A Taste of Categorical Logic — Tutorial Notes

Lars Birkedal (birkedal@cs.au.dk) Aleš Bizjak (abizjak@cs.au.dk)

June 12, 2014

Contents

1 Introduction **2**

2 Higher-order predicate logic **2**

3 A first set-theoretic model **4**

4 Hyperdoctrine **8**

4.1 Interpretation of higher-order logic in a hyperdoctrine 9

4.2 A class of **Set**-based hyperdoctrines 14

4.3 Examples based on monoids 16

4.4 BI-hyperdoctrines 18

4.5 Guarded recursion for predicates 19

4.5.1 Application to the logic 21

5 Complete ordered families of equivalences **23**

5.1 $\mathcal{U}$-based hyperdoctrine 25

6 Constructions on the category $\mathcal{U}$ **31**

6.1 A typical recursive domain equation 32

6.2 Explicit construction of fixed points of locally contractive functors in $\mathcal{U}$ 36

7 Further Reading — the Topos of Trees **40**

1 Introduction

We give a taste of categorical logic and present selected examples. The choice of examples is guided by the wish to prepare the reader for understanding current research papers on step-indexed models for modular reasoning about concurrent higher-order imperative programming languages.

These tutorial notes are supposed to serve as a companion when reading up on introductory category theory, e.g., as described in Awodey's book [Awo10], and are aimed at graduate students in computer science.

The material described in Sections 5 and 6 has been formalized in the Coq proof assistant and there is an accompanying tutorial on the Coq formalization, called the ModuRes tutorial, available online at

`http://cs.au.dk/~birke/modures/tutorial`

The Coq ModuRes tutorial has been developed primarily by Filip Sieczkowski, with contributions from Aleš Bizjak, Yannick Zakowski, and Lars Birkedal.

We have followed the "design desiderata" listed below when writing these notes:

- keep it brief, with just enough different examples to appreciate the point of generalization;
- do not write an introduction to category theory; we may recall some definitions, but the reader should refer to one of the many good introductory books for an introduction
- use simple definitions rather than most general definitions; we use a bit of category theory to understand the general picture needed for the examples, but refer to the literature for more general definitions and theorems
- selective examples, requiring no background beyond what an undergraduate computer science student learns, and aimed directly at supporting understanding of step-indexed models of modern programming languages

For a much more comprehensive and general treatment of categorical logic we recommend Jacobs' book [Jac99]. See also the retrospective paper by Pitts [Pit02] and Lawvere's originial papers, e.g., [Law69].

2 Higher-order predicate logic

In higher-order predicate logic we are concerned with sequents of the form $\Gamma \mid \Xi \vdash \psi$. Here Γ is a *type context* and specifices which free variables are allowed in Ξ and ψ. Ξ is the *proposition context* which is a lists of propositions. ψ is a proposition. The reading of $\Gamma \mid \Xi \vdash \psi$ is that ψ (the conclusion) follows from the assumptions (or hypotheses) in Ξ. For example

$$x : \mathbb{N}, y : \mathbb{N} \mid \mathbf{odd}(x), \mathbf{odd}(y) \vdash \mathbf{even}(x + y) \tag{1}$$

is a sequent expressing that the sum of two odd natural numbers is an even natural number.

However that is not really the case. The sequent we wrote is just a piece of syntax and the intuitive description we have given is suggested by the suggestive names we have used for predicate symbols (**odd**, **even**), function symbols (+) and sorts (also called types) ($\mathbb{N}$). To express the *meaning* of the sequent we need a model where the meaning of, for instance, $\mathbf{odd}(x)$ will be that x is an odd natural number. We now make this precise.

To have a useful logic we need to start with some basic things; a signature.

Definition 2.1. A *signature* $(\mathcal{T}, \mathcal{F})$ for higher-order predicate logic consists of

- A set of base *types* (or *sorts*) $\mathcal{T}$ including a special type $\texttt{Prop}$ of propositions.
- A set of typed *function symbols* $\mathcal{F}$ meaning that each $F \in \mathcal{F}$ has a type $F : \sigma_1, \sigma_2, \ldots, \sigma_n \to \sigma_{n+1}$ for $\sigma_1, \ldots, \sigma_{n+1} \in \mathcal{T}$ associated with it. We read $\sigma_1, \ldots, \sigma_n$ as the type of arguments and σ_{n+1} as the result type.

We sometimes call function symbols $\texttt{P}$ with codomain $\texttt{Prop}$, i.e., $\texttt{P} : \sigma_1, \sigma_2, \ldots, \sigma_n \to \texttt{Prop}$ *predicate symbols.* ■

Example 2.2. Taking $\mathcal{T} = \{\mathbb{N}, \texttt{Prop}\}$ and $\mathcal{F} = \{\textbf{odd} : \mathbb{N} \to \texttt{Prop}, \textbf{even} : \mathbb{N} \to \texttt{Prop}, + : \mathbb{N}, \mathbb{N} \to \mathbb{N}\}$ we have that $(\mathcal{T}, \mathcal{F})$ is a signature. ■

Given a signature $\Sigma = (\mathcal{T}, \mathcal{F})$ we have a typed language of *terms.* This is simply typed lambda calculus with base types in $\mathcal{T}$ and base constants in $\mathcal{F}$ and these are the terms whose properties we specify and prove in the logic. The typing rules are listed in Figure 1. The set of types $\mathcal{C}(\mathcal{T})$ is inductively defined to be the least set containing $\mathcal{T}$ and closed under $\mathbf{1}$ (the unit type) product ($\times$) and arrow ($\to$). We write $M\,[N/x]$ denote for capture-avoiding substitution of term N for free variable x in M. We write $M\,[N_1/x_1, N_2/x_2, \ldots N_n/x_n]$ for *simultaneous* capture-avoiding substitution of N_i for x_i in M.

$$\frac{\sigma \in \mathcal{C}(\mathcal{T})}{x : \sigma \vdash x : \sigma}\ \textbf{identity} \qquad \frac{\Gamma \vdash M : \tau}{\Gamma, x : \sigma \vdash M : \tau}\ \textbf{weakening} \qquad \frac{\Gamma, x : \sigma, y : \sigma \vdash M : \tau}{\Gamma, x : \sigma \vdash M\,[x/y] : \tau}\ \textbf{contraction}$$

$$\frac{\Gamma, x : \sigma, y : \sigma', \Delta \vdash M : \tau}{\Gamma, x : \sigma', y : \sigma, \Delta \vdash M\,[y/x, x/y] : \tau}\ \textbf{exchange} \qquad \frac{\Gamma \vdash M_1 : \tau_1 \qquad \ldots \qquad \Gamma \vdash M_n : \tau_n}{\Gamma \vdash F(M_1, \ldots, M_n) : \tau_{n+1}}\ \begin{array}{c}\textbf{function symbol}\\ F : \tau_1, \ldots, \tau_n \to \tau_{n+1} \in \mathcal{F}\end{array}$$

$$\frac{\Gamma \vdash M : \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash \langle M, N \rangle : \tau \times \sigma}\ \textbf{pairing} \qquad \frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \pi_1\, M : \tau}\ \textbf{proj-1} \qquad \frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \pi_2\, M : \sigma}\ \textbf{proj-2} \qquad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau}\ \textbf{abs}$$

$$\frac{\Gamma \vdash M : \tau \to \sigma \qquad \Gamma \vdash N : \tau}{\Gamma \vdash M\,N : \sigma}\ \textbf{app} \qquad \frac{}{\Gamma \vdash \langle\rangle : \mathbf{1}}\ \textbf{unit}$$

Figure 1: Typing rules relative to a signature $(\mathcal{T}, \mathcal{F})$. Γ is a type context, i.e., a list $x_1 : \sigma_1, x_2 : \sigma_2, \ldots, x_n : \sigma_n$ and when we write $\Gamma, x : \sigma$ we assume that x does not occur in Γ.

Since we are dealing with higher-order logic there is no real distinction between propositions and terms. However there are special connectives that only work for terms of type $\texttt{Prop}$, i.e., propositions. These are

- $\bot$ falsum
- $\top$ the true proposition
- $\varphi \wedge \psi$ conjunction
- $\varphi \vee \psi$ disjunction
- $\varphi \Rightarrow \psi$ implication
- $\forall x : \sigma, \varphi$ universal quantification over $\sigma \in \mathcal{C}(\mathcal{T})$)

- $\exists x : \sigma, \varphi$ existential quantification over $\sigma \in \mathcal{C}(\mathcal{T})$)

The typing rules for these are listed in Figure 2. Capture avoiding substitution is extended in the obvious way to these connectives.

Notice that we did not include an equality predicate. This is just for brevity. In higher-order logic equality can be defined as Leibniz equality, see, e.g., [Jac99]. (See the references in the introduction for how equality can be modeled in hyperdoctrines using left adjoints to reindexing along diagonals.)

$$\frac{}{\Gamma \vdash \bot : \mathtt{Prop}}\ \textbf{false} \qquad \frac{}{\Gamma \vdash \top : \mathtt{Prop}}\ \textbf{true}$$

$$\frac{\Gamma \vdash \varphi : \mathtt{Prop} \qquad \Gamma \vdash \psi : \mathtt{Prop}}{\Gamma \vdash \varphi \wedge \psi : \mathtt{Prop}}\ \textbf{conj} \qquad \frac{\Gamma \vdash \varphi : \mathtt{Prop} \qquad \Gamma \vdash \psi : \mathtt{Prop}}{\Gamma \vdash \varphi \vee \psi : \mathtt{Prop}}\ \textbf{disj}$$

$$\frac{\Gamma \vdash \varphi : \mathtt{Prop} \qquad \Gamma \vdash \psi : \mathtt{Prop}}{\Gamma \vdash \varphi \Rightarrow \psi : \mathtt{Prop}}\ \textbf{impl} \qquad \frac{\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}}{\Gamma \vdash \forall x : \sigma, \varphi : \mathtt{Prop}}\ \textbf{forall} \qquad \frac{\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}}{\Gamma \vdash \exists x : \sigma, \varphi : \mathtt{Prop}}\ \textbf{exists}$$

Figure 2: Typing rules for logical connectives. Note that these are not introduction and elimination rules for connectives. These merely state that some things are propositions, i.e., of type `Prop`

We can now describe sequents and provide basic rules of natural deduction. If $\psi_1, \psi_2, \ldots, \psi_n$ have type `Prop` in context Γ we write $\Gamma \vdash \psi_1, \psi_2, \ldots, \psi_n$ and call $\Xi = \psi_1, \ldots, \psi_n$ the propositional context. Given $\Gamma \vdash \Xi$ and $\Gamma \vdash \varphi$ we have a new judgment $\Gamma \mid \Xi \vdash \varphi$. The rules for deriving these are listed in Figure 3.

3 A first set-theoretic model

What we have described up to now is a system for deriving two judgments, $\Gamma \vdash M : \tau$ and $\Gamma \mid \Xi \vdash \varphi$. We now describe a first model where we give meaning to types, terms, propositions and sequents.

We interpret the logic in the category **Set** of sets and functions. There are several things to interpret.

- The signature $(\mathcal{T}, \mathcal{F})$.
- The types $\mathcal{C}(\mathcal{T})$
- The terms of simply typed lambda calculus
- Logical connectives
- The sequent $\Gamma \mid \Xi \vdash \psi$

Interpretation of the signature For a signature $(\mathcal{T}, \mathcal{F})$ we pick interpretations. That is, for each $\tau \in \mathcal{T}$ we pick a set X_τ but for `Prop` we pick the two-element set of "truth-values" $2 = \{0, 1\}$. For each $F : \tau_1, \tau_2, \ldots, \tau_n \to \tau_{n+1}$ we pick a function f from $X_{\tau_1} \times X_{\tau_2} \times \cdots \times X_{\tau_n}$ to $X_{\tau_{n+1}}$.

Rules for manipulation of contexts

$$\frac{\Gamma \vdash \varphi : \texttt{Prop}}{\Gamma \mid \varphi \vdash \varphi}\ \textbf{identity} \qquad \frac{\Gamma \mid \Theta \vdash \varphi \qquad \Gamma \mid \Xi, \varphi \vdash \psi}{\Gamma \mid \Theta, \Xi \vdash \psi}\ \textbf{cut} \qquad \frac{\Gamma \mid \Theta \vdash \varphi \qquad \Gamma \vdash \psi : \texttt{Prop}}{\Gamma \mid \Theta, \psi \vdash \varphi}\ \textbf{weak-prop}$$

$$\frac{\Gamma \mid \Theta, \varphi, \varphi \vdash \psi}{\Gamma \mid \Theta, \varphi \vdash \psi}\ \textbf{contr-prop} \qquad \frac{\Gamma \mid \Theta, \varphi, \psi, \Xi \vdash \chi}{\Gamma \mid \Theta, \psi, \varphi, \Xi \vdash \chi}\ \textbf{exch-prop} \qquad \frac{\Gamma \mid \Theta \vdash \varphi}{\Gamma, x : \sigma \mid \Theta \vdash \varphi}\ \textbf{weak-type}$$

$$\frac{\Gamma, x : \sigma, y : \sigma \mid \Theta \vdash \varphi}{\Gamma, x : \sigma \mid \Theta\,[y/x] \vdash \varphi\,[y/x]}\ \textbf{contr-type} \qquad \frac{\Gamma, x : \sigma, y : \rho, \Delta \mid \Theta \vdash \varphi}{\Gamma, y : \rho, x : \sigma \mid \Theta \vdash \varphi}\ \textbf{exch-type}$$

$$\frac{\Gamma \vdash M : \sigma \qquad \Delta, x : \sigma, \Delta' \mid \Theta \vdash \psi}{\Delta, \Gamma, \Delta' \mid \Theta\,[M/x] \vdash \psi\,[M/x]}\ \textbf{substitution}$$

Rules for introduction and elimination of connectives

$$\frac{}{\Gamma \mid \Theta \vdash \top}\ \textbf{true} \qquad \frac{}{\Gamma \mid \Theta, \bot \vdash \psi}\ \textbf{false}$$

$$\frac{\Gamma \mid \Theta \vdash \varphi \qquad \Gamma \mid \Theta \vdash \psi}{\Gamma \mid \Theta \vdash \varphi \wedge \psi}\ \textbf{and-I} \qquad \frac{\Gamma \mid \Theta \vdash \varphi \wedge \psi}{\Gamma \mid \Theta \vdash \varphi}\ \textbf{and-E1} \qquad \frac{\Gamma \mid \Theta \vdash \varphi \wedge \psi}{\Gamma \mid \Theta \vdash \psi}\ \textbf{and-E2}$$

$$\frac{\Gamma \mid \Theta \vdash \varphi}{\Gamma \mid \Theta \vdash \varphi \vee \psi}\ \textbf{or-I1} \qquad \frac{\Gamma \mid \Theta \vdash \psi}{\Gamma \mid \Theta \vdash \varphi \vee \psi}\ \textbf{or-I2} \qquad \frac{\Gamma \mid \Theta, \varphi \vdash \chi \qquad \Gamma \mid \Theta, \psi \vdash \chi}{\Gamma \mid \Theta, \varphi \vee \psi \vdash \chi}\ \textbf{or-E}$$

$$\frac{\Gamma \mid \Theta, \varphi \vdash \psi}{\Gamma \mid \Theta \vdash \varphi \Rightarrow \psi}\ \textbf{imp-I} \qquad \frac{\Gamma \mid \Theta \vdash \varphi \Rightarrow \psi \qquad \Gamma \mid \Theta \vdash \varphi}{\Gamma \mid \Theta \vdash \psi}\ \textbf{imp-E}$$

$$\frac{\Gamma, x : \sigma \mid \Theta \vdash \varphi}{\Gamma \mid \Theta \vdash \forall x : \sigma, \varphi}\ \forall\textbf{-I} \qquad \frac{\Gamma \vdash M : \sigma \qquad \Gamma \mid \Theta \vdash \forall x : \sigma, \varphi}{\Gamma \mid \Theta \vdash \varphi\,[M/x]}\ \forall\textbf{-E}$$

$$\frac{\Gamma \vdash M : \sigma \qquad \Gamma \mid \Theta \vdash \varphi\,[M/x]}{\Gamma \mid \Theta \vdash \exists x : \sigma, \varphi}\ \exists\textbf{-I} \qquad \frac{\Gamma \mid \Theta \vdash \exists x : \sigma, \varphi \qquad \Gamma, x : \sigma \mid \Xi, \varphi \vdash \psi}{\Gamma \mid \Theta, \Xi \vdash \psi}\ \exists\textbf{-E}$$

Figure 3: Natural deduction rules for higher-order logic. Note that by convention x does not appear free in Θ, Ξ or ψ in the rules $\forall$**-I** and $\exists$**-E** since we implicitly have that x is not in Γ and Θ, Ξ and ψ are well formed in context Γ.

Interpretation of simply typed lambda calculus Having interpreted the signature we extend the interpretation to types and terms of simply typed lambda calculus. Each type $\tau \in \mathcal{C}(\mathcal{T})$ is assigned a set $\llbracket\tau\rrbracket$ by induction

$$\begin{aligned} \llbracket\tau\rrbracket &= X_\tau \qquad \text{if } \tau \in \mathcal{T} \\ \llbracket\tau \times \sigma\rrbracket &= \llbracket\tau\rrbracket \times \llbracket\sigma\rrbracket \\ \llbracket\tau \to \sigma\rrbracket &= \llbracket\sigma\rrbracket^{\llbracket\tau\rrbracket} \end{aligned}$$

where on the right the operations are on sets, that is $A \times B$ denotes the cartesian product of sets and B^A denotes the set of all functions from A to B.

Interpretation of terms proceeds in a similarly obvious way. We interpret the typing judgment $\Gamma \vdash M : \tau$. For such a judgment we define $\llbracket\Gamma \vdash M : \tau\rrbracket$ as a function from $\llbracket\Gamma\rrbracket$ to $\llbracket\tau\rrbracket$, where $\llbracket\Gamma\rrbracket = \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket \times \cdots \llbracket\tau_n\rrbracket$ for $\Gamma = x_1 : \tau_1, x_2 : \tau_2, \ldots, x_n : \tau_n$. The interpretation is defined as usual in cartesian closed categories.

We then have the following result which holds for any cartesian closed category, in particular **Set**.

Proposition 3.1. *The interpretation of terms validates all the* β *and* η *rules, i.e., if* $\Gamma \vdash M \equiv N : \sigma$ *then* $[\![\Gamma \vdash M : \sigma]\!] = [\![\Gamma \vdash M : \tau]\!]$.

The β and η rules are standard computation rules for simply typed lambda calculus. We do not write them here explicitly and do not prove this proposition since it is a standard result relating simply typed lambda calculus and cartesian closed categories. But it is good exercise to try and prove it.

Exercise 3.1. Prove the proposition. Consider all the rules that generate the equality judgment $\equiv$ and prove for each that it is validate by the model. ♢

Interpretation of logical connectives Recall that the interpretation of `Prop` is 2, the two element set $\{0, 1\}$. We take 1 to mean "true" and 0 to mean "false". If we order 2 by postulating that $0 \leqslant 1$ then 2 becomes a complete Boolean algebra which in particular means that it is a complete Heyting algebra.

Exercise 3.2. Show that given any set X, the set of functions from X to 2, i.e., $\mathrm{Hom}_{\mathbf{Set}}(X, 2)$ is a complete Heyting algebra for operations defined pointwise.

Moreover, check for any two sets X and Y and any function $f : X \to Y$, $\mathrm{Hom}_{\mathbf{Set}}(f, 2)$ is a Heyting algebra homomorphism. ♢

In higher-order logic propositions are just terms so they are interpreted in the same way. However instead of using the cartesian closed structure of the category **Set** we use the Heyting algebra structure on $\mathrm{Hom}_{\mathbf{Set}}(X, 2)$ to interpret logical connectives. We write $\top_X$, $\bot_X$, $\wedge_X$, $\vee_X$ and $\Rightarrow_X$ for Heyting algebra operations in $\mathrm{Hom}_{\mathbf{Set}}(X, 2)$.

$$\begin{aligned}
[\![\Gamma \vdash \top : \mathtt{Prop}]\!] &= \top_{[\![\Gamma]\!]} \\
[\![\Gamma \vdash \bot : \mathtt{Prop}]\!] &= \bot_{[\![\Gamma]\!]} \\
[\![\Gamma \vdash \varphi \wedge \psi : \mathtt{Prop}]\!] &= ([\![\Gamma \vdash \varphi : \mathtt{Prop}]\!]) \wedge_{[\![\Gamma]\!]} ([\![\Gamma \vdash \psi : \mathtt{Prop}]\!]) \\
[\![\Gamma \vdash \varphi \vee \psi : \mathtt{Prop}]\!] &= ([\![\Gamma \vdash \varphi : \mathtt{Prop}]\!]) \vee_{[\![\Gamma]\!]} ([\![\Gamma \vdash \psi : \mathtt{Prop}]\!]) \\
[\![\Gamma \vdash \varphi \Rightarrow \psi : \mathtt{Prop}]\!] &= ([\![\Gamma \vdash \varphi : \mathtt{Prop}]\!]) \Rightarrow_{[\![\Gamma]\!]} ([\![\Gamma \vdash \psi : \mathtt{Prop}]\!])
\end{aligned}$$

It only remains to interpret quantifiers $\forall$ and $\exists$. Recall the formation rules from Figure 2. The interpretation of $\Gamma \vdash \forall x : \sigma, \varphi : \mathtt{Prop}$ should be a function $f : [\![\Gamma]\!] \to 2$ and we are given the interpretation of $\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}$, which is interpreted as a function $g : [\![\Gamma]\!] \times [\![\sigma]\!] \to 2$. What we need, then, is a function function $\forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]}$

$$\forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]} : \mathrm{Hom}_{\mathbf{Set}}([\![\Gamma]\!] \times [\![\sigma]\!], 2) \to \mathrm{Hom}_{\mathbf{Set}}([\![\Gamma]\!], 2).$$

There are many such functions, but only two that have all the necessary properties. One for universal and one for existential quantification. In fact we can be more general. We define

$$\forall_X^Y, \exists_X^Y : \mathrm{Hom}_{\mathbf{Set}}(X \times Y, 2) \to \mathrm{Hom}_{\mathbf{Set}}(X, 2)$$

for any sets X and Y and $\varphi : X \times Y \to 2$ as

$$\forall_X^Y(\varphi) = \lambda x. \begin{cases} 1 & \text{if } \forall y \in Y, \varphi(x,y) = 1 \\ 0 & \text{otherwise} \end{cases} = \lambda x. \begin{cases} 1 & \text{if } \{x\} \times Y \subseteq \varphi^{-1}[1] \\ 0 & \text{otherwise} \end{cases}$$

$$\exists_X^Y(\varphi) = \lambda x. \begin{cases} 1 & \text{if } \exists y \in Y, \varphi(x,y) = 1 \\ 0 & \text{otherwise} \end{cases} = \lambda x. \begin{cases} 1 & \text{if } \{x\} \times Y \cap \varphi^{-1}[1] \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

To understand these definitions and to present them graphically a presentation of functions from $X \to 2$ as subsets of X is useful. Consider the problem of obtaining a subset of X given a subset of $X \times Y$. One natural way to do this is to “project out” the second component, i.e., map a subset $A \subseteq X \times Y$ to $\pi[A] = \{\pi(z) \mid z \in A\}$ where $\pi : X \times Y \to X$ is the first projection. Observe that this gives rise to $\exists_X^Y$. Geometrically, if we draw X on the horizontal axis and Y on the vertical axis, A is a region on the graph. The image $\pi[A]$ includes all $x \in X$ such that the vertical line at x intersects A in at least one point.

We could instead choose to include only points $x \in X$ such that the vertical line at x is a subset of A. This way, we would get exactly $\forall_X^Y(A)$.

To further see that these are not arbitrary definitions but in fact essentially unique show the following.

Exercise 3.3. Let $\pi_{X,Y}^* = \mathrm{Hom}_{\mathbf{Set}}(\pi, 2) : \mathrm{Hom}_{\mathbf{Set}}(X, 2) \to \mathrm{Hom}_{\mathbf{Set}}(X \times Y, 2)$. Show that $\forall_X^Y$ and $\exists_X^Y$ are monotone functions (i.e., functors) and that $\forall_X^Y$ is the *right* adjoint to $\pi_{X,Y}^*$ and $\exists_X^Y$ its *left* adjoint.

Concretely the last part means to show for any $\varphi : X \to 2$ and $\psi : X \times Y \to 2$ that

$$\pi_{X,Y}^*(\varphi) \leqslant \psi \iff \varphi \leqslant \forall_X^Y(\psi)$$

and

$$\exists_X^Y(\psi) \leqslant \varphi \iff \psi \leqslant \pi_{X,Y}^*(\varphi).$$

◊

Moreover, $\forall_X^Y$ and $\exists_X^Y$ have essentially the same definition for all X, i.e., they are natural in X. This is expressed as the commutativity of the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbf{Set}}(X' \times Y, 2) \arrow[r, "\mathrm{Hom}_{\mathbf{Set}}(s \times \mathrm{id}_Y, 2)"] \arrow[d, "\forall_{X'}^Y"] & \mathrm{Hom}_{\mathbf{Set}}(X \times Y, 2) \arrow[d, "\forall_X^Y"] \\
\mathrm{Hom}_{\mathbf{Set}}(X', 2) \arrow[r, "\mathrm{Hom}_{\mathbf{Set}}(s, 2)"] & \mathrm{Hom}_{\mathbf{Set}}(X, 2)
\end{tikzcd}$$

for any $s : X \to X'$ (remember that the functor $\mathrm{Hom}_{\mathbf{Set}}(-, 2)$ is contravariant) and analogously for $\exists$.

This requirement that $\forall_X^Y$ and $\exists_X^Y$ are “natural” is often called the *Beck-Chevalley* condition.

Exercise 3.4. Show that $\exists_X^Y$ and $\forall_X^Y$ are natural in X. ◊

Using these adjoints we can finish the interpretation of propostions:

$$[\![\Gamma \vdash \forall x : \sigma, \varphi : \mathtt{Prop}]\!] = \forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]}\left([\![\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}]\!]\right)$$

$$[\![\Gamma \vdash \exists x : \sigma, \varphi : \mathtt{Prop}]\!] = \exists_{[\![\Gamma]\!]}^{[\![\sigma]\!]}\left([\![\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}]\!]\right)$$

Given a sequence of terms $\vec{M} = M_1, M_2, \ldots, M_n$ of type $\vec{\sigma} = \sigma_1, \sigma_2, \ldots, \sigma_n$ in context Γ we define $[\![\Gamma \vdash \vec{M} : \vec{\sigma}]\!]$ as the tupling of interpretations of individual terms.

Exercise 3.5. Show that given contexts $\Gamma = y_1 : \sigma_1, \ldots, y_m : \sigma_m$ and $\Delta = x_1 : \delta_1, \ldots, x_n : \delta_n$ we have the following property of the interpretation for any N of type τ in context Δ and any sequence of terms $\vec{M}$ of appropriate types

$$\left[\!\!\left[\Gamma \vdash N\left[\vec{M}/\vec{x}\right] : \tau\right]\!\!\right] = [\![\Delta \vdash N : \tau]\!] \circ [\![\Gamma \vdash \vec{M} : \vec{\delta}]\!]$$

To show this proceed by induction on the typing derivation for N. You will need to use the naturality of quantifiers. ♢

Remark 3.2. If you have done Exercise 3.5, you will have have notices that the perhaps mysterious Beck-Chevalley condition is nothing but the requirement that the model respects substitution, i.e., that the interpretation of

$$(\forall y : \sigma, \varphi)\, [M/x]$$

is equal to the interpretation of

$$\forall y : \sigma, (\varphi\, [M/x])$$

for $x \neq y$. ■

4 Hyperdoctrine

Using the motivating example above we now define the concept of a hyperdoctrine, which will be our general notion of a model of higher-order logic for which we prove soundness of the interpretation defined above.

Definition 4.1. A *hyperdoctrine* is a cartesian closed category $\mathcal{C}$ together with an object $\Omega \in \mathcal{C}$ (called the generic object) and for each object $X \in \mathcal{C}$ a choice of a partial order on the set $\mathrm{Hom}_{\mathcal{C}}(X, \Omega)$ such that the conditions below hold. We write $\mathcal{P}$ for the contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-, \Omega)$.

- $\mathcal{P}$ restricts to a contravariant functor $\mathcal{C}^{\mathrm{op}} \to$ **Heyt**, from $\mathcal{C}$ to the category of Heyting algebras and Heyting algebra homomorphisms, i.e., for each X, $\mathcal{P}(X)$ is a Heyting algebra and for each f, $\mathcal{P}(f)$ is a Heyting algebra homomorphisms, in particular it is monotone.
- For any objects $X, Y \in \mathcal{C}$ and the projection $\pi : X \times Y \to X$ there exist *monotone functions*[1] $\exists_X^Y$ and $\forall_X^Y$ such that $\exists_X^Y$ is a left adjoint to $\mathcal{P}(\pi) : \mathcal{P}(X) \to \mathcal{P}(X \times Y)$ and $\forall_X^Y$ is its right adjoint. Moreover, these adjoints are natural in X, meaning that for any morphism $s : X \to X'$ the diagrams

$$\begin{tikzcd}
\mathcal{P}(X' \times Y) \arrow[r, "\mathcal{P}(s \times \mathrm{id}_Y)"] \arrow[d, "\forall_{X'}^Y"] & \mathcal{P}(X \times Y) \arrow[d, "\forall_X^Y"] \\
\mathcal{P}(X') \arrow[r, "\mathcal{P}(s)"] & \mathcal{P}(X)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{P}(X' \times Y) \arrow[r, "\mathcal{P}(s \times \mathrm{id}_Y)"] \arrow[d, "\exists_{X'}^Y"] & \mathcal{P}(X \times Y) \arrow[d, "\exists_X^Y"] \\
\mathcal{P}(X') \arrow[r, "\mathcal{P}(s)"] & \mathcal{P}(X)
\end{tikzcd}$$

commute.

[1] We do *not* require them to be Heyting algebra homomorphisms.

■

Example 4.2. The category **Set** together with the object 2 for the generic object which we described in Section 3 is a hyperdoctrine. See the discussion and exercises in Section 3 for the definitions of adjoints. ■

4.1 Interpretation of higher-order logic in a hyperdoctrine

The interpretation of higher-order logic in a general hyperdoctrine proceeds much the same as the interpretation in Section 3.

First, we choose objects of $\mathcal{C}$ for base types and morphisms for function symbols. We must, of course, choose the interpretation of the type `Prop` to be Ω.

We then interpret the terms of simply typed lambda calculus using the cartesian closed structure of $\mathcal{C}$ and the logical connectives using the fact that each hom-set is a Heyting algebra. The interpretation is spelled out in Figure 4.

Note that the interpretation itself requires no properties of the adjoints to $\mathcal{P}(\pi)$. However, to show that the interpretation is sound, i.e., that it validates all the rules in Figure 3, all the requirements in the definition of a hyperdoctrine are essential. A crucial property of the interpretation is that it maps substitution into composition in the following sense.

Proposition 4.3. *Let* $\vec{M} = M_1, M_2, \dots M_n$ *be a sequence of terms and* Γ *a context such that for all* $i \in \{1, 2, \dots, n\}$*,* $\Gamma \vdash M_i : \delta_i$*. Let* $\Delta = x_1 : \delta_1, x_2 : \delta_2, \dots, x_n : \delta_n$ *be a context and* N *be a term such that* $\Delta \vdash N : \tau$*. Then the following equality holds*

$$\left[\!\!\left[\Gamma \vdash N\left[\vec{M}/\vec{x}\right] : \tau\right]\!\!\right] = [\![\Delta \vdash N : \tau]\!] \circ \left[\!\!\left[\Gamma \vdash \vec{M} : \vec{\delta}\right]\!\!\right] \tag{2}$$

where

$$\left[\!\!\left[\Gamma \vdash \vec{M} : \vec{\delta}\right]\!\!\right] = \langle [\![\Gamma \vdash M_i : \delta_i]\!] \rangle_{i=1}^{n}.$$

Further, if N *is of type* `Prop`*, i.e., if* $\tau = \texttt{Prop}$ *then*

$$\left[\!\!\left[\Gamma \vdash N\left[\vec{M}/\vec{x}\right] : \texttt{Prop}\right]\!\!\right] = \mathcal{P}\left(\left[\!\!\left[\Gamma \vdash \vec{M} : \vec{\delta}\right]\!\!\right]\right)([\![\Delta \vdash N : \texttt{Prop}]\!]) \tag{3}$$

Proof. Only the proof of the first equality requires work since if we know that substitution is mapped to composition then the second equality is just the first equality hidden by using the $\mathcal{P}$ functor since it acts on morphisms by precomposition.

To prove (2) we proceed by induction on the derivation of $\Delta \vdash N : \tau$. All of the cases are straightforward. We only show some of them to illustrate key points. To remove the clutter we omit explicit contexts and types, i.e., we write $[\![N]\!]$ instead of $[\![\Delta \vdash N : \tau]\!]$.

- When $N = K\,L$ and $\Delta \vdash K : \sigma \to \tau$ and $\Delta \vdash L : \sigma$. Recall that substitution distributes over application and that we can use the induction hypothesis for K and L. We have

  $$\begin{aligned}\left[\!\!\left[(K\,L)\left[\vec{M}/\vec{x}\right]\right]\!\!\right] &= \left[\!\!\left[\left(K\left[\vec{M}/\vec{x}\right]\right)\left(L\left[\vec{M}/\vec{x}\right]\right)\right]\!\!\right] \\ &= \varepsilon \circ \left\langle \left[\!\!\left[K\left[\vec{M}/\vec{x}\right]\right]\!\!\right], \left[\!\!\left[L\left[\vec{M}/\vec{x}\right]\right]\!\!\right] \right\rangle\end{aligned}$$

  which by induction is equal to

  $$= \varepsilon \circ \left\langle [\![K]\!] \circ \left[\!\!\left[\vec{M}\right]\!\!\right], [\![L]\!] \circ \left[\!\!\left[\vec{M}\right]\!\!\right] \right\rangle$$

Interpretation of types assuming a chosen interpretation of base types. We write $X \times Y$ and X^Y for the product and exponential in $\mathcal{C}$ respectively.

$$\begin{aligned}
\llbracket \mathbf{1} \rrbracket &= 1 \\
\llbracket \sigma \times \tau \rrbracket &= \llbracket \sigma \rrbracket \times \llbracket \tau \rrbracket \\
\llbracket \sigma \to \tau \rrbracket &= \llbracket \tau \rrbracket^{\llbracket \sigma \rrbracket}
\end{aligned}$$

Interpretation of terms (including logical connectives) assuming interpretations of function symbols. We use $\delta_X = \langle \mathrm{id}_X, \mathrm{id}_X, \rangle : X \to X \times X$ and $\xi_{X,Y} = \langle \pi', \pi \rangle : X \times Y \to Y \times X$. We use $\Lambda(f) : X \to Z^Y$ for the transpose of a morphism $f : X \times Y \to Z$ and $\varepsilon : X \times Y^X \to Y$ for the evaluation map.

$$\begin{aligned}
\llbracket x : \sigma \vdash x : \sigma \rrbracket &= \mathrm{id}_{\llbracket \sigma \rrbracket} \\
\llbracket \Gamma, x : \sigma \vdash M : \tau \rrbracket &= \llbracket \Gamma \vdash M : \tau \rrbracket \circ \pi \\
\llbracket \Gamma, x : \sigma \vdash M\,[x/y] : \tau \rrbracket &= \llbracket \Gamma, x : \sigma, y : \sigma \vdash M : \tau \rrbracket \circ \mathrm{id}_{\llbracket \Gamma \rrbracket} \times \delta_{\llbracket \sigma \rrbracket} \\
\llbracket \Gamma, x : \sigma', y : \sigma, \Delta \vdash M\,[y/x, x/y] : \tau \rrbracket &= \llbracket \Gamma, x : \sigma, y : \sigma', \Delta \vdash M : \tau \rrbracket \circ \mathrm{id}_{\llbracket \Gamma \rrbracket} \times \xi_{\llbracket \sigma' \rrbracket, \llbracket \sigma \rrbracket} \times \mathrm{id}_{\llbracket \Delta \rrbracket} \\
\llbracket \Gamma \vdash F(M_1, \ldots, M_n) : \tau_{n+1} \rrbracket &= \llbracket F \rrbracket \circ \langle \llbracket \Gamma \vdash M_i : \tau_i \rrbracket \rangle_{i=1}^{n} \\
\llbracket \Gamma \vdash \langle M, N \rangle : \tau \times \sigma \rrbracket &= \langle \llbracket \Gamma \vdash M : \tau \rrbracket, \llbracket \Gamma \vdash N : \sigma \rrbracket \rangle \\
\llbracket \Gamma \vdash \pi_1\, M : \tau \rrbracket &= \pi \circ \llbracket \Gamma \vdash M : \tau \times \sigma \rrbracket \\
\llbracket \Gamma \vdash \pi_2\, M : \tau \rrbracket &= \pi' \circ \llbracket \Gamma \vdash M : \tau \times \sigma \rrbracket \\
\llbracket \Gamma \vdash \lambda x.M : \sigma \to \tau \rrbracket &= \Lambda\left(\llbracket \Gamma, x : \sigma \vdash M : \tau \rrbracket\right) \\
\llbracket \Gamma \vdash M\, N : \sigma \rrbracket &= \varepsilon \circ \langle \llbracket \Gamma \vdash N : \tau \rrbracket, \llbracket \Gamma \vdash M : \tau \to \sigma \rrbracket \rangle \\
\llbracket \Gamma \vdash \top : \mathtt{Prop} \rrbracket &= \top_{\llbracket \Gamma \rrbracket} \\
\llbracket \Gamma \vdash \bot : \mathtt{Prop} \rrbracket &= \bot_{\llbracket \Gamma \rrbracket} \\
\llbracket \Gamma \vdash \varphi \wedge \psi : \mathtt{Prop} \rrbracket &= \llbracket \Gamma \vdash \varphi : \mathtt{Prop} \rrbracket \wedge_{\llbracket \Gamma \rrbracket} \llbracket \Gamma \vdash \psi : \mathtt{Prop} \rrbracket \\
\llbracket \Gamma \vdash \varphi \vee \psi : \mathtt{Prop} \rrbracket &= \llbracket \Gamma \vdash \varphi : \mathtt{Prop} \rrbracket \vee_{\llbracket \Gamma \rrbracket} \llbracket \Gamma \vdash \psi : \mathtt{Prop} \rrbracket \\
\llbracket \Gamma \vdash \varphi \Rightarrow \psi : \mathtt{Prop} \rrbracket &= \llbracket \Gamma \vdash \varphi : \mathtt{Prop} \rrbracket \Rightarrow_{\llbracket \Gamma \rrbracket} \llbracket \Gamma \vdash \psi : \mathtt{Prop} \rrbracket \\
\llbracket \Gamma \vdash \forall x : \sigma, \varphi : \mathtt{Prop} \rrbracket &= \forall_{\llbracket \Gamma \rrbracket}^{\llbracket \sigma \rrbracket}\left(\llbracket \Gamma, x : \sigma \vdash \varphi : \mathtt{Prop} \rrbracket\right) \\
\llbracket \Gamma \vdash \exists x : \sigma, \varphi : \mathtt{Prop} \rrbracket &= \exists_{\llbracket \Gamma \rrbracket}^{\llbracket \sigma \rrbracket}\left(\llbracket \Gamma, x : \sigma \vdash \varphi : \mathtt{Prop} \rrbracket\right)
\end{aligned}$$

Figure 4: Interpretation of higher-order logic in a hyperdoctrine.

which by a simple property of products gives us

$$\begin{aligned} &= \varepsilon \circ \langle [\![K]\!], [\![L]\!]\rangle \circ [\![\vec{M}]\!] \\ &= [\![K\,L]\!] \circ [\![\vec{M}]\!] \end{aligned}$$

- When $N = \lambda x.K$ and $\Delta \vdash K : \sigma \to \tau$ we first use the fact that when $\Gamma \vdash M_i : \delta_i$ then $\Gamma, y : \sigma \vdash M_i : \delta_i$ by a single application of weakening and we write $\pi^*(\vec{M})$ for $\vec{M}$ in this extended context. So we have

  $$\begin{aligned} \left[\!\!\left[(\lambda x.K)\left[\vec{M}/\vec{x}\right]\right]\!\!\right] &= \left[\!\!\left[\lambda y.K\left(\left[\pi^*\left(\vec{M}\right)/\vec{x}, y/x\right]\right)\right]\!\!\right] \\ &= \Lambda\left(\left[\!\!\left[K\left(\left[\pi^*\left(\vec{M}\right)/\vec{x}, y/x\right]\right)\right]\!\!\right]\right) \\ &= \Lambda\left([\![K]\!] \circ \left[\!\!\left[\pi^*\left(\vec{M}\right), y\right]\!\!\right]\right) && \text{induction hypothesis for } \vec{M}, y \end{aligned}$$

  and since the interpretation no weakening is precomposition with the projection we have

  $$= \Lambda\left([\![K]\!] \circ \left\langle [\![\vec{M}]\!] \circ \pi, \pi'\right\rangle\right)$$

  which by a simple property of products gives us

  $$= \Lambda\left([\![K]\!] \circ \left([\![\vec{M}]\!] \times \mathrm{id}_{[\![\sigma]\!]}\right)\right)$$

  which by a simple property of exponential transposes finally gives us

  $$= \Lambda\left([\![K]\!]\right) \circ [\![\vec{M}]\!] = [\![N]\!] \circ [\![\vec{M}]\!] .$$

  Admittedly we are a bit sloppy with the bound variable x but to be more precise we would have to define simultaneous subsitution precisely which is out of scope of this tutorial and we have not skipped anything essential.

- When $N = \varphi \wedge \psi$ we have

  $$\begin{aligned} \left[\!\!\left[(\varphi \wedge \psi)\left[\vec{M}/\vec{x}\right]\right]\!\!\right] &= \left[\!\!\left[\left(\varphi\left[\vec{M}/\vec{x}\right]\right) \wedge \left(\psi\left[\vec{M}/\vec{x}\right]\right)\right]\!\!\right] \\ &= \left[\!\!\left[\varphi\left[\vec{M}/\vec{x}\right]\right]\!\!\right] \wedge \left[\!\!\left[\psi\left[\vec{M}/\vec{x}\right]\right]\!\!\right] \end{aligned}$$

  which by the induction hypothesis and the definition of $\mathcal{P}$ gives us

  $$\begin{aligned} &= [\![\varphi]\!] \circ [\![\vec{M}]\!] \wedge [\![\psi]\!] \circ [\![\vec{M}]\!] \\ &= \mathcal{P}\left([\![\vec{M}]\!]\right)([\![\varphi]\!]) \wedge \mathcal{P}\left([\![\vec{M}]\!]\right)([\![\psi]\!]) \end{aligned}$$

  and since by definition $\mathcal{P}$ is a Heyting algebra homomorphism it commutes with $\wedge$ giving us

  $$= \mathcal{P}\left([\![\vec{M}]\!]\right)([\![\varphi]\!] \wedge [\![\psi]\!])$$

  and again using the definition of $\mathcal{P}$ but in the other direction

  $$\begin{aligned} &= ([\![\varphi]\!] \wedge [\![\psi]\!]) \circ [\![\vec{M}]\!] \\ &= [\![\varphi \wedge \psi]\!] \circ [\![\vec{M}]\!] \end{aligned}$$

  which is conveniently exactly what we want. All the other binary connectives proceed in exactly the same way; use the fact that $\mathcal{P}$ is a Heyting algebra homomorphism and naturality of Θ.

- When $\mathsf{N} = \forall x : \sigma, \varphi$ we have

  $$\left[\!\left[(\forall x : \sigma, \varphi)\left[\vec{M}/\vec{x}\right]\right]\!\right] = \left[\!\left[\forall y : \sigma, \left(\varphi\left[\pi^*(\vec{M})/\vec{x}, y/x\right]\right)\right]\!\right]$$

  the definition of the interpretation of $\forall$ gives us

  $$= \forall\left(\left[\!\left[\varphi\left[\pi^*(\vec{M})/\vec{x}, y/x\right]\right]\!\right]\right)$$

  where we use π^* for the same purpose as in the case for λ-abstraction. The induction hypothesis for φ now gives us

  $$= \forall\left([\![\varphi]\!] \circ [\![\pi^*(\vec{M}), y]\!]\right)$$

  and by the same reasoning as in the λ-abstraction case we get

  $$= \forall\left([\![\varphi]\!] \circ \left([\![\vec{M}]\!] \times \mathrm{id}_{[\![\sigma]\!]}\right)\right).$$

  Using the definition of $\mathcal{P}$ we have

  $$= \forall\left(\mathcal{P}\left([\![\vec{M}]\!] \times \mathrm{id}_{[\![\sigma]\!]}\right)([\![\varphi]\!])\right).$$

  Now we are in a situation where we can use the Beck-Chevalley condition to get

  $$= \mathcal{P}\left([\![\vec{M}]\!]\right)(\forall([\![\varphi]\!]))$$

  which by the same reasoning as in the last step of the previous case gives us

  $$\begin{aligned} &= \forall([\![\varphi]\!]) \circ [\![\vec{M}]\!] \\ &= [\![\forall x : \sigma, \varphi]\!] \circ [\![\vec{M}]\!]. \end{aligned}$$

These four cases cover the essential ideas in the proof. The other cases are all essentially the same as one of the four cases covered. □

Theorem 4.4 (Soundness). *Let $\Theta = \vartheta_1, \vartheta_2, \ldots, \vartheta_n$ be a propositional context. If $\Gamma \mid \Theta \vdash \varphi$ is derivable using the rules in Figure 3 then*

$$\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \leqslant [\![\Gamma \vdash \varphi : \mathtt{Prop}]\!]$$

in the Heyting algebra $\mathcal{P}([\![\Gamma]\!])$.

In particular if $\Gamma \mid - \vdash \varphi$ is derivable then $[\![\Gamma \vdash \varphi : \mathtt{Prop}]\!] = \top$.

Proof. The proof is, of course, by induction on the derivation $\Gamma \mid \Theta \vdash \varphi$. Most of the cases are straightforward. We only show the cases for the universal quantifier where we also use Proposition 4.3. In the proof we again omit explicit contexts to avoid clutter.

First, the introduction rule. We assume that the claim holds for $\Gamma, x : \sigma \mid \Theta \vdash \varphi$ and show that it also holds for $\Gamma \mid \Theta \vdash \forall x : \sigma, \varphi$.

By definition

$$[\![\forall x : \sigma, \varphi]\!] = \forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]}([\![\varphi]\!])$$

and thus we need to show

$$\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \leqslant \forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]} \left([\![\varphi]\!]\right).$$

Since by definition $\forall$ is the right adjoint to $\mathcal{P}(\pi)$ this is equivalent to

$$\mathcal{P}(\pi)\left(\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]\right) \leqslant [\![\varphi]\!]$$

where $\pi : [\![\Gamma]\!] \times [\![\sigma]\!] \to [\![\Gamma]\!]$ is of course the first projection. We cannot do much with the right side, so let us simplify the left-hand side. By definition $\mathcal{P}(\pi)$ is a Heyting algebra homomorphism so in particular it commutes with conjuction which gives us

$$\mathcal{P}(\pi)\left(\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]\right) = \bigwedge_{i=1}^{n} \mathcal{P}(\pi)\left([\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]\right)$$

using the definition of $\mathcal{P}$ we get

$$= \bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \circ \pi.$$

Now recall the definition of the interpretation of terms, in particular the definition of the interpretation of weakening in Figure 4. It gives us that

$$[\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \circ \pi = [\![\Gamma, x : \sigma \vdash \vartheta_i : \mathtt{Prop}]\!].$$

so we get

$$\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \circ \pi = \bigwedge_{i=1}^{n} [\![\Gamma, x : \sigma \vdash \vartheta_i : \mathtt{Prop}]\!]$$

By the induction hypothesis we have

$$\bigwedge_{i=1}^{n} [\![\Gamma, x : \sigma \vdash \vartheta_i : \mathtt{Prop}]\!] \leqslant [\![\varphi]\!]$$

which concludes the proof of the introduction rule for $\forall$.

Exercise 4.1. Where did we use the side-condition that x does not appear in Θ? ◇

For the elimination rule assume that $\Gamma \vdash M : \sigma$ and that the claim holds for $\Gamma \mid \Theta \vdash \forall x : \sigma, \varphi$. We need to show it for $\Gamma \mid \Theta \vdash \varphi\,[M/x]$, so we need to show

$$\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!] \leqslant [\![\Gamma \vdash \varphi\,[M/x] : \mathtt{Prop}]\!]$$

From Proposition 4.3 (the second equality) we have

$$[\![\Gamma \vdash \varphi\,[M/x] : \mathtt{Prop}]\!] = \mathcal{P}\left(\left\langle \mathrm{id}_{[\![\Gamma]\!]}, [\![\Gamma \vdash M : \sigma]\!]\right\rangle\right)\left([\![\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}]\!]\right). \tag{4}$$

Since $\mathcal{P}(\pi)$ is *left* adjoint to $\forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]}$ we have in particular that

$$\mathcal{P}(\pi) \circ \forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]} \leqslant \mathrm{id}_{\mathcal{P}([\![\Gamma, x:\sigma]\!])}$$

which is the counit of the adjunction. Thus

$$[\![\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}]\!] \geqslant \left(\mathcal{P}(\pi) \circ \forall_{[\![\Gamma]\!]}^{[\![\sigma]\!]}\right)([\![\Gamma, x : \sigma \vdash \varphi : \mathtt{Prop}]\!])$$

whose right-hand side is, by definition of the interpretation of the universal quantifier, equal to

$$= \mathcal{P}(\pi)([\![\Gamma \vdash \forall x : \sigma, \varphi : \mathtt{Prop}]\!]),$$

which by induction hypothesis and monotonicity of $\mathcal{P}(\pi)$ is greater than

$$\geqslant \mathcal{P}(\pi)\left(\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]\right).$$

Further, since $\mathcal{P}$ is a *contravariant functor* we have

$$\mathcal{P}\left(\langle \mathrm{id}_{[\![\Gamma]\!]}, [\![\Gamma \vdash M : \sigma]\!]\rangle\right) \circ \mathcal{P}(\pi) = \mathcal{P}\left(\pi \circ \langle \mathrm{id}_{[\![\Gamma]\!]}, [\![\Gamma \vdash M : \sigma]\!]\rangle\right) = \mathcal{P}\left(\mathrm{id}_{[\![\Gamma]\!]}\right).$$

Thus combining the last two results with (4) we have

$$[\![\Gamma \vdash \varphi[M/x] : \mathtt{Prop}]\!] \geqslant \mathcal{P}\left(\mathrm{id}_{[\![\Gamma]\!]}\right)\left(\bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]\right) = \bigwedge_{i=1}^{n} [\![\Gamma \vdash \vartheta_i : \mathtt{Prop}]\!]$$

concluding the proof. □

4.2 A class of Set-based hyperdoctrines

To get other examples of **Set**-based hyperdoctrines, we can keep the base category **Set** and replace the generic object 2 with a different complete Heyting algebra.

Definition 4.5. A *complete Heyting algebra* is a Heyting algebra that is complete as a lattice. ■

Exercise 4.2. Show that any complete Heyting algebra satisfies the infinite distributivity law

$$x \wedge \bigvee_{i \in I} y_i = \bigvee_{i \in I}(x \wedge y_i)$$

Hint: use your category theory lessons (left adjoints preserve. . .). ♢

Exercise 4.3. Show that if H is a (complete) Heyting algebra and X any set then the set of all functions from X to (the underlying set of) H when ordered pointwise, i.e., $\varphi \leqslant_{H^X} \psi \iff \forall x \in X, \varphi(x) \leqslant_H \psi(x)$, is a (complete) Heyting algebra with operations also inherited pointwise from H, e.g. $(\varphi \wedge_{H^X} \psi)(x) = \varphi(x) \wedge_H \psi(x)$. ♢

Theorem 4.6. *Let H be a complete Heyting algebra. Then* **Set** *together with the functor $Hom_{\mathbf{Set}}(-, H)$ and the generic object H is a hyperdoctrine.*

Proof. Clearly **Set** is a cartesian closed category and from Exercise 4.3 we know that $\mathrm{Hom}_{\mathbf{Set}}(X, H)$ is a complete Heyting algebra. To show that $\mathrm{Hom}_{\mathbf{Set}}(-, H)$ is a functor into **Heyt** we need to establish that for any function f, $\mathrm{Hom}_{\mathbf{Set}}(f, H)$ is a Heyting algebra homomorphism. We use greek letters $\varphi, \psi, \ldots$ for elements of $\mathrm{Hom}_{\mathbf{Set}}(X, H)$.

Recall that the action of the hom-functor on morphisms is by precomposition: $\mathrm{Hom}_{\mathbf{Set}}(f, H)(\varphi) = \varphi \circ f$. We now show that for any $f : X \to Y$, $\mathrm{Hom}_{\mathbf{Set}}(f, H)$ preserves conjunction and leave the other operations as an exercise since the proof is essentially the same. Let $\varphi, \psi \in \mathrm{Hom}_{\mathbf{Set}}(X, H)$ and $y \in Y$ then

$$\mathrm{Hom}_{\mathbf{Set}}(f, H)(\varphi \wedge_{H^X} \psi)(y) = ((\varphi \wedge_{H^X} \psi) \circ f)(y) = \varphi(f(y)) \wedge_H \psi(f(y)) = ((\varphi \circ f) \wedge_{H^Y} (\psi \circ f))(y).$$

As y was arbitrary we have $\mathrm{Hom}_{\mathbf{Set}}(f, H)(\varphi \wedge_{H^X} \psi) = (\varphi \circ f) \wedge_{H^Y} (\psi \circ f)$, as needed.

Observe that we have not yet used completeness of H anywhere. We need completeness to define adjoints $\forall_X^Y$ and $\exists_X^Y$ to $\mathrm{Hom}_{\mathbf{Set}}(\pi, H)$ for $\pi : X \times Y \to X$ which we do now.

To understand the definitions of adjunctions recall that universal quantification is akin to an infinite conjunction and existential quantification is akin to infinite disjunction. Let X and Y be sets and $\varphi \in \mathrm{Hom}_{\mathbf{Set}}(X \times Y, H)$. Define

$$\exists_X^Y(\varphi) = \lambda x. \bigvee_{y \in Y} \varphi(x, y)$$
$$\forall_X^Y(\varphi) = \lambda x. \bigwedge_{y \in Y} \varphi(x, y).$$

It is a straightforward exercise to show that $\exists_X^Y$ and $\forall_X^Y$ are monotone. We now show that $\exists_X^Y$ is left adjoint to $\mathrm{Hom}_{\mathbf{Set}}(\pi, H)$ and leave the proof that $\forall_X^Y$ is right adjoint as another exercise. We show the two implications separately.

Let $\varphi \in \mathrm{Hom}_{\mathbf{Set}}(X \times Y, H)$ and $\psi \in \mathrm{Hom}_{\mathbf{Set}}(X, H)$. Assume that $\exists_X^Y(\varphi) \leqslant \psi$. We are to show $\varphi \leqslant \mathrm{Hom}_{\mathbf{Set}}(\pi, H)(\psi)$ which reduces to showing for any $x \in X$ and $y \in Y$ that $\varphi(x, y) \leqslant \psi(\pi(x, y))$ which further reduces to showing $\varphi(x, y) \leqslant \psi(x)$.

Let $x \in X$ and $y \in Y$. By assumption $\exists_X^Y(\varphi)(x) \leqslant \psi(x)$ which simplifies to $\bigvee_{y \in Y} \varphi(x, y) \leqslant \psi(x)$. By definition of supremum $\varphi(x, y) \leqslant \bigvee_{y \in Y} \varphi(x, y)$ so we get $\varphi(x, y) \leqslant \psi(x)$ by transitivity.

Note that for this direction we only needed that $\bigvee_{y \in Y} \varphi(x, y)$ is an *upper bound* of the set $\{\varphi(x, y) \mid y \in Y\}$, not that it is the *least upper bound.* We need this last property for the other direction.

For the other direction let again $\varphi \in \mathrm{Hom}_{\mathbf{Set}}(X \times Y, H)$ and $\psi \in \mathrm{Hom}_{\mathbf{Set}}(X, H)$. Assume that $\varphi \leqslant \mathrm{Hom}_{\mathbf{Set}}(\pi, \psi)$. We are to show $\exists_X^Y(\varphi) \leqslant \psi$ which reduces to showing for any $x \in X$, $\bigvee_{y \in Y} \varphi(x, y) \leqslant \psi(x)$. Let $x \in X$. The assumption $\varphi \leqslant \mathrm{Hom}_{\mathbf{Set}}(\pi, \psi)$ gives us that for any $y \in Y$, $\varphi(x, y) \leqslant \psi(x)$ which means that $\psi(x)$ is the upper bound of the set $\{\varphi(x, y) \mid y \in Y\}$. But by definition of supremum, $\bigvee_{y \in Y} \varphi(x, y)$ is the *least* upper bound, so $\bigvee_{y \in Y} \varphi(x, y) \leqslant \psi(x)$.

Exercise 4.4. Show that $\forall_X^Y$ is the right adjoint to $\mathrm{Hom}_{\mathbf{Set}}(\pi, H)$. ◇

What we are still missing is the Beck-Chevalley condition for $\exists_X^Y$ and $\forall_X^Y$. Again, we show this for $\exists_X^Y$ and leave the other as an exercise for the reader.

Let X and X' be sets and $s : X \to X'$ a function. We need to show that $\exists_X^Y \circ \mathrm{Hom}_{\mathbf{Set}}(s \times \mathrm{id}_Y, H) = \mathrm{Hom}_{\mathbf{Set}}(s, H) \circ \exists_{X'}^Y$. Let $\varphi \in \mathrm{Hom}_{\mathbf{Set}}(X' \times Y, H)$. Then

$$\left(\exists_X^Y \circ \mathrm{Hom}_{\mathbf{Set}}(s \times \mathrm{id}_Y, H)\right)(\varphi) = \exists_X^Y(\varphi \circ (s \times \mathrm{id}_Y)) = \lambda x. \bigvee_{y \in Y} \varphi(s(x), y)$$

and

$$\left(\mathrm{Hom}_{\mathbf{Set}}(s, H) \circ \exists_{X'}^Y\right)(\varphi) = \exists_{X'}^Y(\varphi) \circ s.$$

For any $x \in X'$ we have

$$\left(\exists_{X'}^{Y}(\varphi) \circ s\right)(x) = \exists_{X'}^{Y}(\varphi)(s(x)) = \bigvee_{y \in Y} \varphi(s(x), y)$$

which means $\exists_{X'}^{Y}(\varphi) \circ s = \lambda x. \bigvee_{y \in Y} \varphi(s(x), y)$, which is exactly what we need it to be.

Exercise 4.5. Show that the Beck-Chevalley condition also holds for $\forall_X^Y$. ♢

□

We now give some examples of complete Heyting algebras. We only give definitions and leave the straightforward verifications of the axioms as an exercise

Exercise 4.6. Let P be a *preordered* set (i.e., a set with a reflexive and transitive relation $\leqslant$). Show that the set of upwards closed subsets of P, $\mathcal{P}^{\uparrow}(P)$

$$\mathcal{P}^{\uparrow}(P) = \{A \subseteq P \mid \forall x \in A, \forall y \in P, x \leqslant y \Rightarrow x \in A\}$$

is a complete Heyting algebra for the following operations

$$\begin{array}{llll} \top = P & \bot = \emptyset & A \vee B = A \cup B & A \wedge B = A \cap B \\ \bigvee_{i \in I} A_i = \bigcup_{i \in I} A_i & \bigwedge_{i \in I} A_i = \bigcap_{i \in I} A_i & A \Rightarrow B = \{x \in P \mid \forall y \geqslant x, y \in A \Rightarrow y \in B\} & \end{array}$$

Concretely show that all these operations are well defined (that the sets defined are again upwards closed) and that they satisfy the axioms of a complete Heyting algebra.

Also show that the set of *downwards closed* subsets of P, $\mathcal{P}^{\downarrow}(P)$ is a complete Heyting algebra (you only need to change the definition of one of the operations). ♢

4.3 Examples based on monoids

Another set of examples is useful in modeling various logics dealing with resources. We need some definitions.

Definition 4.7. Let $f, g : A \rightharpoonup B$ be two partial functions and $a \in A$. We write $f(a) =_{\downarrow} g(a)$ for *Kleene* equality meaning that if either of the sides is defined then both are and they are equal. ■

Definition 4.8. A *partial commutative monoid* M is a set M together with a partial function $\cdot : M \times M \rightharpoonup M$ (multiplication) and an element $1 \in M$ (the unit) such that the following axioms hold:

- for all $m \in M$, $m \cdot 1 =_{\downarrow} 1 \cdot m =_{\downarrow} m$ (in particular $1 \cdot m$ and $m \cdot 1$ are always defined)
- for $m, n \in M$, $m \cdot n =_{\downarrow} n \cdot m$ (commutativity)
- for $\ell, m, n \in M$, $\ell \cdot (m \cdot n) =_{\downarrow} (\ell \cdot m) \cdot n$.

We write $a \# b$ to say that $a \cdot b$ is defined. ■

Example 4.9. Let $\mathbb{H}$ be the set of finite partial maps from $\mathbb{N}$ to X where X is some set. It could for instance be the set of values of some programming language. Then $\mathbb{H}$ would be a model of the heap.

Define the operation $\cdot : \mathbb{H} \times \mathbb{H} \rightharpoonup \mathbb{H}$ as follows

$$f \cdot g = \begin{cases} f \uplus g & \text{if } \mathbf{dom}(f) \cap \mathbf{dom}(g) = \emptyset \\ \text{undefined} & \text{otherwise} \end{cases}$$

where

$$(f \uplus g)(x) = \begin{cases} f(x) & x \in \mathbf{dom}(f) \\ g(x) & x \in \mathbf{dom}(g) \\ \text{undefined} & \text{otherwise} \end{cases}$$

Then it is easy to see that $\mathbb{H}$ with $\cdot$ is a partial commutative monoid with the unit the everywhere undefined function. ■

Given a partial commutative monoid M there is a canonical preorder associated with it that arises from multiplication $\cdot$. It is called the *extension order.* Concretely, we define

$$m \leqslant n \iff \exists k \in M, m \cdot k =_{\downarrow} n$$

(note that associativity of $\cdot$ is used to show that $\leqslant$ is transitive).

Example 4.10. For the example partial commutative monoid $\mathbb{H}$ above the extension order can equivalently be defined as

$$f \leqslant g \iff \mathbf{dom}(f) \subseteq \mathbf{dom}(g) \wedge \forall x \in \mathbf{dom}(f), f(x) =_{\downarrow} g(x)$$

If we think of f and g as heaps then $f \leqslant g$ if the heap g is derived from f by allocating some new locations. ■

As we have seen in Exercise 4.6 given a preordered set P, the set of upwards closed subsets of P is a complete Heyting algebra. It turns out that given a partial commutative monoid and its derived preorder we can lift the multiplication of the monoid to multiplication of upwards closed subsets, giving rise to a (complete) BI-algebra.

Definition 4.11. A (complete) BI-algebra H is a (complete) Heyting algebra with an additional constant I and two binary operations $\star$ and $\mathrel{-\!\!\star}$ such that the following axioms hold

- $\star$ is monotone: for any h, h', g, g', if $h \leqslant h'$ and $g \leqslant g'$ then $h \star g \leqslant h' \star g'$.
- I is the unit for $\star$.
- $\star$ is commutative and associative
- for any $h, h', h'' \in H$, $h \star h' \leqslant h'' \iff h \leqslant h' \mathrel{-\!\!\star} h''$ ($\mathrel{-\!\!\star}$ is right adjoint to $\star$).

■

Note in contrast to the operations of a (complete) Heyting algebra, which are uniquely determined by the order relation (why?), there can be (potentially) many different definitions of $\star$, $\mathrel{-\!\!\star}$ and I (although $\mathrel{-\!\!\star}$ is determined by $\star$).

Exercise 4.7. Any (complete) Heyting algebra is trivially a (complete) BI algebra. What can we choose for operations $\star$, I and $-\!\!\star$? ♢

Exercise 4.8. Show that if H is a (complete) BI-algebra and X is any set, then the set of functions from X to H is another (complete) BI-algebra with operations defined pointwise. ♢

Of course, we want nontrivial examples. Partial commutative monoids give rise to such.

Example 4.12. Let M be a partial commutative monoid. Then the set of upwards closed subsets of M (with respect to the extension order) is a complete BI-algebra.

We already know that it is a complete Heyting algebra. We need to define I, $\star$ and $-\!\!\star$. The operation $\star$ is a pointwise lifting of the operation $\cdot$ of the monoid in the sense

$$A \star B = \{m \cdot n \mid m \in A, n \in B, m \cdot n \text{ defined}\}.$$

The unit I is the whole monoid M.

Recalling that the order on $\mathcal{P}^{\uparrow}(M)$ is subset inclusion it is clear that $\star$ is monotone. To see that M is the unit for $\star$ we prove two inclusions. Let $A \in \mathcal{P}^{\uparrow}(M)$. We wish to show $A \star M = A$.

Suppose $m \in A$. Since $1 \in M$ and $m \cdot 1 =_{\downarrow} m$ clearly, $m \in A \star M$. Conversely, suppose $m \in A \star M$. By definition there exists $a \in A$ and $n \in M$, such that $m =_{\downarrow} a \cdot n$. This means (recall the definition of the extension order) that $m \geqslant a$. Since A is upwards closed by definition and $a \in A$, it must be that $m \in A$ as well.

Showing $M \star A = A$ is analogous. The fact that it is commutative and associative likewise follows easily.

Exercise 4.9. Show that $\star$ is commutative and associative. ♢

Finally, the operation $-\!\!\star$ is defined as

$$A -\!\!\star B = \{m \in M \mid \forall a \in A, m \cdot a \in B\}$$

Exercise 4.10. Show that $A -\!\!\star B$ is well defined (i.e., upwards closed) and that it is the right adjoint to $\star$. ♢

■

4.4 BI-hyperdoctrines

Definition 4.13. A *BI-hyperdoctrine* is a hyperdoctrine $(\mathcal{C}, \Omega)$ such that $\mathcal{P}$ restricts to a functor into the category of BI-algebras and BI-algebra homomorphisms. ■

Example 4.14. Let H be a *complete* BI-algebra. Then **Set** together with the hom-functor $\mathrm{Hom}_{\mathbf{Set}}(-, H)$ is a BI-hyperdoctrine.

Since a complete BI-algebra is in particular a complete Heyting algebra, we know that the hom-functor forms a hyperdoctrine. From Exercise 4.8 we know that for each X, $\mathrm{Hom}_{\mathbf{Set}}(X, H)$ is a BI-algebra. It remains to show that for any function f, $\mathrm{Hom}_{\mathbf{Set}}(f, H)$ is a BI-algebra homomorphism. This is straightforward and we leave it as an exercise for the reader. ■

BI-hyperdoctrines can be used to model higher-order separation logic. See [BBTS07] for details of how this is done.

A canonical example of a BI-hyperdoctrine is the hyperdoctrine arising from the partial commutative monoid of heaps from Example 4.9. Predicates are modeled as upwards closed sets of heaps and observe that for predicates P and Q the predicate $\mathsf{P} \star \mathsf{Q}$ contains those heaps that can be split into two disjoint heaps; a heap satisfying P and a heap satisfying Q.

More generally, we can take a partial commutative monoid that represents abstract resources and build a model of higher-order separation logic. Then for predicates P and Q the predicate $\mathsf{P} \star \mathsf{Q}$ will contain resources which can be split into resources satisfying P and resources satisfying Q. But the separation does not have to be as literal as with heaps, that is, the splitting does not have to represent actual splitting of the heap but only some fiction of separation, depending on what the monoid of resources is.

4.5 Guarded recursion for predicates

The set of natural numbers $\mathbb{N}$ with the usual order

$$0 \leqslant 1 \leqslant 2 \leqslant 3 \leqslant \cdots$$

is obviously a preordered set. Hence the set of *downwards* closed subsets of $\mathbb{N}$, $\mathcal{P}^{\downarrow}(\mathbb{N})$ is a complete Heyting algebra. It is however a very special Heyting algebra in the sense that it allows us to use induction to prove that an element is equal to $\top = \mathbb{N}$. More concretely, we can define a unary operation $\triangleright : \mathcal{P}^{\downarrow}(\mathbb{N}) \to \mathcal{P}^{\downarrow}(\mathbb{N})$ (pronounced "later") as

$$\triangleright(A) = \{0\} \cup \{n + 1 \mid n \in A\}$$

The operation $\triangleright$ is obviously well-defined and monotone. Moreover, we can express the usual induction principle for natural numbers as the property that $\triangleright A \leqslant A$ implies $A = \mathbb{N}$.

Exercise 4.11. Show that if $\triangleright A \leqslant A$ then $A = \mathbb{N}$. ♢

The operation $\triangleright$ works well with other operations of a Heyting algebra; it commutes with all of them except $\bot$.

Exercise 4.12. Show that $\triangleright$ commutes with all operations of the Heyting algebra $\mathcal{P}^{\downarrow}(\mathbb{N})$ except $\bot$. Concretely, show

$$\begin{aligned}
\triangleright\top &= \top \\
\triangleright\left(\bigwedge_{i \in I} A_i\right) &= \bigwedge_{i \in I} \triangleright A_i \\
\triangleright\left(\bigvee_{i \in I} A_i\right) &= \bigvee_{i \in I} \triangleright A_i && \text{if } I \neq \emptyset \\
\triangleright(A \Rightarrow B) &= \triangleright A \Rightarrow \triangleright B
\end{aligned}$$

♢

Recall from Exercise 4.3 that given any set X, the set of functions $\mathrm{Hom}_{\mathbf{Set}}\left(X, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ is again a complete Heyting algebra for operations defined pointwise. Similarly, we can extend the $\triangleright$ operation pointwise to the complete Heyting algebra $\mathrm{Hom}_{\mathbf{Set}}\left(X, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$. It is straightforward to show that in this case we have a generalization of the induction principle

$$\triangleright\varphi \leqslant \varphi \Rightarrow \varphi = \top.$$

Exercise 4.13. Show that if $\triangleright\varphi \leqslant \varphi$ then φ is the top element of $\mathrm{Hom}_{\mathbf{Set}}\left(X, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$.

Moreover, show that $\triangleright$ on $\mathrm{Hom}_{\mathbf{Set}}\left(X, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ also commutes with the same Heyting algebra operations as $\triangleright$ on $\mathcal{P}^{\downarrow}(\mathbb{N})$.

Finally, show that if $f : X \to Y$ is any function then for any $\varphi \in \mathrm{Hom}_{\mathbf{Set}}\left(Y, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ we have

$$\triangleright\left(\mathrm{Hom}_{\mathbf{Set}}\left(f, \mathcal{P}^{\downarrow}(\mathbb{N})\right)(\varphi)\right) = \mathrm{Hom}_{\mathbf{Set}}\left(f, \mathcal{P}^{\downarrow}(\mathbb{N})\right)(\triangleright(\varphi))$$

which means that all the Heyting algebra morphisms $\mathrm{Hom}_{\mathbf{Set}}\left(f, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ also preserve the operation $\triangleright$. ♢

All of these are straightforward to show directly from the definitions of all the operations but it is good practice to show some of them to get used to the definitions.

The reason for introducing the $\triangleright$ operation is that we can use it to show existence of certain *guarded* recursively defined predicates. To show this, we need some auxiliary definitions. Until the end of this section we are working in some complete Heyting algebra $H = \mathrm{Hom}_{\mathbf{Set}}\left(X, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ for some set X.

Definition 4.15. Let $\varphi, \psi \in H$. For $n \in \mathbb{N}$ we define $\lfloor\varphi\rfloor_n \in H$ as

$$\lfloor\varphi\rfloor_n(x) = \{k \in \varphi(x) \mid k < n\}$$

and we write $\varphi \overset{n}{=} \psi$ for

$$\lfloor\varphi\rfloor_n = \lfloor\psi\rfloor_n.$$

Note that for any $\psi, \varphi \in H$ we have $\varphi \overset{0}{=} \psi$ and that $\varphi \overset{n+1}{=} \psi \Rightarrow \varphi \overset{n}{=} \psi$ and finally that if $\forall n, \varphi \overset{n}{=} \psi$ then $\psi = \varphi$.

We say that a function $\Phi : H \to H$ is *non-expansive* if for any $\varphi, \psi \in H$ and any $n \in \mathbb{N}$ we have

$$\varphi \overset{n}{=} \psi \Rightarrow \Phi(\varphi) \overset{n}{=} \Phi(\psi)$$

and we say that it is *contractive* if for any $\varphi, \psi \in H$ and any $n \in \mathbb{N}$ we have

$$\varphi \overset{n}{=} \psi \Rightarrow \Phi(\varphi) \overset{n+1}{=} \Phi(\psi).$$

■

We can now put $\triangleright$ to good use.

Exercise 4.14. Show that $\triangleright$ is contractive. Show that composition (either way) of a contractive and non-expansive function is contractive. Conclude that if Φ is a non-expansive function on H then $\Phi \circ \triangleright$ and $\triangleright \circ \Phi$ are contractive. ♢

Finally the property we were looking for.

Proposition 4.16. *If $\Phi : H \to H$ is a contractive function then it has a unique fixed point, i.e., there is a unique $\varphi \in H$ such that $\Phi(\varphi) = \varphi$.*

We will prove a more general theorem later (Theorem 5.10) so we skip the proof at this point. However, uniqueness is easy to show and is a good exercise.

Exercise 4.15. Show that if $\Phi : H \to H$ is contractive then the fixed point (if it exists) must necessarily be unique.

Hint: Use contractiveness of Φ together with the fact that if $\lfloor\varphi\rfloor_n = \lfloor\psi\rfloor_n$ for all $n \in \mathbb{N}$ then $\varphi = \psi$. ♢

4.5.1 Application to the logic

Suppose that we extend the basic higher-order logic with an operation $\triangleright$ on propositions. Concretely, we add the typing judgment

$$\frac{\Gamma \vdash \varphi : \texttt{Prop}}{\Gamma \vdash \triangleright\varphi : \texttt{Prop}}$$

together with the following introduction and elimination rules

$$\frac{\Gamma \mid \Xi \vdash \varphi}{\Gamma \mid \Xi \vdash \triangleright\varphi}\ \textbf{mono} \qquad \frac{\Gamma \mid \Xi, \triangleright\varphi \vdash \varphi}{\Gamma \mid \Xi \vdash \varphi}\ \textbf{Löb}$$

We can interpret this extended logic in the hyperdoctrine arising from the complete Heyting algebra $\mathcal{P}^{\downarrow}(\mathbb{N})$ by extending the basic interpretation with

$$[\![\Gamma \vdash \triangleright\varphi : \texttt{Prop}]\!] = \triangleright\left([\![\Gamma \vdash \varphi : \texttt{Prop}]\!]\right).$$

The properties of $\triangleright$ from Exercise 4.13 then give us the following properties of the logic. Judgments

$$\frac{\Gamma \mid \Xi \vdash \triangleright(\varphi \wedge \psi)}{\Gamma \mid \Xi \vdash \triangleright\varphi \wedge \triangleright\psi} \qquad \frac{\Gamma \mid \Xi \vdash \triangleright\varphi \wedge \triangleright\psi}{\Gamma \mid \Xi \vdash \triangleright(\varphi \wedge \psi)}$$

and if σ is inhabited, that is if there exists a term M such that $- \vdash M : \sigma$ then

$$\frac{\Gamma \mid \Xi \vdash \triangleright(\exists x : \sigma, \varphi)}{\Gamma \mid \Xi \vdash \exists x : \sigma, \triangleright(\varphi)} \qquad \frac{\Gamma \mid \Xi \vdash \exists x : \sigma, \triangleright(\varphi)}{\Gamma \mid \Xi \vdash \triangleright(\exists x : \sigma, \varphi)}$$

and similar rules for all the other connectives except $\perp$ are all valid in the model.

Moreover, the property that for any function f, $\mathrm{Hom}_{\mathbf{Set}}\left(f, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ preserves $\triangleright$ gives us that the rules

$$\frac{\Gamma \mid \Xi \vdash \triangleright\left(\varphi\left[N/x\right]\right)}{\Gamma \mid \Xi \vdash \left(\triangleright\varphi\right)\left[N/x\right]} \qquad \frac{\Gamma \mid \Xi \vdash \left(\triangleright\varphi\right)\left[N/x\right]}{\Gamma \mid \Xi \vdash \triangleright\left(\varphi\left[N/x\right]\right)}$$

are valid, i.e., that $\triangleright$ commutes with substitution. This is a property that must hold for the connective to be useful since we use substitution constantly in reasoning, most of the time implicitly. For instance every time we instantiate a universally quantified formula or when we prove an existential, we use substitution.

Exercise 4.16. Show that the rules we listed are valid. ♢

Finally, we would like show that we have fixed points of guarded recursively defined predicates. More precisely, suppose the typing judgment $\Gamma, p : \texttt{Prop}^{\tau} \vdash \varphi : \texttt{Prop}^{\tau}$ is valid and that p in φ only occurs under a $\triangleright$ (or not at all). Then we would like there to exist a unique term $\mu p.\varphi$ of type $\texttt{Prop}^{\tau}$ in context Γ, i.e.,

$$\Gamma \vdash \mu p.\varphi : \texttt{Prop}^{\tau}$$

such that the following sequents hold

$$\Gamma, x : \tau \mid \left(\varphi\left[\mu p.\varphi/p\right]\right) x \vdash \left(\mu p.\varphi\right) x \qquad \Gamma \mid \left(\mu p.\varphi\right) x \vdash \left(\varphi\left[\mu p.\varphi/p\right]\right) x. \tag{5}$$

Observe that this implies

$$\Gamma \mid - \vdash \forall x : \tau, (\varphi\, [\mu p.\varphi/p])\; x \Leftrightarrow (\mu p.\varphi)\, x$$

Recall that when interpreting higher-order logic in the hyperdoctrine $\mathrm{Hom}_{\mathbf{Set}}\left(-, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ the term φ is interpreted as

$$[\![\Gamma, p : \mathtt{Prop}^{\tau} \vdash \varphi : \mathtt{Prop}^{\tau}]\!] : [\![\Gamma]\!] \times H \to H$$

where $H = [\![\tau]\!] \to [\![\mathtt{Prop}]\!] = [\![\tau]\!] \to \mathcal{P}^{\downarrow}(\mathbb{N})$. Suppose that for each $\gamma \in [\![\Gamma]\!]$ the function $\Phi_{\gamma} : H \to H$ defined as

$$\Phi_{\gamma}(h) = [\![\Gamma, p : \mathtt{Prop}^{\tau} \vdash \varphi : \mathtt{Prop}^{\tau}]\!]\,(\gamma, h)$$

were contractive. Then we could appeal to Proposition 4.16 applied to Φ_{γ} so that for each $\gamma \in \Gamma$ we would get a unique element $h_{\gamma} \in H$, such that $\Phi_{\gamma}(h) = h_{\gamma}$, or, in other words, we would get a function from Γ to H, mapping γ to h_{γ}. Define

$$[\![\Gamma \vdash \mu p.\varphi : \mathtt{Prop}^{\tau}]\!]$$

to be this function. We then have

$$\begin{aligned}[\![\Gamma \vdash \mu p.\varphi : \mathtt{Prop}^{\tau}]\!] = h_{\gamma} &= [\![\Gamma, p : \mathtt{Prop}^{\tau} \vdash \varphi : \mathtt{Prop}^{\tau}]\!]\,(\gamma, h_{\gamma})\\ &= [\![\Gamma, p : \mathtt{Prop}^{\tau} \vdash \varphi : \mathtt{Prop}^{\tau}]\!]\,(\gamma, [\![\Gamma \vdash \mu p.\varphi : \mathtt{Prop}^{\tau}]\!])\\ &= [\![\Gamma \vdash \varphi\,[\mu p.\varphi/p] : \mathtt{Prop}^{\tau}]\!]\end{aligned}$$

The last equality following from Proposition 4.3. Observe that this is exactly what we need to validate the rules (5).

However not all interpretations where the free variable p appears under a $\triangleright$ will be contractive. The reason for this is that can choose interpretations of base constants from the signature to be arbitrarily bad and a single use of $\triangleright$ will not make these non-expansive. The problem comes from the fact that we are using a **Set**-based hyperdoctrine and so interpretations of terms (including basic function symbols) can be any functions. If we instead used a category where we had a meaningful notion of non-expansiveness and contractiveness and all morphisms would be non-expansive by definition, then perhaps every term with a free variable p guarded by a $\triangleright$ would be contractive and thus define a fixed point.

Example 4.17. Consider a signature with a single function symbol of type $F : \mathtt{Prop} \to \mathtt{Prop}$ and the interpretation in the hyperdoctrine $\mathrm{Hom}_{\mathbf{Set}}\left(-, \mathcal{P}^{\downarrow}(\mathbb{N})\right)$ where we choose to interpret F as

$$[\![F]\!] = \lambda A. \begin{cases} \triangleright(A) & \text{if } A \neq \mathbb{N} \\ \emptyset & \text{if } A = \mathbb{N} \end{cases}$$

Exercise 4.17. Show that $[\![F]\!]$ is *not* non-expansive and that $[\![F]\!] \circ \triangleright$ and $[\![F]\!] \circ \triangleright$ are also *not* non-expansive. Show also that $[\![F]\!] \circ \triangleright$ and $\triangleright \circ [\![F]\!]$ have no fixed-points. ♢

This example (together with the exercise) shows that even though p appears under a $\triangleright$ in

$$p : \mathtt{Prop} \vdash F\,(\triangleright(p)) : \mathtt{Prop}$$

the interpretation of $p : \mathtt{Prop} \vdash F\,(\triangleright(p)) : \mathtt{Prop}$ has no fixed points and so we are not justified in adding them to the logic. ■

This brings us to the next topic, namely the definition of a category in which all morphisms are suitably non-expansive.

5 Complete ordered families of equivalences

Ordered families of equivalences (o.f.e.'s) are sets equipped with a family of equivalence relations that approximate the actual equality on the set X. These relations must satisfy some basic coherence conditions.

Definition 5.1 (o.f.e.)**.** An *ordered family of equivalences* is a pair $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ where X is a set and for each n, the binary relation $\overset{n}{=}$ is an equivalence relation on X such that the relations $\overset{n}{=}$ satisfy the following conditions

- $\overset{0}{=}$ is the total relation on X, i.e., everything is equal at stage 0.
- for any $n \in \mathbb{N}$, $\overset{n+1}{=} \subseteq \overset{n}{=}$ (monotonicity)
- for any $x, x' \in X$, if $\forall n \in \mathbb{N}, x \overset{n}{=} x'$ then $x = x'$.

We say that an o.f.e. $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ is *inhabited* if there exists an element $x \in X$. ■

Example 5.2. A canonical example of an o.f.e. is a set of strings (finite and infinite) over some alphabet. The strings x, x' are n-equal, $x \overset{n}{=} x'$ if they agree for the first n characters. ■

Example 5.3. The set $\mathcal{P}^{\downarrow}(\mathbb{N})$ together with the relations $\overset{n}{=}$ from Definition 4.15 is an o.f.e. ■

Remark 5.4. If you are familiar with metric spaces observe that o.f.e.'s are but a different presentation of bisected 1-bounded ultrametric spaces. ■

Definition 5.5 (Cauchy sequences and limits)**.** Let $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ be an o.f.e. and $\{x_n\}_{n=0}^{\infty}$ be a sequence of elements of X. Then $\{x_n\}_{n=0}^{\infty}$ is a *Cauchy sequence* if

$$\forall k \in \mathbb{N}, \exists j \in \mathbb{N}, \forall n \geqslant j, x_j \overset{k}{=} x_n$$

or in words, the elements of the chain get arbitrarily close.

An element $x \in X$ is the *limit* of the sequence $\{x_n\}_{n=0}^{\infty}$ if

$$\forall k \in \mathbb{N}, \exists j \in \mathbb{N}, \forall n \geqslant j, x \overset{k}{=} x_n.$$

A sequence may or may not have a limit. If it has we say that the sequence *converges.* The limit is necessarily unique in this case (Exercise 5.1) and we write $\lim_{n\to\infty} x_n$ for it. ■

Remark 5.6. These are the usual Cauchy sequence and limit definitions for metric spaces specialized to o.f.e.'s. ■

Exercise 5.1. Show that limits are unique. That is, suppose that x and y are limits of $\{x_n\}_{n=0}^{\infty}$. Show $x = y$. ♢

One would perhaps intuitively expect that every Cauchy sequence has a limit. This is not the case in general.

Exercise 5.2. Show that if the alphabet Σ contains at least one letter then the set of *finite* strings over Σ admits a Cauchy sequence without a limit. The equivalence relation $\overset{n}{=}$ relates strings that have the first n characters equal.

Hint: Pick $\sigma \in \Sigma$ and consider the sequence $x_n = \sigma^n$ (i.e., x_n is n σ's). ♢

We are interested in spaces which do have the property that every Cauchy sequence has a limit. These are called *complete*. Completeness allows us to have fixed points of suitable contractive functions which we define below.

Definition 5.7 (c.o.f.e.)**.** A *complete ordered family of equivalences* is an ordered family of equivalences $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ such that every Cauchy sequence in X has a limit in X. ■

Example 5.8. A canonical example of a c.o.f.e. is the set of infinite strings over an alphabet. The relation $\overset{n}{=}$ relates streams that agree on at least the first n elements. ■

Exercise 5.3. Show the claims made in Example 5.8.

Show that $\mathcal{P}^{\downarrow}(\mathbb{N})$ with relations from Definition 4.15 is a c.o.f.e. (We show a more general result later in Proposition 5.12.) ♢

To have a category we also need morphisms between (complete) ordered families of equivalences.

Definition 5.9. Let $\left(X, \left(\overset{n}{=}_X\right)_{n=0}^{\infty}\right)$ and $\left(Y, \left(\overset{n}{=}_Y\right)_{n=0}^{\infty}\right)$ be two ordered families of equivalences and f a function from the set X to the set Y. The function f is

- *non-expansive* if for any $x, x' \in X$, and any $n \in \mathbb{N}$,

$$x \underset{X}{\overset{n}{=}} x' \Rightarrow f(x) \underset{Y}{\overset{n}{=}} f(x')$$

- *contractive* if for any $x, x' \in X$, and any $n \in \mathbb{N}$,

$$x \underset{X}{\overset{n}{=}} x' \Rightarrow f(x) \underset{Y}{\overset{n+1}{=}} f(x')$$

■

Exercise 5.4. Show that non-expansive functions preserve limits, i.e., show that if f is a non-expansive function and $\{x_n\}_{n=0}^{\infty}$ is a converging sequence, then so is $\{f(x_n)\}_{n=0}^{\infty}$ and that

$$f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f(x_n).$$

♢

The reason for introducing *complete* ordered families of equivalences, as opposed to just o.f.e.'s, is that any contractive function on a inhabited c.o.f.e. has a unique fixed point.

Theorem 5.10 (Banach's fixed point theorem)**.** *Let* $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ *be a an inhabited c.o.f.e. and* $f : X \to X$ *a contractive function. Then* f *has a unique fixed point.*

Proof. First we show uniqueness. Suppose x and y are fixed points of f, i.e. $f(x) = x$ and $f(y) = y$. By definition of c.o.f.e.'s we have $x \overset{0}{=} y$. From contractiveness we then get $f(x) \overset{1}{=} f(y)$ and so $x \overset{1}{=} y$. Thus by induction we have $\forall n, x \overset{n}{=} y$. Hence by another property in the definition of c.o.f.e.'s we have $x = y$.

To show existence, we take any $x_0 \in X$ (note that this exists since by assumption X is inhabited). We then define $x_{n+1} = f(x_n)$ and claim that $x_n \overset{n}{=} x_{n+m}$ for any n and m which we prove by induction on n. For $n = 0$ this is trivial. For the inductive step we have, by contractiveness of f

$$x_{n+1} = f(x_n) \overset{n+1}{=} f(x_{n+m}) = x_{n+m+1},$$

as required. This means that the sequence $\{x_n\}_{n=0}^{\infty}$ is Cauchy. Now we use completeness to conclude that $\{x_n\}_{n=0}^{\infty}$ has a limit, which we claim is the fixed point of f. Let $x = \lim_{n\to\infty} x_n$. We have (using Exercise 5.4)

$$f(x) = f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_{n+1} = \lim_{n\to\infty} x_n = x$$

concluding the proof. □

Definition 5.11 (The category $\mathcal{U}$)**.** The category $\mathcal{U}$ of complete ordered families of equivalences has as objects complete ordered families of equivalences and as morphisms non-expansive functions. ■

From now on, we often use the underlying set X to denote a (complete) o.f.e. $\left(X, \left(\overset{n}{=}_X\right)_{n=0}^{\infty}\right)$, leaving the family of equivalence relations implicit.

Exercise 5.5. Show that $\mathcal{U}$ is indeed a category. Concretely, show that composition of non-expansive morphisms is non-expansive and that the identity function is non-expansive. ♢

Exercise 5.6. Show that if f is contractive and g is non-expansive, then $f \circ g$ and $g \circ f$ are contractive. ♢

Exercise 5.7. Show that the **Set** is a coreflective subcategory of $\mathcal{U}$. Concretely, this means that there is an inclusion functor $\Delta : \mathbf{Set} \to \mathcal{U}$ which maps a set X to a c.o.f.e. with equivalence relation $\overset{n}{=}$ being the equality on X for $n > 0$ and the total relation for 0.

Show that the functor Δ is full and faithful and that it has a right adjoint, the forgetful functor $F : \mathcal{U} \to \mathbf{Set}$ that "forgets" the equivalence relations.

Further, show that the only contractive functions from any c.o.f.e. to $\Delta(Y)$ are constant. ♢

The last part of the exercise is one of the reasons why we can define fixed points of guarded recursive predicates in the $\mathcal{U}$ hyperdoctrine which we describe below but not in a **Set**-based hyperdoctrine from Section 4.5.

If we wish to find a fixed point of a function f from a *set* X to a *set* Y we really have nothing to go on. What the o.f.e.'s give us is the ability to get closer and closer to a fixed point, if f is well-behaved. What the c.o.f.e.'s additionally give us is that the "thing" we get closer and closer to is in fact an element of the o.f.e.

5.1 $\mathcal{U}$-based hyperdoctrine

We now wish to imitate the **Set**-based hyperdoctrine arising from a preordered set P; the hyperdoctrine with $\mathcal{P} = \mathrm{Hom}_{\mathbf{Set}}\left(-, \mathcal{P}^{\uparrow}(P)\right)$ but in a way that would allow us also to model $\triangleright$ in the logic. We can express this in a nice way by combining $\mathcal{P}^{\downarrow}(\mathbb{N})$ with $\mathcal{P}^{\uparrow}(P)$ into *uniform predicates* $\mathbf{UPred}(P)$.

Let P be a preordered set. We define $\mathbf{UPred}(P) \subseteq \mathcal{P}(\mathbb{N} \times P)$ as

$$\mathbf{UPred}(P) = \{A \in \mathcal{P}(\mathbb{N} \times P) \mid \forall n \in \mathbb{N}, p \in P, (n, p) \in A \Rightarrow \forall m \leqslant n, \forall q \geqslant p, (m, q) \in A\}$$

i.e., they are sets *downwards* closed in the natural numbers and *upwards* closed in the order on P.

Observe that $\mathbf{UPred}(P)$ is nothing else than $\mathcal{P}^{\uparrow}(\mathbb{N}^{\mathrm{op}} \times P)$ where the order on the product is component-wise and $\mathbb{N}^{\mathrm{op}}$ are the naturals with the reverse of the usual order relation, i.e., $1 \geqslant 2 \geqslant 3 \geqslant \cdots$. This immediately gives us that $\mathbf{UPred}(P)$ is a complete Heyting algebra (Exercise 4.6).

Proposition 5.12. *For any preorder* P, **UPred** (P) *is a c.o.f.e. with relation* $\overset{n}{=}$ *defined as*

$$A \overset{n}{=} B \iff \lfloor A \rfloor_n = \lfloor B \rfloor_n$$

where

$$\lfloor A \rfloor_n = \{(m, a) \mid (m, a) \in A \wedge m < n\}$$

Proof. First we need to show that the specified data satisfies the requirements of an o.f.e. It is obvious that all the relations are equivalence relations and that $\overset{0}{=}$ is the total relation on **UPred** (P). Regarding monotonicity, suppose $A \overset{n+1}{=} B$. We need to show $\lfloor A \rfloor_n = \lfloor B \rfloor_n$ and we do this by showing that they are included in one another. Since the two inclusions are completely symmetric we only show one.

Let $(k, a) \in \lfloor A \rfloor_n$. By definition $(k, a) \in A$ and $k < n$ which clearly implies that $(k, a) \in \lfloor A \rfloor_{n+1}$. The assumption $A \overset{n+1}{=} B$ gives us $(k, a) \in \lfloor B \rfloor_{n+1}$ but since $k < n$ we also have $(k, a) \in \lfloor B \rfloor_n$ concluding the proof of inclusion.

To show that the intersection of all relations $\overset{n}{=}$ is the identity relation suppose $A \overset{n}{=} B$ for all n. We again show that A and B are equal by showing two inclusions which are completely symmetric so it suffices to show only one.

Suppose $(m, a) \in A$. By definition $(m, a) \in \lfloor A \rfloor_{m+1}$, so from the assumption $(m, a) \in \lfloor B \rfloor_{m+1}$ and thus $(m, a) \in B$, showing that $A \subseteq B$.

We are left with showing completeness. Suppose $\{A_n\}_{n=0}^{\infty}$ is a Cauchy sequence. Recall that this means that for each $n \in \mathbb{N}$ there exists an N_n, such that for any $j \geqslant N_n$, $A_{N_n} \overset{n}{=} A_j$. Because of the monotonicity of the relations $\overset{n}{=}$ we can assume without loss of generality that $N_1 \leqslant N_2 \leqslant N_3 \leqslant \cdots$.

Define $A = \left\{(m, a) \mid (m, a) \in A_{N_{m+1}}\right\}$. We claim that A is the limit of $\{A_n\}_{n=0}^{\infty}$.

First we show that A is in fact an element of **UPred** (P). Take $(m, a) \in A$ and $n \leqslant m$ and $b \geqslant a$. We need to show $(n, b) \in A$. By definition this means showing $(n, b) \in A_{N_{n+1}}$. Recall that $N_{n+1} \leqslant N_{m+1}$ by assumption and from the definition of the numbers N_k we have

$$A_{N_{n+1}} \overset{n+1}{=} A_{N_{m+1}}$$

which again by definition means $\lfloor A_{N_{n+1}} \rfloor_{n+1} = \lfloor A_{N_{m+1}} \rfloor_{n+1}$. But note that by the fact that $A_{N_{m+1}}$ is an element of **UPred** (P) we have $(n, b) \in A_{N_{m+1}}$ and from this we have

$$(n, b) \in \lfloor A_{N_{m+1}} \rfloor_{n+1} = \lfloor A_{N_{n+1}} \rfloor_{n+1} \subseteq A_{N_{n+1}}$$

showing that $(n, b) \in A_{N_{n+1}}$.

Exercise 5.8. Using similar reasoning show that $A \overset{n}{=} A_{N_n}$. ♢

The only thing left to show is that A is in fact the limit of **UPred** (P). Let $n \in \mathbb{N}$ and $k \geqslant N_n$. We have

$$A_k \overset{n}{=} A_{N_n} \overset{n}{=} A.$$

Thus for each $n \in \mathbb{N}$ there exists a N_n such that for every $k \geqslant N_n$, $A_k \overset{n}{=} A$, i.e., A is the limit of the sequence $\{A_n\}_{n=0}^{\infty}$. □

Exercise 5.9. **UPred** (P) can be equivalently presented as monotone functions from $\mathbb{N}^{op}$ to $\mathcal{P}^{\uparrow}(P)$ with the relation $\overset{n}{=}$ being

$$\varphi \overset{n}{=} \psi \iff \forall k < n, \varphi(k) = \psi(k).$$

Show that there exist two non-expansive functions

$$\Phi : \mathbf{UPred}(P) \to \left(\mathbb{N}^{op} \overset{mon}{\to} \mathcal{P}^{\uparrow}(P)\right)$$
$$\Psi : \left(\mathbb{N}^{op} \overset{mon}{\to} \mathcal{P}^{\uparrow}(P)\right) \to \mathbf{UPred}(P)$$

that are mutually inverse, i.e., **UPred** (P) and $\mathbb{N}^{op} \overset{mon}{\to} \mathcal{P}^{\uparrow}(P)$ are isomorphic objects in the category $\mathcal{U}$. Conclude that this means that $\mathbb{N}^{op} \to \mathcal{P}^{\uparrow}(P)$ is also a *complete* ordered family of equivalences. ♢

Exercise 5.10. **UPred** (P) can also be equivalently presented as monotone functions from P to the complete Heyting algebra $\mathcal{P}^{\downarrow}(\mathbb{N})$ with the relations being

$$\varphi \overset{n}{=} \psi \iff \forall p \in P, \varphi(p) \overset{n}{=} \psi(p)$$

Concretely, show that the functions

$$\alpha : \left(\mathbb{N}^{op} \overset{mon}{\to} \mathcal{P}^{\uparrow}(P)\right) \to \left(P \overset{mon}{\to} \mathcal{P}^{\downarrow}(\mathbb{N})\right)$$
$$\beta : \left(P \overset{mon}{\to} \mathcal{P}^{\downarrow}(\mathbb{N})\right) \to \left(\mathbb{N}^{op} \overset{mon}{\to} \mathcal{P}^{\uparrow}(P)\right)$$

defined as

$$\alpha(\varphi)(p) = \{n \mid p \in \varphi(n)\}$$
$$\beta(f)(n) = \{p \mid n \in \varphi(p)\}$$

are well defined, non-expansive and mutually inverse. Conclude that this means that $P \overset{mon}{\to} \mathcal{P}^{\downarrow}(\mathbb{N})$ is also a *complete* ordered family of equivalences. ♢

This last presentation of **UPred** (P) presents it as the subset of the exponential $\mathcal{P}^{\downarrow}(\mathbb{N})^{P}$ consisting of *monotone* functions. To make P an object of $\mathcal{U}$ we equip it with a sequence of identity relations.

Exercise 5.11. Show that **UPred** (P) is *not* isomorphic (in $\mathcal{U}$) to $\Delta(X)$ for any set X (see Exercise 5.7). ♢

Proposition 5.13. *The category $\mathcal{U}$ is cartesian closed. The terminal object is the singleton set (with the unique family of relations). If X and Y are objects of $\mathcal{U}$ then the product object $X \times Y$ is*

$$\left(X \times Y, \left(\underset{X\times Y}{\overset{n}{=}}\right)_{n=0}^{\infty}\right)$$

where

$$(x, y) \underset{X\times Y}{\overset{n}{=}} (x', y') \iff x \underset{X}{\overset{n}{=}} x' \wedge y \underset{Y}{\overset{n}{=}} y'$$

and the exponential object Y^X is

$$\left(\mathit{Hom}_{\mathcal{U}}(X, Y), \left(\underset{Y^X}{\overset{n}{=}}\right)_{n=0}^{\infty}\right)$$

where

$$f \overset{n}{\underset{Y^X}{=}} g \iff \forall x \in X, f(x) \overset{n}{\underset{Y}{=}} g(x).$$

is the exponential object.

Note that the underlying set of the exponential Y^X consists of the non-expansive functions from the underlying set of X to the underlying set of Y.

Exercise 5.12. Prove Proposition 5.13. ♢

Proposition 5.14. *Let Y be an object of $\mathcal{U}$ and P a preordered set. Then $Hom_{\mathcal{U}}(Y, \mathbf{UPred}(P))$ is a complete Heyting algebra for operations defined pointwise.*

Proof. Since $\mathbf{UPred}(P)$ is a complete Heyting algebra we know from Exercise 4.3 that the set of *all functions* from the set X to $\mathbf{UPred}(P)$ is a complete Heyting algebra for operations defined pointwise. Thus we know that the operations satisfy all the axioms of a complete Heyting algebra, *if they are well-defined.* That is, if all operations preserve non-expansiveness of functions. This is what we need to check.

We only show it for $\Rightarrow$. The other cases follow exactly the same pattern.

Recall that the definition of $\Rightarrow$ in $\mathbf{UPred}(P)$ is

$$A \Rightarrow B = \{(n,p) \mid \forall k \leqslant n, \forall q \geqslant p, (k,q) \in A \Rightarrow (k,q) \in B\}.$$

We first show that if $A \overset{n}{=} A'$ and $B \overset{n}{=} B'$ then $A \Rightarrow B \overset{n}{=} A' \Rightarrow B'$ by showing two inclusions. The two directions are symmetric so we only consider one.

Let $(m,p) \in \lfloor A \Rightarrow B \rfloor_n$. By definition $m < n$ and $(m,p) \in A \Rightarrow B$ and we need to show $(m,p) \in \lfloor A' \Rightarrow B' \rfloor_n$. Since we know that $m < n$ it suffices to show $(m,p) \in A' \Rightarrow B'$ and for this take $k \leqslant m$ and $q \geqslant p$ and assume $(k,q) \in A'$. Observe that $k < n$ and since $A \overset{n}{=} A'$ we have $(k,q) \in A$ which implies $(k,q) \in B$ which implies, using the fact that $B \overset{n}{=} B'$ and $k < n$ that $(k,q) \in B'$.

Suppose now that $f, g : X \to \mathbf{UPred}(P)$ are non-expansive and $x, x' \in X$ such that $x \overset{n}{=} x'$. Then by definition of operations we have

$$(f \Rightarrow g)(x) = (f(x) \Rightarrow g(x)) \overset{n}{=} (f(x') \Rightarrow g(x')) = (f \Rightarrow g)(x')$$

where we used the fact that $\Rightarrow$ is “non-expansive” in $\mathbf{UPred}(P)$ (shown above) and non-expansiveness of f and g to get $\overset{n}{=}$ in the middle. □

Recall the motivation for going to the category $\mathcal{U}$; we wanted to be able to talk about guarded recursive functions in general. Similarly to the Heyting algebra $\mathcal{P}^{\downarrow}(\mathbb{N})$ there is an operation $\triangleright$ on $\mathbf{UPred}(P)$ defined as

$$\triangleright(A) = \{(0,p) \mid p \in P\} \cup \{(n+1,p) \mid (n,p) \in A\}.$$

Exercise 5.13. Show that $\triangleright$ is contractive. ♢

This $\triangleright$ can be extended pointwise to the complete Heyting algebra $\mathrm{Hom}_{\mathcal{U}}(Y, \mathbf{UPred}(P))$ for any c.o.f.e. Y and is also contractive (when $\mathrm{Hom}_{\mathcal{U}}(Y, \mathbf{UPred}(P))$ is equipped with the metric defined in Proposition 5.13).

Proposition 5.15. *Let* M *be a partial commutative monoid. The complete Heyting algebra* **UPred** (M) *arising from the extension order on* M *is a complete BI-algebra for the following operations*

$$\begin{aligned}
I &= \mathbb{N} \times M \\
A \star B &= \{(n, a \cdot b) \mid (n, a) \in A, (n, b) \in B, a\#b\} \\
A \mathrel{-\!\!\star} B &= \{(n, a) \mid \forall m \leqslant n, \forall b\#a, (m, b) \in A \Rightarrow (m, a \cdot b) \in B\}
\end{aligned}$$

Exercise 5.14. Prove Proposition 5.15. ♢

With Propositions 5.13, 5.14 and 5.15 we have shown the following.

Theorem 5.16. *Let* M *be a partial commutative monoid. The category* $\mathcal{U}$ *together with the generic object* **UPred** (M) *is a BI-hyperdoctrine.*

We can generalize this construction further, replacing **UPred** (M) by any other c.o.f.e. whose underlying set is a complete BI-algebra with a $\triangleright$.

Definition 5.17. A *Löb* BI-algebra is a c.o.f.e. $\left(H, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ whose underlying set H is a *complete* BI-algebra H with a monotone and contractive operation $\triangleright : H \to H$ satisfying $h \leqslant \triangleright(h)$ (monotonicity) and whenever $\triangleright(h) \leqslant h$ then $h = \top$ (Löb rule).

Further, the BI-algebra operations have to be non-expansive. For instance if I is any index set and for each $i \in I$, $a_i \overset{n}{=} b_i$, then we require

$$\begin{aligned}
\bigwedge_{i \in I} a_i &\overset{n}{=} \bigwedge_{i \in I} b_i \\
\bigvee_{i \in I} a_i &\overset{n}{=} \bigvee_{i \in I} b_i
\end{aligned}$$

to hold.

Additionally, $\triangleright$ is required to satisfy the following equalities

$$\begin{aligned}
\triangleright\top &= \top \\
\triangleright\left(\bigwedge_{i \in I} A_i\right) &= \bigwedge_{i \in I} \triangleright A_i \\
\triangleright\left(\bigvee_{i \in I} A_i\right) &= \bigvee_{i \in I} \triangleright A_i && \text{if } I \neq \emptyset \\
\triangleright(A \Rightarrow B) &= \triangleright A \Rightarrow \triangleright B \\
\triangleright(A \star B) &= \triangleright(A) \star \triangleright(B) \\
\triangleright(A \mathrel{-\!\!\star} B) &= \triangleright(A) \mathrel{-\!\!\star} \triangleright\, (B)
\end{aligned}$$

■

Remark 5.18. In the definition of a Löb BI-algebra we included the requirements that are satisfied by all the examples we consider below. However, it is not clear whether all of the requirements are necessary for applications of the logic or whether they could be weakened (for instance, whether we should require $\triangleright(A \star B) = \triangleright(A) \star \triangleright(B)$ or not). ■

Example 5.19. If M is a partial commutative monoid then **UPred** (M) is a Löb BI-algebra. ■

We then have the following theorem. The proof is much the same as the proof of Proposition 5.14. The requirement that the BI-algebra operations are non-expansive implies that the operations defined pointwise will preserve non-expansiveness of functions.

Theorem 5.20. *Let* H *be a Löb BI-algebra. Then* $\mathrm{Hom}_{\mathcal{U}}(-, \mathsf{H})$ *is a BI-hyperdoctrine for operations defined pointwise that also validates rules involving* $\triangleright$ *from Section 4.5.1.*

Recall again the motivation for introducing c.o.f.e.'s from Section 4.5 and Example 4.17. If we used a **Set**-based hyperdoctrines we could choose to interpret the signature in such a way that even though we guarded free variables using a $\triangleright$, we would have no fixed points since the interpretations of function symbols were arbitrary functions.

However in a $\mathcal{U}$-based hyperdoctrine we must interpret all function symbols as *non-expansive* functions since these are the only morphisms in $\mathcal{U}$. We thus have the following theorem and corollary for the hyperdoctrine $\mathrm{Hom}_{\mathcal{U}}(-, \mathsf{H})$ for a Löb BI-algebra H.

Theorem 5.21. *Assume* φ *satisfies* $\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \sigma$ *and suppose further that all free occurrences of* p *in* φ *occur under a* $\triangleright$*. Then for each* $\gamma \in [\![\Gamma]\!]$ *and* $\delta \in [\![\Delta]\!]$,

$$[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \sigma]\!]\,(\gamma, -, \delta) : [\![\mathtt{Prop}^{\tau}]\!] \to [\![\sigma]\!]$$

is contractive.

Proof. We proceed by induction on the typing derivation $\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \sigma$ and show some selected rules.

- Suppose the last rule used was

  $$\frac{\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \mathtt{Prop}}{\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \triangleright\varphi : \mathtt{Prop}}.$$

  Then by definition, the interpretation $[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \mathtt{Prop}]\!]\,(\gamma, -, \delta)$ is *non-expansive* for each γ and δ (this is because it is interpreted as a morphism in $\mathcal{U}$). By definition, the interpretation

  $$[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \triangleright\varphi : \mathtt{Prop}]\!] = \triangleright \circ [\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \mathtt{Prop}]\!]$$

  and so

  $$[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \triangleright\varphi : \mathtt{Prop}]\!]\,(\gamma, -, \delta) = \triangleright \circ [\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \varphi : \mathtt{Prop}]\!]\,(\gamma, -, \delta).$$

  Exercises 5.13 and 5.6 then give us that $[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \triangleright\varphi : \mathtt{Prop}]\!]\,(\gamma, -, \delta)$ is contractive. Note that we have not used the induction hypothesis here and in fact we could not since p might not be guarded anymore when we go under a $\triangleright$.

- Suppose that the last rule used was the function symbol rule. For simplicity assume that F has only two arguments so that the last rule used was

  $$\frac{\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash M_1 : \tau_1 \qquad \Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash M_2 : \tau_2}{\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \mathsf{F}(M_1, M_2) : \sigma}$$

  To reduce clutter we write $[\![M_1]\!]$ and $[\![M_2]\!]$ for the interpretations of the typing judgments of M_1 and M_2. By definition we have

  $$[\![\Gamma, \mathsf{p} : \mathtt{Prop}^{\tau}, \Delta \vdash \mathsf{F}(M_1, M_2) : \sigma]\!] = [\![\mathsf{F}]\!] \circ \langle [\![M_1]\!], [\![M_2]\!] \rangle\,.$$

Since $[\![F]\!]$ is a morphism in $\mathcal{U}$ it is *non-expansive*. The induction hypothesis gives us that $[\![M_1]\!]\,(\gamma, -, \delta)$ and $[\![M_2]\!]\,(\gamma, -, \delta)$ are contractive. It is easy to see that then $\langle [\![M_1]\!], [\![M_2]\!] \rangle\,(\gamma, -, \delta)$ is also contractive which gives us that $[\![\Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash F(M_1, M_2) : \sigma]\!]\,(\delta, -, \gamma)$ is also contractive (Exercise 5.6).

- Suppose the last rule used was the conjunction rule

$$\frac{\Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash \varphi : \mathtt{Prop} \qquad \Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash \psi : \mathtt{Prop}}{\Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash \varphi \wedge \psi : \mathtt{Prop}}$$

By definition,

$$[\![\Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash \varphi \wedge \psi : \mathtt{Prop}]\!] = [\![\varphi]\!] \wedge [\![\psi]\!]$$

and recall that the definitions of Heyting algebra operations on $\mathrm{Hom}_{\mathcal{U}}\,(X, H)$ are pointwise. Therefore $[\![\varphi]\!] \wedge [\![\psi]\!] = \wedge_H \circ \langle [\![\varphi]\!], [\![\psi]\!] \rangle$ where on the right-hand side $\wedge_H$ is the conjunction of the BI-algebra H. Using the induction hypothesis we have that $[\![\varphi]\!]\,(\gamma, -, \delta)$ and $[\![\psi]\!]\,(\gamma, -, \delta)$ are contractive. By assumption that H is a Löb BI-algebra we have that $\wedge_H$ is non-expansive giving us, using Exercise 5.6 that $[\![\Gamma, p : \mathtt{Prop}^\tau, \Delta \vdash \varphi \wedge \psi : \mathtt{Prop}]\!]\,(\gamma, -, \delta)$ is contractive.

The other cases are similar. □

Corollary 5.22. *Assume* φ *satisfies* $\Gamma, p : \mathtt{Prop}^\tau \vdash \varphi : \mathtt{Prop}^\tau$ *and suppose further that all free occurrences of* p *in* φ *occur under a* $\triangleright$. *Then for each* $\gamma \in [\![\Gamma]\!]$ *there exists a unique* $h_\gamma \in [\![\mathtt{Prop}^\tau]\!]$ *such that*

$$[\![\Gamma, p : \mathtt{Prop}^\tau \vdash \varphi : \mathtt{Prop}^\tau]\!]\,(\gamma, h_\gamma) = h_\gamma$$

and further, this assignment is non-expansive, *i.e., if* $\gamma \overset{n}{=} \gamma'$ *then* $h_\gamma \overset{n}{=} h_{\gamma'}$.

Proof. Existence and uniqueness of fixed points follows from Theorem 5.10 and the fact that $\mathbf{UPred}\,(M)^{[\![\tau]\!]}$ is always inhabited, since $\mathbf{UPred}\,(M)$ is.

Non-expansiveness follows from non-expansivness of $[\![\Gamma, p : \mathtt{Prop}^\tau \vdash \varphi : \mathtt{Prop}^\tau]\!]$ and the fact that if two sequences are pointwise n-equal, so are their respective limits (see the construction of fixed points in Theorem 5.10). □

Using these results we can safely add fixed points of guarded recursively defined predicates as in Section 4.5 to the logic and moreover, we can add rules stating uniqueness of such fixed points (up to equivalence $\iff$).

6 Constructions on the category $\mathcal{U}$

The $\triangleright$ is useful when we wish to construct fixed points of predicates, i.e., functions with codomain some Löb BI-algebra. For models of pure separation logic and guarded recursion we can use uniform predicates as shown above. Pure separation logic provides us with a way to reason about programs that manipulate dynamically allocated mutable state by allowing us to assert full ownership over resources. In general, however, we also wish to specify and reason about shared ownership over resources. This is useful for modeling type systems for references, where the type of a reference cell is an invariant that is shared among all parts of the program, or for modeling program logics that combine ideas from separation logic with rely-guarantee style reasoning, see, e.g., [BRS+11] and the references therein. In these cases, the basic idea is that propositions are indexed over "worlds", which, loosely speaking, contain a description of those invariants that have been established until now. In general, an invariant can be any kind of property, so invariants are propositions. A world can be understood as a finite map from natural numbers to invariants. We then have that propositions are indexed over worlds which contain propositions and hence the space of propositions must satisfy a recursive equation of roughly the following form:

$$\mathrm{Prop} = (\mathbb{N} \overset{\mathrm{fin}}{\rightharpoonup} \mathrm{Prop}) \to \mathbf{UPred}\,(\mathsf{M})\,.$$

For cardinality reasons, this kind of recursive domain equation does not have a solution in **Set**. In this section we show that a solution to this kind of recursive domain equation can be found in the category $\mathcal{U}$ and, moreover, that the resulting recursively defined space will in fact give rise to a BI-hyperdoctrine that also models guarded recursively defined predicates.

To express the equation precisely in $\mathcal{U}$ we will make use of the $\blacktriangleright$ *functor*:

Definition 6.1. The functor $\blacktriangleright$ is a functor on $\mathcal{U}$ defined as

$$\blacktriangleright\left(\mathsf{X}, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right) = \left(\mathsf{X}, \left(\overset{n}{\equiv}\right)_{n=0}^{\infty}\right)$$
$$\blacktriangleright(\mathsf{f}) = \mathsf{f}$$

where $\overset{0}{\equiv}$ is the total relation and $x \overset{n+1}{\equiv} x'$ iff $x \overset{n}{=} x'$ ■

Exercise 6.1. Show that the functor $\blacktriangleright$ is well-defined. ♢

Definition 6.2. The category $\mathcal{U}^{\mathrm{op}}$ has as objects complete ordered families of equivalences and a morphism from X to Y is a morphism from Y to X in $\mathcal{U}$. ■

Definition 6.3. A functor $\mathsf{F} : \mathcal{U}^{\mathrm{op}} \times \mathcal{U} \to \mathcal{U}$ is *locally non-expansive* if for all objects X, X', Y, and Y' in $\mathcal{U}$ and $\mathsf{f}, \mathsf{f}' \in \mathrm{Hom}_{\mathcal{U}}(\mathsf{X}, \mathsf{X}')$ and $\mathsf{g}, \mathsf{g}' \in \mathrm{Hom}_{\mathcal{U}}(\mathsf{Y}', \mathsf{Y})$ we have

$$\mathsf{f} \overset{n}{=} \mathsf{f}' \wedge \mathsf{g} \overset{n}{=} \mathsf{g}' \Rightarrow \mathsf{F}(\mathsf{f}, \mathsf{g}) \overset{n}{=} \mathsf{F}(\mathsf{f}', \mathsf{g}').$$

It is *locally contractive* if the stronger implication

$$\mathsf{f} \overset{n}{=} \mathsf{f}' \wedge \mathsf{g} \overset{n}{=} \mathsf{g}' \Rightarrow \mathsf{F}(\mathsf{f}, \mathsf{g}) \overset{n+1}{=} \mathsf{F}(\mathsf{f}', \mathsf{g}').$$

holds. Note that the equalities are equalities on function spaces. ■

Proposition 6.4. *If* F *is a locally non-expansive functor then* $\blacktriangleright \circ \mathsf{F}$ *and* $\mathsf{F} \circ (\blacktriangleright^{op} \times \blacktriangleright)$ *are locally contractive. Here, the functor* $\mathsf{F} \circ (\blacktriangleright^{op} \times \blacktriangleright)$ *works as*

$$(\mathsf{F} \circ (\blacktriangleright^{op} \times \blacktriangleright))(\mathsf{X}, \mathsf{Y}) = \mathsf{F}(\blacktriangleright^{op}(\mathsf{X}), \blacktriangleright(\mathsf{Y}))$$

on objects and analogously on morphisms and $\blacktriangleright^{op}\colon \mathcal{U}^{op} \to \mathcal{U}^{op}$ *is just* $\blacktriangleright$ *working on* $\mathcal{U}^{op}$ *(i.e., its definition is the same).*

Exercise 6.2. Show Proposition 6.4. ♢

6.1 A typical recursive domain equation

We now consider the typical recursive domain equation mentioned above.

Let X be a c.o.f.e. We write $\mathbb{N} \overset{\mathrm{fin}}{\rightharpoonup} \mathsf{X}$ for the set of finite partial maps from $\mathbb{N}$ to X (no requirement of non-expansiveness).

Proposition 6.5. *If* X *is a c.o.f.e. then the space* $\mathbb{N} \overset{fin}{\rightharpoonup} X$ *is a c.o.f.e. when equipped with the following equivalence relations*

$$f \overset{n}{=} g \iff n = 0 \vee \Big(\mathbf{dom}\,(f) = \mathbf{dom}\,(g) \wedge \forall x \in \mathbf{dom}\,(f)\,, f(x) \overset{n}{=} g(x)\Big)\,.$$

Exercise 6.3. Prove Proposition 6.5. The only non-trivial thing to check is completeness. For this, first show that for any Cauchy sequence $\{f_n\}_{n=0}^{\infty}$ there is an n, such that for any $k \geqslant n$, $\mathbf{dom}\,(f_k) = \mathbf{dom}\,(f_n)$. Then the proof is similar to the proof that the set of non-expansive functions between c.o.f.e.'s is again complete. ♢

We order the space $\mathbb{N} \overset{\text{fin}}{\rightharpoonup} X$ by extension ordering, i.e.,

$$f \leqslant g \iff \mathbf{dom}\,(f) \subseteq \mathbf{dom}\,(g) \wedge \forall n \in \mathbf{dom}\,(f)\,, f(n) = g(n).$$

Note that this is the same order that we used for ordering the monoid of heaps in Example 4.9.

Theorem 6.6. *Let* H *be a Löb BI-algebra and* X *a c.o.f.e. Suppose that the limits in* H *respect the order on* H*, i.e., given two converging sequences* $\{a_n\}_{n=0}^{\infty}$ *and* $\{b_n\}_{n=0}^{\infty}$ *such that for all* n, $a_n \leqslant b_n$ *we also have* $\lim_{n\to\infty} a_n \leqslant \lim_{n\to\infty} b_n$.

Then the set of monotone and non-expansive *functions from* $\mathbb{N} \overset{fin}{\rightharpoonup}$ *to* H *with the metric inherited from the space* $Hom_{\mathcal{U}}\left(\mathbb{N} \overset{fin}{\rightharpoonup} X, H\right)$ *is again a Löb BI-algebra.*

Proof. We know that the set of *non-expansive* functions with operations defined pointwise is again a Löb BI-algebra, but that does not immediately imply that the set of monotone and non-expansive functions is as well.

It is easy to see that limits of Cauchy sequences exists using the fact that limits in H preserve order. Exercise!

It is a standard fact that monotone functions from a preordered set into a complete Heyting algebra again form a complete Heyting algebra for pointwise order and the operations defined as follows

$$(f \Rightarrow g)(x) = \bigwedge_{y \geqslant x} (f(y) \Rightarrow g(y)) \qquad \left(\bigwedge_{i\in I} f_i\right)(x) = \bigwedge_{i\in I} (f_i(x)) \qquad \left(\bigvee_{i\in I} f_i\right)(x) = \bigvee_{i\in I} (f_i(x))\,.$$

We first need to check that the operations are well defined. It is easy to see that given monotone functions as input the operations produces monotone functions as output. It is also easy to see that $\bigwedge$ and $\bigvee$ preserve non-expansiveness. However proving non-expansiveness of $f \Rightarrow g$ is not so straightforward.

Suppose $x \overset{n}{=} x'$. The case when $n = 0$ is not interesting so assume $n > 0$. We need to show that

$$\bigwedge_{y \geqslant x} (f(y) \Rightarrow g(y)) \overset{n}{=} \bigwedge_{y' \geqslant x'} (f(y') \Rightarrow g(y')).$$

By the definition of the equality relation on $\mathbb{N} \overset{\text{fin}}{\rightharpoonup} X$ we have that $\mathbf{dom}\,(x)\,\mathbf{dom}\,(x')$ and that for each $k \in \mathbf{dom}\,(x)\,, x(k) \overset{n}{=} x'(k)$. By the definition of the order relation on $\mathbb{N} \overset{\text{fin}}{\rightharpoonup} X$ we have that if $y \geqslant x$ then $\mathbf{dom}\,(y) \supseteq \mathbf{dom}\,(x)$ and for each $k \in \mathbf{dom}\,(x)$, $x(k) = y(k)$ and similarly for x'. Thus if $y \geqslant x$ and $y' \geqslant x'$ then $\forall k \in \mathbf{dom}\,(x) = \mathbf{dom}\,(x')\,, y(k) \overset{n}{=} y'(k)$. Thus for each $y \geqslant x$ there exists a $y' \geqslant x'$, such that $y \overset{n}{=} y'$ and conversely, for each $y' \geqslant x'$ there exists a $y \geqslant x$, such that $y \overset{n}{=} y'$.

Exercise 6.4. Let I and J be two index sets and $n \in \mathbb{N}$. Suppose that for each $i \in I$ there exists a $j \in J$, such that $a_i \overset{n}{=} b_j$ and conversely that for each $j \in J$ there exists an $i \in I$, such that $a_i \overset{n}{=} b_j$. Show that in this case

$$\bigwedge_{i \in I} a_i \overset{n}{=} \bigwedge_{j \in J} b_j.$$

Hint: Consider the extended index set $K = I \sqcup J$, the disjoint union of I and J. Define elements a'_k and b'_k such that for each $k \in K$, $a'_k \overset{n}{=} b'_k$ and so that

$$\bigwedge_{k \in K} a'_k = \bigwedge_{i \in I} a_i \qquad \bigwedge_{k \in K} b'_k = \bigwedge_{j \in J} b_j.$$

Then use that $\bigwedge$ is non-expansive. ♢

Remark 6.7. Theorem 6.6 considers monotone functions on some particular c.o.f.e. Of course, this can be generalized to monotone functions on any suitable preordered c.o.f.e., see [BST10]. ■

Now we know that the operations are well-defined. Next we need to show that they satisfy the Heyting algebra axioms.

Exercise 6.5. Show that operations so defined satisfy the Heyting algebra axioms. ♢

We also need to establish that the operations are non-expansive. Recall that equality on the function space is defined pointwise. We only consider the implication, the other operations are similar.

Suppose $f \overset{n}{=} f'$ and $g \overset{n}{=} g'$. We then have that for each y, $(f(y) \Rightarrow g(y)) \overset{n}{=} (f'(y) \Rightarrow g'(y))$ and from this it is easy to see that $(f \Rightarrow g) \overset{n}{=} (f' \Rightarrow g')$ by non-expansiveness of $\bigwedge$.

It is easy to see that we can extend the operation $\triangleright$ pointwise, i.e.,

$$\triangleright(f) = \triangleright \circ f.$$

Exercise 6.6. Show that the $\triangleright$ defined this way satisfies all the requirements. ♢

The BI-algebra operations are defined as follows

$$(f \star g)(x) = f(x) \star g(x) \qquad (f \mathrel{-\!\!\star} g)(x) = \bigwedge_{y \geqslant x} (f(y) \mathrel{-\!\!\star} g(y)).$$

We can show in the same way as for $\wedge$ and $\Rightarrow$ that they are well-defined and satisfy the correct axioms. □

Given any partial commutative monoid we have, using Theorem 6.6, that the functor

$$F : \mathcal{U}^{\mathrm{op}} \to \mathcal{U}$$
$$F(X) = (\mathbb{N} \overset{\mathrm{fin}}{\rightharpoonup} X) \underset{n.e.}{\overset{mon}{\to}} \textbf{UPred}\,(M)$$

is well-defined.

The space of propositions will be derived from this functor. However in general this functor does not have a fixed-point; we need to make it locally-contractive by composing with the functor $\blacktriangleright$. Using Theorem 6.9 (described in the next subsection) we have that $G = \blacktriangleright \circ F$ has a unique fixed point which we call PreProp. That is, $\mathsf{G}(\text{PreProp}) \cong \text{PreProp}$ in $\mathcal{U}$. Concretely, we have a non-expansive bijection ι with a non-expansive inverse

$$\iota : \mathsf{G}(\text{PreProp}) \to \text{PreProp}.$$

Since PreProp is a c.o.f.e. we can use Theorem 6.6 to show that the space

$$\text{Prop} = \mathsf{F}(\text{PreProp}) = (\mathbb{N} \overset{\text{fin}}{\rightharpoonup} \text{PreProp}) \underset{n.e.}{\overset{mon}{\to}} \mathbf{UPred}\,(M)$$

is a Löb BI-algebra. Hence the hyperdoctrine $\text{Hom}_{\mathcal{U}}\,(-, \text{Prop})$ is a BI-hyperdoctrine that also models the $\triangleright$ operation and fixed points of guarded recursive predicates (Theorem 5.20).

Summary As a summary, we present the explicit model of propositions in the hyperdoctrine $\text{Hom}_{\mathcal{U}}\,(-, \text{Prop})$ (we include equality, although we have not considered that earlier). Recall that a proposition in context $\Gamma \vdash \varphi : \texttt{Prop}$ is interpreted as a non-expansive function from $[\![\Gamma]\!]$ to Prop. Omitting $: \texttt{Prop}$ from the syntax, we have:

$$\begin{aligned}
[\![\Gamma \vdash M =_\tau N]\!]_\gamma\, w &= \left\{(n, r) \mid [\![\Gamma \vdash M : \tau]\!]_\gamma \overset{n+1}{=} [\![\Gamma \vdash N : \tau]\!]_\gamma \right\}\\
[\![\Gamma \vdash \top]\!]_\gamma\, w &= \mathbb{N} \times M\\
[\![\Gamma \vdash \varphi \wedge \psi]\!]_\gamma\, w &= [\![\Gamma \vdash \varphi]\!]_\gamma\, w \cap [\![\Gamma \vdash \psi]\!]_\gamma\, w\\
[\![\Gamma \vdash \bot]\!]_\gamma\, w &= \emptyset\\
[\![\Gamma \vdash \varphi \vee \psi]\!]_\gamma\, w &= [\![\Gamma \vdash \varphi]\!]_\gamma\, w \cup [\![\Gamma \vdash \psi]\!]_\gamma\, w\\
[\![\Gamma \vdash \varphi \Rightarrow \psi]\!]_\gamma\, w &= \forall w' \geqslant w, \forall n' \leqslant n, \forall r' \geqslant r, (n', r') \in [\![\Gamma \vdash \varphi]\!]_\gamma\, w' \Rightarrow (n', r') \in [\![\Gamma \vdash \psi]\!]_\gamma\, w'\\
[\![\Gamma \vdash \forall x : \sigma, \varphi]\!]_\gamma\, w &= \bigcap_{d \in [\![\sigma]\!]} [\![\Gamma, x : \sigma \vdash \varphi]\!]_{(\gamma, d)}\, w\\
[\![\Gamma \vdash \exists x : \sigma, \varphi]\!]_\gamma\, w &= \bigcup_{d \in [\![\sigma]\!]} [\![\Gamma, x : \sigma \vdash \varphi]\!]_{(\gamma, d)}\, w\\
[\![\Gamma \vdash \triangleright\varphi]\!]_\gamma\, w &= \{(0, r) \mid r \in M\} \cup \{(n+1, r) \mid (n, r) \in [\![\Gamma \vdash \varphi]\!]_\gamma\, w\}\\
[\![\Gamma \vdash I]\!]_\gamma\, w &= \mathbb{N} \times M\\
[\![\Gamma \vdash \varphi \star \psi]\!]_\gamma\, w &= \{(n, r) \mid \exists r_1, r_2, r = r_1 \cdot r_2 \wedge (n, r_1) \in [\![\Gamma \vdash \varphi]\!]_\gamma\, w \wedge (n, r_2) \in [\![\Gamma \vdash \psi]\!]_\gamma\, w\}\\
[\![\Gamma \vdash \varphi \mathrel{-\!\!\star} \psi]\!]_\gamma\, w &= \{(n, r) \mid \forall w' \geqslant w, \forall n' \leqslant n, \forall r' \# r.(n', r') \in [\![\Gamma \vdash \varphi]\!]_\gamma\, w' \wedge (n', r \cdot r') \in [\![\Gamma \vdash \psi]\!]_\gamma\, w'\}
\end{aligned}$$

In particular note that the "resources" r are not used in the interpretation of equality.

Moreover, when p occurs under a $\triangleright$ in φ, then we have a recursively defined predicate:

$$[\![\Gamma \vdash \mu p.\varphi : \texttt{Prop}^\tau]\!]_\gamma = \mathit{fix}(\lambda x : [\![\texttt{Prop}^\tau]\!] \,.\, [\![\Gamma, p : \texttt{Prop}^\tau \vdash \varphi : \texttt{Prop}^\tau]\!]_{(\gamma, x)})$$

Here *fix* yields the fixed point of the contractive function, see Corollary 5.22.

Finally, we can have a new logical connective for expressing invariants. Syntactically

$$\frac{\Gamma \vdash M : \mathbb{N} \qquad \Gamma \vdash \varphi : \texttt{Prop}}{\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}}$$

where $\mathbb{N}$ is a base type, which we interpret by the natural numbers (formally, as the object $\Delta(\mathbb{N})$ in $\mathcal{U}$).

Then we define

$$\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M}\right]\!\!\right]_{\gamma} w = \left\{(n, r) \mid w(\llbracket \Gamma \vdash M \rrbracket_{\gamma}) \overset{n+1}{=} \iota(\llbracket \Gamma \vdash \varphi \rrbracket_{\gamma})\right\}.$$

Let us unfold the definition to see what it means and to see that it makes sense. First, given $\gamma \in \llbracket \Gamma \rrbracket$ we have

$$\llbracket \Gamma \vdash M \rrbracket_{\gamma} \in \llbracket \mathbb{N} \rrbracket = \Delta(\mathbb{N})$$
$$\llbracket \Gamma \vdash \varphi \rrbracket_{\gamma} \in \llbracket \texttt{Prop} \rrbracket = \text{Prop} = \mathsf{F}(\text{PreProp})$$

and we wish to have

$$\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]_{\gamma} \in \llbracket \texttt{Prop} \rrbracket = \text{Prop} = (\mathbb{N} \overset{\text{fin}}{\rightharpoonup} \text{PreProp}) \underset{n.e.}{\overset{mon}{\to}} \textbf{UPred}\,(M).$$

Thus given $w \in \mathbb{N} \overset{\text{fin}}{\rightharpoonup} \text{PreProp}$ we wish to have

$$\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]_{\gamma} w \in \textbf{UPred}\,(M).$$

Now since the underlying set of $\Delta(\mathbb{N})$ is $\mathbb{N}$ we have $w(\llbracket \Gamma \vdash M \rrbracket_{\gamma}) \in \text{PreProp}$. Recall the isomorphism $\iota : \blacktriangleright (\mathsf{F}(\text{PreProp})) \to \text{PreProp}$. Since the underlying set of $\blacktriangleright (\mathsf{F}(\text{PreProp}))$ is the same as the underlying set of $\mathsf{F}(\text{PreProp})$ we can apply ι to $\llbracket \Gamma \vdash \varphi \rrbracket_{\gamma}$ to get

$$\iota\left(\llbracket \Gamma \vdash \varphi \rrbracket_{\gamma}\right) \in \text{PreProp}$$

We then compare for n-equality in the space PreProp.

Now what the definition is supposed to express is that if (n, r) is in $\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]_{\gamma} w$ for some world w, then the invariant for region M in world w is *approximately* φ, where approximately is expressed using n-equality and means, intuitively, that φ cannot be distinguished from the invariant for M in w for n steps. The use of the isomorphism ι is necessary only because we do not have a solution of the domain equation up to equality, but only up to an isomorphism.

Observe also that the $\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]_{\gamma} w$ is oblivious to resources (to $r \in M$).

Exercise 6.7. Check that the interpretation of $\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]$ is well defined. Concretely, check that $\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]$ is non-expansive and that for each $\gamma \in \Gamma$, the function

$$\left[\!\!\left[\Gamma \vdash \boxed{\varphi}^{M} : \texttt{Prop}\right]\!\!\right]_{\gamma}$$

is an element of $\mathsf{F}(\text{PreProp})$ which means that it is non-expansive and monotone in the world w and actually maps into **UPred** (M). ♢

6.2 Explicit construction of fixed points of locally contractive functors in $\mathcal{U}$

In this subsection, we present an elementary construction of *the* fixed point of a locally contractive functor in the category of complete ordered families of equivalences. This fixed point theorem is originally due to America and Rutten [AR89]. In [BST10] one can find a category-theoretic generalization, which shows how to obtain fixed points of locally contractive funtors on categories enriched in $\mathcal{U}$. It is not necessary to understand the proof in this subsection to understand the rest of the material in these notes.

Definition 6.8. A fixed point of a locally contractive functor F is an object $X \in \mathcal{U}$, such that $\mathsf{F}(X, X) \cong X$. ■

Theorem 6.9. *Every locally contractive functor* F *such that* $\mathsf{F}(1, 1)$ *is inhabited has a unique fixed point. The fixed point is unique among inhabited c.o.f.e.'s.*

If in addition $\mathsf{F}(\emptyset, \emptyset)$ *is inhabited then the fixed point of* F *is unique.*

Proof. We first construct a solution. Then show uniqueness.

Define a sequence of spaces $F_n \in \mathcal{U}$ by induction as follows:

$$\begin{aligned} F_0 &= (\{*\}, (=)_{n=0}^{\infty}) \\ F_{n+1} &= \mathsf{F}(F_n, F_n) \end{aligned}$$

together with projections $p_n : F_{n+1} \to F_n$ and embeddings $e_n : F_n \to F_{n+1}$

$$\begin{aligned} p_0 &= \text{the unique map to } F_0 & e_0 &= \text{any map from } F_0 \text{ to } F_1 \\ p_{n+1} &= \mathsf{F}(e_n, p_n) & e_{n+1} &= \mathsf{F}(p_n, e_n) \end{aligned}$$

Note that e_0 exists because by assumption $\mathsf{F}(1, 1)$ is inhabited and constant functions are non-expansive.

Later we will need the fact that e_k and p_k are indeed embeddings and projections, i.e., that

$$\forall k, p_k \circ e_k = \mathrm{id}_{F_k}. \tag{6}$$

which we show by induction. The base case is trivial. For the inductive case we have

$$p_{k+1} \circ e_{k+1} = \mathsf{F}(e_k, p_k) \circ \mathsf{F}(p_k, e_k) = \mathsf{F}(p_k \circ e_k, p_k \circ e_k) = \mathsf{F}\left(\mathrm{id}_{F_k}, \mathrm{id}_{F_k}\right) = \mathrm{id}_{F_{k+1}}.$$

Projection followed by an embedding does not equal the identity function, but it does get closer with increasing k. More precisely, we have

$$\forall k, e_k \circ p_k \overset{k}{=} \mathrm{id}_{F_{k+1}} \tag{7}$$

The base case is trivial, since everything is equal at step 0. For the inductive step we have

$$e_{k+1} \circ p_{k+1} = \mathsf{F}(p_k, e_k) \circ \mathsf{F}(e_k, p_k) = \mathsf{F}(e_k \circ p_k, e_k \circ p_k) \overset{k+1}{=} \mathrm{id}_{F_{k+2}}$$

the last equation holding by the induction hypothesis and contractiveness of F. This is the place where local contractiveness of F is used.

It will be convenient later to use compositions of embeddings $e_k^\ell : F_k \to F_\ell$ and projections $p_k^\ell : F_\ell \to F_k$ which we define as

$$\begin{aligned} p_k^k &= \mathrm{id}_{F_k} & e_k^k &= \mathrm{id}_{F_k} \\ p_k^{k+\ell+1} &= p_k^{k+\ell} \circ p_{k+\ell} & e_k^{k+\ell+1} &= e_{k+\ell} \circ e_k^{k+\ell} \end{aligned}$$

Exercise 6.8. Show that for any $\ell \leqslant k$,

$$p_k^\ell \circ e_k^\ell = \mathrm{id}_{F_k}. \tag{8}$$

♢

Hint: Use (6).

We claim that

$$X = \left\{ x \in \prod_{n \in \mathbb{N}} F_n \;\middle|\; \forall k, p_k\left(x_{k+1}\right) = x_k \right\}$$

is a fixed point of F, i.e., that $F(X, X) \cong X$. The equality on X is defined as

$$x \overset{n}{=}_X x' \iff \forall k, x_k \overset{n}{=}_{F_k} x'_k$$

where $\overset{n}{=}_{F_k}$ denotes n-th equivalence relation on the set F_k.

It is easy to see that $\left(X, \left(\overset{n}{=}\right)_{n=0}^{\infty}\right)$ is indeed an object of $\mathcal{U}$. In fact, it is also inhabited, for instance $(e_0^n(*))_{n=0}^{\infty}$ is an element of X which is easy to see using (8).

To construct an isomorphism between X and $F(X, X)$ we will need auxiliary embeddings $\iota_n : F_n \to X$ and projections $\pi_n : X \to F_n$ defined as follows

$$\pi_n(x) = x_n \qquad\qquad (\iota_n(y))_k = \begin{cases} p_k^n(y) & \text{if } n \geqslant k \\ e_n^k(y) & \text{if } k \geqslant n \end{cases}$$

Using (8) it is easy to see that ι_n is well defined for any n and since p_k and e_k are non-expansive, so are p_k^n and e_n^k and consequently also ι_n (see definition of equality on X).

Using these we can define morphism $\alpha : X \to F(X, X)$ and $\beta : F(X, X) \to X$ and show them mutually inverse. They are defined as follows

$$\beta(z)_n = \begin{cases} * & \text{if } n = 0 \\ F(\iota_m, \pi_m)(z) & \text{if } n = m + 1 \end{cases}$$

and

$$\alpha(x) = \lim_{k \to \infty} F\left(\pi_k, \iota_k\right)\left(x_{k+1}\right)$$

We first need to make sure that these are good definitions, i.e., that they do indeed define morphism in $\mathcal{U}$ between X and $F(X, X)$. First we consider β. To be well-defined it has to actually map into X and be non-expansive. To see that it maps into X we proceed by induction. The base case is trivial since F_1 is a single-element space. For the inductive case we have

$$\begin{aligned} p_{n+1}\left(\beta(z)_{n+2}\right) &= p_{n+1}\left(F(\iota_{n+1}, \pi_{n+1})(z)\right) = F(e_n, p_n)\left(F(\iota_{n+1}, \pi_{n+1})(z)\right) \\ &= F\left(\iota_{n+1} \circ e_n, p_n \circ \pi_{n+1}\right)(z) = F(\iota_n, \pi_n)(z) = \beta(z)_{n+1} \end{aligned}$$

where we have used the fact, which is easily checked, that $\iota_{n+1} \circ e_n = \iota_n$ and $p_n \circ \pi_{n+1} = \pi_n$.

The fact that β is non-expansive follows directly from the fact that $F(\iota_m, \pi_m)$ is non-expansive for all m, since F is a functor mapping into $\mathcal{U}$.

To see that α is well-defined we have to first show that the limit used in its definition actually exists. Recall that we are working with c.o.f.e.'s so we only need to check that the sequence $\{F\left(\pi_k, \iota_k\right)\left(x_{k+1}\right)\}_{k=0}^{\infty}$ is a Cauchy chain for $x \in X$.

We will show that

$$F\left(\pi_k, \iota_k\right)\left(x_{k+1}\right) \overset{k+1}{=} F\left(\pi_{k+\ell}, \iota_{k+\ell}\right)\left(x_{k+\ell+1}\right)$$

for any ℓ with the equality being the equality in $F(X, X)$.

We proceed by induction on ℓ with the base case being trivial by construction.

$$\begin{aligned} F(\pi_k, \iota_k)(x_{k+1}) &= F(\pi_k, \iota_k)(p_{k+1} x_{k+2}) \\ &= F(\pi_k, \iota_k)(F(e_k, p_k)(x_{k+2})) \\ &= F(e_k \circ \pi_k, \iota_k \circ p_k)(x_{k+2}) \end{aligned}$$

and from (7) we have

$$e_k(\pi_k(y)) = e_k(p_k(\pi_{k+1}(y))) \overset{k}{=} \pi_{k+1}(y)$$

since $\pi_k = p_k \circ \pi_{k+1}$ and

$$\iota_k(p_k(y)) = \iota_{k+1}(e_k(p_k(y))) \overset{k}{=} \iota_{k+1}(y)$$

since $\iota_{k+1} \circ e_k = \iota_k$. Combining these together with the fact that F is contractive we have

$$F(e_k \circ \pi_k, \iota_k \circ p_k)(x_{k+2}) \overset{k+1}{=} F(\pi_{k+1}, \iota_{k+1})(x_{k+2})$$

and using the induction hypothesis for ℓ we get

$$F(\pi_{k+1}, \iota_{k+1})(x_{k+2}) \overset{k+1}{=} F(\pi_{k+1+\ell}, \iota_{k+1+\ell})(x_{k+2+\ell}) = F(\pi_{k+\ell+1}, \iota_{k+\ell+1})(x_{k+1+\ell+1})$$

concluding the proof.

We have thus established that the sequence used in the definition of α is a Cauchy chain, hence it has a limit by completeness.

Exercise 6.9. It is a good exercise to show that α is non-expansive or more generally, that given two Cauchy-chain that are pointwise n-equal, then the limits are also n-equal. That is, given two Cauchy-chains $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$ such that $\forall n, a_n \overset{k}{=} b_n$, then $\lim_{n\to\infty} a_n \overset{k}{=} \lim_{n\to\infty} b_n$. ♢

Thus we have α and β, two non-expansive maps. Now we need to show that they are inverses. We first consider $\alpha \circ \beta$.

$$(\alpha \circ \beta)(z) = \lim_{k\to\infty} F(\pi_k, \iota_k)(F(\iota_k, \pi_k)(z)) = \lim_{k\to\infty} F(\iota_k \circ \pi_k, \iota_k \circ \pi_k)(z)$$

We wish to show that the limit is z. To that end we show that $\iota_k \circ \pi_k \overset{k}{=} \mathrm{id}_X$. Let $x \in X$. We have for $\ell \geqslant k$

$$\iota_k(\pi_k(x))_\ell = \begin{cases} x_\ell & \text{if } \ell \leqslant k \\ e_k^\ell(x_k) & \text{if } k \leqslant \ell \end{cases}$$

so clearly $\iota_k(\pi_k(x))_\ell \overset{k}{=} x_\ell$ for $\ell \leqslant k$. For $k \leqslant \ell$ we have

$$\iota_k(\pi_k(x))_\ell = e_k^\ell(x_k) = e_k^\ell(p_k^\ell(x_\ell)) \overset{k}{=} x_\ell$$

where we have used

Exercise 6.10. Show that for any $\ell \geqslant k$, $e_k^\ell \circ p_k^\ell \overset{k}{=} \mathrm{id}_{F_\ell}$. ♢

Hint: Use induction and (7).

Since F is contractive we have shown that z is the limit of $\lim_{k\to\infty} \mathsf{F}(\iota_k \circ \pi_k, \iota_k \circ \pi_k)(z)$ and so $\alpha(\beta(z)) = z$.

To show $\beta(\alpha(x)) = x$ we proceed as follows

$$\beta(\alpha(x))_{n+1} = \mathsf{F}(\iota_n, \pi_n)\left(\lim_{k\to\infty} \mathsf{F}(\pi_k, \iota_k)(x_{k+1})\right)$$

and since non-expansive functions preserve limits we get

$$\lim_{k\to\infty} \mathsf{F}(\iota_n, \pi_n)(\mathsf{F}(\pi_k, \iota_k)(x_{k+1})) = \lim_{k\to\infty} \mathsf{F}(\pi_k \circ \iota_n, \pi_n \circ \iota_k)(x_{k+1})$$

Exercise 6.11. For $k \geqslant n$ we have $\pi_k \circ \iota_n = e_n^k$ and $\pi_n \circ \iota_k = p_n^k$ and additionally $\mathsf{F}(e_n^k, p_n^k) = p_{n+1}^k$. ♢

Using the result of the last exercise we get

$$\lim_{k\to\infty} \mathsf{F}(\pi_k \circ \iota_n, \pi_n \circ \iota_k)(x_{k+1}) = \lim_{k\to\infty} p_{n+1}^k(x_{k+1}) = \lim_{k\to\infty} x_{n+1} = x_{n+1}$$

concluding the proof that $\beta \circ \alpha = \mathrm{id}_X$.

Now to show uniqueness (up to isomorphism) suppose Y is another *inhabited* solution, i.e., $\gamma : \mathsf{F}(Y, Y) \cong Y$. We need to show there is an isomorphism between X and Y and we proceed similarly as we did in the construction of an isomorphisms between $\mathsf{F}(X, X)$ and X.

Define embedding projection pairs $\xi_n : Y \to F_n$ and $\zeta_n : F_n \to Y$ by induction as

$$\begin{aligned} \xi_0 &= \text{the unique map to } F_0 & \zeta_0 &= \text{any map from } F_0 \text{ to } Y \\ \xi_{n+1} &= \mathsf{F}(\zeta_n, \xi_n) \circ \gamma^{-1} & \zeta_{n+1} &= \gamma \circ \mathsf{F}(\xi_n, \zeta_n) \end{aligned}$$

Then define $\varepsilon : Y \to X$ as $\varepsilon(y)_n = \xi_n(y)$ and $\delta : X \to Y$ as $\delta(x) = \lim_{k\to\infty} \zeta_k(x)$.

Exercise 6.12. Show that ε and δ are well-defined, non-expansive and mutually inverse. Additionally show that $\gamma \circ \mathsf{F}(\varepsilon, \delta) = \delta \circ \beta$. ♢

Exercise 6.13. Find an example of a locally contractive functor that has two fixed points, an inhabited one and $\emptyset$. ♢

□

7 Further Reading — the Topos of Trees

The first hyperdoctrine we considered in these notes was the one for the set-theoretic model of higher-order logic, namely **Set** with 2 as the generic object. One of the particular properties of this hyperdoctrine is that $\mathrm{Hom}_{\mathbf{Set}}(X, 2)$ is naturally isomorphic to subobjects of X. In other words, 2 is a *subobject classifier* in **Set**. A *topos* is a cartesian closed category with a subobject classifier.

The category $\mathcal{U}$ is a full subcategory of the topos of trees $\mathcal{S}$, which is the category of presheaves over the natural numbers. The ▶ functor extends to $\mathcal{S}$ and one can also find solutions to recursive domain equations in $\mathcal{S}$. See [BMSS12] for a discussion of that and also for an application to a "synthetic" step-indexed model of a programming language with dynamically allocated references. In [SB14], $\mathcal{S}$ is used as the ambient logic in which a model of a program logic called iCAP is defined. We emphasize, however, that the model of iCAP can also be given more explicitly using the approach detailed in the previous section.

References

[AR89] 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.

[Awo10] S. Awodey. *Category Theory.* Oxford Logic Guides. Oxford University Press, 2010.

[BBTS07] Bodil Biering, Lars Birkedal, and Noah Torp-Smith. Bi-hyperdoctrines, higher-order separation logic, and abstraction. *ACM Trans. Program. Lang. Syst.*, 29(5), August 2007.

[BMSS12] L. Birkedal, R. Møgelberg, J. Schwinghammer, and K. Støvring. First steps in synthetic guarded domain theory: step-indexing in the topos of trees. *Logical Methods in Computer Science*, 8(4), October 2012.

[BRS$^+$11] L. Birkedal, B. Reus, J. Schwinghammer, K. Støvring, J. Thamsborg, and H. Yang. Step-indexed kripke models over recursive worlds. In Thomas Ball and Mooly Sagiv, editors, *Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2011, Austin, TX, USA, January 26-28, 2011*, pages 119–132. ACM, 2011.

[BST10] L. Birkedal, K. Støvring, and J. Thamsborg. The category-theoretic solution of recursive metric-space equations. *Theor. Comput. Sci.*, 411(47):4102–4122, 2010.

[Jac99] B. Jacobs. *Categorical Logic and Type Theory*, volume 141 of *Studies in Logic and the Foundations of Mathematics.* North-Holland Publishing Co., Amsterdam, 1999.

[Law69] F.W. Lawvere. Adjointness in foundations. *Dialectica*, 23(3/4):281–296, 1969.

[Pit02] A. M. Pitts. Tripos theory in retrospect. *Math. Structures Comput. Sci.*, 12(3):265–279, 2002.

[SB14] K. Svendsen and L. Birkedal. Impredicative Concurrent Abstract Predicates. In *Proceedings of ESOP*, 2014.