q \\ & \{P\}e\{Q\} \mid P \otimes Q \mid \cdots \end{aligned}$$

where the dots refer to atomic predicates and recursively defined predicates of the form $(\mu\alpha(x).P)(e)$ with α in P only occurring in "contractive" positions. (For space reasons, we de not formalize recursively defined assertions syntactically, but just treat them semantically, see below.) Unlike in standard separation logic, assertions are used both to describe predicates on heaps and to describe specifications of commands.

Indeed, the assertion $\{P\}e\{Q\}$ means, intuitively, that the value of e is a quoted command 'C' which satisfies the Hoare triple with precondition P and postcondition Q in the usual sense of separation logic. Since Hoare triples are assertions, they can appear in pre- and post-conditions of other triples. Such *nested* triples are useful for reasoning about stored code: the specification of a command C can depend on the specification of other code in the heap, e.g.,

$$\{P * \exists y.\, x \mapsto y \wedge \{P'\}y\{Q'\}\}`C`\{Q\}\,. \tag{58}$$

Here a part of the precondition of C is that x points to a command y satisfying $\{P'\}y\{Q'\}$. Presumably, the reason is that C contains one or more occurrences of eval $[x]$.

The assertion $P \otimes Q$ should be thought of as "the assertion P extended with the invariant Q" and this assertion form is used to codify higher-order frame rules [19]. See [44] for detailed discussion of soundness and unsoundness of variations higher-order frame rules in the presence of higher-order store.

Proof Rules The proof rules include the standard rules for intuitionistic predicate logic and the logic of bunched implications [36]. Moreover, there are variations of standard separation logic proof rules (for dereferencing, sequencing, and so on). The proof rules can be found in Figure 12. Here Γ ranges over finite sets of variables.

Rule ($\otimes$-FRAME) is a deep frame rule in which the invariant Q intuitively is added to all pre- and post-conditions inside P. The latter intuition is captured by the axioms in Figure 13. Rule ($*$-FRAME) is a shallow (first-order) frame axiom. Finally, rule (EVAL) is the rule for executing stored code. Here, $e \mapsto R[\_]$ is an abbreviation of $\exists x.\, e \mapsto x \wedge R[x]$ (for an x not free in R).

D.3 A step-indexed model

To model invariant extension $P \otimes Q$, Schwinghammer et. al. [44] models an assertion as a *function* that takes the meaning of a second, arbitrary assertion (to be thought of as the "invariant" that the first assertion is extended with) and gives a predicate on heaps.[11] This approach introduces a circularity, however, since such a function will in particular be applicable to itself. In the next section we show how to formalize and solve the circularity using metric spaces.

D.3.1 Semantic predicates

Following Section 2.3, we let $UPred(H)$ be the set of subsets of $\mathbb{N} \times H$ that are downwards closed in the first component:

$$\{p \subseteq \mathbb{N} \times H \mid \forall (k, h) \in p. \forall j \leq k. (j, h) \in p\}.$$

[11] This idea follows earlier work on invariant extension [19, 20], which does not, however, deal with nested Hoare triples.

$$
\begin{array}{rcll}
([e_1] := e_2,\, h) & \rightsquigarrow & (\mathsf{skip}, h[n \mapsto [\![e_2]\!]]) & \text{if } [\![e_1]\!] = n \text{ and } n \in \mathrm{dom}(h) \\
(\mathsf{let}\ x = [e]\ \mathsf{in}\ C,\, h) & \rightsquigarrow & (C[v/x], h) & \text{if } [\![e]\!] = n \text{ and } h(n) = v \\
(\mathsf{eval}\ [e],\, h) & \rightsquigarrow & (C, h) & \text{if } [\![e]\!] = n \text{ and } h(n) = \text{`}C\text{`} \\
(\mathsf{let}\ x = \mathsf{new}(e)\ \mathsf{in}\ C,\, h) & \rightsquigarrow & (C[n/x],\, h * [n \mapsto [\![e]\!]]) & \text{if } n \notin \mathrm{dom}(h) \\
(\mathsf{free}\ e,\, h) & \rightsquigarrow & (\mathsf{skip}, h') & \text{if } [\![e]\!] = n \text{ and } h = h' * [n \mapsto v] \\
(C_1; C_2,\, h) & \rightsquigarrow & (C_1'; C_2,\, h') & \text{if } (C_1, h) \rightsquigarrow (C_1', h') \\
(\mathsf{skip}; C_2,\, h) & \rightsquigarrow & (C_2, h) & \\
(\mathsf{if}\ (e_1 = e_2)\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2,\, h) & \rightsquigarrow & (C_1, h) & \text{if } [\![e_1]\!] = [\![e_2]\!] \\
(\mathsf{if}\ (e_1 = e_2)\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2,\, h) & \rightsquigarrow & (C_2, h) & \text{if } [\![e_1]\!] \neq [\![e_2]\!] \\
([e_1] := e_2,\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } [\![e_1]\!] = \text{`}C\text{`} \text{ or } [\![e_1]\!] = n \text{ where } n \notin \mathrm{dom}(h) \\
(\mathsf{let}\ x = [e]\ \mathsf{in}\ C,\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } [\![e]\!] = \text{`}C\text{`} \text{ or } [\![e]\!] = n \text{ where } n \notin \mathrm{dom}(h) \\
(\mathsf{eval}\ [e],\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } [\![e]\!] = \text{`}C\text{`} \text{ or } [\![e]\!] = n \text{ where } n \notin \mathrm{dom}(h) \\
(\mathsf{eval}\ [e],\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } [\![e]\!] = n \text{ where } h(n) = m \\
(\mathsf{free}\ e,\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } [\![e]\!] = \text{`}C\text{`} \text{ or } [\![e]\!] = n \text{ where } n \notin \mathrm{dom}(h) \\
(C_1; C_2,\, h) & \rightsquigarrow & \mathsf{abort} & \text{if } (C_1, h) \rightsquigarrow \mathsf{abort}
\end{array}
$$

Figure 11. Operational semantics.

$$
\begin{array}{rcl@{\qquad}l}
P \circ R & \stackrel{def}{=} & (P \otimes R) * R & \{P\}e\{Q\} \otimes R \iff \{P \circ R\}e\{Q \circ R\} \\
(\kappa x. P) \otimes R & \iff & \kappa x. (P \otimes R) & (\kappa \in \{\forall, \exists\},\ x \notin \mathrm{fv}(R)) \\
(P \oplus Q) \otimes R & \iff & (P \otimes R) \oplus (Q \otimes R) & (\oplus \in \{\Rightarrow, \wedge, \vee, *, -\!\!*\}) \\
P \otimes R & \iff & P & (P \text{ is } \mathsf{true}, \mathsf{false}, \mathsf{emp}, e_1 = e_2, e_1 \mapsto e_2, \text{ or } \mathsf{int}(e)) \\
(P \otimes R) \otimes R' & \iff & P \otimes (R \circ R') & P \otimes \mathsf{emp} \iff P
\end{array}
$$

Figure 13. Axioms for invariant extension.

$$\frac{\Gamma, x \vdash \{P * e \mapsto x\}\text{`}C\text{`}\{Q\}}{\Gamma \vdash \{\exists x.\, P * e \mapsto x\}\text{`}\mathsf{let}\ x = [e]\ \mathsf{in}\ C\text{`}\{Q\}}\ (x \notin \mathrm{fv}(e, Q)) \quad \text{(DEREF)}$$

$$\frac{}{\Gamma \vdash \{e \mapsto \_ * P\}\text{`}[e] := e_0\text{`}\{e \mapsto e_0 * P\}} \quad \text{(UPDATE)}$$

$$\frac{\Gamma, x \vdash \{P * x \mapsto e\}\text{`}C\text{`}\{Q\}}{\Gamma \vdash \{P\}\text{`}\mathsf{let}\ x = \mathsf{new}(e)\ \mathsf{in}\ C\text{`}\{Q\}}\ (x \notin \mathrm{fv}(P, e, Q)) \quad \text{(NEW)}$$

$$\frac{}{\Gamma \vdash \{e \mapsto \_ * P\}\text{`}\mathsf{free}\ e\text{`}\{P\}} \quad \text{(FREE)}$$

$$\frac{}{\Gamma \vdash \{P\}\text{`}\mathsf{skip}\text{`}\{P\}} \quad \text{(SKIP)}$$

$$\frac{\Gamma \vdash \{P\}\text{`}C_1\text{`}\{R\} \qquad \Gamma \vdash \{R\}\text{`}C_2\text{`}\{Q\}}{\Gamma \vdash \{P\}\text{`}C_1; C_2\text{`}\{Q\}} \quad \text{(SEQ)}$$

$$\frac{\Gamma \vdash \{P \wedge e_1 = e_2\}\text{`}C_1\text{`}\{Q\} \qquad \Gamma \vdash \{P \wedge e_1 \neq e_2\}\text{`}C_2\text{`}\{Q\}}{\Gamma \vdash \{P\}\text{`}\mathsf{if}\ (e_1 = e_2)\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\text{`}\{Q\}} \quad \text{(IF)}$$

$$\frac{\Gamma \vdash P' \Rightarrow P \qquad \Gamma \vdash Q \Rightarrow Q'}{\Gamma \vdash \{P\}e\{Q\} \Rightarrow \{P'\}e\{Q'\}} \quad \text{(CONSEQ)}$$

$$\frac{\Gamma \vdash P}{\Gamma \vdash P \otimes Q} \quad \text{($\otimes$-FRAME)}$$

$$\frac{}{\Gamma \vdash \{P\}e\{Q\} \Rightarrow \{P * R\}e\{Q * R\}} \quad \text{($*$-FRAME)}$$

$$\frac{\Gamma, k \vdash R[k] \Rightarrow \{P * e \mapsto R[\_]\}k\{Q\}}{\Gamma \vdash \{P * e \mapsto R[\_]\}\text{`}\mathsf{eval}\ [e]\text{`}\{Q\}} \quad \text{(EVAL)}$$

Figure 12. Proof rules for Hoare triples.

We give $UPred(H)$ the same distance function as in Section 2.3; the set then becomes a complete, bounded ultrametric space. Using Theorem 2.1 we obtain a unique $W \in \mathbf{CBUlt}_{\mathrm{ne}}$ satisfying

$$W \cong \tfrac{1}{2}(W \to UPred(H)). \tag{59}$$

Define $Pred = \frac{1}{2}(W \to UPred(H))$ and let $i : Pred \to W$ be the isomorphism. We will model assertions as elements of $Pred$.

Let the letters p and q range over elements of $Pred$. We order the elements of $Pred$ pointwise:

$$p \leq q \iff \forall w \in W.\, p(w) \subseteq q(w)$$

Lemma D.2. With the ordering above and the following operations, $Pred$ is a complete BI-algebra [17]:

$$
\begin{aligned}
emp(w) &= \{(n, []) \mid n \in \mathbb{N}\} \\
(p * q)(w) &= \{(n, h) \mid \exists h_1, h_2.\, h = h_1 \cdot h_2 \\
&\qquad \wedge (n, h_1) \in p(w) \wedge (n, h_2) \in q(w)\} \\
(p -\!\!* q)(w) &= \{(n, h) \mid \forall m \leq n. \\
&\qquad ((m, h') \in p(w) \wedge h \# h') \Rightarrow (m, h \cdot h') \in q(w)\}
\end{aligned}
$$

The fact that $Pred$ is a complete BI algebra immediately gives us a sound interpretation of most of the assertions in the logic [17], but to interpret recursive predicates we also need to know that the operations are non-expansive:

Lemma D.3. The BI-algebra operations on $Pred$ given by the previous lemma are non-expansive:

$$
\begin{gathered}
, -\!\!, \to, \wedge, \vee : Pred \times Pred \to Pred \\
\textstyle\bigvee_I, \bigwedge_I : (I \to Pred) \to Pred.
\end{gathered}
$$

(In the last two operations, the indexing set I is given the discrete metric.)

Proof. Easy verification. One first shows the analogous property for $UPred(H)$. To illustrate what follows, consider $*$: $UPred(H) \times UPred(H) \to UPred(H)$: It suffices to show that if $p \stackrel{n}{=} p'$ and $q \stackrel{n}{=} q'$, then also $(p * q) \stackrel{n}{=} (p' * q')$. The latter is equivalent to showing that $\forall m < n.\, (m, h) \in p * q \iff (m, h) \in p' * q'$, which follows easily by the assumption. □

D.3.2 Interpretation of invariant extension

To interpret invariant-extension assertions $P \otimes Q$, we need a operator $\otimes$ on the set of semantic predicates $Pred$. The most convenient way to specify $\otimes$ is to give a certain recursive equation that it must satisfy. Using the metric-space setup we can then prove that there exists a unique operator satisfying this specification, by an easy application of Banach's fixed point theorem, as in [44].

Proposition D.4. There exists a unique function $\otimes : Pred \times W \to Pred$ in $\mathbf{CBUlt}_{\mathrm{ne}}$ satisfying

$$p \otimes w = \lambda w'.\, p(w \circ w')$$

where $\circ : W \times W \to W$ is given by

$$w_1 \circ w_2 = i((i^{-1}(w_1) \otimes w_2) * i^{-1}(w_2))\,.$$

Observe that it is here that we exploit that we have obtained a proper solution to the world equation (59) as a metric space such that we can now easily establish the existence of the recursively-defined $\otimes$-operation.

The basic properties of $\otimes$ and $\circ$ are conveniently summarized as follows:

Proposition D.5. 1. $(W, \circ, \mathsf{emp})$ is a monoid.

2. The operator $\otimes$ is a monoid action of W on $Pred$: for all $P \in Pred$ and $w_1, w_2 \in W$ we have $P \otimes \mathsf{emp} = P$ and $(P \otimes w_1) \otimes w_2 = P \otimes (w_1 \circ w_2)$.

D.3.3 Interpretation of assertions

We next define a semantic interpretation of Hoare triples. To this end we let Safe_m be the set of configurations in the operational semantics that are safe for m reduction steps, that is, those configurations that do not reduce to abort in m (or fewer) steps. We write $\rightsquigarrow_k$ for the k-step reduction relation of the operational semantics.

Now say that $w \models_n (p, C, q)$ holds iff: For all $r \in UPred$, all $m < n$ and all heaps h, if $(m, h) \in p(w) * i^{-1}(w)(\mathsf{emp}) * r$, then:

1. $(C, h) \in \mathrm{Safe}_m$.
2. For all $k \le m$ and all $h' \in H$, if $(C, h) \rightsquigarrow_k (\mathsf{skip}, h')$, then $(m - k, h') \in q(w) * i^{-1}(w)(\mathsf{emp}) * r$.

This definition is similar to the one in [44] with its use of the invariant w and the baking-in of the first order frame rule, i.e., the quantification over r. The difference is that the meaning is now relative to the operational semantics (rather than denotational) and that we use step indexing to measure to what extent pre- and post-conditions should hold.

The intention is, of course, that a Hoare-triple assertion is interpreted using the above semantic construct. However, to see that this interpretation gives a well-defined member of $Pred$, we need to know that a semantic Hoare triple is "non-expansive in w":

Proposition D.6. If $w =_k w'$ and $w \models_n (p, C, q)$, then $w' \models_{n \wedge (k-1)} (p, C, q)$.

Proof. Easy verification, using the fact that the separating conjunction $*$ on $UPred(V)$ is non-expansive (Lemma D.3). □

The interpretation of an assertion $\Gamma \vdash P$ is now defined to be an element $[\![P]\!]_\eta$ in $Pred$, for η an environment mapping the variables in the domain of Γ to V. The definition uses the complete BI-algebra structure on $Pred$ given earlier to interpret the standard logical connectives, e.g.,

$$[\![P * Q]\!]_\eta w = [\![P]\!]_\eta w * [\![Q]\!]_\eta w.$$

Invariant extension is interpreted as follows:

$$[\![P \otimes Q]\!]_\eta w = \Big([\![P]\!]_\eta \otimes i([\![Q]\!]_\eta)\Big)\, w$$

and, finally, Hoare triples are interpreted like this:

$$[\![\{P\}e\{Q\}]\!]_\eta w = \begin{cases} \{(n, h) \mid w \models_n ([\![P]\!]_\eta, C, [\![Q]\!]_\eta)\} & \text{if } [\![e]\!]_\eta = \text{`}C\text{`} \\ \emptyset & \text{otherwise.} \end{cases}$$

The concrete interpretation of all the logical connectives can be found in Figure 14. As in [44], recursively defined predicates are interpreted via Banach's fixed point theorem:

Proposition D.7. Let I be a set and suppose that, for each $i \in I$, $F_i : Pred^I \to Pred$ is a contractive function. Then there exists a unique $\vec{p} = (p_i)_{i \in I} \in Pred^I$ such that $F_i(\vec{p}) = p_i$, for all $i \in I$.

D.3.4 Soundness of proof rules

We define semantic validity of (open) assertions as follows: For an assertion P with free variables belonging to Γ, say that $\Gamma \models P$ iff: For all environments η with $\Gamma \subseteq \mathrm{dom}(\eta)$ and all $w \in W$ we have $[\![P]\!]_\eta w = \mathbb{N} \times H$. This amounts to saying that $[\![P]\!]_\eta$ is the top element of the BI algebra $Pred$.

Theorem D.8. If $\Gamma \vdash P$, then $\Gamma \models P$.

Proof. By showing the stronger property that each proof rule holds semantically, that is, with $\vdash$ replaced by $\models$. We only include the proof case for $\mathsf{eval}\ [e]$ (the other interesting cases are the ones for invariant extension; there one uses Proposition D.5). We must show: if $\Gamma, z \models R[z] \Rightarrow \{P * e \mapsto R[\_]\}z\{Q\}$, then $\Gamma \models \{P * e \mapsto R[\_]\}\text{`}\mathsf{eval}\ [e]\text{`}\{Q\}$.

Let η be an environment with $\Gamma \subseteq \mathrm{dom}(\eta)$, and let w and n be arbitrary. We must show that

$$w \models_n \{[\![P * e \mapsto R[\_]]\!]\eta\}\text{`}\eta(\mathsf{eval}\ [e])\text{`}\{[\![Q]\!]\eta\}. \qquad (60)$$

So let $k < n$ and $r \in UPred$ and let $(k, h) \in [\![P * e \mapsto R[\_]]\!]\eta(w) * i^{-1}(w)(\mathsf{emp}) * r$. Then $h = h_1 * [l \mapsto v] * h_2 * h_3$, where $(k, h_1) \in [\![P]\!]\eta(w)$ and $[\![e]\!]\eta = l$ and $(k, [l \mapsto v]) \in [\![R[z]]\!]\eta[z \mapsto v](w)$ and $(k, h_2) \in i^{-1}(w)(\mathsf{emp})$ and $(k, h_3) \in r$. Using validity of the premise, we get that $(k, [l \mapsto v]) \in [\![\{P * e \mapsto R[z]\}z\{Q\}]\!]\eta[z \mapsto v](w)$, which means that $v = \text{`}C\text{`}$ for some C, and that $w \models_k \{[\![P * e \mapsto R[z]]\!]\eta\}C\{[\![Q]\!]\eta\}$. Now, if $k = 0$, then conditions 1 and 2 in the definition of $\models$ are clearly satisfied (item 2 because $(\eta(\mathsf{eval}\ [e]), h)$ takes a reduction step), so (60) holds, as required. If $k > 0$ then, first observe that by downwards closure we have $(k - 1, h) \in [\![P * e \mapsto R[\_]]\!]\eta(w) * i^{-1}(w)(\mathsf{emp}) * r$. Therefore, $(C, h) \in \mathrm{Safe}_{k-1}$, which implies that $(\eta(\mathsf{eval}\ [e]), h) \in \mathrm{Safe}_k$, so condition 1 in definition of $\models$ is satisfied. For condition 2, we finally assume that $(\eta(\mathsf{eval}\ [e]), h) \rightsquigarrow_m (\mathsf{skip}, h')$ for some h' and $m \le k$. Then $(C, h) \rightsquigarrow_{m-1} (\mathsf{skip}, h')$. Since $m - 1 \le k - 1$, we then get $((k - 1) - (m - 1), h') \in [\![Q]\!]\eta(w) * i^{-1}(w)(\mathsf{emp}) * r$, as required. □

D.4 Discussion

In summary, we have developed a new step-indexed model of separation logic with nested Hoare triples for reasoning about higher-order store. The new model is arguably simpler than the one in [44], since it is phrased directly in terms of the operational semantics without passing through a domain-theoretic denotational semantics. A usual advantage of using domain-theory is a more abstract semantics, but in [44], it was in necessary to employ certain "step-like," rank functions, so in the end the model of *loc.cit.* was not more abstract than the new one presented here.

$$
\begin{aligned}
[\![\mathsf{false}]\!]_\eta w &= \emptyset \\
[\![\mathsf{true}]\!]_\eta w &= \mathbb{N} \times H \\
[\![P \wedge Q]\!]_\eta w &= [\![P]\!]_\eta w \cap [\![Q]\!]_\eta w \\
[\![P \vee Q]\!]_\eta w &= [\![P]\!]_\eta w \cup [\![Q]\!]_\eta w \\
[\![P \Rightarrow Q]\!]_\eta w &= \{(n,h) \mid \forall m \leq n.\, (m,h) \in [\![P]\!]_\eta w \Rightarrow (m,h) \in [\![Q]\!]_\eta w \\
[\![\forall x.P]\!]_\eta w &= \textstyle\bigcap_{v \in V} [\![P]\!]_{\eta[x \mapsto v]} w \\
[\![\exists x.P]\!]_\eta w &= \textstyle\bigcup_{v \in V} [\![P]\!]_{\eta[x \mapsto v]} w \\
[\![\mathsf{int}(e)]\!]_\eta w &= \begin{cases} \mathbb{N} \times H & \text{if } [\![e]\!]_\eta = m \text{ for some } m \in \mathbb{Z} \\ \emptyset & \text{otherwise} \end{cases} \\
[\![e_1 = e_2]\!]_\eta w &= \begin{cases} \mathbb{N} \times H & \text{if } [\![e_1]\!]_\eta = [\![e_2]\!]_\eta \\ \emptyset & \text{otherwise} \end{cases} \\
[\![e_1 \leq e_2]\!]_\eta w &= \begin{cases} \mathbb{N} \times H & \text{if } [\![e_1]\!]_\eta = m_1 \text{ and } [\![e_2]\!]_\eta = m_2 \text{ where } m_1 \leq m_2 \\ \emptyset & \text{otherwise} \end{cases} \\
[\![e_1 \mapsto e_2]\!]_\eta w &= \begin{cases} \{(n, [m \mapsto [\![e_2]\!]_\eta]) \mid n \in \mathbb{N}\} & \text{if } [\![e_1]\!]_\eta = m \text{ for some } m \in \mathbb{Z} \\ \emptyset & \text{otherwise} \end{cases} \\
[\![\mathsf{emp}]\!]_\eta w &= \mathbb{N} \times \{[\,]\} \\
[\![P * Q]\!]_\eta w &= [\![P]\!]_\eta w * [\![Q]\!]_\eta w \\
[\![P \mathrel{-\!\!*} Q]\!]_\eta w &= [\![P]\!]_\eta w \mathrel{-\!\!*} [\![Q]\!]_\eta w \\
[\![\{P\}e\{Q\}]\!]_\eta w &= \begin{cases} \{(n,h) \mid w \models_n ([\![P]\!]_\eta, C, [\![Q]\!]_\eta)\,\} & \text{if } [\![e]\!]_\eta = \text{`}C\text{`} \\ \emptyset & \text{otherwise} \end{cases} \\
[\![P \otimes Q]\!]_\eta w &= \Big([\![P]\!]_\eta \otimes i([\![Q]\!]_\eta)\Big)\, w
\end{aligned}
$$

Figure 14. Interpretation of assertions.