Temporal Refinements for Guarded Recursive Types (full version)

Guilhem Jaber, Colin Riba

Temporal Refinements for Guarded Recursive Types

Guilhem Jaber[1] and Colin Riba[2]

Université de Nantes, LS2N CNRS, Inria, France guilhem.jaber@univ-nantes.fr
Univ Lyon, EnsL, UCBL, CNRS, LIP, F-69342, LYON Cedex 07, France
colin.riba@ens-lyon.fr

Abstract. We propose a logic for temporal properties of higher-order programs that handle infinite objects like streams or infinite trees, represented via coinductive types. Specifications of programs use safety and liveness properties. Programs can then be proven to satisfy their specification in a compositional way, our logic being based on a type system. The logic is presented as a refinement type system over the guarded λ-calculus, a λ-calculus with guarded recursive types. The refinements are formulae of a modal μ-calculus which embeds usual temporal modal logics such as LTL and CTL. The semantics of our system is given within a rich structure, the topos of trees, in which we build a realizability model of the temporal refinement type system. We use in a crucial way the connection with set-theoretic semantics to handle liveness properties.

Keywords: coinductive types, guarded recursive types, μ-calculus, refinement types, topos of trees.

1 Introduction

Functional programming is by now well established to handle infinite data, thanks to declarative definitions and equational reasoning on high-level abstractions, in particular when infinite objects are represented with coinductive types. In such settings, programs in general do not terminate, but are expected to compute a part of their output in finite time. For example, a program expected to generate a stream should produce the next element in finite time: it is *productive*.

Our goal is to prove input-output temporal properties of higher-order programs that handle coinductive types. Logics like LTL, CTL or the modal μ-calculus are widely used to formulate, on infinite objects, safety and liveness properties. Safety properties state that some "bad" event will not occur, while liveness properties specify that "something good" will happen (see e.g. [9]). Typically, modalities like $\Box$ (*always*) or $\Diamond$ (*eventually*) are used to write properties of streams or infinite trees and specifications of programs over such data.

We consider temporal refinement types $\{A \mid \varphi\}$, where A is a standard type of our programming language, and φ is a formula of the modal μ-calculus. Using refinement types [24], temporal connectives are not reflected in the programming language, and programs are formally independent from the shape of their temporal specifications. One can thus give different refinement types to the same program. For example, the following two types can be given to the same map function on streams:

$$\begin{array}{l} \mathsf{map} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathsf{Str}\, B \mid \Box\Diamond[\mathsf{hd}]\psi\} \longrightarrow \{\mathsf{Str}\, A \mid \Box\Diamond[\mathsf{hd}]\varphi\} \\ \mathsf{map} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathsf{Str}\, B \mid \Diamond\Box[\mathsf{hd}]\psi\} \longrightarrow \{\mathsf{Str}\, A \mid \Diamond\Box[\mathsf{hd}]\varphi\} \end{array} \quad (\star)$$

These types mean that given $f : B \to A$ s.t. $f(b)$ satisfies φ if b satisfies ψ, the function ($\mathsf{map}\ f$) takes a stream with infinitely many (resp. ultimately all) elements satisfying ψ to one with infinitely many (resp. ultimately all) elements satisfying φ. For φ a formula over A, $[\mathsf{hd}]\varphi$ is a formula over streams of A's which holds on a given stream if φ holds on its head element.

It is undecidable whether a given higher-order program satisfies a given input-output temporal property written with formulae of the modal μ-calculus [45]. Having a type system is a partial workaround to this obstacle, which moreover enables to reason compositionally on programs, by decomposing a specification to the various components of a program in order to prove its global specification.

Our system is built on top of the guarded λ-calculus [20], a higher-order programming language with guarded recursion [57]. Guarded recursion is a simple device to control and reason about unfoldings of fixpoints. It can represent coinductive types [55] and provides a syntactic compositional productivity check [5].

Safety properties (e.g. $\Box[\mathsf{hd}]\varphi$) can be correctly represented with guarded fixpoints, but not liveness properties (e.g. $\Diamond[\mathsf{hd}]\varphi$, $\Diamond\Box[\mathsf{hd}]\varphi$, $\Box\Diamond[\mathsf{hd}]\varphi$). Combining liveness with guarded recursion is a challenging problem since guarded fixpoints tend to have unique solutions. Existing approaches to handle temporal types in presence of guarded recursion face similar difficulties. Functional reactive programming (FRP) [23] provides a Curry-Howard correspondence for temporal logics [35,36,18] in which logical connectives are reflected as programming constructs. When combining FRP with guarded recursion [48,7], and in particular to handle liveness properties [8], uniqueness of guarded fixpoints is tempered by specific recursors for temporal types.

Our approach is different from [8], as we wish as much as possible the logical level not to impact the program level. We propose a two level system, with the lower or *internal* level, which interacts with guarded recursion and at which only safety properties are correctly represented, and the higher or *external* one, at which liveness properties are correctly handled, but without direct access to guarded recursion. By restricting to the alternation-free modal μ-calculus, in which fixpoints can always be computed in ω-steps, one can syntactically reason on finite unfoldings of liveness properties, thus allowing for crossing down the safety barrier. Soundness is proved by a realizability interpretation based on the semantics of guarded recursion in the topos of trees [13], which correctly represents the usual set-theoretic final coalgebras of polynomial coinductive types [55].

We provide example programs involving linear structures (colists, streams, fair streams [18,8]) and branching structures (resumptions *à la* [48]), for which we prove liveness properties similar to ($\star$) above. Our system also handles safety properties on breadth-first (infinite) tree traversals *à la* [39] and [10].

$$
\begin{aligned}
\mathsf{Cons}^{\mathsf{g}} &:= \lambda x.\lambda s.\,\mathsf{fold}(\langle x, s\rangle) : A \to \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \to \mathsf{Str}^{\mathsf{g}}\, A \\
\mathsf{hd}^{\mathsf{g}} &:= \lambda s.\pi_0(\mathsf{unfold}\ s) \quad : \mathsf{Str}^{\mathsf{g}}\, A \to A \\
\mathsf{tl}^{\mathsf{g}} &:= \lambda s.\pi_1(\mathsf{unfold}\ s) \quad : \mathsf{Str}^{\mathsf{g}}\, A \to \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \\
\mathsf{map}^{\mathsf{g}} &:= \lambda f.\mathsf{fix}(g).\lambda s.\,\mathsf{Cons}^{\mathsf{g}}\ (f(\mathsf{hd}^{\mathsf{g}}\ s))\ (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \ \ : (B \to A) \to \mathsf{Str}^{\mathsf{g}}\, B \to \mathsf{Str}^{\mathsf{g}}\, A
\end{aligned}
$$

Fig. 1. Constructor, Destructors and Map on Guarded Streams.

Organization of the paper. We give an overview of our approach in §2. Then §3 presents the syntax of the guarded λ-calculus. Our base temporal logic (without liveness) is introduced in §4, and is used to define our refinement type system in §5. Liveness properties are handled in §6. The semantics is given in §7, and §8 presents examples. Finally, we discuss related work in §9 and future work in §10. Table 4 (§8) gathers the main refinement types we can give to example functions, most of them defined in Table 3. Omitted material is available in the Appendices.

2 Outline

Overview of the Guarded $\boldsymbol{\lambda}$-Calculus. Guarded recursion enforces productivity of programs using a type system equipped with a type modality $\blacktriangleright$, in order to indicate that one has access to a value not right now but only "later". One can define guarded streams $\mathsf{Str}^{\mathsf{g}}\, A$ over a type A via the guarded recursive definition $\mathsf{Str}^{\mathsf{g}}\, A = A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A$. Streams that inhabit this type have their head available now, but their tail only one step in the future. The type modality $\blacktriangleright$ is reflected in programs with the next operation. One also has a fixpoint constructor on terms $\mathsf{fix}(x).M$ for guarded recursive definitions. They are typed with

$$
\frac{\mathcal{E} \vdash M : A}{\mathcal{E} \vdash \mathsf{next}(M) : \blacktriangleright A}
\qquad\qquad
\frac{\mathcal{E}, x : \blacktriangleright A \vdash M : A}{\mathcal{E} \vdash \mathsf{fix}(x).M : A}
$$

This allows for the constructor and basic destructors on guarded streams to be defined as in Fig. 1, where $\mathsf{fold}(-)$ and $\mathsf{unfold}(-)$ are explicit operations for folding and unfolding guarded recursive types. In the following, we use the infix notation $a ::^{\mathsf{g}} s$ for $\mathsf{Cons}^{\mathsf{g}}\ a\ s$. Using the fact that the type modality $\blacktriangleright$ is an applicative functor [54], we can distribute $\blacktriangleright$ over the arrow type. This is represented in the programming language by the infix applicative operator $\circledast$. With it, one can define the usual map function on guarded streams as in Fig. 1.

Compositional Safety Reasoning on Streams. Given a property φ on a type A, we would like to consider a subtype of $\mathsf{Str}^{\mathsf{g}}\, A$ that selects those streams whose elements all satisfy φ. To do so, we use a temporal modal formula $\Box[\mathsf{hd}]\varphi$, and consider the *refinement type* $\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$. Suppose for now that we

Typed Formulae	**Provability**	**Refinement Types**	**Subtyping**	**Typing**
$\Sigma \vdash \varphi : A$ (§4)	$\vdash^A \varphi$ (where $\vdash \varphi : A$, §4)	$\{A \mid \varphi\}$ (where $\vdash \varphi : A$, §5)	$T \leq U$ (T, U refinement types, §5)	$\mathcal{E} \vdash M : T$

Table 1. Syntactic Classes and Judgments.

can give the following refinement types to the basic stream operations:

$$\begin{aligned}
\mathsf{hd}^{\mathsf{g}} &: \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \{A \mid \varphi\} \\
\mathsf{tl}^{\mathsf{g}} &: \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \\
\mathsf{Cons}^{\mathsf{g}} &: \{A \mid \varphi\} \longrightarrow \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}
\end{aligned}$$

By using the standard typing rules for λ-abstraction and application, together with the rules to type $\mathsf{fix}(x).M$ and $\circledast$, we can type the function $\mathsf{map}^{\mathsf{g}}$ as

$$\mathsf{map}^{\mathsf{g}} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

A Manysorted Temporal Logic. Our logical language, taken with minor adaptations from [33], is *manysorted*: for each type A we have formulae *of type* A (notation $\vdash \varphi : A$), where φ selects inhabitants of A.

We use atomic modalities ($[\pi_i], [\mathsf{fold}], [\mathsf{next}], \dots$) in refinements to navigate between types (see Fig. 5, §4). For instance, a formula φ of type A_0, specifying a property over the inhabitants of A_0, can be lifted to the formula $[\pi_0]\varphi$ of type $A_0 \times A_1$, which intuitively describes those inhabitants of $A_0 \times A_1$ whose first component satisfy φ. Given a formula φ of type A, one can define its "head lift" $[\mathsf{hd}]\varphi$ of type $\mathsf{Str}^{\mathsf{g}}\, A$, that enforces φ to be satisfied on the head of the provided stream. Also, one can define a modality $\bigcirc$ such that given a formula $\psi : \mathsf{Str}^{\mathsf{g}}\, A$, the formula $\bigcirc\psi : \mathsf{Str}^{\mathsf{g}}\, A$ enforces ψ to be satisfied on the tail of the provided stream. These modalities are obtained resp. as $[\mathsf{hd}]\varphi := [\mathsf{fold}][\pi_0]\varphi$ and $\bigcirc\varphi := [\mathsf{fold}][\pi_1][\mathsf{next}]\varphi$. We similarly have atomic modalities $[\mathsf{in}_0], [\mathsf{in}_1]$ on sum types. For instance, on the type of guarded colists defined as $\mathsf{CoList}^{\mathsf{g}}\, A := \mathsf{Fix}(X).\ \mathbf{1} + A \times \blacktriangleright X$, we can express the fact that a colist is empty (resp. non-empty) with the formula $[\mathsf{nil}] := [\mathsf{fold}][\mathsf{in}_0]\top$ (resp. $[\neg\mathsf{nil}] := [\mathsf{fold}][\mathsf{in}_1]\top$).

We also provide a deduction system $\vdash^A \varphi$ on temporal modal formulae. This deduction system is used to define a subtyping relation $T \leq U$ between refinement types, with $\{A \mid \varphi\} \leq \{A \mid \psi\}$ when $\vdash^A \varphi \Rightarrow \psi$. The subtyping relation thus incorporates logical reasoning in the type system.

In addition, we have greatest fixpoints formulae $\nu\alpha\varphi$ (so that formulae can have free typed propositional variables), equipped with Kozen's reasoning principles [47]. In particular, we can form an *always* modality as $\Box\varphi := \nu\alpha.\ \varphi \wedge \bigcirc\alpha$, with $\Box\varphi : \mathsf{Str}^{\mathsf{g}}\, A$ if $\varphi : \mathsf{Str}^{\mathsf{g}}\, A$. The formula $\Box\varphi$ holds on a stream $s = (s_i \mid i \geq 0)$, iff φ holds on every substream $(s_i \mid i \geq n)$ for $n \geq 0$. If we rather start with $\psi : A$, one first need to lift it to $[\mathsf{hd}]\psi : \mathsf{Str}^{\mathsf{g}}\, A$. Then $\Box[\mathsf{hd}]\psi$ means that all the elements of the stream satisfies ψ, since all its suffixes satisfy $[\mathsf{hd}]\psi$.

Table 1 summarizes the different judgments used in this paper.

Beyond Safety. In order to handle liveness properties, we also need to have least fixpoints formulae $\mu\alpha\varphi$. For example, this would give the *eventually* modality $\Diamond\varphi := \mu\alpha.\ \varphi \vee \bigcirc\alpha$. With Kozen-style rules, one could then give the following two types to the guarded stream constructor:

$$\begin{array}{l}\mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi\} \longrightarrow \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond[\mathsf{hd}]\varphi\} \\ \mathsf{Cons}^{\mathsf{g}} : A \longrightarrow \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond[\mathsf{hd}]\varphi\}\end{array}$$

But consider a finite base type $\mathtt{B}$ with two distinguished elements $\mathtt{a}, \mathtt{b}$, and suppose that we have access to a modality $[\mathtt{b}]$ on $\mathtt{B}$ so that terms inhabiting $\{\mathtt{B} \mid [\mathtt{b}]\}$ must be equal to $\mathtt{b}$. Using the above types for $\mathsf{Cons}^{\mathsf{g}}$, we could type the stream with constant value $\mathtt{a}$, defined as $\mathsf{fix}(s).\mathtt{a} ::^{\mathsf{g}} s$, with the type $\{\mathsf{Str}^{\mathsf{g}}\, \mathtt{B} \mid \Diamond[\mathsf{hd}][\mathtt{b}]\}$ that is supposed to enforce the existence of an occurrence of $\mathtt{b}$ in the stream. Similarly, on colists we would have $\mathsf{fix}(s).\mathtt{a} ::^{\mathsf{g}} s$ of type $\{\mathsf{CoList}^{\mathsf{g}}\, \mathtt{B} \mid \Diamond[\mathsf{nil}]\}$, while $\Diamond[\mathsf{nil}]$ expresses that a colist will eventually contain a nil, and is thus finite. Hence, liveness properties may interact quite badly with guarded recursion. Let us look at this in a semantic model of guarded recursion.

***Internal* Semantics in the Topos of Trees.** The types of the guarded λ-calculus can be interpreted as sequences of sets $(X(n))_{n>0}$ where $X(n)$ represents the values available "at time n". In order to interpret guarded recursion, one also needs to have access to functions $r^X_n : X(n+1) \to X(n)$, which tell how values "at $n+1$" can be restricted (actually most often truncated) to values "at n". This means that the objects used to represent types are in fact *presheaves* over the poset $(\mathbb{N} \setminus \{0\}, \leq)$. The category $\mathcal{S}$ of such presheaves is the *topos of trees* [13]. For instance, the type $\mathsf{Str}^{\mathsf{g}}\, \mathtt{B}$ of guarded streams over a finite base type $\mathtt{B}$ is interpreted in $\mathcal{S}$ as $(\mathtt{B}^n)_{n>0}$, with restriction maps taking $(\mathtt{b}_0, \ldots, \mathtt{b}_{n-1}, \mathtt{b}_n)$ to $(\mathtt{b}_0, \ldots, \mathtt{b}_{n-1})$. We write $[\![A]\!]$ for the interpretation of a type A in $\mathcal{S}$.

The Necessity of an *External* Semantics. The topos of trees cannot correctly handle liveness properties. For instance, the formula $\Diamond[\mathsf{hd}][\mathtt{b}]$ cannot describe in $\mathcal{S}$ the set of streams that contain at least one occurrence of $\mathtt{b}$. Indeed, the interpretation of $\Diamond[\mathsf{hd}][\mathtt{b}]$ in $\mathcal{S}$ is a sequence $(C(n))_{n>0}$ with $C(n) \subseteq \mathtt{B}^n$. But any element of $\mathtt{B}^n$ can be extended to a stream which contains an occurrence of $\mathtt{b}$. Hence $C(n)$ should be equal to $\mathtt{B}^n$, and the interpretation of $\Diamond[\mathsf{hd}][\mathtt{b}]$ is the whole $[\![\mathsf{Str}^{\mathsf{g}}\, \mathtt{B}]\!]$. More generally, guarded fixpoints have unique solutions in the topos of trees [13], and $\Diamond\varphi = \mu\alpha.\ \varphi \vee \bigcirc\varphi$ gets the same interpretation as $\nu\alpha.\ \varphi \vee \bigcirc\alpha$.

We thus have a formal system with least and greatest fixpoints, that has a semantics inside the topos of trees, but which does not correctly handle least fixpoints. On the other hand, it was shown by [55] that the interpretation of guarded polynomial (*i.e.* first-order) recursive types in $\mathcal{S}$ induces final coalgebras for the corresponding polynomial functors on the category **Set** of usual sets and functions. This applies e.g. to streams and colists. Hence, it makes sense to think of interpreting least fixpoint formulae over such types *externally*, in **Set**.

Internal **External**

$$\begin{tikzcd} \mathcal{S} \arrow[loop left, "\nu"] \arrow[rr, bend left, "\boldsymbol{\Gamma}"] \arrow[rr, phantom, "\top"] & & \mathbf{Set} \arrow[ll, bend left, "\boldsymbol{\Delta}"] \arrow[loop right, "\nu{,}\mu"] \end{tikzcd}$$

$[\![\varphi]\!]$ subobject of $[\![A]\!]$ $\{|\varphi|\}$ subset of $\boldsymbol{\Gamma}[\![A]\!]$

$$[\![\blacksquare A]\!] := \boldsymbol{\Delta}\boldsymbol{\Gamma}[\![A]\!]$$
$$[\![[\mathsf{box}]\varphi]\!] := \boldsymbol{\Delta}\,\{|\varphi|\} \quad (\varphi : A,\ [\mathsf{box}]\varphi : \blacksquare A)$$
$$\{|\varphi|\} \;=\; \boldsymbol{\Gamma}[\![\varphi]\!] \qquad \text{(if } \varphi \text{ is safe)}$$

Fig. 2. Internal and External Semantics

The Constant Type Modality. Figure 2 represents adjoint functors $\boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ and $\boldsymbol{\Delta} : \mathbf{Set} \to \mathcal{S}$. To correctly handle least fixpoints $\mu\alpha\varphi : A$, we would like to see them as subsets of $\boldsymbol{\Gamma}[\![A]\!]$ in $\mathbf{Set}$ rather than subobjects of $[\![A]\!]$ in $\mathcal{S}$. On the other hand, the internal semantics in $\mathcal{S}$ is still necessary to handle definitions by guarded recursion. We navigate between the internal semantics in $\mathcal{S}$ and the external semantics in $\mathbf{Set}$ via the adjunction $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$. This adjunction induces a comonad $\boldsymbol{\Delta}\boldsymbol{\Gamma}$ on $\mathcal{S}$, which is represented in the guarded λ-calculus of [20] by the *constant* type modality $\blacksquare$. This gives *coinductive* versions of guarded recursive types, e.g. $\mathsf{Str}\,A := \blacksquare\,\mathsf{Str}^{\mathsf{g}}\,A$ for streams and $\mathsf{CoList}\,A := \blacksquare\,\mathsf{CoList}^{\mathsf{g}}\,A$ for colists, which allow for productive but not causal programs [20, Ex. 1.10.(3)].

Each formula gets two interpretations: $[\![\varphi]\!]$ in $\mathcal{S}$ and $\{|\varphi|\}$ in $\mathbf{Set}$. The external semantics $\{|\varphi|\}$ handles least fixpoints in the standard set-theoretic way, thus the two interpretations differ in general. But we do have $\{|\varphi|\} = \boldsymbol{\Gamma}[\![\varphi]\!]$ when φ is *safe* (Def. 6.5), that is, when φ describes a safety property. We have a modality $[\mathsf{box}]\varphi$ which lifts $\varphi : A$ to $\blacksquare A$. By defining $[\![[\mathsf{box}]\varphi]\!] := \boldsymbol{\Delta}\,\{|\varphi|\}$, we correctly handle the least fixpoints which are guarded by a $[\mathsf{box}]$ modality. When φ is safe, we can navigate between $\{\blacksquare A \mid [\mathsf{box}]\varphi\}$ and $\blacksquare\,\{A \mid \varphi\}$, thus making available the comonad structure of $\blacksquare$ on $[\mathsf{box}]\varphi$. Note that $[\mathsf{box}]$ is unrelated to $\Box$.

Approximating Least Fixpoints. For proving liveness properties on functions defined by guarded recursion, one needs to navigate between e.g. $[\mathsf{box}]\Diamond\varphi$ and $\Diamond\varphi$, while $\Diamond\varphi$ is in general unsafe. The fixpoint $\Diamond\varphi = \mu\alpha.\varphi \vee \bigcirc\alpha$ is *alternation-free* (see e.g. [17, §4.1]). This implies that $\Diamond\varphi$ can be seen as the supremum of the $\bigcirc^m\varphi$ for $m \in \mathbb{N}$, where each $\bigcirc^m\varphi$ is safe when φ is safe. More generally, we can approximate alternation-free $\mu\alpha\varphi$ by their finite unfoldings $\varphi^m(\bot)$, *à la* Kleene. We extend the logic with finite iterations $\mu^k\alpha\varphi$, where k is an *iteration variable*, and where $\mu^k\alpha\varphi$ is seen as $\varphi^k(\bot)$. Let $\Diamond^k\varphi := \mu^k\alpha.\ \varphi\vee\bigcirc\alpha$. If φ is safe then so is $\Diamond^k\varphi$. For safe φ, ψ, we have the following refinement typings for the guarded recursive $\mathsf{map}^{\mathsf{g}}$ and its coinductive lift map:

$$\begin{array}{ll} \mathsf{map}^{\mathsf{g}} & : (\{B \mid \psi\} \to \{A \mid \varphi\}) \to \left\{\mathsf{Str}^{\mathsf{g}}\,B \;\middle|\; \Diamond^k[\mathsf{hd}]\psi\right\} \quad\; \to \left\{\mathsf{Str}^{\mathsf{g}}\,A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\} \\ \mathsf{map} & : (\{B \mid \psi\} \to \{A \mid \varphi\}) \to \{\mathsf{Str}\,B \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\psi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \end{array}$$

3 The Pure Calculus

Our system lies on top of the guarded λ-calculus of [20]. We briefly review it here. We consider values and terms from the grammar given in Fig. 3 (left). In

$$
\begin{array}{lll}
v \ ::= & M, N \ ::= \ v \mid x & E \ ::= \ \bullet \\
\mid \lambda x.M & \mid MN & \mid EM \\
\mid \langle M_0, M_1 \rangle & \mid \pi_0(M) & \mid \pi_0(E) \\
\mid \langle\rangle & \mid \pi_1(M) & \mid \pi_1(E) \\
\mid \mathsf{in}_0(M) & \mid \mathsf{case}\, M \,\mathsf{of} & \mid \mathsf{case}\, E \,\mathsf{of} \\
\mid \mathsf{in}_1(M) & \quad (x.M_0|x.M_1) & \quad (x.M_0|x.M_1) \\
\mid \mathsf{fold}(M) & \mid \mathsf{unfold}(M) & \mid \mathsf{unfold}(E) \\
\mid \mathsf{box}_\sigma(M) & \mid \mathsf{unbox}(M) & \mid \mathsf{unbox}(E) \\
\mid \mathsf{next}(M) & \mid \mathsf{prev}_\sigma(M) & \mid \mathsf{prev}_{[]}(E) \\
 & \mid M \circledast N & \mid E \circledast M \\
 & \mid \mathsf{fix}(x).M & \mid v \circledast E
\end{array}
$$

$$
\begin{array}{rcl}
(\lambda x.M)N & \rightsquigarrow & M[N/x] \\
\pi_i(\langle M_0, M_1 \rangle) & \rightsquigarrow & M_i \\
\mathsf{case}\,\mathsf{in}_i(M)\,\mathsf{of}\,(x.N_0|x.N_1) & \rightsquigarrow & N_i[M/x] \\
\mathsf{unfold}(\mathsf{fold}(M)) & \rightsquigarrow & M \\
\mathsf{fix}(x).M & \rightsquigarrow & M[\mathsf{next}(\mathsf{fix}(x).M)/x] \\
\mathsf{next}(M) \circledast \mathsf{next}(N) & \rightsquigarrow & \mathsf{next}(MN) \\
\mathsf{unbox}(\mathsf{box}_\sigma(M)) & \rightsquigarrow & M\sigma \\
\mathsf{prev}_{[]}(\mathsf{next}(M)) & \rightsquigarrow & M \\
\mathsf{prev}_\sigma(M) & \rightsquigarrow & \mathsf{prev}_{[]}(M\sigma) \quad (\sigma \neq [])
\end{array}
$$

$$
\frac{M \ \rightsquigarrow \ N}{E[M] \ \rightsquigarrow \ E[N]}
$$

Fig. 3. Syntax and Operational Semantics of the Pure Calculus.

both $\mathsf{box}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$, σ is a *delayed substitution* of the form $\sigma = [x_1 \mapsto M_1, \dots, x_k \mapsto M_k]$ and such that $\mathsf{box}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$ bind $x_1, \dots, x_k$ in M. We use the following conventions of [20]: $\mathsf{box}(M)$ and $\mathsf{prev}(M)$ (without indicated substitution) stand resp. for $\mathsf{box}_{[]}(M)$ and $\mathsf{prev}_{[]}(M)$ *i.e.* bind no variable of M. Moreover, $\mathsf{box}_\iota(M)$ stands for $\mathsf{box}_{[x_1 \mapsto x_1, \dots, x_k \mapsto x_k]}(M)$ where $x_1, \dots, x_k$ is a list of all free variables of M, and similarly for $\mathsf{prev}_\iota(M)$. We consider the weak call-by-name reduction of [20], recalled in Fig. 3 (right).

Pure types (notation $A, B,$ etc.) are the closed types over the grammar

$$A \ ::= \ \mathbf{1} \mid A + A \mid A \times A \mid A \to A \mid \blacktriangleright A \mid X \mid \mathsf{Fix}(X).A \mid \blacksquare A$$

where, (1) in the case $\mathsf{Fix}(X).A$, each occurrence of X in A must be guarded by a $\blacktriangleright$, and (2) in the case of $\blacksquare A$, the type A is closed (*i.e.* has no free type variable). Guarded recursive types are built with the fixpoint constructor $\mathsf{Fix}(X).A$, which allows for X to appear in A both at positive and negative positions, but only under a $\blacktriangleright$. In this paper we shall only consider positive types.

Example 3.1. We can code a finite base type $\mathtt{B} = \{\mathtt{b}_1, \dots, \mathtt{b}_n\}$ as a sum of unit types $\sum_{i=1}^{n} \mathbf{1} = \mathbf{1} + (\cdots + \mathbf{1})$, where the ith component of the sum is intended to represent the element $\mathtt{b}_i$ of $\mathtt{B}$. At the term level, the elements of $\mathtt{B}$ are represented as compositions of injections $\mathsf{in}_{j_1}(\mathsf{in}_{j_2}(\dots \mathsf{in}_{j_i}\langle\rangle))$. For instance, Booleans are represented by $\mathsf{Bool} := \mathbf{1} + \mathbf{1}$, with $\mathsf{tt} := \mathsf{in}_0(\langle\rangle)$ and $\mathsf{ff} := \mathsf{in}_1(\langle\rangle)$.

Example 3.2. Besides streams ($\mathsf{Str}^{\mathsf{g}}\, A$), colists ($\mathsf{CoList}^{\mathsf{g}}\, A$), conatural numbers ($\mathsf{CoNat}^{\mathsf{g}}$) and infinite binary trees ($\mathsf{Tree}^{\mathsf{g}}\, A$), we consider a type $\mathsf{Res}^{\mathsf{g}}\, A$ of *resumptions* (parametrized by $\mathtt{I}, \mathtt{O}$) adapted from [48], and a higher-order recursive type $\mathsf{Rou}^{\mathsf{g}}\, A$, used in Martin Hofmann's breadth-first tree traversal (see e.g. [10]):

$$
\begin{array}{rlrl}
\mathsf{Tree}^{\mathsf{g}}\, A := & \mathsf{Fix}(X).\ A \times (\blacktriangleright X \times \blacktriangleright X) & \mathsf{CoNat}^{\mathsf{g}} := & \mathsf{Fix}(X).\ \mathbf{1} + \blacktriangleright X \\
\mathsf{Res}^{\mathsf{g}}\, A := & \mathsf{Fix}(X).\ A + (\mathtt{I} \to (\mathtt{O} \times \blacktriangleright X)) & \mathsf{Rou}^{\mathsf{g}}\, A := & \mathsf{Fix}(X).\ \mathbf{1} + ((\blacktriangleright X \to \blacktriangleright A) \to A)
\end{array}
$$

Some typing rules of the pure calculus are given in Fig. 4, where a pure type A is *constant* if each occurrence of $\blacktriangleright$ in A is guarded by a $\blacksquare$ modality. The omitted rules are the standard ones for simple types with finite sums and products (§A).

$$\frac{\mathcal{E} \vdash M : A[\mathsf{Fix}(X).A/X]}{\mathcal{E} \vdash \mathsf{fold}(M) : \mathsf{Fix}(X).A} \qquad \frac{\mathcal{E} \vdash M : \mathsf{Fix}(X).A}{\mathcal{E} \vdash \mathsf{unfold}(M) : A[\mathsf{Fix}(X).A/X]} \qquad \frac{\mathcal{E} \vdash M : \blacktriangleright(B \to A) \qquad \mathcal{E} \vdash N : \blacktriangleright B}{\mathcal{E} \vdash M \circledast N : \blacktriangleright A}$$

$$\frac{\mathcal{E} \vdash M : A}{\mathcal{E} \vdash \mathsf{next}(M) : \blacktriangleright A} \qquad \frac{x_1 : A_1, \dots, x_k : A_k \vdash M : \blacktriangleright A \qquad \mathcal{E} \vdash M_i : A_i \text{ with } A_i \text{ constant for } 1 \le i \le k}{\mathcal{E} \vdash \mathsf{prev}_{[x_1 \mapsto M_1, \dots, x_k \mapsto M_k]}(M) : A}$$

$$\frac{x_1 : A_1, \dots, x_k : A_k \vdash M : A \qquad \mathcal{E} \vdash M_i : A_i \text{ with } A_i \text{ constant for } 1 \le i \le k}{\mathcal{E} \vdash \mathsf{box}_{[x_1 \mapsto M_1, \dots, x_k \mapsto M_k]}(M) : \blacksquare A} \qquad \frac{\mathcal{E} \vdash M : \blacksquare A}{\mathcal{E} \vdash \mathsf{unbox}(M) : A}$$

Fig. 4. Typing Rules of the Pure Calculus (excerpt).

Example 3.3. Figure 1 defines some operations on guarded streams. On other types of Ex. 3.2, we have e.g. the constructors of colists $\mathsf{Nil}^{\mathsf{g}} := \mathsf{fold}(\mathsf{in}_0\langle\rangle) : \mathsf{CoList}^{\mathsf{g}}\,A$ and $\mathsf{Cons}^{\mathsf{g}} := \lambda x.\lambda xs.\mathsf{fold}(\mathsf{in}_1\langle x, xs\rangle) : A \to \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\,A \to \mathsf{CoList}^{\mathsf{g}}\,A$. Infinite binary trees $\mathsf{Tree}^{\mathsf{g}}\,A$ have operations $\mathsf{son}^{\mathsf{g}}_d : \mathsf{Tree}^{\mathsf{g}}\,A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A$ for $d \in \{\ell, r\}$, $\mathsf{Node}^{\mathsf{g}} : A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A \to \mathsf{Tree}^{\mathsf{g}}\,A$ and $\mathsf{label}^{\mathsf{g}} : \mathsf{Tree}^{\mathsf{g}}\,A \to A$.

Example 3.4. Coinductive types are guarded recursive types under a $\blacksquare$. For instance $\mathsf{Str}\,A := \blacksquare\,\mathsf{Str}^{\mathsf{g}}\,A$, $\mathsf{CoList}\,A := \blacksquare\,\mathsf{CoList}^{\mathsf{g}}\,A$, $\mathsf{CoNat} := \blacksquare\,\mathsf{CoNat}^{\mathsf{g}}$ and $\mathsf{Res}\,A := \blacksquare\,\mathsf{Res}^{\mathsf{g}}\,A$, with A, $\mathtt{I}$, $\mathtt{O}$ *constant.* Basic operations on guarded types lift to coinductive ones. For instance

$$\begin{aligned}
\mathsf{Cons} &:= \lambda x.\lambda s.\mathsf{box}_\iota\big(\mathsf{Cons}^{\mathsf{g}}\ x\ \mathsf{next}(\mathsf{unbox}\ s)\big) && : A \to \mathsf{Str}\,A \to \mathsf{Str}\,A \\
\mathsf{hd} &:= \lambda s.\mathsf{hd}^{\mathsf{g}}\ (\mathsf{unbox}\ s) && : \mathsf{Str}\,A \to A \\
\mathsf{tl} &:= \lambda s.\mathsf{box}_\iota\big(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))\big) && : \mathsf{Str}\,A \to \mathsf{Str}\,A
\end{aligned}$$

These definitions follow a general pattern to lift a function over a guarded recursive type into one over its coinductive version, by performing an η-expansion with some box and unbox inserted in the right places. For example, one can define the map function on coinductive streams as:

$$\mathsf{map} := \lambda f.\lambda s.\mathsf{box}_\iota\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)\big) : (B \to A) \longrightarrow \mathsf{Str}\,B \longrightarrow \mathsf{Str}\,A$$

4 A Temporal Modal Logic

We present here a logic of (modal) temporal specifications. We focus on syntactic aspects. The semantics is discussed in §7. For the moment the logic has only one form of fixpoints ($\nu\alpha\varphi$). It is extended with least fixpoints ($\mu\alpha\varphi$) in §6.

Manysorted Modal Temporal Formulae. The main ingredient of this paper is the logical language we use to annotate pure types when forming refinement types. This language, that we took with minor adaptations from [33], is *manysorted*: for each pure type A we have formulae φ *of type* A (notation $\vdash \varphi : A$). The formulation rules of formulae are given in Fig. 5.

Example 4.1. Given a finite base type $\mathtt{B} = \{\mathtt{b}_1, \dots, \mathtt{b}_n\}$ as in Ex. 3.1, with element $\mathtt{b}_i$ represented by $\mathsf{in}_{j_1}(\mathsf{in}_{j_2}(\dots \mathsf{in}_{j_i}\langle\rangle))$, the formula $[\mathsf{in}_{j_1}][\mathsf{in}_{j_2}]\dots[\mathsf{in}_{j_i}]\top$ represents the singleton subset $\{\mathtt{b}_k\}$ of $\mathtt{B}$. On Bool, we have the formulae $[\mathsf{tt}] := [\mathsf{in}_0]\top$ and $[\mathsf{ff}] := [\mathsf{in}_1]\top$ representing resp. $\mathtt{tt}$ and $\mathtt{ff}$.

$$\frac{(\alpha : A) \in \Sigma}{\Sigma \vdash \alpha : A} \qquad \frac{}{\Sigma \vdash \bot : A} \qquad \frac{}{\Sigma \vdash \top : A} \qquad \frac{\Sigma \vdash \varphi : A}{\Sigma, \alpha : B \vdash \varphi : A}$$

$$\frac{\Sigma \vdash \varphi : A \qquad \Sigma \vdash \psi : A}{\Sigma \vdash \varphi \Rightarrow \psi : A} \qquad \frac{\Sigma \vdash \varphi : A \qquad \Sigma \vdash \psi : A}{\Sigma \vdash \varphi \wedge \psi : A} \qquad \frac{\Sigma \vdash \varphi : A \qquad \Sigma \vdash \psi : A}{\Sigma \vdash \varphi \vee \psi : A}$$

$$\frac{\Sigma \vdash \varphi : A_i}{\Sigma \vdash [\pi_i]\varphi : A_0 \times A_1} \qquad \frac{\Sigma \vdash \varphi : A_i}{\Sigma \vdash [\mathsf{in}_i]\varphi : A_0 + A_1} \qquad \frac{\Sigma \vdash \psi : B \quad \Sigma \vdash \varphi : A}{\Sigma \vdash [\mathsf{ev}(\psi)]\varphi : B \to A}$$

$$\frac{\Sigma \vdash \varphi : A[\mathsf{Fix}(X).A/X]}{\Sigma \vdash [\mathsf{fold}]\varphi : \mathsf{Fix}(X).A} \qquad \frac{\Sigma \vdash \varphi : A}{\Sigma \vdash [\mathsf{next}]\varphi : \blacktriangleright A} \qquad \frac{\vdash \varphi : A}{\vdash [\mathsf{box}]\varphi : \blacksquare A}$$

$$(\nu\text{-F})\ \frac{\Sigma, \alpha : A \vdash \varphi : A \qquad \alpha \text{ Pos } \varphi}{\Sigma \vdash \nu\alpha\varphi : A}\ (\alpha \text{ guarded in } \varphi)$$

Fig. 5. Formation Rules of Formulae (where A, B are pure types).

Example 4.2. (a) The formula $[\mathsf{hd}][\mathsf{a}] \Rightarrow \bigcirc[\mathsf{hd}][\mathsf{b}]$ means that if the head of a stream is $\mathtt{a}$, then its second element (the head of its tail) should be $\mathtt{b}$.

(b) On colists, we let $[\mathsf{hd}]\varphi := [\mathsf{fold}][\mathsf{in}_1][\pi_0]\varphi$ and $\bigcirc\psi := [\mathsf{fold}][\mathsf{in}_1][\pi_1][\mathsf{next}]\psi$.

(c) On (guarded) infinite binary trees over A, we also have a modality $[\mathsf{lbl}]\varphi := [\mathsf{fold}][\pi_0]\varphi : \mathsf{Tree}^{\mathsf{g}}\,A$ (provided $\varphi : A$). Moreover, we have modalities $\bigcirc_\ell$ and $\bigcirc_r$ defined on formulae $\varphi : \mathsf{Tree}^{\mathsf{g}}\,A$ as $\bigcirc_\ell\varphi := [\mathsf{fold}][\pi_1][\pi_0][\mathsf{next}]\varphi$ and $\bigcirc_r\varphi := [\mathsf{fold}][\pi_1][\pi_1][\mathsf{next}]\varphi$. Intuitively, $[\mathsf{lbl}]\varphi$ should hold on a tree t over A iff the root label of t satisfies φ, and $\bigcirc_\ell\varphi$ (resp. $\bigcirc_r\varphi$) should hold on t iff φ holds on the left (resp. right) immediate subtree of t.

Formulae have fixpoints $\nu\alpha\varphi$. The rules of Fig. 5 thus allow for the formation of formulae with free typed propositional variables (ranged over by $\alpha, \beta, \dots$), and involve contexts Σ of the form $\alpha_1 : A_1, \dots, \alpha_n : A_n$. In the formation of a fixpoint, the side condition "α guarded in φ" asks that each occurrence of α is beneath a $[\mathsf{next}]$ modality. Because we are ultimately interested in the *external* set-theoretic semantics of formulae, we assume a usual positivity condition of α in φ. It is defined with relations α Pos φ and α Neg φ (see App. B). We just mention here that $[\mathsf{ev}(-)](-)$ is contravariant in its first argument. Note that $[\mathsf{box}]\varphi$ can only be formed for *closed* φ.

Example 4.3. (a) The modality $\Box$ makes it possible to express a range of safety properties. For instance, assuming $\varphi, \psi : \mathsf{Str}^{\mathsf{g}}\,A$, the formula $\Box(\psi \Rightarrow \bigcirc\varphi)$ is intended to hold on a stream $s = (s_i \mid i \geq 0)$ iff, for all $n \in \mathbb{N}$, if $(s_i \mid i \geq n)$ satisfies ψ, then $(s_i \mid i \geq n+1)$ satisfies φ.

(b) The modality $\Box$ has its two CTL-like variants on $\mathsf{Tree}^{\mathsf{g}}\,A$, namely $\forall\Box\varphi := \nu\alpha.\ \varphi \wedge (\bigcirc_\ell\alpha \wedge \bigcirc_r\alpha)$ and $\exists\Box\varphi := \nu\alpha.\ \varphi \wedge (\bigcirc_\ell\alpha \vee \bigcirc_r\alpha)$. Assuming $\psi : A$, $\forall\Box[\mathsf{lbl}]\psi$ is intended to hold on a tree $t : \mathsf{Tree}^{\mathsf{g}}\,A$ iff all node-labels of t satisfy ψ, while $\exists\Box[\mathsf{lbl}]\psi$ holds on t iff ψ holds on all nodes of *some* infinite path from the root of t.

Name	Formulation	$[\pi_i]$	$[\mathsf{fold}]$	$[\mathsf{next}]$	$[\mathsf{in}_i]$	$[\mathsf{ev}(\psi)]$	$[\mathsf{box}]$	$[\mathsf{hd}]$	$\bigcirc$
(RM)	$\dfrac{\vdash \psi \Rightarrow \varphi}{\vdash [\triangle]\psi \Rightarrow [\triangle]\varphi}$	✓	✓	✓	✓	✓	✓	✓	✓
(C)	$[\triangle]\varphi \wedge [\triangle]\psi \implies [\triangle](\varphi \wedge \psi)$	✓	✓	✓	✓	✓	✓	✓	✓
(N)	$[\triangle]\top$	✓	✓	✓		✓	✓	✓	✓
(P)	$[\triangle]\bot \implies \bot$	✓	✓	**(C)**	✓		✓	✓	**(C)**
($\mathsf{C}_\vee$)	$[\triangle](\varphi \vee \psi) \implies [\triangle]\varphi \vee [\triangle]\psi$	✓	✓	✓	✓		✓	✓	✓
($\mathsf{C}_\Rightarrow$)	$([\triangle]\psi \Rightarrow [\triangle]\varphi) \Rightarrow [\triangle](\psi \Rightarrow \varphi)$	✓	✓	**(C)**			✓	✓	**(C)**

Table 2. Modal Axioms and Rules. Types are omitted in $\vdash$ and **(C)** marks axioms assumed for $\vdash_c$ but not for $\vdash$. Properties of the non-atomic $[\mathsf{hd}]$ and $\bigcirc$ are derived.

Modal Theories. Formulae are equipped with a modal deduction system which enters the type system via a subtyping relation (§5). For each pure type A, we have an intuitionistic theory $\vdash^A$ (the general case) and a classical theory $\vdash^A_c$ (which is only assumed under $\blacksquare/[\mathsf{box}]$), summarized in Fig. 6 and Table 2 (where we also give properties of the derived modalities $[\mathsf{hd}]$, $\bigcirc$). In any case, $\vdash^A_{(c)} \varphi$ is only defined when $\vdash \varphi : A$ (and so when φ has no free propositional variable).

Fixpoints $\nu\alpha\varphi$ are equipped with their usual Kozen axioms [47]. The atomic modalities $[\pi_i]$, $[\mathsf{fold}]$, $[\mathsf{next}]$, $[\mathsf{in}_i]$ and $[\mathsf{box}]$ have deterministic branching (see Fig. 12, §7). We can get the axioms of the intuitionistic (normal) modal logic **IK** [61] (see also e.g. [65,53]) for $[\pi_i]$, $[\mathsf{fold}]$ and $[\mathsf{box}]$ but not for $[\mathsf{in}_i]$ nor for the intuitionistic $[\mathsf{next}]$. For $[\mathsf{next}]$, in the intuitionistic case this is due to semantic issues with step indexing (discussed in §7) which are absent from the classical case. As for $[\mathsf{in}_i]$, we have a logical theory allowing for a coding of finite base types as finite sum types, which allows to derive, for a finite base type $\mathtt{B}$:

$$\vdash^{\mathsf{B}} \quad \bigvee_{\mathsf{a}\in\mathsf{B}} \left([\mathsf{a}] \quad \wedge \quad \bigwedge_{\substack{\mathsf{b}\in\mathsf{B}\\ \mathsf{b}\neq\mathsf{a}}} \neg[\mathsf{b}]\right)$$

Definition 4.4 (Modal Theories). *For each pure type A, the* intuitionistic *and* classical *modal theories $\vdash^A \varphi$ and $\vdash^A_c \varphi$ (where $\vdash \varphi : A$) are defined by mutual induction:*

- *The theory $\vdash^A$ is deduction for intuitionistic propositional logic augmented with the check-marked (✓) axioms and rules of Table 2 and the axioms and rules of Fig. 6 (for $\vdash^A$).*
- *The theory $\vdash^A_c$ is $\vdash^A$ augmented with the axioms* (P) *and* ($\mathsf{C}_\Rightarrow$) *for* $[\mathsf{next}]$ *and with the axiom* (CL) *(Fig. 6).*

For example, we have $\vdash^{\mathsf{Str}^{\mathsf{g}}\,A} \Box\psi \Rightarrow (\psi \wedge \bigcirc\Box\psi)$ and $\vdash^{\mathsf{Str}^{\mathsf{g}}\,A} (\psi \wedge \bigcirc\Box\psi) \Rightarrow \Box\psi$.

$$\frac{\vdash^{B} \psi \Rightarrow \phi \qquad \vdash \varphi : A}{\vdash^{B \to A} [\mathsf{ev}(\phi)]\varphi \Rightarrow [\mathsf{ev}(\psi)]\varphi} \qquad \frac{}{\vdash^{B \to A} ([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi) \Rightarrow [\mathsf{ev}(\psi_0 \vee \psi_1)]\varphi}$$

$$\frac{}{\vdash^{A}_{c} ((\varphi \Rightarrow \psi) \Rightarrow \varphi) \Rightarrow \varphi}\ (\mathsf{CL}) \qquad \frac{\vdash^{A}_{c} \varphi}{\vdash^{\blacksquare A} [\mathsf{box}]\varphi} \qquad \frac{}{\vdash^{A_0 + A_1} \big([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\big) \wedge \neg\big([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\big)}$$

$$\frac{}{\vdash^{A_0 + A_1} ([\mathsf{in}_i]\top) \Rightarrow (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)} \qquad \frac{}{\vdash^{A} \nu\alpha\varphi \Rightarrow \varphi[\nu\alpha\varphi/\alpha]} \qquad \frac{\vdash^{A} \psi \Rightarrow \varphi[\psi/\alpha]}{\vdash^{A} \psi \Rightarrow \nu\alpha\varphi}$$

Fig. 6. Modal Axioms and Rules.

$$\frac{}{T \leq |T|} \qquad \frac{}{A \leq \{A \mid \top\}} \qquad \frac{\vdash^{A} \varphi \Rightarrow \psi}{\{A \mid \varphi\} \leq \{A \mid \psi\}} \qquad \frac{\vdash^{A}_{c} \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathsf{box}]\varphi\} \leq \{\blacksquare A \mid [\mathsf{box}]\psi\}}$$

$$\frac{}{\{\blacktriangleright A \mid [\mathsf{next}]\varphi\} \equiv \blacktriangleright \{A \mid \varphi\}} \qquad \frac{}{\{B \to A \mid [\mathsf{ev}(\psi)]\varphi\} \equiv \{B \mid \psi\} \to \{A \mid \varphi\}}$$

Fig. 7. Subtyping Rules (excerpt).

5 A Temporally Refined Type System

Temporal refinement types (or *types*), notation T, U, V, etc., are defined by:

$$T, U ::= A \mid \{A \mid \varphi\} \mid T + T \mid T \times T \mid T \to T \mid \blacktriangleright T \mid \blacksquare T$$

where $\vdash \varphi : A$ and, in the case of $\blacksquare T$, the type T has no free type variable. So types are built from (closed) pure types A and temporal refinements $\{A \mid \varphi\}$. They allow for all the type constructors of pure types.

As a refinement type $\{A \mid \varphi\}$ intuitively represents a subset of the inhabitants of A, it is natural to equip our system with a notion of *subtyping*. In addition to the usual rules for product, arrow and sum types, our subtyping relation is made of two more ingredients. The first follows the principle that our refinement type system is meant to prove properties of programs, and not to type more programs, so that (say) a type of the form $\{A \mid \varphi\} \to \{B \mid \psi\}$ is a subtype of $A \to B$. We formalize this with the notion of *underlying pure type* $|T|$ of a type T. The second ingredient is the modal theory $\vdash^{A} \varphi$ of §4. The subtyping rules concerning refinements are given in Fig. 7, where $T \equiv U$ enforces both $T \leq U$ and $U \leq T$. The full set of rules is given in Fig. 17 in §C. Notice that subtyping does not incorporate (un)folding of guarded recursive types.

Typing for refinement types is given by the rules of Fig. 8, together with the rules of §3 *extended to refinement types*, where T is *constant* if $|T|$ is constant. Modalities $[\pi_i]$, $[\mathsf{in}_i]$, $[\mathsf{fold}]$ and $[\mathsf{ev}(-)]$ (but not $[\mathsf{next}]$) have introduction rules extending those of the corresponding term formers.

$$(\text{PI}_i\text{-I})\ \frac{\mathcal{E} \vdash M_i : \{A_i \mid \varphi\} \qquad \mathcal{E} \vdash M_{1-i} : A_{1-i}}{\mathcal{E} \vdash \langle M_0, M_1\rangle : \{A_0 \times A_1 \mid [\pi_i]\varphi\}} \qquad (\text{PI}_i\text{-E})\ \frac{\mathcal{E} \vdash M : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}{\mathcal{E} \vdash \pi_i(M) : \{A_i \mid \varphi\}}$$

$$(\text{EV-I})\ \frac{\mathcal{E}, x : \{B \mid \psi\} \vdash M : \{A \mid \varphi\}}{\mathcal{E} \vdash \lambda x.M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}} \qquad (\text{EV-E})\ \frac{\mathcal{E} \vdash M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\} \qquad \mathcal{E} \vdash N : \{B \mid \psi\}}{\mathcal{E} \vdash MN : \{A \mid \varphi\}}$$

$$(\text{FD-I})\ \frac{\mathcal{E} \vdash M : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}{\mathcal{E} \vdash \mathsf{fold}(M) : \{\mathsf{Fix}(X).A \mid [\mathsf{fold}]\varphi\}} \qquad (\text{FD-E})\ \frac{\mathcal{E} \vdash M : \{\mathsf{Fix}(X).A \mid [\mathsf{fold}]\varphi\}}{\mathcal{E} \vdash \mathsf{unfold}(M) : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}$$

$$(\text{INJ}_i\text{-E})\ \frac{\mathcal{E} \vdash M : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\} \qquad \mathcal{E}, x : \{A_i \mid \varphi\} \vdash N_i : U \qquad \mathcal{E}, x : A_{1-i} \vdash N_{1-i} : U}{\mathcal{E} \vdash \mathsf{case}\, M \;\mathsf{of}\; (x.N_0 | x.N_1) : U}$$

$$(\vee\text{-E})\ \frac{\mathcal{E} \vdash M : \{A \mid \varphi_0 \vee \varphi_1\} \qquad \overset{\text{for } i \in \{0,1\},}{\mathcal{E}, x : \{A \mid \varphi_i\} \vdash N : U}}{\mathcal{E} \vdash N[M/x] : U} \qquad (\text{INJ}_i\text{-I})\ \frac{\mathcal{E} \vdash M : \{A_i \mid \varphi\}}{\mathcal{E} \vdash \mathsf{in}_i(M) : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\}}$$

$$(\text{MP})\ \frac{\mathcal{E} \vdash M : \{A \mid \psi \Rightarrow \varphi\} \quad \mathcal{E} \vdash M : \{A \mid \psi\}}{\mathcal{E} \vdash M : \{A \mid \varphi\}} \qquad (\text{EXF})\ \frac{\mathcal{E} \vdash M : \{A \mid \bot\} \quad \mathcal{E} \vdash N : |U|}{\mathcal{E} \vdash N : U}$$

$$(\text{SUB})\ \frac{\mathcal{E} \vdash M : T \quad T \leq U}{\mathcal{E} \vdash M : U}$$

Fig. 8. Typing Rules for Refined Modal Types.

Example 5.1. Since $\varphi \Rightarrow \psi \Rightarrow (\varphi \wedge \psi)$ and using two times the rule (MP), we get the first derived rule below, from which we can deduce the second one:

$$\frac{\mathcal{E} \vdash M : \{A \mid \varphi\} \quad \mathcal{E} \vdash M : \{A \mid \psi\}}{\mathcal{E} \vdash M : \{A \mid \varphi \wedge \psi\}} \qquad \frac{\mathcal{E} \vdash M : \{A \mid \varphi\} \quad \mathcal{E} \vdash N : \{B \mid \psi\}}{\mathcal{E} \vdash \langle M, N\rangle : \{A \times B \mid [\pi_0]\varphi \wedge [\pi_1]\psi\}}$$

Example 5.2. We have the following derived rules:

$$\frac{\mathcal{E} \vdash M : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box\varphi\}}{\mathcal{E} \vdash M : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi \wedge \bigcirc\Box\varphi\}} \qquad \text{and} \qquad \frac{\mathcal{E} \vdash M : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi \wedge \bigcirc\Box\varphi\}}{\mathcal{E} \vdash M : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box\varphi\}}$$

Example 5.3. We have $\mathsf{Cons}^{\mathsf{g}} : A \to \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \to \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\}$ as well as $\mathsf{tl}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \to \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\}$.

Example 5.4 ("Always" ($\Box$) on Guarded Streams). The refined types of $\mathsf{Cons}^{\mathsf{g}}$, hd^{g}, tl^{g} and $\mathsf{map}^{\mathsf{g}}$ mentioned in §2 are easy to derive. We also have the type

$$\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi_0\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi_1\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\mathsf{hd}]\varphi_0 \vee [\mathsf{hd}]\varphi_1)\}$$

for the $\mathsf{merge}^{\mathsf{g}}$ function which takes two guarded streams and interleaves them:

$$\begin{array}{ll} \mathsf{merge}^{\mathsf{g}} : & \mathsf{Str}^{\mathsf{g}}\, A \longrightarrow \mathsf{Str}^{\mathsf{g}}\, A \longrightarrow \mathsf{Str}^{\mathsf{g}}\, A \\ & := \mathsf{fix}(g).\lambda s_0.\lambda s_1.\ (\mathsf{hd}^{\mathsf{g}}\ s_0) ::^{\mathsf{g}} \mathsf{next}\big((\mathsf{hd}^{\mathsf{g}}\ s_1) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s_0) \circledast (\mathsf{tl}^{\mathsf{g}}\ s_1))\big) \end{array}$$

6 The Full System

The system presented so far has only one form of fixpoints in formulae ($\nu\alpha\varphi$). We now present our full system, which also handles least fixpoints ($\mu\alpha\varphi$) and thus liveness properties. A key role is played by *polynomial* guarded recursive types, that we discuss first.

$$(\mu\text{-F})\ \frac{\Sigma, \alpha : A \vdash \varphi : A}{\Sigma \vdash \mu\alpha\varphi : A} \qquad \frac{\Sigma, \alpha : A \vdash \varphi : A}{\Sigma \vdash \mu^{\mathtt{t}}\alpha\varphi : A} \qquad \frac{\Sigma, \alpha : A \vdash \varphi : A}{\Sigma \vdash \nu^{\mathtt{t}}\alpha\varphi : A}$$

Fig. 9. Extended Formation Rules of Formulae (with α Pos φ and α guarded in φ).

$$\frac{}{\vdash^A \varphi[\mu\alpha\varphi/\alpha] \Rightarrow \mu\alpha\varphi} \qquad \frac{\vdash^A \varphi[\psi/\alpha] \Rightarrow \psi}{\vdash^A \mu\alpha\varphi \Rightarrow \psi}$$

$$\frac{}{\vdash^A \theta^{\mathtt{t}+1}\alpha\varphi \ \Leftrightarrow\ \varphi[\theta^{\mathtt{t}}\alpha\varphi/\alpha]} \qquad \frac{}{\vdash^A \mu^0\alpha\varphi \ \Leftrightarrow\ \bot} \qquad \frac{}{\vdash^A \nu^0\alpha\varphi \ \Leftrightarrow\ \top}$$

$$\frac{[\![\mathtt{t}]\!] \leq [\![\mathtt{u}]\!]}{\vdash^A \mu^{\mathtt{t}}\alpha\varphi \ \Rightarrow\ \mu^{\mathtt{u}}\alpha\varphi} \qquad \frac{}{\vdash^A \mu^{\mathtt{t}}\alpha\varphi \ \Rightarrow\ \mu\alpha\varphi} \qquad \frac{[\![\mathtt{t}]\!] \geq [\![\mathtt{u}]\!]}{\vdash^A \nu^{\mathtt{t}}\alpha\varphi \ \Rightarrow\ \nu^{\mathtt{u}}\alpha\varphi} \qquad \frac{}{\vdash^A \nu\alpha\varphi \ \Rightarrow\ \nu^{\mathtt{t}}\alpha\varphi}$$

Fig. 10. Extended Modal Axioms and Rules (with A a pure type and θ either μ or ν).

Strictly Positive and Polynomial Types. *Strictly positive types* (notation P^+, Q^+, etc.) are given by

$$P^+ ::= A \mid X \mid \blacktriangleright P^+ \mid P^+ + P^+ \mid P^+ \times P^+ \mid \mathsf{Fix}(X).P^+ \mid B \to P^+$$

where A, B are (closed) *constant* pure types. Strictly positive types are a convenient generalization of polynomial types. A guarded recursive type $\mathsf{Fix}(X).P(X)$ is *polynomial* if $P(X)$ is induced by

$$P(X) ::= A \ \mid\ \blacktriangleright X \ \mid\ P(X) + P(X) \ \mid\ P(X) \times P(X) \ \mid\ B \to P(X)$$

where A, B are (closed) *constant* pure types. Note that if $\mathsf{Fix}(X).P(X)$ is polynomial, X cannot occur on the left of an arrow ($\to$) in $P(X)$. We say that $\mathsf{Fix}(X).P(X)$ (resp. P^+) is *finitary* polynomial (resp. *finitary* strictly positive) if B is a finite base type (see Ex. 3.1) in the above grammars. The set-theoretic counterpart of our polynomial recursive types are the *exponent* polynomial functors of [34], which all have final **Set**-coalgebras (see e.g. [34, Cor. 4.6.3]).

Example 6.1. For A a constant pure type, e.g. $\mathsf{Str}^{\mathsf{g}}\, A$, $\mathsf{CoList}^{\mathsf{g}}\, A$ and $\mathsf{Tree}^{\mathsf{g}}\, A$ as well as $\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A)$, $\mathsf{CoList}^{\mathsf{g}}(\mathsf{Str}\, A)$ and $\mathsf{Res}^{\mathsf{g}}\, A$ (with $\mathtt{I}$, $\mathtt{O}$ constant) are polynomial. More generally, polynomial types include all recursive types $\mathsf{Fix}(X).P(X)$ where $P(X)$ is of the form $\sum_{i=0}^{n} A_i \times (\blacktriangleright X)^{B_i}$ with A_i, B_i constant. The non-strictly positive recursive type $\mathsf{Rou}^{\mathsf{g}}\, A$ of Ex. 3.2, used in Hofmann's breadth-first traversal (see e.g. [10]), is *not* polynomial.

The Full Temporal Modal Logic. We assume given a first-order signature of *iteration terms* (notation $\mathtt{t}, \mathtt{u}$, etc.), with *iteration variables* k, ℓ, etc., and for each iteration term $\mathtt{t}(k_1, \ldots, k_m)$ with variables as shown, a given primitive recursive function $[\![\mathtt{t}]\!] : \mathbb{N}^m \to \mathbb{N}$. We assume a term $\mathtt{0}$ for $0 \in \mathbb{N}$ and a term $k{+}\mathtt{1}$ for the successor function $n \in \mathbb{N} \mapsto n + 1 \in \mathbb{N}$.

The formulae of the *full temporal modal logic* extend those of Fig. 5 with least fixpoints $\mu\alpha\varphi$ and with *approximated fixpoints* $\mu^{\mathtt{t}}\alpha\varphi$ and $\nu^{\mathtt{t}}\alpha\varphi$ where $\mathtt{t}$ is an iteration term. The additional formation rule for formulae are given in Fig. 9. We use θ as a generic notation for μ and ν. Least fixpoints $\mu\alpha\varphi$ are equipped with their usual Kozen axioms. In addition, iteration formulae $\nu^{\mathtt{t}}\alpha\varphi(\alpha)$ and $\mu^{\mathtt{t}}\alpha\varphi(\alpha)$ have axioms expressing that they are indeed iterations of $\varphi(\alpha)$ from resp. $\top$ and $\bot$. A fixpoint logic with iteration variables was already considered in [68].

Definition 6.2 (Full Modal Theories). *The* full *intuitionistic and classical modal theories (still denoted* $\vdash^A$ *and* $\vdash^A_{\mathrm{c}}$*) are defined by extending Def. 4.4 with the axioms and rules of Fig. 10.*

Example 6.3. Least fixpoints allow us to define liveness properties. On streams and colists, we have $\Diamond\varphi := \mu\alpha.\ \varphi \vee \bigcirc\alpha$ and $\varphi \mathbin{\mathsf{U}} \psi := \mu\alpha.\ \psi \vee (\varphi \wedge \bigcirc\alpha)$. On trees, we have the CTL-like $\exists\Diamond\varphi := \mu\alpha.\ \varphi \vee (\bigcirc_\ell\alpha \vee \bigcirc_r\alpha)$ and $\forall\Diamond\varphi := \mu\alpha.\ \varphi \vee (\bigcirc_\ell\alpha \wedge \bigcirc_r\alpha)$. The formula $\exists\Diamond\varphi$ is intended to hold on a tree if there is a finite path which leads to a subtree satisfying φ, while $\forall\Diamond\varphi$ is intended to hold if every infinite path crosses a subtree satisfying φ.

Remark 6.4. On *finitary trees* (as in Ex. 6.1 but with A_i, B_i finite base types), we have all formulae of the modal μ-calculus. For this fragment, satisfiability is decidable (see e.g. [17]), as well as the *classical* theory $\vdash_{\mathrm{c}}$ by completeness of Kozen's axiomatization [73] (see [63] for completeness results on fragments of the μ-calculus).

The Safe and Smooth Fragments. We now discuss two related but distinct fragments of the temporal modal logic. Both fragments directly impact the refinement type system by allowing for more typing rules.

The *safe* fragment plays a crucial role, because it reconciles the internal and external semantics of our system (see §7). It gives subtyping rules for $\blacksquare$ (Fig. 11), which makes available the comonad structure of $\blacksquare$ on $[\mathsf{box}]\varphi$ when φ is safe.

Definition 6.5 (Safe Formula). *Say* $\alpha_1 : A_1, \dots, \alpha_n : A_n \vdash \varphi : A$ *is* safe *if*

(i) the types $A_1, \dots, A_n, A$ *are strictly positive, and*
(ii) for each occurrence in φ *of a modality* $[\mathsf{ev}(\psi)]$*, the formula* ψ *is closed, and*
(iii) each occurrence in φ *of a least fixpoint (*$\mu\alpha(-)$*) and of an implication (*$\Rightarrow$*) is guarded by a* $[\mathsf{box}]$*.*

Note that the safe restriction imposes no condition on approximated fixpoints $\theta^{\mathtt{t}}\alpha$. Recalling that the theory under a $[\mathsf{box}]$ is $\vdash^A_{\mathrm{c}}$, the only propositional connectives accessible to $\vdash^A$ in safe formulae are those on which $\vdash^A$ and $\vdash^A_{\mathrm{c}}$ coincide. The formula $[\neg\mathsf{nil}] = [\mathsf{fold}][\mathsf{in}_1]\top$ is safe. Moreover:

Example 6.6. Any formula without fixpoint nor $[\mathsf{ev}(-)]$ is equivalent in $\vdash_{\mathrm{c}}$ to a safe one. It φ is safe, then so are $[\mathsf{hd}]\varphi$, $[\mathsf{lbl}]\varphi$, as well as $\triangle\varphi$ (for $\triangle \in \{\Box, \forall\Box, \exists\Box\}$) and $[\mathsf{box}]\triangle\varphi$ (for $\triangle \in \{\Diamond, \exists\Diamond, \forall\Diamond\}$).

Definition 6.7 (Smooth Formula). *A formula* $\alpha_1 : A_1, \ldots, \alpha_n : A_n \vdash \varphi : A$ *is* smooth *if*

(i) *the types* $A_1, \ldots, A_n, A$ *are* finitary *strictly positive, and*
(ii) *for each occurrence in* φ *of a modality* $[\mathsf{ev}(\psi)]$*, the formula* ψ *is closed, and*
(iii) φ *is* alternation-free*: for* $\theta, \theta' \in \{\mu, \nu\}$*, (1) if* $\theta\beta_0\psi_0$ *is a subformula of* φ*, and* $\theta'\beta_1\psi_1$ *is a subformula of* ψ_0 *s.t.* β_0 *occurs free in* ψ_1*, then* $\theta = \theta'$*, (2) if some* α_i *occurs in two subformulae* $\theta\beta_0\psi_0$ *and* $\theta'\beta_1\psi_1$ *of* φ*, then* $\theta = \theta'$*, and (3) if some* α_i *occurs in a subformula* $\theta'\beta\psi$ *of* φ*, then* α_i Pos ψ*.*

Our notion of alternation freedom is adapted from [17], in which propositional (fixpoint) variables are always positive. Note that the smooth restriction imposes no further conditions on approximated fixpoints $\theta^{\mathtt{t}}\alpha$. In the smooth fragment, greatest and least fixpoints can be thought about resp. as

$$\bigwedge_{m\in\mathbb{N}} \varphi^m(\top) \qquad \text{and} \qquad \bigvee_{m\in\mathbb{N}} \varphi^m(\bot)$$

Iteration terms allow for formal reasoning about such unfoldings. Assuming $[\![\mathtt{t}]\!] = m \in \mathbb{N}$, the formula $\nu^{\mathtt{t}}\alpha\varphi(\alpha)$ (resp. $\mu^{\mathtt{t}}\alpha\varphi(\alpha)$) can be read as $\varphi^m(\top)$ (resp. $\varphi^m(\bot)$). This gives the rules (ν-I) and (μ-E) (Fig. 11), which allow for reductions to the safe case (see examples in §8).

Remark 6.8. It is well-known (see e.g. [17, §4.1]) that on *finitary trees* (see Rem. 6.4) the alternation-free fragment is equivalent to *Weak* MSO (MSO with second-order variables restricted to *finite* sets). In the case of streams $\mathsf{Str}\,\mathtt{B}$ (for a finite base type $\mathtt{B}$), Weak MSO is in turn equivalent to the full modal μ-calculus. In particular, the alternation-free fragment contains all the *flat* fixpoints of [63] and thus LTL on $\mathsf{Str}\,\mathtt{B}$ and CTL on $\mathsf{Tree}\,\mathtt{B}$ and on $\mathsf{Res}\,\mathtt{B}$ with $\mathtt{I}$, $\mathtt{O}$, $\mathtt{B}$ finite base types. A typical property on $\mathsf{Tree}\,\mathtt{B}$ which *cannot* be expressed with alternation-free formulae is “there is an infinite path with infinitely many occurrences of $\mathtt{b}$” for a fixed $\mathtt{b} : \mathtt{B}$ (see e.g. [17, §2.2]).

Example 6.9. Any formula without fixpoint nor $[\mathsf{ev}(-)]$ is smooth. It φ is smooth, then so are $[\mathsf{hd}]\varphi$, $[\mathsf{lbl}]\varphi$ and $\triangle\varphi$ for $\triangle \in \{\Box, \forall\Box, \exists\Box, \Diamond, \exists\Diamond, \forall\Diamond\}$.

The Full System. We extend the types of §5 with universal quantification over iteration variables ($\forall k \cdot T$). The type system of §5 is extended with the rules of Fig. 11.

Example 6.10. The logical rules of Fig. 10 give the following derived typing rules (where β Pos γ):

$$(\mu\text{-I})\ \frac{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\mu^{\mathtt{t}}\alpha\varphi/\beta]\}}{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\mu\alpha\varphi/\beta]\}} \qquad (\nu\text{-E})\ \frac{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\nu\alpha\varphi/\beta]\}}{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\nu^{\mathtt{t}}\alpha\varphi/\beta]\}}$$

$$\frac{\varphi \text{ safe}}{\{\blacksquare A \mid [\mathsf{box}]\varphi\} \equiv \blacksquare\{A \mid \varphi\}} \qquad \frac{}{\forall k \cdot \blacktriangleright T \equiv \blacktriangleright \forall k \cdot T}$$

$$(\forall\text{-I})\ \frac{\mathcal{E} \vdash M : T}{\mathcal{E} \vdash M : \forall k \cdot T} \qquad (\forall\text{-CI})\ \frac{\mathcal{E} \vdash M : T[\mathtt{0}/k] \qquad \mathcal{E} \vdash M : T[k{+}\mathtt{1}/k]}{\mathcal{E} \vdash M : \forall k \cdot T}$$

$$(\nu\text{-I})\ \frac{\mathcal{E} \vdash M : \left\{\blacksquare A \;\middle|\; [\mathsf{box}]\gamma[\nu^\ell \alpha\psi/\beta]\right\}}{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\nu\alpha\psi/\beta]\}} \qquad (\forall\text{-E})\ \frac{\mathcal{E} \vdash M : \forall k \cdot T}{\mathcal{E} \vdash M : T[\mathtt{t}/k]}$$

$$(\mu\text{-E})\ \frac{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\mu\alpha\psi/\beta]\} \qquad \mathcal{E}, x : \left\{\blacksquare A \;\middle|\; [\mathsf{box}]\gamma[\mu^\ell\alpha\psi/\beta]\right\} \vdash N : U}{\mathcal{E} \vdash N[M/x] : U}$$

Fig. 11. Extended (Sub)Typing Rules for Refinement Types (where k is not free in $\mathcal{E}$ in ($\forall$-I) & ($\forall$-CI), ℓ is fresh in (ν-I) & (μ-E), $\theta\alpha\psi$ and γ are smooth, and β Pos γ).

7 Semantics

We present the main ingredients of the semantics of our type system. We take as base the denotational semantics of guarded recursion in the topos of trees.

Denotational Semantics in the Topos of Trees. The *topos of trees* $\mathcal{S}$ provides a natural model of guarded recursion [13]. Formally, $\mathcal{S}$ is the category of presheaves over $(\mathbb{N} \setminus \{0\}, \leq)$. In words, the objects of $\mathcal{S}$ are indexed sets $X = (X(n))_{n>0}$ equipped with *restriction maps* $r_n^X : X(n+1) \to X(n)$. Excluding 0 from the indexes is a customary notational convenience ([13]). The morphisms from X to Y are families of functions $f = (f_n : X(n) \to Y(n))_{n>0}$ which commute with restriction, that is $f_n \circ r_n^X = r_n^Y \circ f_{n+1}$. As any presheaf category, $\mathcal{S}$ has (pointwise) limits and colimits, and is Cartesian closed (see e.g. [52, §I.6]). We write $\boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ for the *global section functor*, which takes X to $\mathcal{S}[\mathbf{1}, X]$, the set of morphisms $\mathbf{1} \to X$ in $\mathcal{S}$, where $\mathbf{1} = (\{\bullet\})_{n>0}$ is terminal in $\mathcal{S}$.

A typed term $\mathcal{E} \vdash M : T$ is to be interpreted in $\mathcal{S}$ as a morphism

$$[\![M]\!] : [\![|\mathcal{E}|]\!] \longrightarrow [\![|T|]\!]$$

where $[\![|\mathcal{E}|]\!] = [\![|T_1|]\!] \times \cdots \times [\![|T_n|]\!]$ for $\mathcal{E} = x_1 : T_1, \ldots, x_n : T_n$. In particular, a closed term $M : T$ is to be interpreted as a global section $[\![M]\!] \in \boldsymbol{\Gamma}[\![|T|]\!]$. The $\times/+/\to$ fragment of the calculus is interpreted by the corresponding structure in $\mathcal{S}$. The $\blacktriangleright$ modality is interpreted by the functor $\blacktriangleright : \mathcal{S} \to \mathcal{S}$ of [13]. This functor shifts indexes by 1 and inserts a singleton set $\mathbf{1}$ at index 1. The term constructor next is interpreted by the natural map with component $\mathsf{next}^X : X \to \blacktriangleright X$ as in

$$\begin{tikzcd}
X \arrow[d, "\mathsf{next}^X"'] & X_1 \arrow[d, "\mathbf{1}"'] & X_2 \arrow[l, "r_1^X"'] \arrow[d, "r_1^X"'] & \cdots \arrow[l, dotted] & X_n \arrow[l, dotted] \arrow[d, "r_{n-1}^X"'] & X_{n+1} \arrow[l, "r_n^X"'] \arrow[d, "r_n^X"'] & \cdots \arrow[l, dotted] \\
\blacktriangleright X & \mathbf{1} & X_1 \arrow[l, "\mathbf{1}"] & \cdots \arrow[l, dotted] & X_{n-1} \arrow[l, dotted] & X_n \arrow[l, "r_{n-1}^X"] & \cdots \arrow[l, dotted]
\end{tikzcd}$$

$$\begin{aligned}
\{\![\pi_i]\varphi]\!\} &:= \{x \in \boldsymbol{\Gamma}[\![A_0 \times A_1]\!] \mid \pi_i \circ x \in \{\![\varphi]\!\}\} & \{\![[\mathsf{next}]\varphi]\!\} &:= \{\mathsf{next} \circ x \in \boldsymbol{\Gamma}[\![\blacktriangleright A]\!] \mid x \in \{\![\varphi]\!\}\}\\
\{\![[\mathsf{fold}]\varphi]\!\} &:= \{x \in \boldsymbol{\Gamma}[\![\mathsf{Fix}(X).A]\!] \mid \mathsf{unfold} \circ x \in \{\![\varphi]\!\}\} & \{\![[\mathsf{box}]\varphi]\!\} &:= \{x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!] \mid x_1(\bullet) \in \{\![\varphi]\!\}\}
\end{aligned}$$

$$\begin{aligned}
\{\![[\mathsf{in}_i]\varphi]\!\} &:= \big\{x \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \;\big|\; \exists y \in \boldsymbol{\Gamma}[\![A_i]\!]\big(x = \mathsf{in}_i \circ y \;\text{ and }\; y \in \{\![\varphi]\!\}\big)\big\}\\
\{\![[\mathsf{ev}(\psi)]\varphi]\!\} &:= \big\{x \in \boldsymbol{\Gamma}[\![B \to A]\!] \;\big|\; \forall y \in \boldsymbol{\Gamma}[\![B]\!]\big(y \in \{\![\psi]\!\} \implies \mathsf{ev} \circ \langle x, y\rangle \in \{\![\varphi]\!\}\big)\big\}
\end{aligned}$$

Fig. 12. External Semantics (for closed formulae).

The guarded fixpoint combinator fix is interpreted by the morphism fix^X : $X^{\blacktriangleright X} \to X$ of [13, Thm. 2.4].

The constant type modality $\blacksquare$ is interpreted as the comonad $\boldsymbol{\Delta\Gamma} : \mathcal{S} \to \mathcal{S}$, where the left adjoint $\boldsymbol{\Delta} : \mathbf{Set} \to \mathcal{S}$ is the *constant object functor*, which takes a set S to the constant family $(S)_{n>0}$. In words, all components $[\![\blacksquare A]\!](n)$ are equal to $\boldsymbol{\Gamma}[\![A]\!]$, and the restriction maps of $[\![\blacksquare A]\!]$ are identities. In particular, a global section $x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!]$ is a constant family $(x_n)_n$ describing a unique global section $x_{n+1}(\bullet) = x_n(\bullet) \in \boldsymbol{\Gamma}[\![A]\!]$. We refer to [20] and §D for the interpretation of prev, box and unbox. Just note that the unit $\eta : \mathrm{Id}_{\mathbf{Set}} \to \boldsymbol{\Gamma\Delta}$ is an iso.

Together with an interpretation of guarded recursive types, this gives a denotational semantics of the pure calculus of §3. See [13,20] for details. We write fold : $[\![A[\mathsf{Fix}(X).A/X]]\!] \to [\![\mathsf{Fix}(X).A]\!]$ and $\mathsf{unfold} : [\![\mathsf{Fix}(X).A]\!] \to [\![A[\mathsf{Fix}(X).A/X]]\!]$ for the two components of the iso $[\![\mathsf{Fix}(X).A]\!] \simeq [\![A[\mathsf{Fix}(X).A/X]]\!]$.

External Semantics. Møgelberg [55] has shown that for polynomial types such as $\mathsf{Str}^{\mathsf{g}}\, B$ with B a constant type, the set of global sections $\boldsymbol{\Gamma}[\![\mathsf{Str}^{\mathsf{g}}\, B]\!]$ is equipped with the usual final coalgebra structure of streams over B in $\mathbf{Set}$. To each polynomial recursive type $\mathsf{Fix}(X).P(X)$, we associate a polynomial functor $P_{\mathbf{Set}} : \mathbf{Set} \to \mathbf{Set}$ in the obvious way.

Theorem 7.1 ([55] (see also [20])). *If* $\mathsf{Fix}(X).P(X)$ *is polynomial, then the set* $\boldsymbol{\Gamma}[\![\mathsf{Fix}(X).P(X)]\!]$ *carries a final* $\mathbf{Set}$*-coalgebra structure for* $P_{\mathbf{Set}}$.

We devise a $\mathbf{Set}$ interpretation $\{\![\varphi]\!\} \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ of formulae $\varphi : A$. We rely on the (complete) Boolean algebra structure of powersets for propositional connectives and on Knaster-Tarski Fixpoint Theorem for fixpoints μ and ν. The interpretations of $\nu^{\mathtt{t}}\alpha\varphi(\alpha)$ and $\mu^{\mathtt{t}}\alpha\varphi(\alpha)$ (for $\mathtt{t}$ closed) are defined to be the interpretations resp. of $\varphi^{[\![\mathtt{t}]\!]}(\top)$ and $\varphi^{[\![\mathtt{t}]\!]}(\bot)$, where e.g. $\varphi^0(\top) := \top$ and $\varphi^{n+1}(\top) := \varphi(\varphi^n(\top))$. We give the cases of the atomic modalities in Fig. 12 (where for simplicity we assume formulae to be closed). It can be checked that, when restricting to polynomial types, one gets the coalgebraic semantics of [33] (with sums as in [34]) extended to fixpoints.

Internal Semantics of Formulae. We would like to have adequacy w.r.t. the external semantics of formulae, namely that given $M : \{A \mid \varphi\}$, the global section $[\![M]\!] \in \boldsymbol{\Gamma}[\![A]\!]$ satisfies $\{\![\varphi]\!\} \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ in the sense that $[\![M]\!] \in \{\![\varphi]\!\}$. But in general we can only have adequacy w.r.t. an *internal* semantics $[\![\varphi]\!] \in \mathrm{Sub}([\![A]\!])$

of formulae $\varphi : A$. We sketch it here. First, $\mathrm{Sub}(X)$ is the (complete) Heyting algebra of *subobjects* of an object X of $\mathcal{S}$. Explicitly, we have $S = (S(n))_n \in \mathrm{Sub}(X)$ iff for all $n > 0$, $S(n) \subseteq X(n)$ and $r^X_n(t) \in S(n)$ whenever $t \in S(n+1)$. For propositional connectives and fixpoints, the internal $[\![-]\!]$ is defined similarly as the external $\{\!|-|\!\}$, but using (complete) Heyting algebras of subobjects rather than (complete) Boolean algebras of subsets.

As for modalities, let $[\triangle]$ be of the form $[\pi_i]$, $[\mathsf{in}_i]$, $[\mathsf{next}]$ or $[\mathsf{fold}]$, and assume $[\triangle]\varphi : B$ whenever $\varphi : A$. Standard topos theoretic constructions give posets morphisms $[\![[\triangle]]\!] : \mathrm{Sub}([\![A]\!]) \to \mathrm{Sub}([\![B]\!])$ such that $[\![[\pi_i]]\!]$, $[\![[\mathsf{fold}]]\!]$ are maps of Heyting algebras, $[\![[\mathsf{in}_i]]\!]$ preserves $\vee, \bot$ and $\wedge$, while $[\![[\mathsf{next}]]\!]$ preserves $\wedge, \top$ and $\vee$. With $[\![[\triangle]\varphi]\!] := [\![[\triangle]]\!]([\![\varphi]\!])$, all the axioms and rules of Table 2 are validated for these modalities. To handle guarded recursion, it is crucial to have $[\![[\mathsf{next}]\varphi]\!] := \blacktriangleright([\![\varphi]\!])$, with $[\![[\mathsf{next}]\varphi]\!]$ true at time 1, independently from φ. As a consequence, $[\mathsf{next}]$ and $\bigcirc$ do not validate axiom (P) (Table 2), and $\Diamond[\mathsf{hd}]\varphi$ can "lie" about the next time step. We let $[\![[\mathsf{box}]\varphi]\!] := \boldsymbol{\Delta}(\{\!|\varphi|\!\})$.

The modality $[\mathsf{ev}(\psi)]$ is a bit more complex. For $\psi : B$ and $\varphi : A$, the formula $[\mathsf{ev}(\psi)]\varphi$ is interpreted as a *logical predicate* in the sense of [32, §9.2 & Prop. 9.2.4]. The idea is that for a term $M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}$, the global section $\mathsf{ev} \circ \langle [\![M]\!], x\rangle \in \boldsymbol{\Gamma}[\![A]\!]$ should satisfy φ whenever $x \in \boldsymbol{\Gamma}[\![B]\!]$ satisfies ψ. We refer to §D for details.

Our semantics are both correct w.r.t. the full modal theories of Def. 6.2.

Lemma 7.2. *If $\vdash^A_{\mathrm{c}} \varphi$ then $\{\!|\varphi|\!\} = \{\!|\top|\!\}$. If $\vdash^A \varphi$ then $[\![\varphi]\!] = [\![\top]\!]$.*

The Safe Fragment. For α (positive and) guarded in φ, the internal semantics of $\theta\alpha\varphi$ is somewhat meaningless because $\mathcal{S}$ has *unique* guarded fixpoints [13, §2.5]. In particular, the typing $\mathsf{fix}(s).\mathsf{Cons}^{\mathsf{g}}\ a\ s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond[\varphi]\}$ for arbitrary $a : A$ and $\varphi : \mathsf{Str}^{\mathsf{g}}\, A$ (extending §2) is indeed verified by the $\mathcal{S}$ semantics $[\![-]\!]$. This prevents us from adequacy w.r.t. the external semantics in general. But this is possible for *safe* formulae since in this case we have:

Proposition 7.3. *If $\varphi : A$ is safe then $\{\!|\varphi|\!\} = \boldsymbol{\Gamma}[\![\varphi]\!]$.*

Proposition 7.3 gives the subtyping rule $\{\blacksquare A \mid [\mathsf{box}]\varphi\} \equiv \blacksquare\{A \mid \varphi\}$ (Fig. 11), which makes available the comonad structure of $\blacksquare$ on $[\mathsf{box}]\varphi$ when φ is safe. Recall that in safe formulae, implications can only occur under a $[\mathsf{box}]$ modality and thus in *closed* subformulae. It is crucial for Prop. 7.3 that infs and sups are pointwise in the subobject lattices of $\mathcal{S}$, so that conjunctions and disjunctions are interpreted as with the usual classical Kripke semantics (see e.g. [52, §VI.7]). This does not hold for implications!

The second key to Prop. 7.3 is the following. For L a complete lattice, a Scott *cocontinuous* function $L \to L$ is a Scott continuous function $L^{\mathrm{op}} \to L^{\mathrm{op}}$, *i.e.* which preserves codirected infs. For a safe $\alpha : A \vdash \varphi : A$, the poset maps $[\![\varphi]\!] : \mathrm{Sub}([\![A]\!]) \to \mathrm{Sub}([\![A]\!])$ and $\{\!|\varphi|\!\} : \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]) \to \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ are Scott cocontinuous. The greatest fixpoint $\nu\alpha\varphi(\alpha)$ can thus be interpreted, *both in* **Set** *and* $\mathcal{S}$, using Kleene's Fixpoint Theorem, as the infs of the interpretations of $\varphi^m(\top)$ for $m \in \mathbb{N}$. This leads to the expected coincidence of the two semantics for safe formulae.

$x \Vvdash_n \{A \mid \varphi\}$	iff	$x_n(\bullet) \in [\![\varphi]\!]^A(n)$	$x \Vvdash_n \mathsf{Fix}(X).A$ iff $\mathsf{unfold} \circ x \Vvdash_n A[\mathsf{Fix}(X).A/X]$
$x \Vvdash_n T_0 + T_1$	iff	$\exists i \in \{0,1\},\ \exists y \in \boldsymbol{\Gamma}[\![\lvert T_i\rvert]\!],\ x = \mathsf{in}_i \circ y$ and $y \Vvdash_n T_i$	
$x \Vvdash_n T_0 \times T_1$	iff	$\pi_0 \circ x \Vvdash_n T_0$ and $\pi_1 \circ x \Vvdash_n T_1$	$x \Vvdash_n \mathbf{1}$
$x \Vvdash_n U \to T$	iff	$\forall k \leq n,\ \forall y \in \boldsymbol{\Gamma}[\![\lvert U\rvert]\!],\ y \Vvdash_k U \implies \mathsf{ev} \circ \langle x, y\rangle \Vvdash_k T$	
$x \Vvdash_{n+1} \blacktriangleright T$	iff	$\exists y \in \boldsymbol{\Gamma}[\![\lvert T\rvert]\!],\ x = \mathsf{next} \circ y$ and $y \Vvdash_n T$	$x \Vvdash_1 \blacktriangleright T$
$x \Vvdash_n \blacksquare T$	iff	$\forall m > 0,\ x_n(\bullet) \Vvdash_m T$	(where $x \in \boldsymbol{\Gamma}[\![\lvert\blacksquare T\rvert]\!]$)
$x \Vvdash_n \forall k \cdot T$	iff	$x \Vvdash_n T[\mathtt{t}/k]$ for all closed iteration terms $\mathtt{t}$	

Fig. 13. The Realizability Semantics.

The Smooth Fragment. The *smooth* restriction allows for continuity properties needed to compute fixpoints iteratively, following Kleene's Fixpoint Theorem. This implies the correctness of the typing rules (ν-I) and (μ-E) of Fig. 11.

Lemma 7.4. *Given a closed smooth $\nu\alpha\varphi(\alpha) : A$ (resp. $\mu\alpha\varphi(\alpha) : A$), the function $\{\lvert\varphi\rvert\} : \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]) \to \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ is Scott-cocontinuous (resp. Scott-continuous). We have $\{\lvert\nu\alpha\varphi(\alpha)\rvert\} = \bigcap_{m\in\mathbb{N}} \{\lvert\varphi^m(\top)\rvert\}$ (resp. $\{\lvert\mu\alpha\varphi(\alpha)\rvert\} = \bigcup_{m\in\mathbb{N}} \{\lvert\varphi^m(\bot)\rvert\}$).*

The Realizability Semantics. The correctness of the type system w.r.t. its semantics in $\mathcal{S}$ is proved with a realizability relation.

Definition 7.5 (Realizability). *Given a type T without free iteration variable, a global section $x \in \boldsymbol{\Gamma}[\![\lvert T\rvert]\!]$ and $n > 0$, we define the realizability relation $x \Vvdash_n T$ by induction on lexicographicaly ordered pairs (n, T) in Fig. 13.*

Lemma 7.6. *Given types T, U without free iteration variable, if $x \Vvdash_n U$ and $U \leq T$ then $x \Vvdash_n T$.*

Theorem 7.7 (Adequacy). *If $\vdash M : T$, where T has no free iteration variable, then $[\![M]\!] \Vvdash_n T$ for all $n > 0$.*

By Thm. 7.7, a program $M : B \to A$ induces a set-theoretic function $\boldsymbol{\Gamma}[\![M]\!] : \boldsymbol{\Gamma}[\![B]\!] \to \boldsymbol{\Gamma}[\![A]\!]$, $x \mapsto [\![M]\!] \circ x$. When B and A are polynomial (e.g. streams $\mathsf{Str}^{\mathsf{g}}\,\mathtt{B}$, $\mathsf{Str}^{\mathsf{g}}\,\mathtt{A}$ with $\mathtt{B}$, $\mathtt{A}$ constant), Møgelberg's Thm. 7.1 says that $\boldsymbol{\Gamma}[\![M]\!]$ is a function on the usual final coalgebra for B, A in **Set** (e.g. the set of usual streams over $\mathtt{B}$ and $\mathtt{A}$). Moreover, if e.g. $M : \{\mathsf{Str}\,\mathtt{B} \mid [\mathsf{box}]\psi\} \to \{\mathsf{Str}\,\mathtt{A} \mid [\mathsf{box}]\varphi\}$, then (modulo $\boldsymbol{\Gamma\Delta} \simeq \mathrm{Id}_{\mathbf{Set}}$) given a stream x that satisfies ψ (*i.e.* $x \in \{\lvert\psi\rvert\}$) the stream $\boldsymbol{\Gamma}[\![M]\!](x)$ satisfies φ (*i.e.* $\boldsymbol{\Gamma}[\![M]\!](x) \in \{\lvert\varphi\rvert\}$). See §8 for examples.

8 Examples

We exemplified basic manipulations of our system over §3-6. We give further examples here. The functions used in our main examples are gathered in Table 3, with the following conventions. We use the infix notation $a ::^{\mathsf{g}} s$ for $\mathsf{Cons}^{\mathsf{g}}\ a\ s$ and write $[]^{\mathsf{g}}$ for the empty colist $\mathsf{Nil}^{\mathsf{g}}$. Moreover, we use some syntactic sugar for pattern matching, e.g. assuming $s : \mathsf{CoList}^{\mathsf{g}}\,A$ we write $\mathsf{case}\,s\,\mathsf{of}$ $([]^{\mathsf{g}} \mapsto N \mid x ::^{\mathsf{g}} xs \mapsto M)$ for $\mathsf{case}(\mathsf{unfold}\ s)$ of $(y.N[\langle\rangle/y] \mid y.M[\pi_0(y)/x\,,\ \pi_1(y)/xs])$. Most of the

$$\begin{array}{lll}
\mathbf{append} & : & \mathsf{CoList}\,A \longrightarrow \mathsf{CoList}\,A \longrightarrow \mathsf{CoList}\,A \\
 & := & \lambda s.\lambda t. \\
 & & \quad \mathsf{box}_\iota(\mathsf{append}^{\mathsf{g}}\ (\mathsf{unbox}\ s)\ (\mathsf{unbox}\ t))
\end{array}
\qquad
\begin{array}{lll}
\mathbf{sched} & : & \mathsf{Res}\,A \longrightarrow \mathsf{Res}\,A \longrightarrow \mathsf{Res}\,A \\
 & := & \lambda p.\lambda q. \\
 & & \quad \mathsf{box}_\iota(\mathsf{sched}^{\mathsf{g}}\ (\mathsf{unbox}\ p)\ (\mathsf{unbox}\ q))
\end{array}$$

$$\begin{array}{lll}
\mathbf{append^{g}} & : & \mathsf{CoList}^{\mathsf{g}}\,A \to \mathsf{CoList}^{\mathsf{g}}\,A \to \mathsf{CoList}^{\mathsf{g}}\,A \\
 & := & \mathsf{fix}(g).\lambda s.\lambda t.\mathsf{case}\ s\ \mathsf{of} \\
 & & \mid [\,]^{\mathsf{g}} \ \mapsto\ t \\
 & & \mid x ::^{\mathsf{g}} xs \ \mapsto\ x ::^{\mathsf{g}} (g \circledast xs \circledast (\mathsf{next}\ t))
\end{array}
\qquad
\begin{array}{lll}
\mathbf{sched^{g}} & : & \mathsf{Res}^{\mathsf{g}}\,A \longrightarrow \mathsf{Res}^{\mathsf{g}}\,A \longrightarrow \mathsf{Res}^{\mathsf{g}}\,A \\
 & := & \mathsf{fix}(g).\lambda p.\lambda q.\ \mathsf{case}\ p\ \mathsf{of} \\
 & & \mid \mathsf{Ret}^{\mathsf{g}}\ a \ \mapsto\ \mathsf{Ret}^{\mathsf{g}}\ a \\
 & & \mid \mathsf{Cont}^{\mathsf{g}}\ k \ \mapsto \\
 & & \quad \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o, t\rangle = ki \\
 & & \qquad\qquad\quad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\
 & & \quad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h
\end{array}$$

$$\begin{array}{rll}
\mathbf{diag} & := \lambda s.\mathsf{box}_\iota\big(\mathsf{diag}^{\mathsf{g}}\ (\mathsf{unbox}\ s)\big) & : \mathsf{Str}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}\,A \\
\mathbf{diag^{g}} & := \mathsf{diagaux}^{\mathsf{g}}\ (\lambda x.x) & : \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A
\end{array}$$

$$\begin{array}{rll}
\mathbf{diagaux^{g}} & : & (\mathsf{Str}\,A \to \mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \\
 & := & \mathsf{fix}(g).\lambda t.\lambda s.\ \mathsf{Cons}^{\mathsf{g}}\ \big((\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s)\big)\ \big(g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)\big)
\end{array}$$

$$\begin{array}{ll}
\mathbf{fb}: & \mathsf{CoNat} \longrightarrow \mathsf{CoNat} \longrightarrow \mathsf{Str}\,\mathsf{Bool} \\
:= & \lambda c.\lambda m.\ \mathsf{box}_\iota(\mathsf{fb}^{\mathsf{g}}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m))
\end{array}
\qquad
\begin{array}{lll}
\mathbf{fb^{g}} & : & \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \\
 & := & \mathsf{fix}(g).\lambda c.\lambda m.\ \mathsf{case}\ c\ \mathsf{of} \\
 & & \mid \mathsf{Z}^{\mathsf{g}} \ \mapsto\ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m)) \\
 & & \mid \mathsf{S}^{\mathsf{g}} n \ \mapsto\ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m)
\end{array}$$

$$\begin{array}{lll}
\mathbf{extract} & : & \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \longrightarrow \mathsf{CoList}^{\mathsf{g}}\,A \\
 & := & \mathsf{fix}(g).\lambda c.\ \mathsf{case}\ c\ \mathsf{of} \\
 & & \mid \mathsf{Over}^{\mathsf{g}} \ \mapsto\ \mathsf{Nil}^{\mathsf{g}} \\
 & & \mid \mathsf{Cont}^{\mathsf{g}} f \ \mapsto\ f g^{\circledast}
\end{array}
\qquad
\begin{array}{lll}
\mathbf{unfold} & : & \mathsf{Rou}^{\mathsf{g}}\,A \longrightarrow (\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\,A \to \blacktriangleright A) \longrightarrow \blacktriangleright A \\
 & := & \lambda c.\ \mathsf{case}\ c\ \mathsf{of} \\
 & & \mid \mathsf{Over}^{\mathsf{g}} \ \mapsto\ \lambda k.\ k\ (\mathsf{next}\ \mathsf{Over}^{\mathsf{g}}) \\
 & & \mid \mathsf{Cont}^{\mathsf{g}} f \ \mapsto\ \lambda k.\ \mathsf{next}(fk)
\end{array}$$

$$\mathbf{bft^{g}} := \lambda t.\ \mathsf{extract}\ (\mathsf{bftaux}\ t\ \mathsf{Over}^{\mathsf{g}}) : \mathsf{Tree}^{\mathsf{g}}\,A \longrightarrow \mathsf{CoList}^{\mathsf{g}}\,A$$

$$\begin{array}{lll}
\mathbf{bftaux} & : & \mathsf{Tree}^{\mathsf{g}}\,A \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \\
 & := & \mathsf{fix}(g).\lambda t.\lambda c.\ \mathsf{Cont}\ \big(\lambda k.\ (\mathsf{label}^{\mathsf{g}}\ t) ::^{\mathsf{g}} \mathsf{unfold}\ c\ \big(k \circ (g \circledast (\mathsf{son}^{\mathsf{g}}_{\ell} t))^{\circledast} \circ (g \circledast (\mathsf{son}^{\mathsf{g}}_{r} t))^{\circledast}\big)\big)
\end{array}$$

Table 3. Code of the Examples.

functions of Table 3 are obtained from usual recursive definitions by inserting $\circledast$ and next at the right places. We often write $\psi \Vert\!\!\mapsto \varphi$ for $[\mathsf{ev}(\psi)]\varphi$. Table 4 recaps our main examples of refinement typings, all of which (for A, B, $\mathtt{O}$, $\mathtt{I}$ constant, $\mathtt{I}$ finite and φ, ψ safe and smooth) can be derived syntactically for the functions of Table 3. We use intermediate typings requiring iteration terms whenever a $\Diamond$ is involved. Below, "$\boldsymbol{\Gamma}[\![M]\!]$ satisfies φ" means $\boldsymbol{\Gamma}[\![M]\!] \in \{\!|\varphi|\!\}$ (modulo $\boldsymbol{\Gamma\Delta} \simeq \mathrm{Id}_{\mathbf{Set}}$, see §7). We refer to §E for details.

Example 8.1 (The Append Function on CoLists). Our system can derive that $\boldsymbol{\Gamma}[\![\mathsf{append}]\!]$ returns a non-empty colist if one of its argument is non-empty. Using $\Diamond[\mathsf{nil}]$ (which says that a colist is finite), we can derive that $\boldsymbol{\Gamma}[\![\mathsf{append}]\!]$ returns a finite colist if its arguments are both finite. This involves the intermediate typing

$$\forall k \cdot \forall \ell \cdot \big(\big\{\mathsf{CoList}^{\mathsf{g}}\,A \bigm| \Diamond^{k}[\mathsf{nil}]\big\} \to \big\{\mathsf{CoList}^{\mathsf{g}}\,A \bigm| \Diamond^{\ell}[\mathsf{nil}]\big\} \to \big\{\mathsf{CoList}^{\mathsf{g}}\,A \bigm| \Diamond^{k+\ell}[\mathsf{nil}]\big\}\big)$$

In addition, if the first argument of $\boldsymbol{\Gamma}[\![\mathsf{append}]\!]$ has an element which satisfies φ, then the result has an element which satisfies φ. The same holds if the first argument is finite while the second one has an element which satisfies φ. $\square$

Map over coinductive streams (with $\triangle$ either $\Box$, $\Diamond$, $\Diamond\Box$ or $\Box\Diamond$)
$\mathsf{map} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathsf{Str}\, B \mid [\mathsf{box}]\triangle[\mathsf{hd}]\psi\} \longrightarrow \{\mathsf{Str}\, A \mid [\mathsf{box}]\triangle[\mathsf{hd}]\varphi\}$
Diagonal of coinductive streams of streams (with $\triangle$ either $\Box$ or $\Diamond\Box$)
$\mathsf{diag} : \{\mathsf{Str}(\mathsf{Str}\, A) \mid [\mathsf{box}]\triangle[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}\, A \mid [\mathsf{box}]\triangle[\mathsf{hd}]\varphi\}$
A fair stream of Booleans (adapted from [18,8])
$\mathsf{fb} \quad : \mathsf{CoNat} \longrightarrow \mathsf{CoNat} \longrightarrow \mathsf{Str}\,\mathsf{Bool}$
$\mathsf{fb}\ 0\ 1 : \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}] \quad\wedge\quad [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}$
Append on guarded recursive colists
$\mathsf{append}^{\mathsf{g}} : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\} \longrightarrow \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\}$
$\mathsf{append}^{\mathsf{g}} : \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\}$
Append on coinductive colists
$\mathsf{append} : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \longrightarrow \mathsf{CoList}\, A \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\}$
$\mathsf{append} : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\}$
$\mathsf{append} : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\}$
Breadth-first tree traversal
$\mathsf{bft}^{\mathsf{g}} : \{\mathsf{Tree}^{\mathsf{g}}\, C \mid \forall\Box[\mathsf{lbl}]\vartheta\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, C \mid \Box[\mathsf{hd}]\vartheta\}$
(à la [39] or with Hofmann's algorithm (see e.g. [10]))
A scheduler of resumptions (adapted from [48])
$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{Ret}]\}$
$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{now}]\psi\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{now}]\psi\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Diamond[\mathsf{now}]\psi\}$
$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\}$
$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{out}]\vartheta\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{out}]\vartheta\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{out}]\vartheta\}$
(where $\Diamond$ is either $\forall\Diamond$ or $\exists\Diamond$, $\Box$ is either $\forall\Box$ or $\exists\Box$, and $[\mathsf{out}]$ is either $[\wedge\mathsf{out}]$ or $[\vee\mathsf{out}]$)

Table 4. Some Refinement Typings (functions defined in Table 3).

Example 8.2 (The Map Function on Streams). The composite modalities $\Box\Diamond$ and $\Diamond\Box$ over streams are read resp. as "infinitely often" and "eventually always". Provided with a function $f : \boldsymbol{\Gamma}[\![B]\!] \to \boldsymbol{\Gamma}[\![A]\!]$ taking $b \in \boldsymbol{\Gamma}[\![B]\!]$ satisfying ψ to $f(b) \in \boldsymbol{\Gamma}[\![B]\!]$ satisfying φ, the function $\boldsymbol{\Gamma}[\![\mathsf{map}]\!]$ on set-theoretic streams returns a stream which infinitely often (resp. eventually always) satisfies φ whenever its stream argument infinitely often (resp. eventually always) satisfies ψ. $\Box$

Example 8.3 (The Diagonal Function). Consider a stream of streams s. We have $s = (s_i \mid i \geq 0)$ where each s_i is itself a stream $s_i = (s_{i,j} \mid j \geq 0)$. The *diagonal* of s is then the stream $(s_{i,i} \mid i \geq 0)$. Note that $s_{i,i} = \mathsf{hd}(\mathsf{tl}^i(\mathsf{hd}(\mathsf{tl}^i(s))))$. Indeed, $\mathsf{tl}^i(s)$ is the stream of streams $(s_k \mid k \geq i)$, so that $\mathsf{hd}(\mathsf{tl}^i(s))$ is the stream s_i and $\mathsf{tl}^i(\mathsf{hd}(\mathsf{tl}^i(s)))$ is the stream $(s_{i,k} \mid k \geq i)$. Taking its head thus gives $s_{i,i}$. In the diag function of Table 3, the auxiliary higher-order function $\mathsf{diagaux}^{\mathsf{g}}$ iterates the coinductive tl over the head of the stream of streams s. We write $\circ$ for function composition, so that assuming $s : \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A)$ and $t : \mathsf{Str}\, A \to \mathsf{Str}\, A$, we have (on the *coinductive* type $\mathsf{Str}\, A$), $(\mathsf{hd}^{\mathsf{g}}\ s) : \mathsf{Str}\, A$ and

$$(\mathsf{hd} \circ t) : \mathsf{Str}\, A \to A \qquad (\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s) : A \qquad (t \circ \mathsf{tl}) : \mathsf{Str}\, A \to \mathsf{Str}\, A$$

The expected refinement types for diag (Table 4) say that if its argument is a stream whose component streams all satisfy $\Box\varphi$, then $\boldsymbol{\Gamma}[\![\mathsf{diag}]\!]$ returns a stream whose elements all satisfy φ. Also, if the argument of $\boldsymbol{\Gamma}[\![\mathsf{diag}]\!]$ is a stream such that eventually all its component streams satisfy $\Box\varphi$, then it returns a stream which eventually always satisfies φ. See §E.4 for details. $\square$

Example 8.4 (A Fair Stream of Booleans). The non-regular stream (fb 0 1), adapted from [18,8], is of the form $\mathsf{ff}\cdot\mathsf{tt}\cdot\mathsf{ff}\cdot\mathsf{tt}^2\cdot\mathsf{ff}\cdots\mathsf{ff}\cdot\mathsf{tt}^m\cdot\mathsf{ff}\cdot\mathsf{tt}^{m+1}\cdot\mathsf{ff}\cdots$. It thus contains infinitely many tt's and infinitely many ff's. We indeed have (see §E.5 for details) $(\mathsf{fb}\ 0\ 1) : \{\mathsf{Str\,Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}] \quad\wedge\quad [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}$. $\square$

Example 8.5 (Resumptions). The type of resumptions $\mathsf{Res}^{\mathsf{g}}\,A$ (see Ex. 3.2) is adapted from [48]. Its guarded constructors are

$$\begin{array}{ll}\mathsf{Ret}^{\mathsf{g}} & := \lambda a.\ \mathsf{fold}(\mathsf{in}_0\ a) : A \longrightarrow \mathsf{Res}^{\mathsf{g}}\,A \\ \mathsf{Cont}^{\mathsf{g}} & := \lambda k.\ \mathsf{fold}(\mathsf{in}_1\ k) : (\mathtt{I} \to (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A)) \longrightarrow \mathsf{Res}^{\mathsf{g}}\,A\end{array}$$

$\mathsf{Ret}^{\mathsf{g}}(a)$ represents a computation which returns the value $a : A$, while $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$ (with $\langle f,k\rangle : \mathtt{I} \to (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A)$) represents a computation which on input $\mathtt{i} : \mathtt{I}$ outputs $f\mathtt{i} : \mathtt{O}$ and continues with $k\mathtt{i} : \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A$. Given $p, q : \mathsf{Res}^{\mathsf{g}}\,A$, the scheduler $(\mathsf{sched}^{\mathsf{g}}\ p\ q)$, adapted from [48], first evaluates p. If p returns, then the whole computation returns, with the same value. Otherwise, p evaluates to say $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$. Then $(\mathsf{sched}^{\mathsf{g}}\ p\ q)$ produces a computation which on input $\mathtt{i} : \mathtt{I}$ outputs $f\mathtt{i}$ and continues with $(\mathsf{sched}^{\mathsf{g}}\ q\ (k\mathtt{i}))$, thus switching arguments.

Let $\mathtt{I}$ be a finite base type (so that $\mathsf{Res}^{\mathsf{g}}\,A$ is *finitary* polynomial). Let $\psi : A$, $\vartheta : \mathtt{O}$ and $\varphi : \mathsf{Res}^{\mathsf{g}}\,A$. We have the following formulae (where $\mathtt{i} : \mathtt{I}$):

$$\begin{array}{rlrl}[\mathsf{Ret}] & := [\mathsf{fold}][\mathsf{in}_0]\top & [\mathsf{out}_{\mathtt{i}}]\vartheta & := [\mathsf{fold}][\mathsf{in}_1]\,([\mathtt{i}] \Vdash\!\!\!\to [\pi_0]\vartheta) \\ [\mathsf{now}]\psi & := [\mathsf{fold}][\mathsf{in}_0]\psi & \bigcirc_{\mathtt{i}}\varphi & := [\mathsf{fold}][\mathsf{in}_1]\,([\mathtt{i}] \Vdash\!\!\!\to [\pi_1][\mathsf{next}]\varphi)\end{array}$$

The formula [Ret] (resp. $[\mathsf{now}]\psi$) holds on a resumption which immediately returns (resp. with a value satisfying ψ) and we have $\mathsf{Ret}^{\mathsf{g}} : A \to \{\mathsf{Res}^{\mathsf{g}}\,A \mid [\mathsf{Ret}]\}$, $\mathsf{Ret}^{\mathsf{g}} : \{A \mid \psi\} \to \{\mathsf{Res}^{\mathsf{g}}\,A \mid [\mathsf{now}]\psi\}$. Moreover, the typings

$$\begin{array}{ll}\mathsf{Cont}^{\mathsf{g}} : \{\mathtt{I} \to (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A) \mid [\mathtt{i}] \Vdash\!\!\!\to [\pi_0]\vartheta\} & \longrightarrow \{\mathsf{Res}^{\mathsf{g}}\,A \mid [\mathsf{out}_{\mathtt{i}}]\vartheta\} \\ \mathsf{Cont}^{\mathsf{g}} : \{\mathtt{I} \to (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A) \mid [\mathtt{i}] \Vdash\!\!\!\to [\pi_1][\mathsf{next}]\varphi\} & \longrightarrow \{\mathsf{Res}^{\mathsf{g}}\,A \mid \bigcirc_{\mathtt{i}}\varphi\}\end{array}$$

express that $[\mathsf{out}_{\mathtt{i}}]\vartheta : \mathsf{Res}^{\mathsf{g}}\,A$ is satisfied by $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$ if $f\mathtt{i}$ satisfies ϑ, and that $\bigcirc_{\mathtt{i}}\varphi : \mathsf{Res}^{\mathsf{g}}\,A$ is satisfied by $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$ if $k\mathtt{i}$ satisfies $[\mathsf{next}]\varphi$. Since $\mathtt{I}$ is a finite base type, it is possible to quantify over its inhabitants. We thus obtain CTL-like variants of $\Box$ and $\Diamond$ (Ex. 4.3.(b) and Ex. 6.3). Namely:

$$\begin{array}{rlrl}[\wedge\mathsf{out}]\vartheta & := \wedge_{\mathtt{i}\in\mathtt{I}}[\mathsf{out}_{\mathtt{i}}]\vartheta : \mathsf{Res}^{\mathsf{g}}\,A & \owedge\,\varphi & := \wedge_{\mathtt{i}\in\mathtt{I}} \bigcirc_{\mathtt{i}}\,\varphi \ : \mathsf{Res}^{\mathsf{g}}\,A \\ [\vee\mathsf{out}]\vartheta & := \vee_{\mathtt{i}\in\mathtt{I}}[\mathsf{out}_{\mathtt{i}}]\vartheta : \mathsf{Res}^{\mathsf{g}}\,A & \ovee\,\varphi & := \vee_{\mathtt{i}\in\mathtt{I}} \bigcirc_{\mathtt{i}}\,\varphi \ : \mathsf{Res}^{\mathsf{g}}\,\varphi \\ \forall\Box\varphi & := \nu\alpha.\ \varphi \wedge \owedge\,\alpha : \mathsf{Res}^{\mathsf{g}}\,A & \forall\Diamond\varphi & := \mu\alpha.\ \varphi \vee \owedge\,\alpha : \mathsf{Res}^{\mathsf{g}}\,A \\ \exists\Box\varphi & := \nu\alpha.\ \varphi \wedge \ovee\,\alpha : \mathsf{Res}^{\mathsf{g}}\,A & \exists\Diamond\varphi & := \mu\alpha.\ \varphi \vee \ovee\,\alpha : \mathsf{Res}^{\mathsf{g}}\,A\end{array}$$

Our system can prove that $\boldsymbol{\Gamma}[\![\mathsf{sched}]\!]$ returns in finite time when so do its arguments, either along *some* or along *any* sequence of inputs. We moreover have expected $\Box\Diamond$ properties for all possible (consistent) combinations of $\exists/\forall$ and [Ret]/$[\vee\mathsf{out}]$/$[\wedge\mathsf{out}]$ (Table 4, with $\psi : A$, $\vartheta : \mathtt{O}$ safe and smooth). See §E.7. $\square$

Example 8.6 (Breadth-First Traversal). The function $\mathsf{bft}^{\mathsf{g}}$ of Table 3 (where $g^{\circledast}$ stands for $\lambda x.g \circledast x$) implements Martin Hofmann's algorithm for breadth-first tree traversal. This algorithm involves the higher-order type $\mathsf{Rou}^{\mathsf{g}}\, A$ (see Ex. 3.2) with constructors $\mathsf{Over}^{\mathsf{g}} := \mathsf{fold}(\mathsf{in}_0\langle\rangle) : \mathsf{Rou}^{\mathsf{g}}\, A$ and

$$\mathsf{Cont}^{\mathsf{g}} := \lambda f.\mathsf{fold}(\mathsf{in}_1 f) : \big((\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\, A \to \blacktriangleright A) \to A\big) \to \mathsf{Rou}^{\mathsf{g}}\, A$$

We refer to [10] for explanations. Consider a formula $\varphi : A$. We can lift φ to

$$[\mathsf{Rou}]\varphi := \nu\alpha.\ [\mathsf{fold}][\mathsf{in}_1](([\mathsf{next}]\alpha \Vdash\!\!\to [\mathsf{next}]\varphi) \Vdash\!\!\to \varphi) : \mathsf{Rou}^{\mathsf{g}}\, A$$

We then easily derive the expected refinement type of $\mathsf{bft}^{\mathsf{g}}$ (Table 4, where $\vartheta : C$). Assume that ϑ is safe. On the one hand it is not clear what the meaning of $[\mathsf{Rou}]\vartheta$ is, because it is an unsafe formula over a non-polynomial type. On the other hand, the type of $\mathsf{bft}^{\mathsf{g}}$ in Tab. 4 has its standard expected meaning (namely: if all nodes of a tree satisfy ϑ then so do all elements of its traversal) because the types $\mathsf{Tree}^{\mathsf{g}}\, C$, $\mathsf{CoList}^{\mathsf{g}}\, C$ are polynomial and the formulae $\forall\Box[\mathsf{lbl}]\vartheta$, $\Box[\mathsf{hd}]\vartheta$ are safe. Hence, our system can prove standard statements via detours through non-standard ones, which illustrates its compositionality. We have the same typing for a usual breadth-first tree traversal with forests (*à la* [39]). See §E.8. $\Box$

9 Related Work

Type systems based on guarded recursion have been designed to enforce properties of programs handling coinductive types, like causality [49], productivity [5,55,20,6,28,27], or termination [67]. These properties are captured by the type systems, meaning that all well-typed programs satisfy these properties.

In an initially different line of work, temporal logics have been used as type systems for functional reactive programming (FRP), starting from LTL [35,36] to the intuitionistic modal μ-calculus [18]. These works follow the Curry-Howard "proof-as-programs" paradigm, and reflect in the programming languages the constructions of the temporal logic.

The FRP approach has been adapted to guarded recursion, e.g. for the absence of space leaks [48], or the absence of time leaks, with the Fitch-style system of [7]. This more recently lead [8] to consider liveness properties with an FRP approach based on guarded recursion. In this system, the guarded λ-calculus (presented in a Fitch-style type system) is extended with a delay modality (written $\bigcirc$) together with a "until type" A Until B. Following the Curry-Howard correspondence, A Until B is eliminated with a specific recursor, based on the usual unfolding of Until in LTL, and distinct from the guarded fixpoint operator.

In these Curry-Howard approaches, temporal operators are wired into the structure of types. This means that there is no separation between the program and the proof that it satisfies a given temporal property. Different type formers having different program constructs, different temporal specifications for the same program may lead to different actual code.

We have chosen a different approach, based on refinement types, with which the structure of formulae is not reflected in the structure of types. This allows for our examples to be mostly written in a usual guarded recursive fashion (see Table 3). Of course, we indeed use the modality $\blacksquare$ at the type level as a separation between safety and liveness properties. But different liveness properties (e.g. $\Diamond$, $\Diamond\Box$, $\Box\Diamond$) are uniformly handled with the same $\blacksquare$-type, which is moreover the expected one in the guarded λ-calculus [20].

Higher-order model checking (HOMC) [59,43] has been introduced to check *automatically* that higher-order recursion schemes, a simple form of higher-order programs with *finite* data-types, satisfy a μ-calculus formula. Automatic verification of higher-order programs with infinite data-types (integers) has been explored for safety [44], termination [50], and more generally ω-regular [56] properties. In presence of infinite datatypes, semi-automatic extensions of HOMC have recently been proposed [74]. In contrast with this paper, most HOMC approaches do not consider input-output behaviors on coalgebraic data. A notable exception is [45,26], but it does not handle higher-order functions (such as map), nor polynomial types such as $\mathsf{Str}(\mathsf{Str}\,A)$ (Ex. 8.3) or non-positive types such as $\mathsf{Rou}\,A$ (Ex. 8.6) and imposes a strong linearity constraint on pattern matching.

Event-driven approaches consider effects generating streams of events [66], which can be checked for temporal properties with algorithms based on (HO)MC [30,31], or, in presence of infinite datatypes, with refinement type systems [46,58]. Our iteration terms can be seen as oracles, as required by [46] to handle liveness properties, but we do not know if they allow for the non-regular specifications of [58]. While such approaches can handle infinite data types with good levels of automation, they do not have coinductive types nor branching time properties, such as the temporal specification of sched on resumptions (Ex. 8.5)

Along similar lines, branching was approached via non-determinism in [69], which also handles universal and existential properties on traces. This framework can handle CTL-like properties of the form $\exists/\forall$-$\Box/\Diamond$ (with our notation of Ex. 8.5), but not nested combinations of these (as e.g. $\exists\Box\forall\Diamond$ for sched in Ex. 8.5). It moreover does not handle coinductive types.

10 Conclusion and Future Work

We have presented a refinement type system for the guarded λ-calculus, with refinements expressing temporal properties stated as (alternation-free) μ-calculus formulae. As we have seen, the system is general enough to prove precise behavioral input/output properties of coinductively-typed programs. Our main contribution is to handle liveness properties in presence of guarded recursive types. As seen in §2, this comes with inherent difficulties. In general, once guarded recursive functions are packed into coinductive ones using $\blacksquare$, the logical reasoning is made in our system directly on top of programs, following their shape, but requiring no further modification. We thus believe to have achieved some separation between programs and proofs.

We provided several examples. While they demonstrate the flexibility of our system, they also show that more abstraction would be welcomed when proving liveness properties. In addition, our system lacks expressiveness to prove e.g. liveness properties on breadth-first tree traversals.

We believe that our approach could be generalized to other programming languages with inductive or coinductive types. The key requirement are: (1) modalities in the temporal logic to navigate through the types of the languages, (2) a semantics to indicate when a program satisfies a formula of the temporal logic, which is sufficiently closed to the set-theoretic one for liveness properties to get their expected meaning, and (3) inference rules to reason over this realizability semantics.

Extensions of the guarded λ-calculus with dependent types have been explored [14,11,6,27]. It may be possible to extend our work to these systems. This would require to work in a Fitch-style presentation of the $\blacksquare$ modality, as in [7,12], since it is not known how to extend delayed substitutions to dependent types while retaining decidability of type-checking [15]. Also, it is appealing to investigate the generalization of our approach to sized types [1], in which guarded recursive types are representable [72].

We plan to investigate type checking. For instance, in a decidable fragment like the μ-calculus on streams, one can check that a function of type $\{\mathsf{Str}^{\mathsf{g}}\, C \mid \Diamond\Box[\mathsf{hd}]\vartheta\} \to \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Diamond\Box[\mathsf{hd}]\psi\}$ can be postcomposed with one of type $\{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box\Diamond[\mathsf{hd}]\psi\} \to \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box\Diamond[\mathsf{hd}]\varphi\}$ (since $\Diamond\Box[\mathsf{hd}]\psi \Rightarrow \Box\Diamond[\mathsf{hd}]\psi$). Hence, we expect that some automation is possible for fragments of our logic. In presence of iteration terms, arithmetic extensions of the μ-calculus [41,42] may provide interesting backends. An other direction is the interaction with HOMC. If (say) a stream over A is representable in a suitable format, one may use HOMC to check whether it can be argument of a function expecting e.g. a stream of type $\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box\Diamond[\mathsf{hd}]\varphi\}$. This might provide automation for fragments of the guarded λ-calculus. Besides, the combination of refinement types with automatic techniques like predicate abstraction [62], abstract interpretation [37], or SMT solvers [71,70] has been particularly successful. More recently, the combination of refinement types inference with HOMC has been investigated [64].

We would like to explore temporal specification of general, effectful programs. To do so, we wish to develop the treatment of the coinductive resumptions monad [60], that provides a general framework to reason on effectful computations, as shown by interaction trees [75]. It would be interesting to study temporal specifications we could give to effectful programs encoded in this setting. To formalize reasoning on such examples, we would like to design an embedding of our system in a proof assistant like Coq.

Following [3], guarded recursion has been used to abstract the reasoning on step-indexing [4] that has been used to design Kripke Logical Relations [2] for typed higher-order effectful programming languages. Program logics for reasoning on such logical relations [21,22] uses this representation of step-indexing via guarded recursion. It is also found in Iris [40], a framework for higher-order concurrent separation logic. It would be interesting to explore the incorporation of temporal reasoning, especially liveness properties, in such logics.

References

1. Abel, A., Pientka, B.: Well-founded recursion with copatterns and sized types. J. Funct. Program. **26**, e2 (2016). https://doi.org/10.1017/S0956796816000022, https://doi.org/10.1017/S0956796816000022 25
2. Ahmed, A.: Step-Indexed Syntactic Logical Relations for Recursive and Quantified Types. In: Proceedings of the 15th European Conference on Programming Languages and Systems. pp. 69–83. ESOP'06, Springer-Verlag, Berlin, Heidelberg (2006). https://doi.org/10.1007/11693024_6, https://doi.org/10.1007/11693024_6 25
3. Appel, A., Melliès, P.A., Richards, C., Vouillon, J.: A Very Modal Model of a Modern, Major, General Type System. SIGPLAN Not. **42**(1), 109–122 (2007). https://doi.org/10.1145/1190215.1190235, https://doi.org/10.1145/1190215.1190235 25
4. Appel, A.W., McAllester, D.: An Indexed Model of Recursive Types for Foundational Proof-Carrying Code. ACM Trans. Program. Lang. Syst. **23**(5), 657–683 (2001). https://doi.org/10.1145/504709.504712, https://doi.org/10.1145/504709.504712 25
5. Atkey, R., McBride, C.: Productive coprogramming with guarded recursion. In: Proceedings of the 18th ACM SIGPLAN International Conference on Functional Programming. pp. 197–208. ICFP '13, ACM, New York, NY, USA (2013). https://doi.org/10.1145/2500365.2500597 2, 23
6. Bahr, P., Grathwohl, H.B., Møgelberg, R.E.: The Clocks Are Ticking: No More Delays! In: 2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). pp. 1–12 (2017). https://doi.org/10.1109/LICS.2017.8005097 23, 25
7. Bahr, P., Graulund, C., Møgelberg, R.: Simply RaTT: A Fitch-Style Modal Calculus for Reactive Programming without Space Leaks. Proc. ACM Program. Lang. **3**(ICFP), 109:1–109:27 (2019). https://doi.org/10.1145/3341713 2, 23, 25
8. Bahr, P., Graulund, C., Møgelberg, R.: Diamonds are not Forever: Liveness in Reactive Programming with Guarded Recursion (2020), https://arxiv.org/abs/2003.03170, To Appear in POPL'21 2, 21, 22, 23, 66
9. Baier, C., Katoen, J.P.: Principles of Model Checking. The MIT Press (2008) 1, 48
10. Berger, U., Matthes, R., Setzer, A.: Martin Hofmann's Case for Non-Strictly Positive Data Types. In: Dybjer, P., Espírito Santo, J., Pinto, L. (eds.) 24th International Conference on Types for Proofs and Programs (TYPES 2018), Leibniz International Proceedings in Informatics (LIPIcs), vol. 130, pp. 1:1–1:22. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2019). https://doi.org/10.4230/LIPIcs.TYPES.2018.1, https://hal.archives-ouvertes.fr/hal-02365814 2, 7, 13, 21, 23, 103
11. Birkedal, L., Bizjak, A., Clouston, R., Grathwohl, H.B., Spitters, B., Vezzosi, A.: Guarded cubical type theory. Journal of Automated Reasoning **63**(2), 211–253 (2019). https://doi.org/10.1007/s10817-018-9471-7 25
12. Birkedal, L., Clouston, R., Mannaa, B., Møgelberg, R., Pitts, A.M., Spitters, B.: Modal dependent type theory and dependent right adjoints. Mathematical Structures in Computer Science **30**(2), 118–138 (2020). https://doi.org/10.1017/S0960129519000197 25
13. Birkedal, L., Møgelberg, R.E., Schwinghammer, J., Støvring, K.: First steps in synthetic guarded domain theory: step-indexing in the topos of trees. Logical Methods in Computer Science **8**(4) (2012) 2, 5, 16, 17, 18, 35, 40, 43

14. Bizjak, A., Grathwohl, H.B., Clouston, R., Møgelberg, R.E., Birkedal, L.: Guarded Dependent Type Theory with Coinductive Types. In: Jacobs, B., Löding, C. (eds.) Foundations of Software Science and Computation Structures. pp. 20–35. Springer Berlin Heidelberg, Berlin, Heidelberg (2016) 25
15. Bizjak, A., Møgelberg, R.E.: Denotational semantics for guarded dependent type theory. Mathematical Structures in Computer Science **30**(4), 342–378 (2020). https://doi.org/10.1017/S0960129520000080 25
16. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge Tracts in Theoretical Computer Science, Cambridge University Press (2002) 33
17. Bradfield, J.C., Walukiewicz, I.: The mu-calculus and Model Checking. In: Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R. (eds.) Handbook of Model Checking, pp. 871–919. Springer (2018) 6, 14, 15
18. Cave, A., Ferreira, F., Panangaden, P., Pientka, B.: Fair Reactive Programming. In: Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 361–372. POPL '14, ACM, New York, NY, USA (2014) 2, 21, 22, 23, 66
19. Chellas, B.F.: Modal Logic: An Introduction. Cambridge University Press (1980) 32
20. Clouston, R., Bizjak, A., Bugge Grathwohl, H., Birkedal, L.: The Guarded Lambda-Calculus: Programming and Reasoning with Guarded Recursion for Coinductive Types. Logical Methods in Computer Science **12**(3) (2016) 2, 6, 7, 17, 23, 24, 32, 35, 36, 37, 45, 47, 125, 129
21. Dreyer, D., Ahmed, A., Birkedal, L.: Logical Step-Indexed Logical Relations. Logical Methods in Computer Science **Volume 7, Issue 2** (2011). https://doi.org/10.2168/LMCS-7(2:16)2011, https://lmcs.episciences.org/698 25
22. Dreyer, D., Neis, G., Rossberg, A., Birkedal, L.: A Relational Modal Logic for Higher-order Stateful ADTs. In: Proceedings POPL'10. pp. 185–198. ACM (2010) 25
23. Elliott, C., Hudak, P.: Functional Reactive Animation. In: Proceedings of the Second ACM SIGPLAN International Conference on Functional Programming. pp. 263–273. ICFP'97, ACM, New York, NY, USA (1997). https://doi.org/10.1145/258948.258973, http://doi.acm.org/10.1145/258948.258973 2
24. Freeman, T., Pfenning, F.: Refinement Types for ML. In: Proceedings of the ACM SIGPLAN 1991 Conference on Programming Language Design and Implementation. pp. 268–277. PLDI'91, Association for Computing Machinery, New York, NY, USA (1991). https://doi.org/10.1145/113445.113468, https://doi.org/10.1145/113445.113468 1
25. Frittella, S.: Monotone Modal Logics & Friends. Ph.D. thesis, Aix-Marseille Univ. (2014) 32
26. Fujima, K., Ito, S., Kobayashi, N.: Practical Alternating Parity Tree Automata Model Checking of Higher-Order Recursion Schemes. In: APLAS '13: Proceedings of the 11th Asian Symposium on Programming Languages and Systems - Volume 8301. pp. 17–32. Springer-Verlag, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-319-03542-0_2, https://doi.org/10.1007/978-3-319-03542-0_2 24
27. Gratzer, D., Kavvos, G.A., Nuyts, A., Birkedal, L.: Multimodal dependent type theory. In: Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science. pp. 492–506. LICS '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3373718.3394736, https://doi.org/10.1145/3373718.3394736 23, 25

28. Guatto, A.: A Generalized Modality for Recursion. In: Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science. pp. 482–491. LICS '18, ACM, New York, NY, USA (2018). https://doi.org/10.1145/3209108.3209148 23
29. Hansen, H.H.: Monotonic Modal Logics. Master's thesis, ILLC, Amsterdam (Oct 2003) 32
30. Hofmann, M., Chen, W.: Abstract interpretation from büchi automata. In: Henzinger, T.A., Miller, D. (eds.) Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS '14, Vienna, Austria, July 14 - 18, 2014. pp. 51:1–51:10. ACM (2014). https://doi.org/10.1145/2603088.2603127, https://doi.org/10.1145/2603088.2603127 24
31. Hofmann, M., Ledent, J.: A cartesian-closed category for higher-order model checking. In: 32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017. pp. 1–12. IEEE Computer Society (2017). https://doi.org/10.1109/LICS.2017.8005120, https://doi.org/10.1109/LICS.2017.8005120 24
32. Jacobs, B.: Categorical Logic and Type Theory. Studies in logic and the foundations of mathematics, Elsevier (2001) 18, 41
33. Jacobs, B.: Many-Sorted Coalgebraic Modal Logic: a Model-theoretic Study. ITA **35**(1), 31–59 (2001) 4, 8, 17
34. Jacobs, B.: Introduction to Coalgebra: Towards Mathematics of States and Observation. Cambridge Tracts in Theoretical Computer Science, Cambridge University Press (2016) 13, 17
35. Jeffrey, A.: LTL Types FRP: Linear-time Temporal Logic Propositions As Types, Proofs As Functional Reactive Programs. In: Proceedings of the Sixth Workshop on Programming Languages Meets Program Verification. pp. 49–60. PLPV'12, ACM, New York, NY, USA (2012). https://doi.org/10.1145/2103776.2103783, http://doi.acm.org/10.1145/2103776.2103783 2, 23
36. Jeltsch, W.: An Abstract Categorical Semantics for Functional Reactive Programming with Processes. In: Proceedings of the ACM SIGPLAN 2014 Workshop on Programming Languages Meets Program Verification. pp. 47–58. PLPV'14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2541568.2541573, http://doi.acm.org/10.1145/2541568.2541573 2, 23
37. Jhala, R., Majumdar, R., Rybalchenko, A.: HMC: Verifying functional programs using abstract interpreters. In: International Conference on Computer Aided Verification. pp. 470–485. Springer (2011) 25
38. Johnstone, P.: Sketches of an Elephant: A Topos Theory Compendium. Oxford Logic Guides, Clarendon Press (2002) 39, 45
39. Jones, G., Gibbons, J.: Linear-time Breadth-first Tree Algorithms: An Exercise in the Arithmetic of Folds and Zips. Technical report, University of Auckland (1993) 2, 21, 23
40. Jung, R., Krebbers, R., Jourdan, J.H., Bizjak, A., Birkedal, L., Dreyer, D.: Iris from the ground up: A modular foundation for higher-order concurrent separation logic. Journal of Functional Programming **28** (2018) 25
41. Kobayashi, K., Nishikawa, T., Igarashi, A., Unno, H.: Temporal Verification of Programs via First-Order Fixpoint Logic. In: Chang, B.E. (ed.) Static Analysis - 26th International Symposium, SAS 2019, Porto, Portugal, October 8-11, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11822, pp. 413–436.

Springer (2019). https://doi.org/10.1007/978-3-030-32304-2_20, https://doi.org/10.1007/978-3-030-32304-2_20 25

42. Kobayashi, N., Fedyukovich, G., Gupta, A.: Fold/Unfold Transformations for Fixpoint Logic. In: Biere, A., Parker, D. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 26th International Conference, TACAS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12079, pp. 195–214. Springer (2020). https://doi.org/10.1007/978-3-030-45237-7_12, https://doi.org/10.1007/978-3-030-45237-7_12 25
43. Kobayashi, N., Ong, C.H.L.: A type system equivalent to the modal mu-calculus model checking of higher-order recursion schemes. In: 2009 24th Annual IEEE Symposium on Logic In Computer Science. pp. 179–188. IEEE (2009) 24
44. Kobayashi, N., Sato, R., Unno, H.: Predicate abstraction and CEGAR for higher-order model checking. SIGPLAN Not. **46**(6), 222–233 (2011). https://doi.org/10.1145/1993316.1993525, https://doi.org/10.1145/1993316.1993525 24
45. Kobayashi, N., Tabuchi, N., Unno, H.: Higher-Order Multi-Parameter Tree Transducers and Recursion Schemes for Program Verification. In: POPL '10: Proceedings of the 37th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages. pp. 495–508. Association for Computing Machinery, New York, NY, USA (2010). https://doi.org/10.1145/1707801.1706355, https://doi.org/10.1145/1707801.1706355 2, 24
46. Koskinen, E., Terauchi, T.: Local Temporal Reasoning. In: Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). CSL-LICS'14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2603088.2603138, https://doi.org/10.1145/2603088.2603138 24
47. Kozen, D.: Results on the propositional μ-calculus. Theoretical Computer Science **27**(3), 333 – 354 (1983), special Issue Ninth International Colloquium on Automata, Languages and Programming (ICALP) Aarhus, Summer 1982 4, 10
48. Krishnaswami, N.R.: Higher-order functional reactive programming without spacetime leaks. In: Proceedings of ICFP'13. pp. 221–232. ACM, New York, NY, USA (2013) 2, 7, 21, 22, 23, 91, 92
49. Krishnaswami, N.R., Benton, N.: Ultrametric Semantics of Reactive Programs. In: 2011 IEEE 26th Annual Symposium on Logic in Computer Science. pp. 257–266 (2011). https://doi.org/10.1109/LICS.2011.38 23
50. Kuwahara, T., Terauchi, T., Unno, H., Kobayashi, N.: Automatic Termination Verification for Higher-Order Functional Programs. In: Shao, Z. (ed.) Programming Languages and Systems. pp. 392–411. ESOP'14, Springer Berlin Heidelberg, Berlin, Heidelberg (2014) 24
51. Lambek, J., Scott, P.J.: Introduction to Higher Order Categorical Logic. CUP (1986) 49
52. Mac Lane, S., Moerdijk, I.: Sheaves in geometry and logic: A first introduction to topos theory. Springer (1992) 16, 18, 35, 39, 40, 41, 42, 47, 49, 111
53. Marin, S.: Modal proof theory through a focused telescope. Phd thesis, Université Paris Saclay (Jan 2018), https://hal.archives-ouvertes.fr/tel-01951291 10
54. McBride, C., Paterson, R.: Applicative programming with effects. Journal of Functional Programming **18**(1) (2008). https://doi.org/10.1017/S0956796807006326 3

55. Møgelberg, R.E.: A type theory for productive coprogramming via guarded recursion. In: Proceedings of CSL-LICS 2014. CSL-LICS '14, ACM (2014) 2, 5, 17, 23, 48, 49
56. Murase, A., Terauchi, T., Kobayashi, N., Sato, R., Unno, H.: Temporal Verification of Higher-Order Functional Programs. In: Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 57–68. POPL'16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2837614.2837667, https://doi.org/10.1145/2837614.2837667 24
57. Nakano, H.: A Modality for Recursion. In: Proceedings of LICS'00. pp. 255–266. IEEE Computer Society (2000) 2
58. Nanjo, Y., Unno, H., Koskinen, E., Terauchi, T.: A Fixpoint Logic and Dependent Effects for Temporal Property Verification. In: Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science. pp. 759–768. LICS'18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3209108.3209204, https://doi.org/10.1145/3209108.3209204 24
59. Ong, C.H.L.: On Model-Checking Trees Generated by Higher-Order Recursion Schemes. In: Proceedings of LICS 2006. pp. 81–90. IEEE Computer Society (2006) 24
60. Piróg, M., Gibbons, J.: The coinductive resumption monad. Electronic Notes in Theoretical Computer Science **308**, 273–288 (2014) 25
61. Plotkin, G., Stirling, C.: A Framework for Intuitionistic Modal Logics: Extended Abstract. In: Proceedings of the 1986 Conference on Theoretical Aspects of Reasoning About Knowledge. pp. 399–406. TARK '86, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1986) 10, 33
62. Rondon, P.M., Kawaguci, M., Jhala, R.: Liquid Types. In: Proceedings of the 29th ACM SIGPLAN Conference on Programming Language Design and Implementation. pp. 159–169. PLDI'08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1375581.1375602, https://doi.org/10.1145/1375581.1375602 25
63. Santocanale, L., Venema, Y.: Completeness for flat modal fixpoint logics. Ann. Pure Appl. Logic **162**(1), 55–82 (2010) 14, 15
64. Sato, R., Iwayama, N., Kobayashi, N.: Combining higher-order model checking with refinement type inference. In: Hermenegildo, M.V., Igarashi, A. (eds.) Proceedings of the 2019 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation, PEPM@POPL 2019, Cascais, Portugal, January 14-15, 2019. pp. 47–53. ACM (2019). https://doi.org/10.1145/3294032.3294081, https://doi.org/10.1145/3294032.3294081 25
65. Simpson, A.K.: The Proof Theory and Semantics of Intuitionistic Modal Logic. Phd thesis, University of Edinburgh (Jul 1994), https://www.era.lib.ed.ac.uk/handle/1842/407 10
66. Skalka, C., Smith, S., Van horn, D.: Types and Trace Effects of Higher Order Programs. J. Funct. Program. **18**(2), 179–249 (Mar 2008). https://doi.org/10.1017/S0956796807006466, https://doi.org/10.1017/S0956796807006466 24
67. Spies, S., Krishnaswami, N., Dreyer, D.: Transfinite Step-Indexing for Termination. Proc. ACM Program. Lang. **5**(POPL) (Jan 2021). https://doi.org/10.1145/3434294, https://doi.org/10.1145/3434294 23

68. Sprenger, C., Dam, M.: On the Structure of Inductive Reasoning: Circular and Tree-Shaped Proofs in the μ-Calculus. In: Gordon, A.D. (ed.) Foundations of Software Science and Computational Structures, 6th International Conference, FOSSACS 2003 Held as Part of the Joint European Conference on Theory and Practice of Software, ETAPS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2620, pp. 425–440. Springer (2003). https://doi.org/10.1007/3-540-36576-1_27, https://doi.org/10.1007/3-540-36576-1_27 14
69. Unno, H., Satake, Y., Terauchi, T.: Relatively complete refinement type system for verification of higher-order non-deterministic programs. Proc. ACM Program. Lang. **2**(POPL), 12:1–12:29 (2018). https://doi.org/10.1145/3158100, https://doi.org/10.1145/3158100 24
70. Vazou, N.: Liquid Haskell: Haskell as a theorem prover. Ph.D. thesis, UC San Diego (2016) 25
71. Vazou, N., Seidel, E.L., Jhala, R., Vytiniotis, D., Peyton-Jones, S.: Refinement Types for Haskell. In: Proceedings of the 19th ACM SIGPLAN International Conference on Functional Programming. pp. 269–282. ICFP'14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2628136.2628161, https://doi.org/10.1145/2628136.2628161 25
72. Veltri, N., van der Weide, N.: Guarded Recursion in Agda via Sized Types. In: Geuvers, H. (ed.) 4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019). Leibniz International Proceedings in Informatics (LIPIcs), vol. 131, pp. 32:1–32:19. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany (2019). https://doi.org/10.4230/LIPIcs.FSCD.2019.32, http://drops.dagstuhl.de/opus/volltexte/2019/10539 25
73. Walukiewicz, I.: Completeness of Kozen's Axiomatisation of the Propositional μ-Calculus. Information and Computation **157**(1-2), 142–182 (2000) 14
74. Watanabe, K., Tsukada, T., Oshikawa, H., Kobayashi, N.: Reduction from Branching-Time Property Verification of Higher-Order Programs to HFL Validity Checking. In: Proceedings of the 2019 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation. pp. 22–34. PEPM 2019, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3294032.3294077, https://doi.org/10.1145/3294032.3294077 24
75. Xia, L.Y., Zakowski, Y., He, P., Hur, C.K., Malecha, G., Pierce, B.C., Zdancewic, S.: Interaction Trees: Representing Recursive and Impure Programs in Coq. Proc. ACM Program. Lang. **4**(POPL) (2019). https://doi.org/10.1145/3371119, https://doi.org/10.1145/3371119 25

$$\frac{(x : A) \in \mathcal{E}}{\mathcal{E} \vdash x : A} \qquad \frac{\mathcal{E}, x : B \vdash M : A}{\mathcal{E} \vdash \lambda x.M : B \to A} \qquad \frac{\mathcal{E} \vdash M : B \to A \quad \mathcal{E} \vdash N : B}{\mathcal{E} \vdash MN : A} \qquad \frac{}{\mathcal{E} \vdash \langle\rangle : \mathbf{1}} \qquad \frac{\mathcal{E} \vdash M_0 : A_0 \quad \mathcal{E} \vdash M_1 : A_1}{\mathcal{E} \vdash \langle M_0, M_1 \rangle : A_0 \times A_1}$$

$$\frac{\mathcal{E} \vdash M : A_i}{\mathcal{E} \vdash \mathsf{in}_i(M) : A_0 + A_1} \qquad \frac{\mathcal{E} \vdash M : A_0 + A_1 \quad \begin{array}{c}\text{for } i \in \{0,1\},\\ \mathcal{E}, x : A_i \vdash N_i : B\end{array}}{\mathcal{E} \vdash \mathsf{case}\, M \,\mathsf{of}\, (x.N_0 | x.N_1) : B} \qquad \frac{\mathcal{E} \vdash M : A_0 \times A_1}{\mathcal{E} \vdash \pi_i(M) : A_i} \qquad \frac{\mathcal{E}, x : \blacktriangleright A \vdash M : A}{\mathcal{E} \vdash \mathsf{fix}(x).M : A}$$

$$\frac{\mathcal{E} \vdash M : A[\mathsf{Fix}(X).A/X]}{\mathcal{E} \vdash \mathsf{fold}(M) : \mathsf{Fix}(X).A} \qquad \frac{\mathcal{E} \vdash M : \mathsf{Fix}(X).A}{\mathcal{E} \vdash \mathsf{unfold}(M) : A[\mathsf{Fix}(X).A/X]} \qquad \frac{\mathcal{E} \vdash M : \blacktriangleright(B \to A) \quad \mathcal{E} \vdash N : \blacktriangleright B}{\mathcal{E} \vdash M \circledast N : \blacktriangleright A}$$

$$\frac{\mathcal{E} \vdash M : A}{\mathcal{E} \vdash \mathsf{next}(M) : \blacktriangleright A} \qquad \frac{x_1 : A_1, \ldots, x_k : A_k \vdash M : A \quad \mathcal{E} \vdash M_i : A_i \text{ with } A_i \text{ constant for } 1 \leq i \leq k}{\mathcal{E} \vdash \mathsf{prev}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : A}$$

$$\frac{x_1 : A_1, \ldots, x_k : A_k \vdash M : A \quad \mathcal{E} \vdash M_i : A_i \text{ with } A_i \text{ constant for } 1 \leq i \leq k}{\mathcal{E} \vdash \mathsf{box}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : \blacksquare A} \qquad \frac{\mathcal{E} \vdash M : \blacksquare A}{\mathcal{E} \vdash \mathsf{unbox}(M) : A}$$

Fig. 14. Typing Rules of the Pure Calculus (full version).

A Additional Material for §3 (The Pure Calculus)

The typing rules for our pure calculus (*i.e.* the guarded λ-calculus of [20]) are given in Fig. 14.

B Additional Material for §4 (A Temporal Modal Logic)

Figure 15 presents the definition of the variance predicates α Pos φ and α Neg φ for the *full* logical language (§4 and §6). The intuitionistic propositional deduction rules are given in Fig. 16.

Remark B.1. All modalities ($[\pi_i]$, $[\mathsf{fold}]$, $[\mathsf{next}]$, $[\mathsf{in}_i]$, $[\mathsf{ev}(\psi)]$ and $[\mathsf{box}]$) satisfy the *monotonicity rule* (RM) and are thus monotone in the sense of [19], from which we borrowed the terminology used in Table 2 (see also [29,25]). Assuming the rule (RM), we easily get the following:

(a) Axiom (N) implies the usual *necessitation rule*:

$$\frac{\vdash \varphi}{\vdash [\triangle]\varphi}\ (\mathsf{RN})$$

Proof. Indeed, one can derive

$$\dfrac{(\mathsf{N})\ \dfrac{}{\vdash [\triangle]\top} \qquad \dfrac{\dfrac{\varphi}{\vdash \top \Rightarrow \varphi}}{\vdash [\triangle]\top \Rightarrow [\triangle]\varphi}\ (\mathsf{RM})}{[\triangle]\varphi}$$

□

(b) Axiom (C) implies the usual axiom (K):

$$[\triangle](\varphi \Rightarrow \psi) \implies ([\triangle]\varphi \Rightarrow [\triangle]\psi)$$

$$\frac{}{\alpha \text{ Pos } \alpha} \qquad \frac{\alpha \neq \beta}{\alpha \text{ Pos } \beta} \qquad \frac{}{\alpha \text{ Pos } \top} \qquad \frac{}{\alpha \text{ Pos } \bot}$$

$$\frac{\alpha \text{ Pos } \varphi \qquad \alpha \text{ Pos } \psi}{\alpha \text{ Pos } \varphi \vee \psi} \qquad \frac{\alpha \text{ Pos } \varphi \qquad \alpha \text{ Pos } \psi}{\alpha \text{ Pos } \varphi \wedge \psi} \qquad \frac{\alpha \text{ Neg } \psi \qquad \alpha \text{ Pos } \varphi}{\alpha \text{ Pos } \psi \Rightarrow \varphi}$$

$$\frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\pi_i]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{in}_i]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{fold}]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{next}]\varphi} \qquad \frac{\alpha \text{ Neg } \psi \quad \alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{ev}(\psi)]\varphi}$$

$$\frac{\alpha \text{ Pos } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Pos } \nu\beta\varphi} \qquad \frac{\alpha \text{ Pos } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Pos } \mu\beta\varphi} \qquad \frac{\alpha \text{ Pos } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Pos } \nu^{\mathsf{t}}\beta\varphi} \qquad \frac{\alpha \text{ Pos } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Pos } \mu^{\mathsf{t}}\beta\varphi}$$

$$\frac{\alpha \neq \beta}{\alpha \text{ Neg } \beta} \qquad \frac{}{\alpha \text{ Neg } \top} \qquad \frac{}{\alpha \text{ Neg } \bot}$$

$$\frac{\alpha \text{ Neg } \varphi \qquad \alpha \text{ Neg } \psi}{\alpha \text{ Neg } \varphi \vee \psi} \qquad \frac{\alpha \text{ Neg } \varphi \qquad \alpha \text{ Neg } \psi}{\alpha \text{ Neg } \varphi \wedge \psi} \qquad \frac{\alpha \text{ Pos } \psi \qquad \alpha \text{ Neg } \varphi}{\alpha \text{ Neg } \psi \Rightarrow \varphi}$$

$$\frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\pi_i]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{in}_i]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{fold}]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{next}]\varphi} \qquad \frac{\alpha \text{ Pos } \psi \quad \alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{ev}(\psi)]\varphi}$$

$$\frac{\alpha \text{ Neg } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Neg } \nu\beta\varphi} \qquad \frac{\alpha \text{ Neg } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Neg } \mu\beta\varphi} \qquad \frac{\alpha \text{ Neg } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Neg } \nu^{\mathsf{t}}\beta\varphi} \qquad \frac{\alpha \text{ Neg } \varphi \qquad \alpha \neq \beta}{\alpha \text{ Neg } \mu^{\mathsf{t}}\beta\varphi}$$

Fig. 15. Positive and Negative Occurrences for the Full Logical Language.

Proof. Indeed, one has

$$\cfrac{\cfrac{\cfrac{\cfrac{}{\big((\varphi \Rightarrow \psi) \wedge \varphi\big) \implies \psi}}{[\triangle]\big((\varphi \Rightarrow \psi) \wedge \varphi\big) \implies [\triangle]\psi}\,(\mathsf{RM})}{[\triangle](\varphi \Rightarrow \psi) \wedge [\triangle]\varphi \implies [\triangle]\psi}\,(\mathsf{C})}{[\triangle](\varphi \Rightarrow \psi) \implies ([\triangle]\varphi \Rightarrow [\triangle]\psi)}$$

□

(c) We have the monotonicity axioms

$$[\triangle](\varphi \wedge \psi) \implies [\triangle]\varphi \wedge [\triangle]\psi$$
$$[\triangle]\varphi \vee [\triangle]\psi \implies [\triangle](\varphi \vee \psi)$$

In our context, the normal intuitionistic modal logic **IK** of [61] is $(\mathsf{RM}) + (\mathsf{C}) + (\mathsf{N}) + (\mathsf{P}) + (\mathsf{C}_\vee) + (\mathsf{C}_\Rightarrow)$, while the normal modal logic **K** is **IK** + (CL) (see e.g. [16]).

C Additional Material for §5 (A Temporally Refined Type System)

The definition of the subtyping relation $\leq$ for the *full* system (§5 and §6) is given in Fig. 17.

$$\frac{}{\vdash^A \varphi \vee \varphi \Rightarrow \varphi} \qquad \frac{}{\vdash^A \varphi \Rightarrow \varphi \wedge \varphi} \qquad \frac{}{\vdash^A \varphi \Rightarrow \varphi \vee \psi} \qquad \frac{}{\vdash^A \varphi \wedge \psi \Rightarrow \varphi}$$

$$\frac{}{\vdash^A \varphi \vee \psi \Rightarrow \psi \vee \varphi} \qquad \frac{}{\vdash^A \varphi \wedge \psi \Rightarrow \psi \wedge \varphi} \qquad \frac{\vdash^A \varphi \wedge \psi \Rightarrow \theta}{\vdash^A \varphi \Rightarrow (\psi \Rightarrow \theta)} \qquad \frac{\vdash^A \varphi \Rightarrow (\psi \Rightarrow \theta)}{\vdash^A \varphi \wedge \psi \Rightarrow \theta}$$

$$\frac{\vdash^A \varphi \qquad \vdash^A \varphi \Rightarrow \psi}{\vdash^A \psi} \qquad \frac{\vdash^A \varphi \Rightarrow \psi \qquad \vdash^A \psi \Rightarrow \theta}{\vdash^A \varphi \Rightarrow \theta} \qquad \frac{}{\vdash^A \bot \Rightarrow \varphi} \qquad \frac{\vdash^A \varphi \Rightarrow \psi}{\vdash^A \theta \vee \varphi \Rightarrow \theta \vee \psi}$$

Fig. 16. Intuitionistic Propositional Deduction Rules.

$$\frac{}{T \leq T} \qquad \frac{T \leq U \qquad U \leq V}{T \leq V} \qquad \frac{T \leq U}{\blacktriangleright T \leq \blacktriangleright U} \qquad \frac{U \leq T}{\blacksquare U \leq \blacksquare T}$$

$$\frac{T_0 \leq U_0 \quad T_1 \leq U_1}{T_0 \times T_1 \leq U_0 \times U_1} \qquad \frac{T_0 \leq U_0 \quad T_1 \leq U_1}{T_0 + T_1 \leq U_0 + U_1} \qquad \frac{U_0 \leq T_0 \quad T_1 \leq U_1}{T_0 \to T_1 \leq U_0 \to U_1}$$

$$\frac{}{T \leq |T|} \qquad \frac{}{A \leq \{A \mid \top\}} \qquad \frac{\vdash^A \varphi \Rightarrow \psi}{\{A \mid \varphi\} \leq \{A \mid \psi\}}$$

$$\frac{}{\{B \mid \psi\} \to \{A \mid \varphi\} \equiv \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}}$$

$$\frac{}{\blacktriangleright \{A \mid \varphi\} \equiv \{\blacktriangleright A \mid [\mathsf{next}]\varphi\}} \qquad \frac{}{\forall k \cdot \blacktriangleright T \equiv \blacktriangleright \forall k \cdot T}$$

$$\frac{\varphi \text{ safe}}{\blacksquare \{A \mid \varphi\} \equiv \{\blacksquare A \mid [\mathsf{box}]\varphi\}} \qquad \frac{\vdash^A_c \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathsf{box}]\varphi\} \leq \{\blacksquare A \mid [\mathsf{box}]\psi\}}$$

Fig. 17. Subtyping Rules (full version).

The *underlying pure type* $|T|$ of a refinement type T is inductively defined as follows:

$$\begin{aligned}
|A| &:= A \\
|\{A \mid \varphi\}| &:= A \\
|\forall k \cdot T| &:= |T| \\
|T + U| &:= |T| + |U| \\
|T \times U| &:= |T| \times |U| \\
|U \to T| &:= |U| \to |T| \\
|\blacktriangleright T| &:= \blacktriangleright |T| \\
|\blacksquare T| &:= \blacksquare |T|
\end{aligned}$$

D Additional Material for §7 (Semantics)

This Appendix presents material that we omitted in §7 for space reasons. We follow roughly the same plan. Most proofs a deferred to App. F. We often use θ as a generic notation for μ and ν.

D.1 The Topos of Trees (Basic Structure)

Note D.1. Given an object X of $\mathcal{S}$ and $0 < k \leq n$, we write $t{\uparrow}k$ for the restriction of $t \in X(n)$ into $X(k)$, obtained by composing restriction functions r_i^X for $i = k, \ldots, n-1$.

Full definitions and proofs of the semantic require the explicit manipulation of some of the structure of $\mathcal{S}$. We refer to [13,20] for details.

First, as in any presheaf category, limits and colimits are computed pointwise. In particular binary sums and products are given by

$$(X + Y)(n) = X(n) + Y(n)$$
$$(X \times Y)(n) = X(n) \times Y(n)$$

Moreover, exponentials are induced by the Yoneda Lemma (see e.g. [52, §I.6]). Explicitly, given $\mathcal{S}$ object X and Y, the exponent Y^X at n is the set of all sequences $(f_\ell)_{\ell \leq n}$ of functions $f_\ell : X(\ell) \to Y(\ell)$ which are compatible with restriction (*i.e.* $r_\ell^Y \circ f_{\ell+1} = f_\ell \circ r_\ell^X$).

The morphism $\mathsf{fix}^X : X^{\blacktriangleright X} \to X$ is defined as

$$\mathsf{fix}^X_n((f_m)_{m \leq n}) := (f_n \circ \cdots \circ f_1)(\bullet)$$

The morphism $\mathsf{fix}^X : X^{\blacktriangleright X} \to X$ is natural in X. Given $f : \blacktriangleright X \times Y \to X$ with exponential transpose $f^t : Y \to X^{\blacktriangleright X}$, the morphism $\mathsf{fix}^X \circ f^t : Y \to X$ is unique such that $\mathsf{fix}^X \circ f^t = f \circ \langle \mathsf{next}^X \circ \mathsf{fix}^X \circ f^T, \mathrm{id}^X \rangle$ ([13, Thm. 2.4]).

Since we do not require the explicit constructions, we refer to [13] for the interpretation of guarded recursive types $\mathsf{Fix}(X).A(X)$ and for the definition of the isos

$$\begin{array}{rl} \mathsf{fold} : & [\![A(\mathsf{Fix}(X).A(X))]\!] \longrightarrow [\![\mathsf{Fix}(X).A(X)]\!] \\ \mathsf{unfold} : & [\![\mathsf{Fix}(X).A(X)]\!] \longrightarrow [\![A(\mathsf{Fix}(X).A(X))]\!] \end{array}$$

We now have all the structure we need for the denotational semantics of the $\blacksquare$-free fragment of the pure calculus.

D.2 Global Sections and Constant Objects

As for any presheaf topos, the global section functor $\boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ is right adjoint to the constant object functor $\boldsymbol{\Delta} : \mathbf{Set} \to \mathcal{S}$ (see e.g. [52, §I.6]):

$$\begin{tikzcd} \mathcal{S} \arrow[r, bend left, "\boldsymbol{\Gamma}"] \arrow[r, phantom, "\top"] & \mathbf{Set} \arrow[l, bend left, "\boldsymbol{\Delta}"] \end{tikzcd}$$

We record the following easy well-known facts for later use.

Lemma D.2. *Given a set S and given X, Y objects of $\mathcal{S}$, we have in* $\mathbf{Set}$*:*

(1) the unit $\eta : \mathrm{Id}_{\mathbf{Set}} \to \boldsymbol{\Gamma}\boldsymbol{\Delta}$ of $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$ is an iso,

(2) $\boldsymbol{\Gamma}(X \times Y) \simeq \boldsymbol{\Gamma}X \times \boldsymbol{\Gamma}Y$ *and* $\boldsymbol{\Gamma}\mathbf{1} \simeq \mathbf{1}$
(3) $\boldsymbol{\Gamma}(X + Y) \simeq \boldsymbol{\Gamma}X + \boldsymbol{\Gamma}Y$
(4) $\boldsymbol{\Gamma}(X^{\boldsymbol{\Delta}S}) \simeq (\boldsymbol{\Gamma}X)^S$
(5) $\boldsymbol{\Gamma}(\blacktriangleright X) \simeq \boldsymbol{\Gamma}X$ *(via* $\boldsymbol{\Gamma}(\mathsf{next})$*)*

where all the mentioned isos are natural in X *and* Y *(when applicable).*

Proof.

(1) The unit η_S of $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$ at S takes $a \in S$ to the constant map $(n \mapsto (\bullet \mapsto a)) \in \mathcal{S}[\mathbf{1}, \boldsymbol{\Delta}S]$. Its inverse is the function $\mathcal{S}[\mathbf{1}, \boldsymbol{\Delta}S] \to S$ taking a constant map $x \in \mathcal{S}[\mathbf{1}, \boldsymbol{\Delta}S]$ to $x(0)(\bullet)$.
(2) Since $\boldsymbol{\Gamma}$ is a right adjoint.
(3) Since for any $x \in \mathcal{S}[\mathbf{1}, X + Y]$ there is some $i \in \{0, 1\}$ such that $x(\bullet)(n)$ is of the form $\mathsf{in}_i(x_n)$ for all $n \in \mathbb{N}$.
(4) Using the Cartesian closed structure of $\mathcal{S}$ and the adjunction $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$ we have
$$\begin{aligned}\boldsymbol{\Gamma}(X^{\boldsymbol{\Delta}S}) &= \mathcal{S}[\mathbf{1}, X^{\boldsymbol{\Delta}S}] \\ &\simeq \mathcal{S}[\mathbf{1} \times \boldsymbol{\Delta}S, X] \\ &\simeq \mathcal{S}[\boldsymbol{\Delta}S, X] \\ &\simeq \mathbf{Set}[S, \boldsymbol{\Gamma}X]\end{aligned}$$
(5) We show that $x \in \boldsymbol{\Gamma}X \mapsto \mathsf{next} \circ x \in \boldsymbol{\Gamma}(\blacktriangleright X)$ is a bijection. We first show surjectivity. Consider $x' \in \mathcal{S}[\mathbf{1}, \blacktriangleright X]$. Then for each $n \in \mathbb{N}$, we have $x'_{n+1}(\bullet) \in \blacktriangleright X(n+1) = X(n)$ with $x'_{n+2}(\bullet)\uparrow = x'_{n+1}(\bullet)$. This defines a map $x \in \mathcal{S}[\mathbf{1}, X]$ as $x_n(\bullet) := x'_{n+1}(\bullet)$. Moreover, $(\mathsf{next}_0 \circ x_0)(\bullet) = \bullet = x'_0(\bullet)$ and
$$(\mathsf{next}_{n+1} \circ x_{n+1})(\bullet) \quad = \quad x_{n+1}(\bullet)\uparrow \quad = \quad x'_{n+2}(\bullet)\uparrow \quad = \quad x'_{n+1}(\bullet)$$
We now show injectivity. Let $x, y \in \mathcal{S}[\mathbf{1}, X]$ and assume $\mathsf{next} \circ x = \mathsf{next} \circ y : \mathbf{1} \to_{\mathcal{S}} \blacktriangleright X$. Then for all n we have $x_{n+1}(\bullet)\uparrow = y_{n+1}(\bullet)\uparrow$ and thus $x_n(\bullet) = y_n(\bullet)$. □

Following [20], for a (closed) pure type A, we have
$$[\![\blacksquare A]\!] := \boldsymbol{\Delta}\boldsymbol{\Gamma}[\![A]\!]$$
In words, all components $[\![\blacksquare A]\!](n)$ are equal to $\boldsymbol{\Gamma}[\![A]\!]$, and the restriction maps of $[\![\blacksquare A]\!]$ are identities. In particular, a global section $x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!]$ is a constant family $(x_n)_{n>0}$ describing a unique global section $x_{n+1}(\bullet) = x_n(\bullet) \in \boldsymbol{\Gamma}[\![A]\!]$.

The term constructor $\mathsf{unbox}(-)$ is interpreted as the counit ε of the adjunction $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$: given $\mathcal{E} \vdash M : \blacksquare A$, we let $[\![\mathsf{unbox}(M)]\!]$ be the composite
$$[\![\mathcal{E}]\!] \xrightarrow{[\![M]\!]} [\![\blacksquare A]\!] = \boldsymbol{\Delta}\boldsymbol{\Gamma}[\![A]\!] \xrightarrow{\varepsilon} [\![A]\!]$$

The term constructors box and prev rely on a strong semantic property of constant types, namely that their interpretation lie (modulo isomorphism) in the image of the constant object functor $\boldsymbol{\Delta}$.

Definition D.3 ([20, Def. 2.2]). *An object X of $\mathcal{S}$ is* constant *if $X \simeq \boldsymbol{\Delta} S$ for some set S.*

Note that the restriction maps of constant objects are bijections. Similarly as in [20, Def. 2.2], if $x \in X(n)$ with X constant, then we write $x \in X(k)$ for the unique element of $X(k)$ which is equal to x modulo the bijective restriction maps of X.

Lemma D.4 ([20, Lem. 2.6]). *If A is a constant (pure) type, then $[\![A]\!]$ is a constant object of $\mathcal{S}$.*

We now give the interpretations of $\mathsf{box}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$ (where σ stands for $[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$). Assuming in both cases $[\![M]\!]$ to be defined, for $n > 0$ we let

$$\begin{array}{rcl} & [\![\mathsf{box}_\sigma(M)]\!](n) : [\![\mathcal{E}]\!](n) \longrightarrow \boldsymbol{\Delta\Gamma}[\![A]\!](n) = \boldsymbol{\Gamma}[\![A]\!] & \\ \gamma & \longmapsto & \Big(m \;\mapsto\; [\![M]\!]_m\Big([\![M_1]\!]_n(\gamma)\,,\;\ldots\;,\,[\![M_k]\!]_n(\gamma)\Big)\Big) \end{array}$$

$$\begin{array}{rcl} & [\![\mathsf{prev}_\sigma(M)]\!](n) : [\![\mathcal{E}]\!](n) \longrightarrow \blacktriangleright[\![A]\!](n) = [\![A]\!](n+1) & \\ \gamma & \longmapsto & \Big([\![M]\!]_{n+1}\Big([\![M_1]\!]_n(\gamma)\,,\;\ldots\;,\,[\![M_k]\!]_n(\gamma)\Big)\Big) \end{array}$$

where the mismatches between n and m and between n and $n+1$ are legal since $[\![A_1]\!], \ldots, [\![A_k]\!]$ are constant by Lem. D.4.

D.3 External and Internal Semantics: Global Definitions

We can now give the full **Set** and $\mathcal{S}$ interpretations of the logical language. In both cases, for $\alpha : A \vdash \varphi : A(\alpha)$, we let

$$\begin{array}{llll} \varphi^0(\top) & := \top & \qquad \varphi^0(\bot) & := \bot \\ \varphi^{m+1}(\top) & := \varphi(\varphi^m(\top)) & \qquad \varphi^{m+1}(\bot) & := \varphi(\varphi^m(\bot)) \end{array}$$

(Recall that $\theta^{\mathsf{t}}\alpha\varphi$ is only allowed when φ as at most α as free variable.)

Definition D.5 (External Semantics). *Consider a formula $\alpha_1 : A_1, \ldots, \alpha_k : A_k \vdash \varphi : A$ without free iteration variable. Assume given a valuation v taking each propositional variable α_i for $i = 1, \ldots, k$ to a set $v(\alpha_i) \in \mathcal{P}(\boldsymbol{\Gamma}[\![A_i]\!])$. We define $\{|\varphi|\}^A_v \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ by induction on φ in Fig. 18.*

As for the internal $\mathcal{S}$ semantics $[\![-]\!]$, we give a global definition, in a form similar to Def. D.5.

Definition D.6 (Internal Semantics). *Consider a formula $\alpha_1 : A_1, \ldots, \alpha_k : A_k \vdash \varphi : A$ without free iteration variable. Assume given a valuation v taking each propositional variable α_i for $i = 1, \ldots, k$ to a subobject $v(\alpha_i)$ of $[\![A_i]\!]$. The subobject $[\![\varphi]\!]^A_v$ of $[\![A]\!]$ is defined by induction on φ in Fig. 19.*

The correctness of Def. D.6, namely that we indeed have $[\![\varphi]\!]^A \in \mathrm{Sub}([\![A]\!])$, as well as the correspondence with the presentation of §7 are discussed in App. D.6.

$$
\begin{aligned}
\{\!|\bot|\!\}^A_v &:= \emptyset \qquad\qquad \{\!|\top|\!\}^A_v := \boldsymbol{\Gamma}[\![A]\!] \qquad\qquad \{\!|\alpha_i|\!\}^A_v := v(\alpha_i)\\
\{\!|\varphi \vee \psi|\!\}^A_v &:= \{\!|\varphi|\!\}^A_v \cup \{\!|\psi|\!\}^A_v \qquad\qquad \{\!|\varphi \wedge \psi|\!\}^A_v := \{\!|\varphi|\!\}^A_v \cap \{\!|\psi|\!\}^A_v\\
\{\!|\psi \Rightarrow \varphi|\!\}^A_v &:= \Big(\boldsymbol{\Gamma}[\![A]\!] \setminus \{\!|\psi|\!\}^A_v\Big) \cup \{\!|\varphi|\!\}^A_v\\
\{\!|[\pi_i]\varphi|\!\}^{A_0\times A_1}_v &:= \Big\{x \in \boldsymbol{\Gamma}[\![A_0 \times A_1]\!] \;\Big|\; \pi_i \circ x \in \{\!|\varphi|\!\}^{A_i}_v\Big\}\\
\{\!|[\mathsf{in}_i]\varphi|\!\}^{A_0+A_1}_v &:= \Big\{x \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \;\Big|\; \exists y \in \boldsymbol{\Gamma}[\![A_i]\!]\big(x = \mathsf{in}_i \circ y \;\text{ and }\; y \in \{\!|\varphi|\!\}^{A_i}_v\big)\Big\}\\
\{\!|[\mathsf{fold}]\varphi|\!\}^{\mathsf{Fix}(X).A}_v &:= \Big\{x \in \boldsymbol{\Gamma}[\![\mathsf{Fix}(X).A]\!] \;\Big|\; \mathsf{unfold} \circ x \in \{\!|\varphi|\!\}^{A[\mathsf{Fix}(X).A/X]}_v\Big\}\\
\{\!|[\mathsf{ev}(\psi)]\varphi|\!\}^{B\to A}_v &:= \Big\{x \in \boldsymbol{\Gamma}[\![B \to A]\!] \;\Big|\; \forall y \in \boldsymbol{\Gamma}[\![B]\!],\; y \in \{\!|\psi|\!\}^B_v \implies \mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}^A_v\Big\}\\
\{\!|[\mathsf{box}]\varphi|\!\}^{\blacksquare A} &:= \Big\{x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!] \;\Big|\; x_1(\bullet) \in \{\!|\varphi|\!\}^A\Big\}\\
\{\!|[\mathsf{next}]\varphi|\!\}^{\blacktriangleright A}_v &:= \Big\{\mathsf{next} \circ x \in \boldsymbol{\Gamma}[\![\blacktriangleright A]\!] \;\Big|\; x \in \{\!|\varphi|\!\}^A_v\Big\}\\
\{\!|\nu^{\mathsf{t}}\alpha\varphi(\alpha)|\!\}^A_v &:= \{\!|\varphi^m(\top)|\!\}^A_v \qquad ([\![\mathsf{t}]\!] = m)\\
\{\!|\mu^{\mathsf{t}}\alpha\varphi(\alpha)|\!\}^A_v &:= \{\!|\varphi^m(\bot)|\!\}^A_v \qquad ([\![\mathsf{t}]\!] = m)\\
\{\!|\nu\alpha\varphi|\!\}^A_v &:= \bigcup\Big\{S \;\Big|\; S \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]) \;\text{ and }\; S \subseteq \{\!|\varphi|\!\}^A_{v[S/\alpha]}\Big\}\\
\{\!|\mu\alpha\varphi|\!\}^A_v &:= \bigcap\Big\{S \;\Big|\; S \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]) \;\text{ and }\; \{\!|\varphi|\!\}^A_{v[S/\alpha]} \subseteq S\Big\}
\end{aligned}
$$

Fig. 18. External Semantics.

$$
\begin{aligned}
[\![\bot]\!]^A_v(n) &:= \emptyset \qquad\qquad [\![\top]\!]^A_v := [\![A]\!] \qquad\qquad [\![\alpha_i]\!]^A_v := v(\alpha_i)\\
[\![\varphi \vee \psi]\!]^A_v(n) &:= [\![\varphi]\!]^A_v(n) \cup [\![\psi]\!]^A_v(n) \qquad\qquad [\![\varphi \wedge \psi]\!]^A_v(n) := [\![\varphi]\!]^A_v(n) \cap [\![\psi]\!]^A_v(n)\\
[\![\psi \Rightarrow \varphi]\!]^A_v(n) &:= \big\{t \in [\![A]\!](n) \;\big|\; \forall k \le n,\; t{\uparrow}k \in [\![\psi]\!]^A_v(k) \implies t{\uparrow}k \in [\![\varphi]\!]^A_v(k)\big\}\\
[\![[\pi_i]\varphi]\!]^{A_0\times A_1}_v(n) &:= \big\{t \in [\![A_0 \times A_1]\!](n) \;\big|\; \pi_i(t) \in [\![\varphi]\!]^{A_i}_v(n)\big\}\\
[\![[\mathsf{in}_i]\varphi]\!]^{A_0+A_1}_v(n) &:= \big\{t \in [\![A_0 + A_1]\!](n) \;\big|\; \exists u \in [\![A_i]\!](n),\; t = \mathsf{in}_i(u) \text{ and } u \in [\![\varphi]\!]^{A_i}_v(n)\big\}\\
[\![[\mathsf{fold}]\varphi]\!]^{\mathsf{Fix}(X).A}_v(n) &:= \Big\{t \in [\![\mathsf{Fix}(X).A]\!](n) \;\Big|\; \mathsf{unfold}_n(t) \in [\![\varphi]\!]^{A[\mathsf{Fix}(X).A/X]}_v(n)\Big\}\\
[\![[\mathsf{ev}(\psi)]\varphi]\!]^{B\to A}_v(n) &:= \big\{t \in [\![B \to A]\!](n) \;\big|\; \forall k \le n,\; \forall u \in [\![B]\!](k),\; u \in [\![\psi]\!]^B_v(k) \implies (t{\uparrow}k)(u) \in [\![\varphi]\!]^A_v(k)\big\}\\
[\![[\mathsf{box}]\varphi]\!]^{\blacksquare A}(n) &:= \Big\{t \in [\![\blacksquare A]\!](n) = \boldsymbol{\Gamma}[\![A]\!] \;\Big|\; t \in \{\!|\varphi|\!\}^A\Big\}\\
[\![[\mathsf{next}]\varphi]\!]^{\blacktriangleright A}_v(1) &:= \mathbf{1}\\
[\![[\mathsf{next}]\varphi]\!]^{\blacktriangleright A}_v(n) &:= [\![\varphi]\!]^A_v(n-1) \qquad (n > 1)\\
[\![\nu^{\mathsf{t}}\alpha\varphi(\alpha)]\!]^A_v &:= [\![\varphi^m(\top)]\!]^A_v \qquad ([\![\mathsf{t}]\!] = m)\\
[\![\mu^{\mathsf{t}}\alpha\varphi(\alpha)]\!]^A_v &:= [\![\varphi^m(\bot)]\!]^A_v \qquad ([\![\mathsf{t}]\!] = m)\\
[\![\nu\alpha\varphi]\!]^A_v &:= \bigvee\big\{S \;\big|\; S \in \mathrm{Sub}([\![A]\!]) \;\text{ and }\; S \le [\![\varphi]\!]^A_{v[S/\alpha]}\big\}\\
[\![\mu\alpha\varphi]\!]^A_v &:= \bigwedge\big\{S \;\big|\; S \in \mathrm{Sub}([\![A]\!]) \;\text{ and }\; [\![\varphi]\!]^A_{v[S/\alpha]} \le S\big\}
\end{aligned}
$$

Fig. 19. Internal Semantics.

Remark D.7. For closed formulae we can rephrase Def. D.6 as $t \in [\![\varphi]\!]^A(n)$ iff $t \Vdash_n^A \varphi$, where the *forcing relation* $t \Vdash_n^A \varphi$ is inductively defined as follows.

- $t \nVdash_n^A \bot$.
- $t \Vdash_n^A \top$.
- $t \Vdash_n^A \varphi \vee \psi$ iff $t \Vdash_n^A \varphi$ or $t \Vdash_n^A \psi$.
- $t \Vdash_n^A \varphi \wedge \psi$ iff $t \Vdash_n^A \varphi$ and $t \Vdash_n^A \psi$.
- $t \Vdash_n^A \psi \Rightarrow \varphi$ iff for all $k \leq n$, $t{\uparrow}k \Vdash_k^A \varphi$ whenever $t{\uparrow}k \Vdash_k^A \psi$.
- $t \Vdash_n^{A_0 \times A_1} [\pi_i]\varphi$ iff $\pi_i(t) \Vdash_n^{A_i} \varphi$.
- $t \Vdash_n^{A_0 + A_1} [\mathsf{in}_i]\varphi$ iff there is $u \in [\![A_i]\!](n)$ such that $t = \mathsf{in}_i(u)$ and $u \Vdash_n^{A_i} \varphi$.
- $t \Vdash_n^{B \to A} [\mathsf{ev}(\psi)]\varphi$ iff for all $k \leq n$ and all $u \in [\![B]\!](k)$, $(t{\uparrow}k)(u) \Vdash_k^A \varphi$ whenever $u \Vdash_k^B \psi$.
- $t \Vdash_n^{\mathsf{Fix}(X).A} [\mathsf{fold}]\varphi$ iff $\mathsf{unfold} \circ t \Vdash_n^{A[\mathsf{Fix}(X).A/X]} \varphi$.
- $t \Vdash_0^{\blacktriangleright A} [\mathsf{next}]\varphi$.
- $t \Vdash_{n+1}^{\blacktriangleright A} [\mathsf{next}]\varphi$ iff $t \Vdash_n^A \varphi$.
- $t \Vdash_n^{\blacksquare A} [\mathsf{box}]\varphi$ iff $t \in \{\!|\varphi|\!\}^A$.

D.4 An Open Geometric Morphism

Key properties of the internal semantics of $[\mathsf{box}]$ rely on some further facts on the adjunction $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma}$. We refer to [52,38].

The functor $\boldsymbol{\Delta} : \mathbf{Set} \to \mathcal{S}$ preserves limits (in particular, $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ is a *geometric morphism*). It follows that $\boldsymbol{\Delta}$ preserves monos, so that for each set S the function

$$A \in \mathcal{P}(S) \longmapsto \boldsymbol{\Delta} A \in \mathrm{Sub}(\boldsymbol{\Delta} S)$$

is a meet preserving (and thus monotone) map. It is easy to see that this map has a posetal left adjoint

$$f_! : \mathrm{Sub}(\boldsymbol{\Delta} S) \longrightarrow \mathcal{P}(S)$$

Proof. A subobject A of $\boldsymbol{\Delta} S$ is a family of subsets $A = (A_n)_n$ with $A_n \subseteq S$. Hence we can let $f_!(A) \in \mathcal{P}(S)$ be the set of all $a \in S$ such that $a \in A_n$ for some $n > 0$. Then assuming $f_!(A) \subseteq B$ for some set $B \in \mathcal{P}(S)$, it follows that if $a \in A_n$ then $a \in f_!(A) \subseteq B$ so that $a \in (\boldsymbol{\Delta} B)_n$ and thus $A \leq \boldsymbol{\Delta} B$. Conversely, if $A \leq \boldsymbol{\Delta} B$, then for every $a \in f_!(A)$, since $a \in A_n$ for some $n > 0$, we must have $a \in (\boldsymbol{\Delta} B)_n = B$, so that $f_!(A) \subseteq B$. $\square$

As a consequence, the adjoint pair $\boldsymbol{\Delta} \dashv \boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ is an *open geometric morphism* (in the sense of [52, Def. IX.6.2]), from which it follows that $\boldsymbol{\Delta}$ induces maps of (complete) Heyting algebras $\mathcal{P}(S) \to \mathrm{Sub}(\boldsymbol{\Delta} S)$ (see e.g. [52, Thm. X.3.1 & Lem. X.3.2]). We state this for later use.

Lemma D.8. *For each set S, the functor $\boldsymbol{\Delta}$ induces a map of (complete) Heyting algebras $\mathcal{P}(S) \to \mathrm{Sub}(\boldsymbol{\Delta} S)$.*

This means that the **Set** interpretation $\{\!|\varphi|\!\} \in \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$ can be taken to the subobject $\boldsymbol{\Delta}\{\!|\varphi|\!\} \in \mathrm{Sub}(\boldsymbol{\Delta}\boldsymbol{\Gamma}[\![A]\!]) = \mathrm{Sub}([\![\blacksquare A]\!])$ in $\mathcal{S}$ while respecting the usual **Set** semantics of logical connectives. In particular, we can allow the logical theory under a $[\mathsf{box}]$ to be classical, while the $\mathcal{S}$ semantics imposes the ambient logical theory to be intuitionistic.

D.5 Abstract Modalities

We present here some well-known basic material which will help us proving the correctness of the internal and external semantics.

Definition D.9. *Let $\mathbb{C}$ be a category with pullbacks and consider a morphism $k : X \to_{\mathbb{C}} Y$.*

- *The functor $k^* : \mathbb{C}/Y \to \mathbb{C}/X$ is defined by pullbacks*

$$\begin{tikzcd} A' \arrow[r] \arrow[d, "k^*(g)"'] \arrow[dr, phantom, "\lrcorner", very near start] & A \arrow[d, "g"] \\ X \arrow[r, "k"'] & Y \end{tikzcd}$$

- *The functor $(\exists k) : \mathbb{C}/X \to \mathbb{C}/Y$ is defined by postcomposition:*

$$(g : A \to X) \quad \longmapsto \quad (k \circ g : A \to Y)$$

The following is a basic property of toposes.

Lemma D.10 ([52, Thm. IV.7.2]). *Let $\mathcal{T}$ be a topos and fix a map $k : X \to_{\mathcal{T}} Y$. The functor $(\exists k)$ is left adjoint to $k^* : \mathcal{T}/Y \to \mathcal{T}/X$. Moreover, k^* has a right adjoint $(\forall k)$ and preserves exponentials, and thus preserves subobjects.*

Lemma D.11.

(1) The map $(\exists \mathsf{in}_i) : \mathbf{Set}/S_i \to \mathbf{Set}/(S_0 + S_1)$ induces a map $\mathcal{P}(S_i) \to \mathcal{P}(S_0 + S_1)$.
(2) The map $(\exists \mathsf{in}_i) : \mathcal{S}/X_i \to \mathcal{S}/(X_0 + X_1)$ induces a map $\mathrm{Sub}(X_i) \to \mathrm{Sub}(X_0 + X_1)$.

Proof. Since in both cases the morphism in_i is a mono. $\square$

Lemma D.12. *The map $\mathcal{S}/X \to \mathcal{S}/\blacktriangleright X$ taking $g : Y \to X$ to $\blacktriangleright(g) : \blacktriangleright Y \to \blacktriangleright X$ induces a map $\mathrm{Sub}(X) \to \mathrm{Sub}(\blacktriangleright X)$.*

Proof. The functor $\blacktriangleright$ preserves limits since it has a left adjoint ([13, §2.1]). It thus follows that $\blacktriangleright$ preserves monos. $\square$

D.6 External and Internal Semantics: Local Definitions

Some key properties of the **Set** and $\mathcal{S}$ interpretations are easier to get if one goes through a local presentation, as operations on subobject and powerset lattices, similar to that of $[\![-]\!]$ in §7. The goal is to pave the way toward the correctness of both semantics:

Lemma D.13 (Lem. 7.2). *The following holds w.r.t. the full modal theories of Def. 6.2.*

(1) If $\vdash^A_{\mathsf{c}} \varphi$ then $\{\!|\varphi|\!\} = \boldsymbol{\Gamma}[\![A]\!]$.
(2) If $\vdash^A \varphi$ then $[\![\varphi]\!] = [\![A]\!]$.

The detailed proof of Lem. D.13 is deferred to App. F.1. It relies on the following material.

Internal Semantics We use the material of §D.5 to devise operations on subobject lattices corresponding to our modalities. This formally extends the presentation given in §7.

Definition D.14.

(a) Given $\mathcal{S}$-objects X_0 and X_1, define $[\![[\pi_i]]\!] : \mathrm{Sub}(X_i) \to \mathrm{Sub}(X_0 \times X_1)$ as π_i^*, where $\pi_i : X_0 \times X_1 \to_{\mathcal{S}} X_i$ is the ith projection.
(b) Given $\mathcal{S}$-objects X_0 and X_1, define $[\![[\mathsf{in}_i]]\!] : \mathrm{Sub}(X_i) \to \mathrm{Sub}(X_0 + X_1)$ as $(\exists \mathsf{in}_i)$, where $\mathsf{in}_i : X_i \to_{\mathcal{S}} X_0 + X_1$ is the ith injection.
(c) Given a locally contractive functor T on $\mathcal{S}$, define $[\![[\mathsf{fold}]]\!] : \mathrm{Sub}(T(\mathsf{Fix}(T))) \to \mathrm{Sub}(\mathsf{Fix}(T))$ as unfold^*, where we have $\mathsf{unfold} : \mathsf{Fix}(T) \to_{\mathcal{S}} T(\mathsf{Fix}(T))$.
(d) Given a $\mathcal{S}$-object X, define $[\![[\mathsf{next}]]\!] : \mathrm{Sub}(X) \to \mathrm{Sub}(\blacktriangleright X)$ as $\blacktriangleright(-)$.
(e) Given a set S, define $[\![[\mathsf{box}]]\!] : \mathcal{P}(S) \to \mathrm{Sub}(\boldsymbol{\Delta} S)$ as $\boldsymbol{\Delta}(-)$.

We now discuss the case of $[\mathsf{ev}(\psi)]\varphi$, which is actually interpreted as a *logical predicate*, in the categorical generalization of the usual sense discussed in [32, §9.2 & Prop. 9.2.4]. We follow here [52, VI.5].

– First, extending the above discussion, for an object X of $\mathcal{S}$, the (Heyting algebra) exponent
$$(-) \Rightarrow_X (-) : \mathrm{Sub}(X) \times \mathrm{Sub}(X) \longrightarrow \mathrm{Sub}(X)$$
is given by
$$(A \Rightarrow_X B)(n) = \{t \in X(n) \mid \forall k \leq n,\ t{\uparrow}k \in A(k) \Longrightarrow t{\uparrow}k \in B(k)\}$$
(see e.g. [52, Prop. I.8.5]).
– Second, it follows from Lem. D.10 that for objects X, Y of $\mathcal{S}$, taking the pullback of the evaluation map $\mathsf{ev} : X^Y \times Y \to X$ gives a map of subobjects, as in
$$\begin{tikzcd} \mathsf{ev}^*(A) \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & A \arrow[d, hook] \\ X^Y \times Y \arrow[r, "\mathsf{ev}"'] & X \end{tikzcd}$$
which in particular preserves limits and colimits.
– Third, in the internal logic of $\mathcal{S}$, universal quantification over an object Y w.r.t. a predicate $A \in \mathrm{Sub}(X \times Y)$ is given (again via Lem. D.10) by the right adjoint $\forall_Y := \forall(\pi)$ to π^*, where π is the projection $X \times Y \to X$ ([52, §VI.5, p. 300]). Moreover, via the Kripke-Joyal semantics for a presheaf topos ([52, §VI.7, p. 318]), for $A \in \mathrm{Sub}(X \times Y)$, the presheaf $\forall_Y(A)$ at n is
$$\{t \in X(n) \mid \forall k \leq n,\ \forall u \in Y(k),\ (t{\uparrow}k, u) \in A\}$$

We therefore let, for each pure types A and B,
$$[\![[\mathsf{ev}(-)]]\!] : \mathrm{Sub}([\![B]\!]) \longrightarrow \big(\mathrm{Sub}([\![A]\!]) \ \to\ \mathrm{Sub}([\![B \to A]\!])\big)$$

take $S' \in \mathrm{Sub}(\llbracket B \rrbracket)$ to

$$\llbracket[\mathsf{ev}(S')]\rrbracket := S \in \mathrm{Sub}(\llbracket A \rrbracket) \longmapsto \forall_{\llbracket B \rrbracket} \left(\pi^*(S') \quad \Rightarrow_{\llbracket A \rrbracket^{\llbracket B \rrbracket} \times \llbracket B \rrbracket} \quad \mathsf{ev}^*(S)\right)$$

where $\pi : X^Y \times Y \to X^Y$ is a projection.

Now, note that we actually have

Lemma D.15. *Consider a formula $\Sigma \vdash \varphi : A$ and v as in Def. D.6, such that $\llbracket \varphi \rrbracket_v \in \mathrm{Sub}(\llbracket A \rrbracket)$. We have*

(1) $\llbracket [\pi_i]\varphi \rrbracket_v \quad = \quad \llbracket [\pi_i] \rrbracket(\llbracket \varphi \rrbracket_v)$
(2) $\llbracket [\mathsf{in}_i]\varphi \rrbracket_v \quad = \quad \llbracket [\mathsf{in}_i] \rrbracket(\llbracket \varphi \rrbracket_v)$
(3) $\llbracket [\mathsf{fold}]\varphi \rrbracket_v \quad = \quad \llbracket [\mathsf{fold}] \rrbracket(\llbracket \varphi \rrbracket_v)$
(4) $\llbracket [\mathsf{next}]\varphi \rrbracket_v \quad = \quad \llbracket [\mathsf{next}] \rrbracket(\llbracket \varphi \rrbracket_v)$
(5) $\llbracket [\mathsf{box}]\varphi \rrbracket \quad = \quad \llbracket [\mathsf{box}] \rrbracket(\llbracket \varphi \rrbracket)$
(6) $\llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket_v \quad = \quad \llbracket [\mathsf{ev}(\llbracket \psi \rrbracket_v)] \rrbracket(\llbracket \varphi \rrbracket_v)$ *for each* $\vdash \psi : B$ *such that* $\llbracket \psi \rrbracket \in \mathrm{Sub}(\llbracket B \rrbracket)$.

Proof.

(1) Since limits are computed pointwise in presheaves, we have

$$\llbracket [\pi_i] \rrbracket(\llbracket \varphi \rrbracket^{A_i})(n) = \{(t, u) \in \llbracket A_0 \times A_1 \rrbracket(n) \times \llbracket \varphi \rrbracket(n) \mid u = \pi_i(t)\}$$

which is clearly in bijection with $\llbracket [\pi_i]\varphi \rrbracket^{A_0 \times A_1}(n)$.
(2) Trivial.
(3) Similar to the case of $[\pi_i]$.
(4) Trivial.
(5) Trivial.
(6) Immediate from the above discussion. □

We thus have done almost all the work to obtain the following basic fact.

Lemma D.16. *Given $\alpha_1 : A_1, \ldots, \alpha_k : A_k \vdash \varphi : A$, and v taking α_i for $i = 1, \ldots, k$ to $v(\alpha_i) \in \mathrm{Sub}(\llbracket A_i \rrbracket)$, we have $\llbracket \varphi \rrbracket_v^A \in \mathrm{Sub}(\llbracket A \rrbracket)$.*

Proof. The proof is by induction on formulae. The interpretation of the propositional connectives follows the corresponding structures in presheaf toposes [52, Prop. I.8.5]. The cases of the modalities $[\triangle]$ follow from the induction hypothesis and Lem. D.15. The cases of $\theta\alpha\varphi$ simply amount to the fact that for presheaf toposes, subobjects lattices are complete ([52, Prop. I.8.5]). The cases of $\theta^{\mathtt{t}}\alpha\varphi$ for $\mathtt{t}$ an iteration term are trivial. □

We now turn to the logical theory. We immediately get from the above:

Corollary D.17.

(1) The maps $\llbracket [\pi_i] \rrbracket$, $\llbracket [\mathsf{fold}] \rrbracket$ and $\llbracket [\mathsf{box}] \rrbracket$ are maps of Heyting algebras.
(2) The maps $\llbracket [\mathsf{in}_i] \rrbracket$ preserve $\vee, \bot$ and $\wedge$.
(3) The maps $\llbracket [\mathsf{next}] \rrbracket$ preserve $\wedge, \top$ and $\vee$.

(4) *For each object X of $\mathcal{S}$ and each fixed $S \in \mathrm{Sub}(X)$, the map $[\![[\mathsf{ev}(S)]]\!]$ preserves $\wedge, \top$.*

Proof.

(1) This directly follows from Lem. D.10 and Lem. D.8.
(2) Preservation of $\vee, \bot$ follows from that fact that $[\![[\mathsf{in}_i]]\!]$ is a left adjoint by Lem. D.10. For binary conjunctions, first note that meets in partial orders are given by pullbacks. In a subobject lattice $\mathrm{Sub}(X_i)$, this can be expressed as

$$\begin{tikzcd} A \wedge B \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d] \\ A \arrow[r] & X_i \end{tikzcd}$$

(where arrows are inclusions maps). Since $\mathsf{in}_i : X_i \to X_0 + X_1$ is a mono, the following is also a pullback in $\mathrm{Sub}(X_0 + X_1)$:

$$\begin{tikzcd} A \wedge B \arrow[rr] \arrow[dd] \arrow[ddrr, phantom, "\lrcorner", very near start] & & B \arrow[d] \\ & & X_i \arrow[d, "\mathsf{in}_i"] \\ A \arrow[r] & X_i \arrow[r, "\mathsf{in}_i"'] & X_0 + X_1 \end{tikzcd}$$

(3) Preservation of $\wedge, \top$ follows from the fact that $\blacktriangleright(-)$ is a right adjoint ([13, §2.1]). As for preservation of $\vee$, we check the details. Consider an object X of $\mathcal{S}$ and subobjects $A, B \in \mathrm{Sub}(X)$. We have to show $\blacktriangleright(A \vee B) = \blacktriangleright(A) \vee \blacktriangleright(B)$. But we have

$$\blacktriangleright(A \vee B)_0 \quad = \quad \mathbf{1} \quad = \quad \mathbf{1} \cup \mathbf{1} \quad = \quad (\blacktriangleright(A) \vee \blacktriangleright(B))_0$$

and

$$\begin{array}{rcl} \blacktriangleright(A \vee B)_{n+1} \quad = \quad (A \vee B)_n & = & A_n \cup B_n \\ & = & \blacktriangleright(A)_{n+1} \cup \blacktriangleright(B)_{n+1} \\ & = & (\blacktriangleright(A) \vee \blacktriangleright(B))_{n+1} \end{array}$$

(4) This directly follows from Lem. D.10, via Lem. D.15 and the definition of $[\![[\mathsf{ev}(-)]]\!]$. □

External Semantics We now turn to operations on powerset lattices for the external semantics.

Definition D.18.

(a) *Given sets S_0 and S_1, define $\{\!|[\pi_i]|\!\} : \mathcal{P}(S_i) \to \mathcal{P}(S_0 \times S_1)$ as π_i^*, where $\pi_i : S_0 \times S_1 \to S_i$ is the ith projection.*

(b) Given sets S_0 *and* S_1*, define* $\{|[\mathsf{in}_i]|\} : \mathcal{P}(S_i) \to \mathcal{P}(S_0 + S_1)$ *as* $(\exists \mathsf{in}_i)$*, where* $\mathsf{in}_i : S_i \to S_0 + S_1$ *is the* i*th injection.*
(c) Given a $\mathcal{S}$ *object* X*, define* $\{|[\mathsf{next}]|\} : \mathcal{P}(\boldsymbol{\Gamma} X) \to \mathcal{P}(\boldsymbol{\Gamma} \blacktriangleright X)$ *as* $((\boldsymbol{\Gamma}\mathsf{next})^{-1})^*$*, where* $(\boldsymbol{\Gamma}\mathsf{next})^{-1} : \boldsymbol{\Gamma}(\blacktriangleright X) \to \boldsymbol{\Gamma} X$ *is the inverse of* $\boldsymbol{\Gamma}(\mathsf{next})$ *(Lem. D.2).*
(d) Given a locally contractive functor T *on* $\mathcal{S}$*, define* $\{|[\mathsf{fold}]|\} : \mathcal{P}(\boldsymbol{\Gamma}(T(\mathsf{Fix}(T)))) \to \mathcal{P}(\boldsymbol{\Gamma}\mathsf{Fix}(T))$ *as* $\boldsymbol{\Gamma}(\mathsf{unfold})^*$*, where* $\mathsf{unfold} : \mathsf{Fix}(T) \to_{\mathcal{S}} T(\mathsf{Fix}(T))$*.*

We trivially have (at appropriate types):

$$\begin{array}{rcl}
\{|[\pi_i]\varphi|\} & = & \{|[\pi_i]|\}\,(\{|\varphi|\}) \\
\{|[\mathsf{in}_i]\varphi|\} & = & \{|[\mathsf{in}_i]|\}\,(\{|\varphi|\}) \\
\{|[\mathsf{next}]\varphi|\} & = & \{|[\mathsf{next}]|\}\,(\{|\varphi|\}) \\
\{|[\mathsf{fold}]\varphi|\} & = & \{|[\mathsf{fold}]|\}\,(\{|\varphi|\})
\end{array}$$

Similarly as in Cor. D.17, we obtain the following.

Lemma D.19.

(1) The functions $\{|[\pi_i]|\}$*,* $\{|[\mathsf{next}]|\}$*,* $\{|[\mathsf{fold}]|\}$ *are maps of Boolean algebras.*
(2) The function $\{|[\mathsf{in}_i]|\}$ *preserves* $\vee, \bot$ *and* $\wedge$*.*

D.7 The Safe Fragment

The property we use on safe formulae for Prop. 7.3 is the following.

Definition D.20 (Scott Cocontinuity). *Let* L *be a complete lattice. A set* $S \subseteq L$ *is* codirected *if it is non-empty and for all* $a, b \in S$*, there is some* $c \in S$ *such that* $c \leq a, b$*. A function* $f : L \to L$ *is* Scott cocontinuous *if it is monotone and preserves infs of codirected sets (for* $S \subseteq L$ *codirected, we have* $f(\bigwedge S) = \bigwedge f(S)$*).*

In other words, a Scott cocontinuous function $L \to L$ is a Scott continuous function $L^{\mathrm{op}} \to L^{\mathrm{op}}$.

Lemma D.21. *The greatest fixpoint of a Scott cocontinuous* $f : L \to L$ *is given by* $\bigwedge_{m \in \mathbb{N}} f^m(\top)$*.*

Lemma D.22. *Given a* safe *formula* $\alpha : A \vdash \varphi(\alpha) : A$*, the following functions are Scott cocontinuous:*

$$[\![\varphi]\!] : \mathrm{Sub}([\![A]\!]) \longrightarrow \mathrm{Sub}([\![A]\!]) \qquad \{|\varphi|\} : \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!])$$

The key for Lem. D.22 is the usual fact that codirected infs commute with infs and finite sups, in **Set** as well as in $\mathcal{S}$. The key case of Prop. 7.3 is that of $\nu\alpha\varphi(\alpha) : A$. We have

$$\{|\nu\alpha\varphi(\alpha)|\} \quad = \quad \bigcap_{m \in \mathbb{N}} \{|\varphi^m(\top)|\} \qquad \text{and} \qquad [\![\nu\alpha\varphi(\alpha)]\!] \quad = \quad \bigwedge_{m \in \mathbb{N}} [\![\varphi^m(\top)]\!]$$

Given a global section $x \in \boldsymbol{\Gamma}[\![\nu\alpha\varphi(\alpha)]\!]$, we have

$$\forall n > 0,\ \forall m \in \mathbb{N}, \quad x_n(\bullet) \in [\![\varphi^m(\top)]\!](n)$$

We then easily conclude $x \in \{|\nu\alpha\varphi(\alpha)|\}$ from $\{|\varphi^m(\top)|\} = \boldsymbol{\Gamma}[\![\varphi^m(\top)]\!]$. Note that this relies on the commutation of the universal quantifications over n and m.

The proofs of Lem. D.21, Lem. D.22 and Prop. 7.3 are deferred to App. F.2.

D.8 The Smooth Fragment

The proof of Lem. 7.4 is deferred to App. F.3.

D.9 Constant Objects, Again

For the adequacy of the typing rules of the term constructors box and prev, we need to generalize Lem. D.4 (§D.2) to refinement types. To this end, it is convenient to extend the notation $[\![-]\!]$ to refinement types.

Definition D.23. *For T is a type without free iteration variables, we define $[\![T]\!]$ by induction as follows:*

$$\begin{aligned}
[\![\{A \mid \varphi\}]\!] &:= [\![\varphi]\!] \\
[\![\forall k \cdot T]\!] &:= \textstyle\bigwedge_{n\in\mathbb{N}} [\![T[\mathtt{n}/k]]\!] \\
[\![T_0 + T_1]\!] &:= [\![T_0]\!] + [\![T_1]\!] \\
[\![T_0 \times T_1]\!] &:= [\![T_0]\!] \times [\![T_1]\!] \\
[\![U \to T]\!] &:= [\![U]\!] \to [\![T]\!] \\
[\![\blacktriangleright T]\!] &:= \blacktriangleright [\![T]\!] \\
[\![\blacksquare T]\!] &:= \boldsymbol{\Delta\Gamma}[\![T]\!]
\end{aligned}$$

We can now extend Lem. D.4. We crucially rely on the fact that $\boldsymbol{\Delta}$ preserves limits (see e.g. [38, Ex. 4.1.4]).

Lemma D.24. *If T is a constant type, then $[\![T]\!]$ is a constant object of $\mathcal{S}$.*

Proof. The proof is by induction on types. The cases of the type constructors $+$, $\times$, $\to$ are easy and discussed in [20, Lem. 2.6]. In the case of $\mathsf{Fix}(X).A$, since all occurrences of X in A should be guarded by a $\blacktriangleright$, and since $\blacksquare$ can only be applied to closed types, it follows that X cannot occur in A. Then $[\![A]\!]$ is constant by induction hypothesis and we are done since $[\![\mathsf{Fix}(X).A]\!] \simeq [\![A]\!]$ in this case. The case of $\blacksquare T$ is trivial. As for $\forall k \cdot T$, since $|T|$ is constant, we have $[\![|T|]\!] \simeq \boldsymbol{\Delta} S$ for some set S. By induction hypothesis for each $n \in \mathbb{N}$ we have $[\![T[\mathtt{n}/k]]\!] \simeq \boldsymbol{\Delta} S_n$ for some set S_n with $\boldsymbol{\Delta} S_n \in \mathrm{Sub}([\![|T|]\!])$. Note that $\boldsymbol{\Delta} S_n$ can be seen as a subobject of $\boldsymbol{\Delta} S$. Recall from §D.4 the posetal left adjoint

$$f_! : \mathrm{Sub}(\boldsymbol{\Delta} S) \longrightarrow \mathcal{P}(S)$$

of the map

$$\boldsymbol{\Delta} : X \in \mathcal{P}(S) \longmapsto \boldsymbol{\Delta} X \in \mathrm{Sub}(\boldsymbol{\Delta} S)$$

In particular $\boldsymbol{\Delta} : \mathcal{P}(S) \to \mathrm{Sub}(\boldsymbol{\Delta} S)$ preserves meets and we get

$$\begin{aligned}
[\![\forall k \cdot T]\!] &= \textstyle\bigwedge_n [\![T[\mathtt{n}/k]]\!] \\
&\simeq \textstyle\bigwedge_n \boldsymbol{\Delta} S_n \\
&\simeq \textstyle\bigwedge_n \boldsymbol{\Delta} f_! \boldsymbol{\Delta} S_n \\
&\simeq \boldsymbol{\Delta} \left(\textstyle\bigcap_n f_! \boldsymbol{\Delta} S_n\right)
\end{aligned}$$

As for refinement types, we show by induction on $\vdash \varphi : A$ with A constant that $[\![\varphi]\!]$ is a constant object.

Cases of $\top$, $\bot$, $\wedge$, $\vee$ and $\Rightarrow$.
All these cases follow from (the induction hypothesis and) the fact that $\boldsymbol{\Delta}$ induces maps of Heyting algebras on subobject lattices (Lem. D.8).

Case of $[\mathsf{box}]\varphi$.
Trivial, since $\llbracket [\mathsf{box}]\varphi \rrbracket$ is in the image of $\boldsymbol{\Delta}$.

Case of $[\mathsf{next}]\varphi$.
This case cannot occur since A is constant.

Case of $[\mathsf{fold}]\varphi$.
In this case, we have $A = \mathsf{Fix}(X).B$. Since X is guarded in B, it must not occur in B, and we have $\llbracket A \rrbracket \simeq \llbracket B \rrbracket$ via unfold. Moreover $\llbracket B \rrbracket$ is constant, with say $\llbracket B \rrbracket \simeq \boldsymbol{\Delta} S$ and by induction hypothesis, $\llbracket [\varphi] \rrbracket$ is a constant subobject of $\llbracket B \rrbracket$, say $\llbracket [\varphi] \rrbracket \simeq \boldsymbol{\Delta}\Phi$. Now, $\llbracket [\mathsf{fold}]\varphi \rrbracket$ lies in the pullback diagram

$$
\begin{tikzcd}
\mathsf{unfold}^*(\llbracket \varphi \rrbracket) \simeq \llbracket [\mathsf{fold}]\varphi \rrbracket \arrow[r, "\pi"] \arrow[d, hook] \arrow[dr, phantom, "\lrcorner", very near start] & \llbracket \varphi \rrbracket \simeq \boldsymbol{\Delta}(\Phi) \arrow[d, hook] \\
\llbracket A \rrbracket \arrow[r, "\mathsf{unfold}"'] & \llbracket B \rrbracket \simeq \boldsymbol{\Delta}(S)
\end{tikzcd}
$$

Since unfold is an iso, the upper arrow π is also an iso, and we are done.

Case of $[\pi_i]\varphi$.
We rely on the description of $\llbracket [\pi_i]\varphi \rrbracket$ as $\llbracket [\pi_i] \rrbracket(\llbracket \varphi \rrbracket)$ in §D.6. By induction hypothesis and recalling that $\boldsymbol{\Delta}$ preserves finite products, consider the pullback

$$
\begin{tikzcd}
\pi^*(\llbracket \varphi \rrbracket) \simeq \llbracket [\pi_i]\varphi \rrbracket \arrow[r] \arrow[d, hook] \arrow[dr, phantom, "\lrcorner", very near start] & \llbracket \varphi \rrbracket \simeq \boldsymbol{\Delta}(\Phi) \arrow[d, hook] \\
\boldsymbol{\Delta}(S_0) \times \boldsymbol{\Delta}(S_1) \arrow[r, "\pi_i"'] & \boldsymbol{\Delta}(S_i)
\end{tikzcd}
$$

Then one can take the corresponding pullback in **Set**

$$
\begin{tikzcd}
\Psi \arrow[r] \arrow[d, hook] \arrow[dr, phantom, "\lrcorner", very near start] & \Phi \arrow[d, hook] \\
S_0 \times S_1 \arrow[r, "\pi_i"'] & S_i
\end{tikzcd}
$$

and this implies that $\llbracket [\pi_i]\varphi \rrbracket \simeq \boldsymbol{\Delta}(\Psi)$ since $\boldsymbol{\Delta}$ preserves finite limits.

Case of $[\mathsf{in}_i]\varphi$.
We rely on the description of $\llbracket [\mathsf{in}_i]\varphi \rrbracket$ as $\llbracket [\mathsf{in}_i] \rrbracket(\llbracket \varphi \rrbracket)$ in §D.6. The result follows from the induction hypothesis and the fact that $\boldsymbol{\Delta}$ preserves finite limits and colimits, as in:

$$\llbracket \varphi \rrbracket \simeq \boldsymbol{\Delta}(\Phi) \hookrightarrow \boldsymbol{\Delta}(S_i) \xrightarrow{\boldsymbol{\Delta}(\mathsf{in}_i)=\mathsf{in}_i} \boldsymbol{\Delta}(S_0) + \boldsymbol{\Delta}(S_1)$$

Case of $[\mathsf{ev}(\psi)]\varphi$.
We rely on the description of $\llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket$ in §D.6, that is

$$\llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket = \forall_{\llbracket B \rrbracket} \left(\pi^*(\llbracket \psi \rrbracket) \quad \Longrightarrow_{\llbracket A \rrbracket^{\llbracket B \rrbracket} \times \llbracket B \rrbracket} \quad \mathsf{ev}^*(\llbracket \varphi \rrbracket) \right)$$

The result then follows from Lem. D.8 and the fact that $\boldsymbol{\Delta}$ thus preserves universal quantifications (see e.g. [52, Thm. X.3.1 & Lem. X.3.2]).

Cases of $\theta^{\mathsf{t}}\alpha\varphi$ and $\theta\alpha\varphi$.

By assumption, the occurrences of α in φ should be guarded by a $[\mathsf{next}]$. Since $[\mathsf{box}]$ can only be applied to closed formulae, this imposes α not to appear in φ. But then the result follows by induction hypothesis. □

D.10 Realizability

We detail the steps toward the Adequacy Theorem 7.7. Full proofs are deferred to App. F.4. The first basic result we need about our notion of realizability is that it is monotone w.r.t. step indexes.

Lemma D.25 (Monotonicity of Realizability). *Let T be a type without free iteration variables. If $x \Vdash_n T$ then $x \Vdash_k T$ for all $k \leq n$.*

The correctness of subtyping requires two additional lemmas. The first one concerns the rule

$$\frac{}{T \leq |T|}$$

Lemma D.26. *For a pure type A and $x \in \boldsymbol{\Gamma}[\![A]\!]$, we have $x \Vdash_n A$ for all $n > 0$.*

Second, we need a result of [20] for the correctness of the subtyping rules

$$\frac{}{\{B \mid \psi\} \to \{A \mid \varphi\} \leq \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}}$$

$$\frac{\mathcal{E}, x : \{B \mid \psi\} \vdash M : \{A \mid \varphi\}}{\mathcal{E} \vdash \lambda x.M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}}$$

An object X of $\mathcal{S}$ is *total* if all its restriction maps $r_n^X : X_{n+1} \to X_n$ are surjective. Hence, if X is total, then given $t \in X_n$ for some $n > 0$, there is a global section $x : \mathbf{1} \to_{\mathcal{S}} X$ such that $x_n(\bullet) = t$.

Lemma D.27 ([20, Cor. 3.8]). *For a pure type A, the object $[\![A]\!]$ is total.*

We then obtain the correctness of subtyping as usual. The rules

$$\frac{\vdash^A \varphi \Rightarrow \psi}{\{A \mid \varphi\} \leq \{A \mid \psi\}} \qquad \frac{\vdash^A_c \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathsf{box}]\varphi\} \leq \{\blacksquare A \mid [\mathsf{box}]\psi\}}$$

rely on Lem. D.13 (Lem. 7.2), while

$$\frac{\varphi \text{ safe}}{\blacksquare\{A \mid \varphi\} \equiv \{\blacksquare A \mid [\mathsf{box}]\varphi\}}$$

is given by Prop. 7.3.

Lemma D.28 (Correctness of Subtyping (Lem. 7.6)). *Given types T, U without free iteration variable, if $x \Vdash_n U$ and $U \leq T$ then $x \Vdash_n T$.*

We now have all we need for the Adequacy Theorem 7.7. As usual it requires a stronger inductive invariant than the statement of Thm. 7.7. Given a typed term

$$x_1 : T_1, \dots, x_k : T_k \vdash M : T$$

and global sections $u_1 \in \boldsymbol{\Gamma}[\![|T_1|]\!], \dots, u_k \in \boldsymbol{\Gamma}[\![|T_k|]\!]$, we obtain a global section

$$[\![M]\!] \circ \langle u_1, \dots, u_k \rangle : \mathbf{1} \longrightarrow [\![|T|]\!]$$

We introduce some notation to manipulate these global sections. Given a typing context $\mathcal{E} = x_1 : T_1, \dots, x_k : T_k$ we write $\rho \models \mathcal{E}$ if ρ takes each x_i for $i = 1, \dots, k$ to some $\rho(x_i) \in \boldsymbol{\Gamma}[\![|T_i|]\!]$. Given a typing judgment $\mathcal{E} \vdash M : T$, we let

$$[\![M]\!]_\rho \quad := \quad [\![M]\!] \circ \langle \rho(x_1), \dots, \rho(x_k) \rangle$$

Given $\rho \models \mathcal{E}$ and $n > 0$, write $\rho \Vdash_n \mathcal{E}$ if $\rho(x_i) \Vdash_n T_i$ for all $i = 1, \dots, k$. Thm. 7.7 is proved under the following form.

Theorem D.29 (Adequacy (Thm. 7.7)). *Let $\mathcal{E}, T$ have free iteration variables among $\overline{\ell}$, and let $\overline{m} \in \mathbb{N}$. If $\mathcal{E} \vdash M : T$ and $\rho \models \mathcal{E}$, then*

$$\forall n > 0, \quad \rho \Vdash_n \mathcal{E}[\overline{\ell}/\overline{m}] \quad \Longrightarrow \quad [\![M]\!]_\rho \Vdash_n T[\overline{\ell}/\overline{m}]$$

Corollary D.30. *(1) Consider a closed term $\vdash M : \{A \mid \varphi\}$ with φ safe. Then $[\![M]\!] : \mathbf{1} \to_{\mathcal{S}} [\![A]\!] \in \{|\varphi|\}$.*
(2) Consider a closed term $\vdash M : \{A \mid \psi\} \to \{A \mid \varphi\}$, with φ, ψ safe. Then $[\![M]\!]$ induces a function $\boldsymbol{\Gamma}[\![M]\!]$ taking $x \in \{|\psi|\}$ to $\boldsymbol{\Gamma}[\![M]\!] = [\![M]\!] \circ x \in \{|\varphi|\}$.

Corollary D.30 of course extends to any arity. As a consequence of Cor. D.30 and Møgelberg's Theorem 7.1 [55], for a closed term $M : \{\blacksquare P \mid [\mathsf{box}]\varphi\}$ with P polynomial, the unique global section $[\![M]\!]_{n+1}(\bullet) = [\![M]\!]_n(\bullet) \in \boldsymbol{\Gamma}[\![P]\!]$ satisfies φ in the standard sense (*i.e.* $[\![M]\!]_{n+1}(\bullet) = [\![M]\!]_n(\bullet) \in \{|\varphi|\}$). Moreover a function, say $M : \{\blacksquare Q \mid [\mathsf{box}]\psi\} \to \{\blacksquare P \mid [\mathsf{box}]\varphi\}$ with Q, P polynomial induces a **Set**-function

$$\begin{aligned} \boldsymbol{\Gamma}[\![M]\!] : \boldsymbol{\Gamma}[\![\blacksquare Q]\!] &\longrightarrow \boldsymbol{\Gamma}[\![\blacksquare P]\!] \\ x &\longmapsto [\![M]\!] \circ x \end{aligned}$$

such that, if $y \in \boldsymbol{\Gamma}[\![Q]\!] \simeq \boldsymbol{\Gamma\Delta\Gamma}[\![Q]\!] = \boldsymbol{\Gamma}[\![\blacksquare Q]\!]$ satisfies ψ in the standard sense (*i.e.* $y \in \{|\varphi|\}$), then the unique global section $\boldsymbol{\Gamma}[\![M]\!](y)_{n+1}(\bullet) = \boldsymbol{\Gamma}[\![M]\!](y)_n(\bullet) \in \boldsymbol{\Gamma}[\![P]\!]$ satisfies φ in the standard sense (*i.e.* belongs to $\{|\varphi|\}$).

D.11 A Galois Connection

It is common for the classification of temporal properties to identify *safety* properties with topologically *closed* sets and to identify *liveness* properties with topologically *dense* sets. As any subset of a topological space is the intersection of a closed set with a dense set, this provides a topological decomposition of temporal properties, which furthermore restricts to regular properties on (finitary) polynomial types. We refer to e.g. [9].

Here, we make explicit the relation between *safe* formulae on polynomial types (in the sense of Def. 6.5) and safety properties understood as closed subsets of the corresponding final **Set**-coalgebras (in view of Møgelberg's Theorem [55]), for the usual tree (or stream) topology.

First, it might be useful to remember what it means for a global section $x \in \boldsymbol{\Gamma} X$ in $\mathcal{S}$ to satisfy a property S, where $S \in \mathrm{Sub}(X)$ is a subobject of X. Following e.g. [52,51], we say that $x \in \boldsymbol{\Gamma} X$ *satisfies* a property $S \in \mathrm{Sub}(X)$ if x factors through S, as in

$$\begin{tikzcd} & S \arrow[d, hook] \\ \mathbf{1} \arrow[ur, dotted] \arrow[r, "x"'] & X \end{tikzcd} \qquad \text{that is:} \quad \forall n > 0, \quad x_n(\bullet) \in S(n)$$

Fix an object X of $\mathcal{S}$. There is a Galois connection between the subobjects of X in $\mathcal{S}$ and the subsets of $\boldsymbol{\Gamma} X$ in **Set**:

$$\mathrm{Pref} \dashv \mathrm{Clos} : \mathrm{Sub}(X) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma} X)$$

where for $S \in \mathcal{P}(\boldsymbol{\Gamma} X)$ and $B \in \mathrm{Sub}(X)$,

$$\begin{aligned} \mathrm{Pref}(S) : &\quad n \longmapsto \{x_n(\bullet) \mid x \in S\} \\ \mathrm{Clos}(B) := &\ \{x \in \boldsymbol{\Gamma} X \mid \forall n > 0,\ x_n(\bullet) \in B(n)\} \end{aligned}$$

Of course, Clos is the restriction of $\boldsymbol{\Gamma} : \mathcal{S} \to \mathbf{Set}$ to the subobjects of X.

Let us spell out the fact that Pref $\dashv$ Clos form a Galois connection. Fix an object X of $\mathcal{S}$. First, it is trivial that the functions

$$\begin{aligned} \mathrm{Pref} : \mathcal{P}(\boldsymbol{\Gamma} X) &\longrightarrow \mathrm{Sub}(X) \\ \mathrm{Clos} : \mathrm{Sub}(X) &\longrightarrow \mathcal{P}(\boldsymbol{\Gamma} X) \end{aligned}$$

are monotone w.r.t. the orders of the lattices $\mathcal{P}(\boldsymbol{\Gamma} X)$ and $\mathrm{Sub}(X)$. Moreover, we have:

Lemma D.31. *We have*

(i) $S \subseteq \mathrm{Clos}(\mathrm{Pref}(S))$ *for* $S \in \mathcal{P}(\boldsymbol{\Gamma} X)$.
(ii) $\mathrm{Pref}(\mathrm{Clos}(B)) \subseteq B$ *for* $B \in \mathrm{Sub}(X)$.

Proof.

(i) Given $x \in S$, by definition we have $x_n(\bullet) \in \mathrm{Pref}(S)(n)$ for all $n > 0$, so $x \in \mathrm{Clos}(\mathrm{Pref}(S))$.
(ii) Given $a \in \mathrm{Pref}(\mathrm{Clos}(B))(n)$, there is some $x \in \mathrm{Clos}(B)$ such that $a = x_n(\bullet)$. But $x \in \mathrm{Clos}(B)$ means $x_k(\bullet) \in B(k)$ for all $k > 0$, so that $a = x_n(\bullet) \in B(n)$. $\square$

As usual, we trivially get

$$\mathrm{Pref}(S) \leq B \qquad \text{iff} \qquad S \subseteq \mathrm{Clos}(B)$$

Say that $S \in \mathcal{P}(\boldsymbol{\Gamma} X)$ is *closed* if $S = \mathrm{Clos}(B)$ for some $B \in \mathrm{Sub}(X)$. It is easy to see that S is closed if and only if $S = \mathrm{Clos}(\mathrm{Pref}(S))$. Note that $S = \mathrm{Clos}(\mathrm{Pref}(S))$ unfolds to

$$\forall x \in \boldsymbol{\Gamma}[\![A]\!], \quad x \in S \quad \text{iff} \quad \forall n > 0,\ \exists y \in S,\ x_n(\bullet) = y_n(\bullet)$$

When A is a polynomial recursive type, Thm. 7.1 thus says that S is closed if and only if S is closed for the corresponding usual tree (or stream) topology. Since Prop. 7.3 can be formulated as

$$\{\!|\varphi|\!\} \quad = \quad \mathrm{Clos}([\![\varphi]\!])$$

it indeed says that $\{\!|\varphi|\!\}$ is closed for the usual topology.

We finally briefly elaborate on this in view of the coincidence of the $\mathcal{S}$ and **Set** semantics for safe formulae (Prop. 7.3). Let us consider the cases of $\Box[\mathsf{hd}]\varphi$ and $\Diamond[\mathsf{hd}]\varphi$ on guarded streams $\mathsf{Str}^{\mathsf{g}}\,\mathsf{B}$. Assume that φ is safe. The equality $\{\!|\Box[\mathsf{hd}]\varphi|\!\} = \boldsymbol{\Gamma}[\![\Box[\mathsf{hd}]\varphi]\!]$ implies that the usual **Set** semantics of $\Box[\mathsf{hd}]\varphi$ is in the image of $\boldsymbol{\Gamma}$. But a subset of $\boldsymbol{\Gamma}[\![\mathsf{Str}^{\mathsf{g}}\,\mathsf{B}]\!]$ which is in the image of $\boldsymbol{\Gamma}$ is necessarily a closed set w.r.t. the usual product topology on streams in **Set**, *i.e.* a safety property. Formulae of the form $\Box[\mathsf{hd}]\varphi$ define safety properties on streams, but liveness properties of the form $\Diamond[\mathsf{hd}]\varphi$ are not closed (for non-trivial φ), and thus cannot be in the image of $\boldsymbol{\Gamma}$.

E Details of the Examples

E.1 Guarded Streams

The Later Modality on Guarded Streams

Example E.1. We have the following basic modal refinement types for $\mathsf{Cons}^{\mathsf{g}}$ and tl^{g}:

$$\begin{array}{rcccc} \mathsf{Cons}^{\mathsf{g}} : A & \longrightarrow & \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} & \longrightarrow & \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \\ \mathsf{tl}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} & \longrightarrow & \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} & & \end{array}$$

Proof. We begin with $\mathsf{Cons}^{\mathsf{g}}$. Recall that $\mathsf{Cons}^{\mathsf{g}} = \lambda x.\lambda s.\mathsf{fold}\langle x, s\rangle$ and that $\bigcirc(-) = [\mathsf{fold}][\pi_1][\mathsf{next}](-)$. The result then follows from the following derivation:

$$\begin{array}{c} \hline x : A,\, s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \\ \hline\hline x : A,\, s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash s : \{\blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{next}]\varphi\} \\ \hline\hline x : A,\, s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash \langle x, s\rangle : \{A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\pi_1][\mathsf{next}]\varphi\} \\ \hline x : A,\, s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash \mathsf{fold}\langle x, s\rangle : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{fold}][\pi_1][\mathsf{next}]\varphi\} \end{array}$$

As for tl^{g}, recalling that $\mathsf{tl}^{\mathsf{g}} = \lambda s.\pi_1(\mathsf{unfold}\ s)$, the result follows from

$$\begin{array}{c} \hline s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{fold}][\pi_1][\mathsf{next}]\varphi\} \\ \hline s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \mathsf{unfold}\ s : \{A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\pi_1][\mathsf{next}]\varphi\} \\ \hline s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \pi_1(\mathsf{unfold}\ s) : \{\blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{next}]\varphi\} \\ \hline\hline s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \pi_1(\mathsf{unfold}\ s) : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \varphi\} \end{array}$$

$\square$

Destructors of Guarded Streams

Example E.2. The types of hd^{g} and tl^{g} can be refined as follows with the *always modality* $\Box$:

$$\begin{array}{rcl} \mathsf{hd}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} & \longrightarrow & \{A \mid \varphi\} \\ \mathsf{tl}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} & \longrightarrow & \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \end{array}$$

Proof. Recall that $[\mathsf{hd}]\varphi = [\mathsf{fold}][\pi_0]\varphi$. We begin with the typing of

$$\mathsf{hd}^{\mathsf{g}} := \lambda s.\pi_0(\mathsf{unfold}\ s) : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \{A \mid \varphi\}$$

We use $\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} \Box[\mathsf{hd}]\varphi \Rightarrow [\mathsf{hd}]\varphi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}} \qquad \dfrac{\dfrac{}{\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} \Box[\mathsf{hd}]\varphi \Rightarrow [\mathsf{hd}]\varphi}}{\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \leq \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}}}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}}}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash \mathsf{unfold}\ s : \{A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\pi_0]\varphi\}}}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash \pi_0(\mathsf{unfold}\ s) : \{A \mid \varphi\}}}{\vdash \lambda s.\pi_0(\mathsf{unfold}\ s) : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \{A \mid \varphi\}}$$

We continue with the typing of

$$\mathsf{tl}^{\mathsf{g}} := \lambda s.\pi_1(\mathsf{unfold}\ s) : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

We use $\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} \Box[\mathsf{hd}]\varphi \Rightarrow \bigcirc\Box[\mathsf{hd}]\varphi$. Recall that $\bigcirc\varphi = [\mathsf{fold}][\pi_1][\mathsf{next}]\varphi$.

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}
\qquad
\dfrac{\dfrac{}{\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} \Box[\mathsf{hd}]\varphi \Rightarrow \bigcirc\Box[\mathsf{hd}]\varphi}}{\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \leq \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\Box[\mathsf{hd}]\varphi\}}
}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\Box[\mathsf{hd}]\varphi\}}
}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash \mathsf{unfold}\ s : \{A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\pi_0][\mathsf{next}]\Box[\mathsf{hd}]\varphi\}}
}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash \pi_1(\mathsf{unfold}\ s) : \{\blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{next}]\Box[\mathsf{hd}]\varphi\}}
}{s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \vdash \pi_1(\mathsf{unfold}\ s) : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}
}{\vdash \lambda s.\pi_1(\mathsf{unfold}\ s) : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}
$$

□

Constructor of Guarded Streams

Example E.3. The type of $\mathsf{Cons}^{\mathsf{g}}$ can be refined as follows with the *always modality* $\Box$:

$$\mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi\} \;\longrightarrow\; \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \;\longrightarrow\; \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

Proof. We show

$$\mathsf{Cons}^{\mathsf{g}} := \lambda x.\lambda s.\mathsf{fold}\langle x, s\rangle : \{A \mid \varphi\} \;\longrightarrow\; \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \;\longrightarrow\; \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

To this end, we use the following derived rule (see Ex. 5.1):

$$\dfrac{\mathcal{E} \vdash M : \{A \mid \varphi\} \qquad \mathcal{E} \vdash N : \{B \mid \psi\}}{\mathcal{E} \vdash \langle M, N\rangle : \{A \times B \mid [\pi_0]\varphi \wedge [\pi_1]\psi\}}$$

Consider the typing context

$$\mathcal{E} := x : \{A \mid \varphi\}\,,\; s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

We know from §E.1 that

$$\mathcal{E} \vdash \mathsf{fold}\langle x, s\rangle : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \bigcirc\Box[\mathsf{hd}]\varphi\}$$

Since $\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} ([\mathsf{hd}]\varphi \wedge \bigcirc\Box[\mathsf{hd}]\varphi) \Rightarrow \Box[\mathsf{hd}]\varphi$, we are done if we show

$$\mathcal{E} \vdash \mathsf{fold}\langle x, s\rangle : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}$$

But this is trivial:

$$
\dfrac{
\dfrac{
\dfrac{}{\mathcal{E} \vdash x : \{A \mid \varphi\}}
}{\mathcal{E} \vdash \langle x, s\rangle : \{A \times \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \mid [\pi_0]\varphi\}}
}{\mathcal{E} \vdash \mathsf{fold}\langle x, s\rangle : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{fold}][\pi_0]\varphi\}}
$$

□

Map over Guarded Streams

Example E.4. We have the following:

$$\begin{array}{ll}\mathsf{map}^{\mathsf{g}} : & (\{A \mid \varphi\} \to \{B \mid \psi\}) \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \\ & := \lambda f.\mathsf{fix}(g).\lambda s.(f\,(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s))\end{array}$$

Proof. We proceed as follows, using §E.1 and §E.1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}}{\mathcal{E} \vdash \mathsf{hd}^{\mathsf{g}}\ s : \{A \mid \varphi\}}}{\mathcal{E} \vdash f(\mathsf{hd}^{\mathsf{g}}\ s) : \{B \mid \psi\}} \qquad \dfrac{\dfrac{\dfrac{}{\mathcal{E} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}}{\mathcal{E} \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}}}{\mathcal{E} \vdash g \circledast (\mathsf{tl}^{\mathsf{g}}\ s) : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\}}}{\dfrac{\mathcal{E} \vdash (f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\}}{\vdash \lambda f.\mathsf{fix}(g).\lambda s.(f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) : T}}$$

where

$$\begin{array}{l}T := (\{A \mid \varphi\} \to \{B \mid \psi\}) \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \\ \mathcal{E} := f : \{A \mid \varphi\} \to \{B \mid \psi\}\,,\ g : \blacktriangleright(\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\}),\ s : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}\end{array}$$

□

Merge over Guarded Streams

Example E.5. We have the following:

$$\begin{array}{ll}\mathsf{merge}^{\mathsf{g}} : & \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_0]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_1]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\} \\ & := \mathsf{fix}(g).\lambda s_0.\lambda s_1.\mathsf{Cons}^{\mathsf{g}}\ (\mathsf{hd}^{\mathsf{g}}\ s_0)\ \big(\mathsf{next}\big(\mathsf{Cons}^{\mathsf{g}}\ (\mathsf{hd}^{\mathsf{g}}\ s_1)\ (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s_0) \circledast (\mathsf{tl}^{\mathsf{g}}\ s_1))\big)\big)\end{array}$$

Proof. Let $\mathcal{E}$ be the context

$$\begin{array}{l}g : \blacktriangleright\big(\,\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_0]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_1]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\}\,\big)\ , \\ s_0 : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_0]\}\ , \\ s_1 : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_1]\}\end{array}$$

We have

$$\begin{array}{ll}\mathcal{E} \vdash \mathsf{hd}^{\mathsf{g}}\ s_0 : \{A \mid \varphi_0\} \qquad & \mathcal{E} \vdash \mathsf{tl}^{\mathsf{g}}\ s_0 : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_0]\} \\ \mathcal{E} \vdash \mathsf{hd}^{\mathsf{g}}\ s_1 : \{A \mid \varphi_1\} \qquad & \mathcal{E} \vdash \mathsf{tl}^{\mathsf{g}}\ s_1 : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\varphi_1]\}\end{array}$$

We thus get

$$g \circledast (\mathsf{tl}^{\mathsf{g}}\ s_0) \circledast (\mathsf{tl}^{\mathsf{g}}\ s_1) : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\}$$

and we are done since using subtyping we have

$$\begin{array}{l}\mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi_0\} \quad \longrightarrow \quad \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\} \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\} \\ \mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi_1\} \quad \longrightarrow \quad \blacktriangleright \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\} \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box([\varphi_0] \vee [\varphi_1])\}\end{array}$$

□

E.2 Operations on Coinductive Streams

Example E.6 (Operations on Coinductive Streams). For a *safe* φ of the appropriate type, we have

$$
\begin{array}{rcl}
\mathsf{hd} : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} & \longrightarrow & \{A \mid \varphi\} \\
\mathsf{tl} : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} & \longrightarrow & \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \\
\mathsf{tl} : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} & \longrightarrow & \{\mathsf{Str}\,A \mid [\mathsf{box}]\varphi\}
\end{array}
$$

Proof.

Case of hd.

Recall that

$$
\begin{array}{rl}
\mathsf{hd} : & \mathsf{Str}\,A \longrightarrow A \\
& := \lambda s.\mathsf{hd}^{\mathsf{g}}\ (\mathsf{unbox}\ s)
\end{array}
$$

We have

$$
\begin{array}{c}
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \qquad \Box[\mathsf{hd}]\varphi \text{ safe} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash s : \blacksquare\{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{unbox}\ s : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{hd}^{\mathsf{g}}(\mathsf{unbox}\ s) : \{A \mid \varphi\} \\
\hline
\vdash \lambda s.\mathsf{hd}^{\mathsf{g}}\ (\mathsf{unbox}\ s) \quad : \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{A \mid \varphi\}
\end{array}
$$

Cases of tl.

Recall that

$$
\begin{array}{rl}
\mathsf{tl} : & \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,A \\
& := \lambda s.\mathsf{box}_\iota(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s)))
\end{array}
$$

We have

$$
\begin{array}{c}
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{unbox}\ s : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s) \quad : \quad \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \qquad \mathsf{Str}\,A \text{ constant} \\
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s)) \quad : \quad \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{box}_\iota(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \blacksquare\{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \qquad \Box[\mathsf{hd}]\varphi \text{ safe} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash \mathsf{box}_\iota(\mathsf{prev}\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \\
\hline
\vdash \lambda s.\mathsf{box}_\iota(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}
\end{array}
$$

and

$$
\begin{array}{c}
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash \mathsf{unbox}\ s : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \bigcirc\varphi\} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash \mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s) \quad : \quad \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\,A \mid \varphi\} \qquad \mathsf{Str}\,A \text{ constant} \\
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash \mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s)) \quad : \quad \{\mathsf{Str}^{\mathsf{g}}\,A \mid \varphi\} \\
\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash \mathsf{box}_\iota(\mathsf{prev}\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \blacksquare\{\mathsf{Str}^{\mathsf{g}}\,A \mid \varphi\} \qquad \varphi \text{ safe} \\
\hline\hline
s : \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \vdash \mathsf{box}_\iota(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\varphi\} \\
\hline
\vdash \lambda s.\mathsf{box}_\iota(\mathsf{prev}_\iota(\mathsf{tl}^{\mathsf{g}}\ (\mathsf{unbox}\ s))) \quad : \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\bigcirc\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\varphi\}
\end{array}
$$

□

E.3 Map over Coinductive Streams

We discuss here the cases of

$$\mathsf{map} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \;\longrightarrow\; \{\mathsf{Str}\, B \mid [\mathsf{box}]\triangle[\mathsf{hd}]\psi\} \;\longrightarrow\; \{\mathsf{Str}\, A \mid [\mathsf{box}]\triangle[\mathsf{hd}]\varphi\}$$

where ψ, φ are *safe and smooth* and where $\triangle \in \{\Box, \Diamond, \Diamond\Box, \Box\Diamond\}$. The case of $\Box$ is handled as in Ex. 5.4, using that $\Box[\mathsf{hd}]\varphi$ and $\Box[\mathsf{hd}]\psi$ are safe. The case of $\Diamond$ is detailed in Ex. E.7 (§E.3). The idea is that since $\Diamond[\mathsf{hd}]\varphi$, $\Diamond[\mathsf{hd}]\psi$ are smooth and since $\Diamond^k[\mathsf{hd}]\varphi$, $\Diamond^k[\mathsf{hd}]\psi$ are safe, we can reduce to typing the *guarded* $\mathsf{map}^{\mathsf{g}}$ as

$$\mathsf{map}^{\mathsf{g}} : (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \forall k \cdot \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^k[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\}\right)$$

The case of $\Diamond\Box$, detailed in Ex. E.8 (§E.3), is more involved. Since $\Diamond\Box[\mathsf{hd}]\varphi$, $\Diamond\Box[\mathsf{hd}]\psi$ are smooth and $\Diamond^k\Box[\mathsf{hd}]\varphi$, $\Diamond^k\Box[\mathsf{hd}]\psi$ are safe, we similarly reduce to showing $(\mathsf{map}^{\mathsf{g}}\ f) : \forall k \cdot T(k)$ where

$$T(k) := \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^k\Box[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k\Box[\mathsf{hd}]\varphi\right\}$$

and assuming f of type $\{B \mid \psi\} \to \{A \mid \varphi\}$. But this is unfortunately too weak. Similarly as with $\Diamond$, it is natural to first assume the type $\blacktriangleright\forall k \cdot T(k)$ for the recursion variable g and then to apply the ($\forall$-CI) rule (Fig. 11) on $\forall k \cdot T(k)$. In the case of $T(k{+}1)$, we unfold

$$\Diamond^{k+1}\Box[\mathsf{hd}]\psi \Leftrightarrow \Box[\mathsf{hd}]\psi \quad\vee\quad \bigcirc\,\Diamond^k\Box[\mathsf{hd}]\psi$$

and apply the ($\vee$-E) rule (Fig. 8). But in the branch of $\Box[\mathsf{hd}]\psi$, giving g the type, say,

$$\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^1\Box[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^1\Box[\mathsf{hd}]\varphi\right\}$$

is not sufficient to derive

$$s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \vdash g \circledast (\mathsf{tl}^{\mathsf{g}}\ s) : \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

The reason is that $[\mathsf{next}]$ (and thus $\bigcirc$) does not satisfy axiom (P) of Table 2 (see §7). The solution is to use the $[\mathsf{ev}(-)]/\Vert\!\!\to$ modality to encode a kind of "intersection" on arrow types, and to type $(\mathsf{map}^{\mathsf{g}} f)$ with

$$\forall k \cdot \left\{\mathsf{Str}^{\mathsf{g}}\, B \to \mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \left(\Diamond^k\Box[\mathsf{hd}]\psi \Vert\!\!\to \Diamond^k\Box[\mathsf{hd}]\varphi\right) \;\wedge\; \left(\Box[\mathsf{hd}]\psi \Vert\!\!\to \Box[\mathsf{hd}]\varphi\right)\right\}$$

We finally turn to $\Box\Diamond$. Using that $\Box\Diamond[\mathsf{hd}]\varphi$ and $\Box\Diamond[\mathsf{hd}]\psi$ are both smooth, we first unfold the $\Box$'s using the rules (ν-I) (Fig. 11) and then (ν-E) (Ex. 6.10), thus reducing to

$$\mathsf{box}_\iota\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)\big) : \left\{\mathsf{Str}\, A \;\middle|\; [\mathsf{box}]\Box^\ell\Diamond[\mathsf{hd}]\varphi\right\}$$

assuming $f : \{B \mid \psi\} \to \{A \mid \varphi\}$ and $s : \left\{\mathsf{Str}\, B \;\middle|\; [\mathsf{box}]\Box^\ell\Diamond[\mathsf{hd}]\psi\right\}$. Then, since $\Diamond[\mathsf{hd}]\varphi$, $\Diamond[\mathsf{hd}]\psi$ are smooth, we can unfold the $\Diamond$'s using the rules (μ-E) and (μ-I) with the non-trivial *smooth* context

$$\gamma(\beta) := \Box^\ell\beta$$

Since the formulae $\Box^\ell\Diamond^k[\mathsf{hd}]\psi$ and $\Box^\ell\Diamond^k[\mathsf{hd}]\varphi$ are safe, we can reduce to showing

$$\begin{array}{l} \lambda s.\ (f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) : \quad \forall \ell \cdot \forall k \cdot U(\ell, k) \\ \qquad\qquad\qquad\qquad U(\ell,k) := \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^\ell\Diamond^k[\mathsf{hd}]\psi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^\ell\Diamond^k[\mathsf{hd}]\varphi\right\} \end{array}$$

assuming $f : \{B \mid \psi\} \to \{A \mid \varphi\}$ and $g : \blacktriangleright\forall\ell \cdot \forall k \cdot U(\ell,k)$. We apply the ($\forall$-CI) rule on $\forall\ell\cdot\forall k\cdot U(\ell,k)$. The case of $\forall k\cdot U(0,k)$ is trivial since $\Box^0\vartheta \Leftrightarrow \top$. We then apply the ($\forall$-CI) rule, this time on $\forall k\cdot U(\ell{+}1,k)$. The case of $U(\ell{+}1,0)$ can be dealt with using the (ExF) rule. In the case of $U(\ell{+}1,k{+}1)$, we conclude with a straightforward case analysis based on the unfoldings

$$\begin{array}{rcl} \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\vartheta \Leftrightarrow \Diamond^{k+1}[\mathsf{hd}]\vartheta & \wedge & \bigcirc\,\Box^\ell\Diamond^{k+1}[\mathsf{hd}]\vartheta \\ \Diamond^{k+1}[\mathsf{hd}]\vartheta \Leftrightarrow [\mathsf{hd}]\vartheta & \vee & \bigcirc\,\Diamond^k[\mathsf{hd}]\vartheta \end{array}$$

See Ex. E.9 (§E.3) for details. Just note that since $\bigcirc\top \Leftrightarrow \top$ (Table 2) we have $\Box^1\vartheta \Leftrightarrow \vartheta$, so that

$$g : \blacktriangleright\forall\ell\cdot\forall k\cdot U(\ell,k) \vdash g : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^k[\mathsf{hd}]\psi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\}$$

The Case of *Eventually* ($\Diamond[\mathsf{hd}]\varphi$)

Example E.7. We have the following, for *safe and smooth* φ and ψ:

$$\begin{array}{l} \mathsf{map} : \ \ (\{B \mid \psi\} \to \{A \mid \varphi\}) \ \longrightarrow\ \{\mathsf{Str}\, B \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\psi\} \ \longrightarrow\ \{\mathsf{Str}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \\ \qquad = \lambda f.\lambda s.\mathsf{box}_\iota\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)\big) \end{array}$$

Proof. Since $\Diamond[\mathsf{hd}]\varphi$ and $\Diamond[\mathsf{hd}]\psi$ are both smooth, we can first reduce to

$$\mathcal{E}_f,\ s : \left\{\mathsf{Str}\, B \;\middle|\; [\mathsf{box}]\Diamond^k[\mathsf{hd}]\psi\right\} \vdash \mathsf{box}_\iota(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)) : \left\{\mathsf{Str}\, A \;\middle|\; [\mathsf{box}]\Diamond^k[\mathsf{hd}]\varphi\right\}$$

where

$$\mathcal{E}_f := f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

Since the formulae $\Diamond^k[\mathsf{hd}]\psi$ and $\Diamond^k[\mathsf{hd}]\varphi$ are safe, we are done if we show

$$\begin{array}{l} \mathsf{map}^{\mathsf{g}} : \ \ (\{B \mid \psi\} \to \{A \mid \varphi\}) \ \longrightarrow\ \forall k \cdot \Big(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^k[\mathsf{hd}]\psi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\}\Big) \\ \qquad = \lambda f.\mathsf{fix}(g).\lambda s.(f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \end{array}$$

Let

$$\begin{array}{lcl} N & := & (f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \\ M & := & \lambda s.N \\ T(k) & := & \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^k[\mathsf{hd}]\psi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\} \\ \mathcal{E} & := & \mathcal{E}_f,\ g : \blacktriangleright\forall k\cdot T(k) \end{array}$$

We show

$$\mathcal{E} \vdash M : \forall k \cdot T(k)$$

We reason by cases on k with the rule

$$\frac{\mathcal{E} \vdash M : T(0) \qquad \mathcal{E} \vdash M : T(k{+}1)}{\mathcal{E} \vdash M : \forall k \cdot T(k)}$$

Case of $T(0)$.

We show

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Diamond^{0}[\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{hd}]\varphi\}$$

Since $\vdash \Diamond^{0}[\psi] \Leftrightarrow \bot$, we conclude with the (ExF) rule

$$\frac{\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Diamond^{0}[\mathsf{hd}]\psi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \bot\} \qquad \mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Diamond^{0}[\mathsf{hd}]\psi\} \vdash N : \mathsf{Str}^{\mathsf{g}}\, A}{\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Diamond^{0}[\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{hd}]\varphi\}}$$

Case of $T(k{+}1)$.

We show

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

Using

$$\vdash \Diamond^{k+1}[\mathsf{hd}]\psi \Leftrightarrow ([\mathsf{hd}]\psi \vee \bigcirc\Diamond^{k}[\mathsf{hd}]\psi)$$

we do a case analysis on the refinement type of s.

(Sub)Case of $[\mathsf{hd}]\psi$.

Since $\vdash [\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$, we reduce to showing

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid [\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}$$

By §E.1 we have

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid [\mathsf{hd}]\psi\} \vdash \mathsf{hd}^{\mathsf{g}}\ s : \{B \mid \psi\}$$

But we are done since

$$\mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi\} \quad\longrightarrow\quad \blacktriangleright \mathsf{Str}^{\mathsf{g}}\, A \quad\longrightarrow\quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}$$

(Sub)Case of $\bigcirc\Diamond^{k}[\mathsf{hd}]\psi$.

Since $\vdash \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$, we reduce to showing

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi\right\}$$

By §E.1 we have

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\} \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}[\mathsf{hd}]\psi\right\}$$

Since

$$\mathcal{E} \vdash g : \forall k \cdot \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

we have

$$\mathcal{E} \vdash g : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

Since moreover by §E.1 we have

$$\mathsf{Cons}^{\mathsf{g}} : A \quad\longrightarrow\quad \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi\right\}$$

we deduce that

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\}$$

$\square$

The Case of *Eventually Always* ($\Diamond\Box[\mathsf{hd}]\varphi$)

Example E.8. We have the following, for *safe and smooth* φ and ψ:

$$\begin{aligned}\mathsf{map} :\ & (\{B \mid \psi\} \to \{A \mid \varphi\}) \ \longrightarrow\ \{\mathsf{Str}\,B \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}]\psi\} \ \longrightarrow\ \{\mathsf{Str}\,A \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}]\varphi\} \\ &= \lambda f.\lambda s.\mathsf{box}_\iota\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)\big)\end{aligned}$$

Proof. Since $\Diamond\Box[\mathsf{hd}]\varphi$ and $\Diamond\Box[\mathsf{hd}]\psi$ are both smooth, we can first reduce to

$$\mathcal{E}_f,\ s : \big\{\mathsf{Str}\,B \bigm| [\mathsf{box}]\Diamond^k\Box[\mathsf{hd}]\psi\big\} \vdash \mathsf{box}_\iota(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)) : \big\{\mathsf{Str}\,A \bigm| [\mathsf{box}]\Diamond^k\Box[\mathsf{hd}]\varphi\big\}$$

where

$$\mathcal{E}_f := f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

Since the formulae $\Diamond^k\Box[\mathsf{hd}]\psi$ and $\Diamond^k\Box[\mathsf{hd}]\varphi$ are safe, we are done if we show

$$\begin{aligned}\mathsf{map}^{\mathsf{g}} :\ & (\{B \mid \psi\} \to \{A \mid \varphi\}) \ \longrightarrow\ \forall k \cdot \big(\big\{\mathsf{Str}^{\mathsf{g}}\,B \bigm| \Diamond^k\Box[\mathsf{hd}]\psi\big\} \ \longrightarrow\ \big\{\mathsf{Str}^{\mathsf{g}}\,A \bigm| \Diamond^k\Box[\mathsf{hd}]\varphi\big\}\big) \\ &= \lambda f.\mathsf{fix}(g).\lambda s.(f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s))\end{aligned}$$

Let

$$\begin{array}{ll} N & := (f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \\ M & := \lambda s.N \\ T(k) & := \big\{\mathsf{Str}^{\mathsf{g}}\,B \to \mathsf{Str}^{\mathsf{g}}\,A \bigm| \big(\Diamond^k\Box[\mathsf{hd}]\psi \Vdash\!\!\to \Diamond^k\Box[\mathsf{hd}]\varphi\big) \ \wedge\ \big(\Box[\mathsf{hd}]\psi \Vdash\!\!\to \Box[\mathsf{hd}]\varphi\big)\big\} \\ \mathcal{E} & := \mathcal{E}_f,\ g : \blacktriangleright\forall k \cdot T(k) \end{array}$$

We show

$$\mathcal{E} \vdash M : \forall k \cdot T(k)$$

We reason by cases on k with the rule

$$\frac{\mathcal{E} \vdash M : T(0) \qquad \mathcal{E} \vdash M : T(k{+}1)}{\mathcal{E} \vdash M : \forall k \cdot T(k)}$$

Case of $T(0)$.

We have to show

$$\begin{array}{rl} & \mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Box[\mathsf{hd}]\psi\} \quad\ \vdash N : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\ \text{and} & \mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Diamond^0\Box[\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Diamond^0\Box[\mathsf{hd}]\varphi\} \end{array}$$

We only detail the latter since the former can be dealt-with as in §E.1. Since

$$\vdash \Diamond^0\Box[\psi] \Leftrightarrow \bot$$

we conclude with the (ExF) rule

$$\frac{\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Diamond^0\Box[\mathsf{hd}]\psi\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \bot\} \qquad \mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Diamond^0\Box[\mathsf{hd}]\psi\} \vdash N : \mathsf{Str}^{\mathsf{g}}\,A}{\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Diamond^0\Box[\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Diamond^0\Box[\mathsf{hd}]\varphi\}}$$

Case of $T(k{+}1)$.

We show

$$
\begin{array}{ll}
 & \mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \qquad\ \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \\
\text{and} & \mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}]\varphi\right\}
\end{array}
$$

We only detail the latter since the former can be dealt-with as in §E.1. Using

$$\vdash \Diamond^{k+1}\Box[\mathsf{hd}]\psi \Leftrightarrow (\Box[\mathsf{hd}]\psi \vee \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi)$$

we do a case analysis on the refinement type of s.

(Sub)Case of $\Box[\mathsf{hd}]\psi$.

We show

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}]\varphi\right\}$$

Note that $\vdash \Box[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}\Box[\mathsf{hd}]\varphi$. We can therefore reduce to

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box[\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

and we can conclude as in §E.1.

(Sub)Case of $\bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi$.

Since $\vdash \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}\Box[\mathsf{hd}]\varphi$, we reduce to showing

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\varphi\right\}$$

By §E.1 we have

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi\right\} \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\psi\right\}$$

Since

$$\mathcal{E} \vdash g : \forall k \cdot \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\varphi\right\}\right)$$

we have

$$\mathcal{E} \vdash g : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\varphi\right\}\right)$$

Since moreover by §E.1 we have

$$\mathsf{Cons}^{\mathsf{g}} : A \quad\longrightarrow\quad \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}\Box[\mathsf{hd}]\varphi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\varphi\right\}$$

we deduce that

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}\Box[\mathsf{hd}]\psi\right\}$$

$\Box$

The Case of *Always Eventually* ($\Box\Diamond[\mathsf{hd}]\varphi$)

Example E.9. We have the following, for *safe and smooth* φ and ψ:

$$\begin{array}{rl} \mathsf{map}: & (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathsf{Str}\, B \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}]\psi\} \longrightarrow \{\mathsf{Str}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}]\varphi\} \\ & := \lambda f.\lambda s.\mathsf{box}_\iota\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)\big) \end{array}$$

Note E.10. We let

$$\begin{array}{l} \Diamond^{\mathsf{t}}\varphi := \mu^{\mathsf{t}}\alpha.\varphi \vee \bigcirc\alpha \\ \Box^{\mathsf{t}}\varphi := \nu^{\mathsf{t}}\alpha.\varphi \wedge \bigcirc\alpha \end{array}$$

Proof. We start in the same spirit as in §E.3 and §E.3. Using that $\Box\Diamond[\mathsf{hd}]\varphi$ and $\Box\Diamond[\mathsf{hd}]\psi$ are both smooth, we first unfold the $\Box$ using the rules (ν-I) and (ν-E). Then, since $\Diamond[\mathsf{hd}]\varphi$ and $\Diamond[\mathsf{hd}]\psi$ are both smooth, we can unfold the $\Diamond$ using the rules (μ-E) and (μ-I) with the non-trivial *smooth* context

$$\gamma(\beta) := \Box^{\ell}\beta$$

We are thus led to deriving

$$\mathcal{E}_f,\ s : \big\{\mathsf{Str}\, B \bigm| [\mathsf{box}]\Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi\big\} \vdash \mathsf{box}_\iota(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{unbox}\ s)) : \big\{\mathsf{Str}\, A \bigm| [\mathsf{box}]\Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi\big\}$$

where

$$\mathcal{E}_f := f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

Since the formulae $\Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi$ and $\Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi$ are safe, we are done if we show

$$\begin{array}{rl} \mathsf{map}^{\mathsf{g}}: & (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \forall k \cdot \forall \ell \cdot \big(\big\{\mathsf{Str}^{\mathsf{g}}\, B \bigm| \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi\big\} \longrightarrow \big\{\mathsf{Str}^{\mathsf{g}}\, A \bigm| \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi\big\}\big) \\ & = \lambda f.\mathsf{fix}(g).\lambda s.(f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \end{array}$$

Let

$$\begin{array}{ll} N & := (f(\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \\ M & := \lambda s.N \\ T(k,\ell) & := \big\{\mathsf{Str}^{\mathsf{g}}\, B \bigm| \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi\big\} \longrightarrow \big\{\mathsf{Str}^{\mathsf{g}}\, A \bigm| \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi\big\} \\ \mathcal{E} & := \mathcal{E}_f,\ g : \blacktriangleright\forall k \cdot \forall \ell \cdot T(k,\ell) \end{array}$$

We show

$$\mathcal{E} \vdash M : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We reason by cases on k and ℓ. This amounts to the derived rule

$$\frac{\mathcal{E} \vdash M : T(\mathsf{0},\mathsf{0}) \qquad \mathcal{E} \vdash M : T(\mathsf{0},\ell{+}\mathsf{1}) \qquad \mathcal{E} \vdash M : T(k{+}\mathsf{1},\mathsf{0}) \qquad \mathcal{E} \vdash M : T(k{+}\mathsf{1},\ell{+}\mathsf{1})}{\mathcal{E} \vdash M : \forall k \cdot \forall \ell \cdot T(k,\ell)}$$

Cases of $T(\mathsf{u},\mathsf{0})$.

We have $\vdash \Box^{\mathsf{0}}\theta \Leftrightarrow \top$, and we are done since

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \top\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \top\}$$

Case of $T(0, \ell{+}1)$.

We have $\vdash \Diamond^{0}[\theta] \Leftrightarrow \bot$, and we reduce to showing

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\bot\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{\ell+1}\bot\right\}$$

But since $\vdash \Box^{\ell+1}\bot \Rightarrow \bot$, we have

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\bot\right\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \bot\}$$

and we conclude with the (ExF) rule

$$\dfrac{\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\bot\right\} \vdash s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \bot\} \qquad \mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\bot\right\} \vdash N : \mathsf{Str}^{\mathsf{g}}\, A}{\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid \Box^{\ell+1}\bot\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box^{\ell+1}\bot\}}$$

Case of $T(k{+}1, \ell{+}1)$.

Using $\vdash^{\mathsf{Str}^{\mathsf{g}}\, A} \Box^{\ell+1}\theta \quad \Leftrightarrow \quad (\theta \wedge \bigcirc\Box^{\ell}\theta)$, we show

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi \ \wedge \ \bigcirc\Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

We consider each conjunct separately.

(Sub)Case of $\Diamond^{k+1}[\mathsf{hd}]\varphi$.

We show

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

Using

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\psi\right\}$$

and $\vdash \Diamond^{k+1}[\mathsf{hd}]\psi \quad \Leftrightarrow \quad ([\mathsf{hd}]\psi \vee \bigcirc\Diamond^{k}[\mathsf{hd}]\psi)$ we do a case analysis on the refinement type of s.

(SubSub)Case of $[\mathsf{hd}]\psi$.

Since (by §E.1)

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid [\mathsf{hd}]\psi\} \vdash \mathsf{hd}^{\mathsf{g}}\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid [\mathsf{hd}]\psi\}$$

we easily deduce that

$$\mathcal{E},\ s : \{\mathsf{Str}^{\mathsf{g}}\, B \mid [\mathsf{hd}]\psi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}$$

and we are done since $\vdash [\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$.

(SubSub)Case of $\bigcirc\Diamond^{k}[\mathsf{hd}]\psi$.

By §E.1 we have

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\} \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}[\mathsf{hd}]\psi\right\}$$

Since

$$\mathcal{E} \vdash g : \forall k \cdot \forall \ell \cdot \blacktriangleright\left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

we have

$$\mathcal{E} \vdash g : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{1}\Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{1}\Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

But $\vdash (\theta \wedge \bigcirc\top) \Leftrightarrow \theta$, so that $\vdash \Box^{1}\theta \Leftrightarrow \theta$, and thus

$$\mathcal{E} \vdash g : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

Since moreover by §E.1 we have

$$\mathsf{Cons}^{\mathsf{g}} : A \quad\longrightarrow\quad \blacktriangleright\left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi\right\}$$

we deduce that

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{hd}]\psi\right\}$$

and we are done since $\vdash \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$.

(Sub)Case of $\bigcirc\Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi$.
We show

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

Since

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \bigcirc\Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\psi\right\}$$

by §E.1 we have

$$\mathcal{E},\ s : \left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell+1}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\psi\right\}$$

But now since

$$\mathcal{E} \vdash g : \forall k \cdot \forall \ell \cdot \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{\ell}\Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

we have

$$\mathcal{E} \vdash g : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, B \;\middle|\; \Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\psi\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi\right\}\right)$$

and we conclude with §E.1, namely

$$\mathsf{Cons}^{\mathsf{g}} : A \quad\longrightarrow\quad \blacktriangleright\left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi\right\} \quad\longrightarrow\quad \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Box^{\ell}\Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

$\Box$

E.4 The Diagonal Function

Consider a stream of streams s. We have $s = (s_i \mid i \geq 0)$ where each s_i is itself a stream $s_i = (s_{i,j} \mid j \geq 0)$. The *diagonal* of s is then the stream $(s_{i,i} \mid i \geq 0)$. Note that $s_{i,i} = \mathsf{hd}(\mathsf{tl}^{i}(\mathsf{hd}(\mathsf{tl}^{i}(s))))$. Indeed, $\mathsf{tl}^{i}(s)$ is the stream of streams $(s_k \mid k \geq i)$, so that $\mathsf{hd}(\mathsf{tl}^i(s))$ is the stream s_i and $\mathsf{tl}^i(\mathsf{hd}(\mathsf{tl}^i(s)))$ is the stream $(s_{i,k} \mid k \geq i)$. Taking its the head thus gives $s_{i,i}$.

We implement the diagonal function as follows:

$$\begin{array}{rll}
\mathsf{diag} & := \lambda s.\mathsf{box}_\iota\big(\mathsf{diag}^{\mathsf{g}}\ (\mathsf{unbox}\ s)\big) & : \mathsf{Str}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}\,A \\
\mathsf{diag}^{\mathsf{g}} & := \mathsf{diagaux}^{\mathsf{g}}\ \mathrm{id} & : \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \\
\mathsf{diagaux}^{\mathsf{g}} : & (\mathsf{Str}\,A \to \mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A & \\
& := \mathsf{fix}(g).\lambda t.\lambda s.\ \mathsf{Cons}^{\mathsf{g}}\ \big((\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s)\big)\ \big(g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)\big) &
\end{array}$$

The auxiliary higher-order function $\mathsf{diagaux}^{\mathsf{g}}$ iterates the coinductive tl over the head of the stream of streams s. We write $\circ$ for function composition, so that assuming $s : \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A)$ and $t : \mathsf{Str}\,A \to \mathsf{Str}\,A$, we have

$$\begin{array}{rr}
(\mathsf{hd}^{\mathsf{g}}\ s) : \mathsf{Str}\,A & (\mathsf{hd} \circ t) : \mathsf{Str}\,A \to A \\
(\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s) : A & (t \circ \mathsf{tl}) : \mathsf{Str}\,A \to \mathsf{Str}\,A
\end{array}$$

This requires the *coinductive* type $\mathsf{Str}\,A$. In Ex. E.11 (§E.4) below, for a *safe* φ we obtain

$$\mathsf{diag}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}$$

This easily follows from the fact that using Ex. 5.3 and Ex. 5.4, we can type $\mathsf{diagaux}^{\mathsf{g}}$ with

$$\begin{array}{l}
\big(\{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) \quad \longrightarrow \\
\qquad\qquad \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}
\end{array}$$

In Ex. E.12 (§E.4) we show that for a *safe and smooth* φ, we have

$$\mathsf{diag} : \{\mathsf{Str}(\mathsf{Str}\,A) \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}]\varphi\}$$

Similarly as for map in §E.3, we reduce to

$$\begin{array}{lrl}
& \mathsf{diagaux}^{\mathsf{g}} : & \forall k \cdot \Big(\big(\{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) \quad \longrightarrow \quad U(k)\Big) \\
\text{where} & U(k) := & \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \to \mathsf{Str}^{\mathsf{g}}\,A \mid \psi_0(k) \quad \wedge \quad \psi_1\} \\
& \psi_0(k) := & \Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi \Vdash\!\!\to \Diamond^k\Box[\mathsf{hd}]\varphi \\
& \psi_1 := & \quad\ \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi \Vdash\!\!\to \quad\ \Box[\mathsf{hd}]\varphi
\end{array}$$

The Guarded Diagonal Function

Example E.11 (The Guarded Diagonal Function). For a *safe* φ, we have

$$\mathsf{diag}^{\mathsf{g}} : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}$$

Recall that

$$\begin{array}{rl}
\mathsf{diag}^{\mathsf{g}} : & \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \quad \longrightarrow \quad \mathsf{Str}^{\mathsf{g}}\,A \\
& := \mathsf{diagaux}^{\mathsf{g}}\ \mathrm{id}
\end{array}$$

$$\begin{array}{rl}
\mathsf{diagaux}^{\mathsf{g}} : & (\mathsf{Str}\,A \to \mathsf{Str}\,A) \quad \longrightarrow \quad \mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \quad \longrightarrow \quad \mathsf{Str}^{\mathsf{g}}\,A \\
& := \mathsf{fix}(g).\lambda t.\lambda s.\mathsf{Cons}^{\mathsf{g}}\ \big((\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s)\big)\ \big(g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)\big)
\end{array}$$

Proof. We reduce to

$$\begin{array}{rcl}\mathsf{diagaux^g} & : & \big(\{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) \quad \longrightarrow \\ & & \{\mathsf{Str^g}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str^g}\,A \mid \Box[\mathsf{hd}]\varphi\}\end{array}$$

Let $\mathcal{E}$ be the context

$$\begin{array}{l} g : \blacktriangleright T\,, \\ t : \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\,, \\ s : \{\mathsf{Str^g}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \end{array}$$

where T is the type

$$\begin{array}{l}\big(\{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) \quad \longrightarrow \\ \qquad \{\mathsf{Str^g}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str^g}\,A \mid \Box[\mathsf{hd}]\varphi\}\end{array}$$

The result directly follows from the following typings, which are themselves given by §E.1, §E.1 and §E.2:

$$\begin{array}{lcl} \mathcal{E} \vdash \mathsf{hd} \circ t & : & \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{A \mid \varphi\} \\ \mathcal{E} \vdash \mathsf{hd^g}\ s & : & \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \\ \mathcal{E} \vdash t \circ \mathsf{tl} & : & \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \\ \mathcal{E} \vdash \mathsf{tl^g}\ s & : & \blacktriangleright \{\mathsf{Str^g}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \end{array}$$

□

The Coinductive Diagonal Function

Example E.12 (The Coinductive Diagonal Function). For a *safe and smooth* φ, we have

$$\begin{array}{rl}\mathsf{diag} : & \{\mathsf{Str}(\mathsf{Str}\,A) \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad \longrightarrow \quad \{\mathsf{Str}\,A \mid [\mathsf{box}]\Diamond\Box[\mathsf{hd}]\varphi\} \\ := & \lambda s.\mathsf{box}_\iota(\mathsf{diag^g}\ (\mathsf{unbox}\ s))\end{array}$$

Proof. Using that $\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi$ and $\Diamond^k\Box[\mathsf{hd}]\varphi$ are both smooth, we can first reduce to

$$s : \big\{\mathsf{Str}(\mathsf{Str}\,A) \bigm| [\mathsf{box}]\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\big\} \vdash \mathsf{box}_\iota(\mathsf{diag^g}\ (\mathsf{unbox}\ s)) : \big\{\mathsf{Str}\,A \bigm| [\mathsf{box}]\Diamond^k\Box[\mathsf{hd}]\varphi\big\}$$

Since the formulae $\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi$ and $\Diamond^k\Box[\mathsf{hd}]\varphi$ are safe, we are done if we show

$$\mathsf{diag^g} : \forall k \cdot \Big(\big\{\mathsf{Str^g}(\mathsf{Str}\,A) \bigm| \Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\big\} \quad \longrightarrow \quad \big\{\mathsf{Str^g}\,A \bigm| \Diamond^k\Box[\mathsf{hd}]\varphi\big\}\Big)$$

Consider the types

$$\begin{array}{l} U(k) := \{\mathsf{Str^g}(\mathsf{Str}\,A) \to \mathsf{Str^g}\,A \mid \psi_0 \quad \wedge \quad \psi_1\} \\ T(k) := \big(\{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\,A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) \quad \longrightarrow \quad U(k) \end{array}$$

where

$$\begin{array}{rl} \psi_0 := & \Diamond^k \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi \mathrel{\|\!\!\to} \Diamond^k \Box[\mathsf{hd}]\varphi \\ \psi_1 := & \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi \mathrel{\|\!\!\to} \Box[\mathsf{hd}]\varphi \end{array}$$

We show

$$\mathsf{diagaux}^{\mathsf{g}} : \forall k \cdot T(k)$$

Let

$$\begin{array}{ll} N & := \mathsf{Cons}^{\mathsf{g}} \left((\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s)\right) \left(g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)\right) \\ M & := \lambda g.\lambda s.N \\ \mathcal{E} & := g : \blacktriangleright \forall k \cdot T(k) \end{array}$$

We reason by cases on k with the rule

$$\frac{\mathcal{E} \vdash M : T(0) \qquad \mathcal{E} \vdash M : T(k{+}1)}{\mathcal{E} \vdash M : \forall k \cdot T(k)}$$

Let

$$\mathcal{E}' := \mathcal{E},\ t : \{\mathsf{Str}\, A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \quad\longrightarrow\quad \{\mathsf{Str}\, A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}$$

We omit the proof of

$$\mathcal{E}' \vdash \lambda s.N : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A) \to \mathsf{Str}^{\mathsf{g}}\, A \mid [\mathsf{ev}(\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi)]\Box[\mathsf{hd}]\varphi\}$$

since it follows that of §E.4.

Case of $T(0)$.
Since $\vdash \Diamond^0\theta \Leftrightarrow \bot$, we reduce to showing

$$\begin{array}{rl} \mathcal{E} \vdash \lambda t.\lambda s.N : \big(\{\mathsf{Str}\, A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \to \{\mathsf{Str}\, A \mid [\mathsf{box}]\Box[\mathsf{hd}]\varphi\}\big) & \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A) \mid \bot\} \\ & \longrightarrow \quad \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Diamond^0\Box[\mathsf{hd}]\varphi\} \end{array}$$

and we conclude using the (ExF) rule.

Case of $T(k{+}1)$.
We show

$$\mathcal{E}',\ s : \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A) \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}]\varphi\right\}$$

Using

$$\vdash \quad \Diamond^{k+1}\theta \quad\Longleftrightarrow\quad \theta \;\vee\; \bigcirc\Diamond^k\theta$$

we reason by cases on the refinement of s. This leads to two subcases.

(Sub)Case of $\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi$.
We show

$$\mathcal{E}',\ s : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}\Box[\mathsf{hd}]\varphi\right\}$$

Since $\vdash \Box[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}\Box[\mathsf{hd}]\varphi$, we can reduce to

$$\mathcal{E}',\ s : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\, A) \mid \Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\} \vdash N : \{\mathsf{Str}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

which is proved as in §E.4.

(Sub)Case of $\bigcirc\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi$.
We show

$$\mathcal{E}',\ s : \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \;\middle|\; \bigcirc\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\} \vdash N : \left\{\mathsf{Str}^{\mathsf{g}}\,A \;\middle|\; \bigcirc\Diamond^k\Box[\mathsf{hd}]\varphi\right\}$$

Let

$$\mathcal{E}'' := \mathcal{E}',\ s : \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \;\middle|\; \bigcirc\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\}$$

Note that $\mathcal{E}'' \vdash g : \blacktriangleright T(k)$, so that by §E.2 we have

$$\mathcal{E}'' \vdash g \circledast \mathsf{next}(t \circ \mathsf{tl}) : \blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \;\middle|\; \Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\} \to \left\{\mathsf{Str}^{\mathsf{g}}\,A \;\middle|\; \Diamond^k\Box[\mathsf{hd}]\varphi\right\}\right)$$

Using §E.1, we derive

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}'' \vdash s : \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \;\middle|\; \bigcirc\Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\}}}{\mathcal{E}'' \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \;\middle|\; \Diamond^k\Box[\mathsf{hd}][\mathsf{box}]\Box[\mathsf{hd}]\varphi\right\}}}{\mathcal{E}'' \vdash g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\,A \;\middle|\; \Diamond^k\Box[\mathsf{hd}]\varphi\right\}}}{\mathcal{E}'' \vdash \mathsf{Cons}^{\mathsf{g}}\ \left((\mathsf{hd} \circ t)(\mathsf{hd}^{\mathsf{g}}\ s)\right)\ \left(g \circledast \mathsf{next}(t \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)\right) : \left\{\mathsf{Str}^{\mathsf{g}}\,A \;\middle|\; \bigcirc\Diamond^k\Box[\mathsf{hd}]\varphi\right\}}$$

$\Box$

E.5 Fair Streams

We discuss here an adaptation of the *fair streams* of [18,8]. We rely on the basic datatypes presented in §E.5. In §E.5 we discuss a function

$$\mathsf{fb} : \mathsf{CoNat} \longrightarrow \mathsf{CoNat} \longrightarrow \mathsf{Str}\,\mathsf{Bool}$$

such that, writing $\mathsf{0}$ for Z and $\mathsf{1}$ for $(\mathsf{S}\ \mathsf{Z})$ (see Ex. E.15), the *non-regular* stream $(\mathsf{fb}\ \mathsf{0}\ \mathsf{1})$, adapted from [18,8], is of the form

$$\mathsf{ff}\quad \mathsf{tt}\quad \mathsf{ff}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{ff}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{ff}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{tt}\quad \mathsf{ff}\quad \dots$$

This stream thus contains infinitely many tt's and infinitely many ff's. This is expressed with the formula $[\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}] \quad\wedge\quad [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]$ where $[\mathsf{tt}]$, $[\mathsf{ff}]$ represent the value of a Boolean, as in

$$\mathsf{tt} : \{\mathsf{Bool} \mid [\mathsf{tt}]\} \qquad\text{and}\qquad \mathsf{ff} : \{\mathsf{Bool} \mid [\mathsf{ff}]\}$$

Examples E.20 and E.22 show that we indeed have

$$(\mathsf{fb}\ \mathsf{0}\ \mathsf{1}) : \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}] \quad\wedge\quad [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}$$

The key are the following refinement typings for the *guarded* fb^{g}, discussed in Ex. E.19 and Ex. E.21:

$$\begin{aligned}
&\mathsf{fb}^{\mathsf{g}} : \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \quad\vee\quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])\}\\
&\mathsf{fb}^{\mathsf{g}} : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\} \to \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \to \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k}\Diamond^{k+\ell}[\mathsf{hd}][\mathsf{ff}]\right\}\right)
\end{aligned}$$

where, as in Not. E.10 (§E.3), we let

$$\Box^{\mathsf{t}}\varphi := \nu^{\mathsf{t}}\alpha.\varphi \wedge \bigcirc\alpha$$

Finally, in §E.5 we discuss a stream scheduler

$$\mathsf{sched} : \mathsf{Str}\,\mathsf{Bool} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \mathsf{Str}(A+B)$$

such that sched can be typed as follows (Ex. E.25):

$$\begin{array}{l} \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}]\} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \{\mathsf{Str}(A+B) \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_0]\top\} \\ \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \{\mathsf{Str}(A+B) \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_1]\top\} \end{array}$$

and thus

$$\mathsf{sched}\ (\mathsf{fb}\ 0\ 1) : \{\mathsf{Str}(A+B) \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_0]\top \quad\wedge\quad [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_1]\top\}$$

Basic Datatypes

Example E.13 (Booleans). Let

$$\mathsf{Bool} := \mathbf{1} + \mathbf{1}$$

with constructors

$$\begin{array}{l} \mathsf{tt} := \mathsf{in}_0(\langle\rangle) : \mathsf{Bool} \\ \mathsf{ff}\ := \mathsf{in}_1(\langle\rangle) : \mathsf{Bool} \end{array}$$

Example E.14 (Formulae on Booleans).

$$\begin{array}{l} [\mathsf{tt}] := [\mathsf{in}_0]\top : \mathsf{Bool} \\ [\mathsf{ff}] := [\mathsf{in}_1]\top : \mathsf{Bool} \end{array}$$

Example E.15 (CoNatural Numbers). Let

$$\begin{array}{ll} \mathsf{CoNat} & := \blacksquare\,\mathsf{CoNat}^{\mathsf{g}} \\ \mathsf{CoNat}^{\mathsf{g}} & := \mathsf{Fix}(X).\mathbf{1} + \blacktriangleright X \end{array}$$

with constructors

$$\begin{array}{llll} \mathsf{Z} := \mathsf{box}_\iota(\mathsf{Z}^{\mathsf{g}}) & : \mathsf{CoNat} & \mathsf{S} := \lambda n.\mathsf{box}_\iota(\mathsf{S}^{\mathsf{g}}\ (\mathsf{unbox}\ n)) & : \mathsf{CoNat} \to \mathsf{CoNat} \\ \mathsf{Z}^{\mathsf{g}} := \mathsf{fold}(\mathsf{in}_0\langle\rangle) & : \mathsf{CoNat}^{\mathsf{g}} & \mathsf{S}^{\mathsf{g}} := \lambda n.\mathsf{fold}(\mathsf{in}_1\ n) & : \blacktriangleright \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \end{array}$$

Example E.16 (Formulae on CoNatural Numbers).

$$\begin{array}{lll} [\mathsf{Z}] & := [\mathsf{fold}][\mathsf{in}_0] & : \mathsf{CoNat}^{\mathsf{g}} \\ [\mathsf{S}] & := [\mathsf{fold}][\mathsf{in}_1] & : \mathsf{CoNat}^{\mathsf{g}} \\ \bigcirc\varphi & := [\mathsf{fold}][\mathsf{in}_1][\mathsf{next}]\varphi & : \mathsf{CoNat}^{\mathsf{g}} \\ \Diamond\varphi & := \mu\alpha.\ \varphi \vee \bigcirc\alpha & : \mathsf{CoNat}^{\mathsf{g}} \\ \Diamond^{\mathsf{t}}\varphi & := \mu^{\mathsf{t}}\alpha.\ \varphi \vee \bigcirc\alpha & : \mathsf{CoNat}^{\mathsf{g}} \end{array}$$

where $\varphi : \mathsf{CoNat}^{\mathsf{g}}$.

A Fair Stream of Booleans

Example E.17.

$$\begin{array}{rl} \mathsf{fb} & : \ \mathsf{CoNat} \longrightarrow \mathsf{CoNat} \longrightarrow \mathsf{Str}\,\mathsf{Bool} \\ & := \lambda c.\lambda m.\ \mathsf{box}_\iota(\mathsf{fb}^{\mathsf{g}}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) \\ \\ \mathsf{fb}^{\mathsf{g}} & : \ \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \\ & := \mathsf{fix}(g).\lambda c.\lambda m.\ \mathsf{case}\ c\ \mathsf{of} \\ & \quad \mid \mathsf{Z}^{\mathsf{g}} \ \mapsto\ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m)) \\ & \quad \mid \mathsf{S}^{\mathsf{g}} n \ \mapsto\ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) \end{array}$$

Example E.18.

$$\begin{array}{l} \mathsf{fb} \ : \{\mathsf{CoNat} \mid [\mathsf{box}]\Diamond[\mathsf{Z}]\} \longrightarrow \mathsf{CoNat} \longrightarrow \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Diamond[\mathsf{hd}][\mathsf{ff}]\} \\ \mathsf{fb}^{\mathsf{g}} : \forall k \cdot \left(\left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^k[\mathsf{Z}]\right\} \longrightarrow \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^k[\mathsf{hd}][\mathsf{ff}]\right\}\right) \end{array}$$

Proof. Let

$$T(k) := \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^k[\mathsf{Z}]\right\} \longrightarrow \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^k[\mathsf{hd}][\mathsf{ff}]\right\}$$

and assume

$$g : \blacktriangleright\forall k \cdot T(k)$$

Let

$$\begin{array}{rl} M(g,c,m) := & \mathsf{case}\ c\ \mathsf{of} \\ & \mid \mathsf{Z}^{\mathsf{g}} \ \mapsto\ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m)) \\ & \mid \mathsf{S}^{\mathsf{g}}\ n \ \mapsto\ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) \end{array}$$

We show

$$\lambda c.\lambda m.M(g,c,m) : \forall k \cdot T(k)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $T(0)$. We get the result from the (ExF) rule since

$$\Diamond^0[\mathsf{Z}] \Leftrightarrow \bot$$

Case of $T(k{+}1)$. We show

$$M(g,c,m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^{k+1}[\mathsf{hd}][\mathsf{ff}]\right\}$$

assuming

$$\begin{array}{l} c \ : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{k+1}[\mathsf{Z}]\right\} \\ m : \mathsf{CoNat}^{\mathsf{g}} \end{array}$$

Using

$$\Diamond^{k+1}[\mathsf{Z}] \Leftrightarrow [\mathsf{Z}] \vee \bigcirc\Diamond^k[\mathsf{Z}]$$

we reason by cases on the refinement type of c. This leads to two subcases.

(Sub)Case of $[\mathsf{Z}]$**.** We apply the ($\textsc{Inj}_0$-E) rule on the refinement type of ($\mathsf{unfold}\ c$). Since

$$[\mathsf{hd}][\mathsf{ff}] \Rightarrow \Diamond^{k+1}[\mathsf{hd}][\mathsf{ff}]$$

the result follows from the fact that

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{ff}]\}$$

(Sub)Case of $\bigcirc\Diamond^k[\mathsf{Z}]$**.** We have

$$\mathsf{unfold}\ c : \left\{\mathbf{1} + \blacktriangleright \mathsf{CoNat}^{\mathsf{g}} \;\middle|\; [\mathsf{in}_1][\mathsf{next}]\Diamond^k[\mathsf{Z}]\right\}$$

By applying the ($\textsc{Inj}_1$-E) rule on the refinement type of ($\mathsf{unfold}\ c$), we are left with showing

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^{k+1}[\mathsf{hd}][\mathsf{ff}]\right\}$$

assuming

$$n : \blacktriangleright \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^k[\mathsf{Z}]\right\}$$

Using

$$\bigcirc\Diamond^k[\mathsf{hd}][\mathsf{ff}] \Rightarrow \Diamond^{k+1}[\mathsf{hd}][\mathsf{ff}]$$

we are done since

$$g \circledast n \circledast (\mathsf{next}\ m) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^k[\mathsf{hd}][\mathsf{ff}]\right\}$$

$\square$

Example E.19. Consider a function

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

such that

- $1 \leq f(k+1, \ell+1)$
- $f(k, \ell+2) \leq f(k+1, \ell+1)$
- $\ell + 1 \leq f(k+1, \ell+1)$
- $f(k, \ell+1) \leq f(k+1, \ell+1)$

for instance $f(k,\ell) = k + \ell$. Then we can give the following refined type to fb^{g}:

$$\forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\} \longrightarrow \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]\right\}\right)$$

Proof. Let

$$\begin{aligned}
U(k,\ell) &:= \{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \varphi(k,\ell) \wedge \psi(\ell)\} \\
\varphi(k,\ell) &:= \Diamond^{\ell}[\mathsf{Z}] \Vdash\!\!\!\rightarrow \Diamond^{\ell+1}[\mathsf{Z}] \Vdash\!\!\!\rightarrow \Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}] \\
\psi(\ell) &:= \Diamond^{\ell}[\mathsf{Z}] \Vdash\!\!\!\rightarrow \top \Vdash\!\!\!\rightarrow \Diamond^{\ell}[\mathsf{hd}][\mathsf{ff}]
\end{aligned}$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot U(k)$$

Let

$$\begin{array}{rl} M(g,c,m) := & \mathsf{case}\ c\ \mathsf{of} \\ & \mid \mathsf{Z}^{\mathsf{g}} \ \mapsto\ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m)) \\ & \mid \mathsf{S}^{\mathsf{g}} n \ \mapsto\ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) \end{array}$$

We show

$$\lambda c.\lambda m.M(g,c,m) : \forall k \cdot \forall \ell \cdot U(k)$$

First, proceeding similarly as in Ex. E.18,

$$\lambda c.\lambda m.M(g,c,m) : \forall \ell \cdot \left\{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}] \Vdash\!\!\to \top \Vdash\!\!\to \Diamond^{\ell}[\mathsf{hd}][\mathsf{ff}]\right\}$$

Let

$$T(k,\ell) := \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\} \longrightarrow \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k}\Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

We show

$$\lambda c.\lambda m.M(g,c,m) : \forall k \cdot \forall \ell \cdot T(k)$$

We apply the ($\forall$-CI) rule on $\forall k$. In the case of $\forall \ell \cdot T(0,\ell)$, the result is trivial since

$$\Box^{0}\Diamond^{\mathtt{f}(0,\ell)}[\mathsf{hd}][\mathsf{ff}] \Leftrightarrow \top$$

In the case of $\forall \ell \cdot T(k+1,\ell)$, we apply the ($\forall$-CI) rule, this time on $\forall \ell$. The case of $T(k+1,0)$ is dealt-with using the (ExF) rule since

$$\Diamond^{0}[\mathsf{Z}] \Leftrightarrow \bot$$

In the case of $T(k+1,\ell+1)$, we show

$$M(g,c,m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k+1}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

assuming

$$\begin{array}{rl} c & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \\ m & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+2}[\mathsf{Z}]\right\} \end{array}$$

We apply the typing rule for case (Fig. 4). This leads to two branches, one for $(\mathsf{unfold}\ c) = \mathsf{fold}(\mathsf{in}_0\langle\rangle)$ (denoted Z^{g}), and one for $(\mathsf{unfold}\ c) = \mathsf{fold}(\mathsf{in}_1\ n)$ (denoted $\mathsf{S}^{\mathsf{g}} n$).

Case of Z^{g}.

We have to show

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k+1}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

We have

$$\Box^{k+1}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}] \Leftrightarrow \Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}] \quad \wedge \quad \bigcirc\,\Box^{k}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$$

and we consider each conjunct separately.

(Sub)Case of $\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$.
We have

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{ff}]\}$$

and as $f(k+1, \ell+1) \geq 1$ we are done with

$$[\mathsf{hd}][\mathsf{ff}] \Rightarrow \Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$$

(Sub)Case of $\bigcirc\Box^k\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$.
Since

$$\begin{array}{ll} m & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+2}[\mathsf{Z}]\right\} \\ \mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m) & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+3}[\mathsf{Z}]\right\} \end{array}$$

we have

$$g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k\Diamond^{\mathtt{f}(k,\ell+2)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

so that

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \bigcirc\Box^k\Diamond^{\mathtt{f}(k,\ell+2)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

But since $f(k, \ell+2) \leq f(k+1, \ell+1)$, we have

$$\Diamond^{\mathtt{f}(k,\ell+2)}[\mathsf{hd}][\mathsf{ff}] \Rightarrow \Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$$

and we obtain

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \bigcirc\Box^k\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

Case of $\mathsf{S}^{\mathsf{g}}n$.
We have to show

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k+1}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

assuming

$$n : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\}$$

We have

$$\Box^{k+1}\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}] \Leftrightarrow \Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}] \quad \wedge \quad \bigcirc\,\Box^k\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$$

and we consider each conjunct separately.
(Sub)Case of $\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$.
Using

$$g : \blacktriangleright \left\{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}] \mathrel{\|\!\!\to} \top \mathrel{\|\!\!\to} \Diamond^{\ell}[\mathsf{hd}][\mathsf{ff}]\right\}$$

we get

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Diamond^{\ell+1}[\mathsf{hd}][\mathsf{ff}]\right\}$$

and the result follows from the fact that

$$\ell + 1 \leq f(k+1, \ell+1)$$

(Sub)Case of $\bigcirc\Box^k\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$.
Since $\ell \leq \ell+1$, we have

$$n : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\}$$

and thus

$$g \circledast n \circledast (\mathsf{next}\ m) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k\Diamond^{\mathtt{f}(k,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

so that

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \bigcirc\Box^k\Diamond^{\mathtt{f}(k,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

But since $f(k, \ell+1) \leq f(k+1, \ell+1)$ we have

$$\Diamond^{\mathtt{f}(k,\ell+1)}[\mathsf{hd}][\mathsf{ff}] \Rightarrow \Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]$$

and we obtain

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \bigcirc\Box^k\Diamond^{\mathtt{f}(k+1,\ell+1)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

□

Example E.20. We have

$$\mathsf{fb}\ \mathsf{Z}\ (\mathsf{S}\ \mathsf{Z}) : \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}$$

Proof. Recall that

$$\begin{array}{rl} \mathsf{fb} : & \mathsf{CoNat} \longrightarrow \mathsf{CoNat} \longrightarrow \mathsf{Str}\,\mathsf{Bool} \\ := & \lambda c.\lambda m.\ \mathsf{box}_\iota(\mathsf{fb}^{\mathsf{g}}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) \end{array}$$

We show

$$\mathsf{fb} : \forall\ell \cdot \left(\left\{\mathsf{CoNat} \;\middle|\; [\mathsf{box}]\Diamond^{\ell}[\mathsf{Z}]\right\} \longrightarrow \left\{\mathsf{CoNat} \;\middle|\; [\mathsf{box}]\Diamond^{\ell+1}[\mathsf{Z}]\right\} \longrightarrow \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}\right)$$

We apply the ($\forall$-I) rule. Assume

$$\begin{array}{rl} c & : \left\{\mathsf{CoNat} \;\middle|\; [\mathsf{box}]\Diamond^{\ell}[\mathsf{Z}]\right\} \\ m & : \left\{\mathsf{CoNat} \;\middle|\; [\mathsf{box}]\Diamond^{\ell+1}[\mathsf{Z}]\right\} \end{array}$$

Since the formulae $\Diamond^{\ell}[\mathsf{Z}]$ and $\Diamond^{\ell+1}[\mathsf{Z}]$ are safe we have

$$\begin{array}{rl} c & : \blacksquare\left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\} \\ m & : \blacksquare\left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \end{array}$$

and thus

$$\begin{array}{rl} (\mathsf{unbox}\ c) & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell}[\mathsf{Z}]\right\} \\ (\mathsf{unbox}\ m) & : \left\{\mathsf{CoNat}^{\mathsf{g}} \;\middle|\; \Diamond^{\ell+1}[\mathsf{Z}]\right\} \end{array}$$

Now, it follows from Ex. E.19 that

$$\mathsf{fb^g}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m) : \left\{\mathsf{Str^g\,Bool}\ \middle|\ \Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

so that

$$\mathsf{box}_\iota(\mathsf{fb^g}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) : \blacksquare \left\{\mathsf{Str^g\,Bool}\ \middle|\ \Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

Since the formula $\Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]$ is safe we have

$$\mathsf{box}_\iota(\mathsf{fb^g}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) : \left\{\mathsf{Str\,Bool}\ \middle|\ [\mathsf{box}]\Box^k \Diamond^{\mathtt{f}(k,\ell)}[\mathsf{hd}][\mathsf{ff}]\right\}$$

The (μ-I) rule then gives

$$\mathsf{box}_\iota(\mathsf{fb^g}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) : \left\{\mathsf{Str\,Bool}\ \middle|\ [\mathsf{box}]\Box^k \Diamond[\mathsf{hd}][\mathsf{ff}]\right\}$$

and the (ν-I) rule gives

$$\mathsf{box}_\iota(\mathsf{fb^g}\ (\mathsf{unbox}\ c)\ (\mathsf{unbox}\ m)) : \{\mathsf{Str\,Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\}$$

The result then follows from the fact that

$$\begin{aligned} \mathsf{Z}\ \ &: \{\mathsf{CoNat} \mid [\mathsf{box}]\Diamond^1[\mathsf{Z}]\} \\ \mathsf{S}\ \mathsf{Z} &: \{\mathsf{CoNat} \mid [\mathsf{box}] \bigcirc \Diamond^1[\mathsf{Z}]\} \end{aligned}$$

□

Example E.21. We have

$$\mathsf{fb^g} : \mathsf{CoNat^g} \longrightarrow \{\mathsf{CoNat^g} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str^g\,Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])\}$$

Proof. Let

$$\begin{aligned} T &:= \{\mathsf{CoNat^g} \to \mathsf{CoNat^g} \to \mathsf{Str^g\,Bool} \mid \varphi \quad \wedge \quad \psi\} \\ \varphi &:= [\mathsf{S}] \Vdash\!\!\to \top \Vdash\!\!\to [\mathsf{hd}][\mathsf{tt}] \\ \psi &:= \top \Vdash\!\!\to [\mathsf{S}] \Vdash\!\!\to \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}]) \end{aligned}$$

and assume

$$g : \blacktriangleright T$$

Let

$$\begin{aligned} M(g, c, m) := {} & \mathsf{case}\ c\ \mathsf{of} \\ & \mid \mathsf{Z^g}\ \ \mapsto\ \ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S^g}\ (\mathsf{next}\ m)) \\ & \mid \mathsf{S^g} n\ \ \mapsto\ \ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) \end{aligned}$$

We show

$$\lambda c.\lambda m.M(g, c, m) : T$$

First, by using the (Inj$_1$-E) rule we easily get

$$\lambda c.\lambda m.M(g, c, m) : \{\mathsf{CoNat^g} \to \mathsf{CoNat^g} \to \mathsf{Str^g\,Bool} \mid [\mathsf{S}] \Vdash\!\!\to \top \Vdash\!\!\to [\mathsf{hd}][\mathsf{tt}]\}$$

It remains to show

$\lambda c.\lambda m.M(g,c,m) : \{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \top \Vdash\!\!\to [\mathsf{S}] \Vdash\!\!\to \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}$

Assume

$$\begin{array}{l} c\ \ : \mathsf{CoNat}^{\mathsf{g}} \\ m : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \end{array}$$

We apply the typing rule for case (Fig. 4). This leads to two branches, one for $(\mathsf{unfold}\ c) = \mathsf{fold}(\mathsf{in}_0\langle\rangle)$ (denoted Z^{g}), and one for $(\mathsf{unfold}\ c) = \mathsf{fold}(\mathsf{in}_1\ n)$ (denoted $\mathsf{S}^{\mathsf{g}}n$).

Case of Z^{g}.

We have to show

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}$$

We have

$$\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}]) \Leftrightarrow ([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}]) \quad \wedge \quad \bigcirc\,\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$$

and we consider each conjunct separately.

(Sub)Case of $([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$.

Since

$$\begin{array}{l} m : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \\ g\ \ : \blacktriangleright(\{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}]\}) \end{array}$$

we get

$$g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}]\}$$

and the result follows.

(Sub)Case of $\bigcirc\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$.

Since

$$\begin{array}{r} \mathsf{S}^{\mathsf{g}}(\mathsf{next}\ m) : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \\ g : \blacktriangleright(\mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}) \end{array}$$

we get

$$g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}$$

and the result follows.

Case of $\mathsf{S}^{\mathsf{g}}n$.

We have to show

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}$$

assuming

$$n : \mathsf{CoNat}^{\mathsf{g}}$$

We have

$$\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}]) \Leftrightarrow ([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}]) \quad \wedge \quad \bigcirc\,\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$$

and we consider each conjunct separately.

(Sub)Case of $([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$**.**
We have

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}]\}$$

(Sub)Case of $\bigcirc\Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])$**.**
Since

$$\begin{array}{r}m : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \\ g : \blacktriangleright(\mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\})\end{array}$$

we get

$$g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \blacktriangleright\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \vee \bigcirc[\mathsf{hd}][\mathsf{tt}])\}$$

and the result follows. □

Example E.22. We have

$$\mathsf{fb}\ \mathsf{Z}\ (\mathsf{S}\ \mathsf{Z}) : \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}]\}$$

Proof. By Ex. E.21 we have

$$\mathsf{fb}^{\mathsf{g}}\ (\mathsf{unbox}\ \mathsf{Z})\ (\mathsf{unbox}\ (\mathsf{S}\ \mathsf{Z})) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])\}$$

so that

$$\mathsf{fb}\ \mathsf{Z}\ (\mathsf{S}\ \mathsf{Z}) : \blacksquare\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \Box\,([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])\}$$

Since the formula $\Box\,([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])$ is safe we get

$$\mathsf{fb}\ \mathsf{Z}\ (\mathsf{S}\ \mathsf{Z}) : \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\,([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}])\}$$

Now, the result follows from the fact that

$$([\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}]) \Rightarrow \Diamond[\mathsf{hd}][\mathsf{tt}]$$

□

The following uses the rule

$$\frac{}{\vdash^{B\to A} ([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi) \Rightarrow [\mathsf{ev}(\psi_0 \vee \psi_1)]\varphi}$$

Example E.23. We have

$$\mathsf{fb}^{\mathsf{g}} : \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}]\}$$

Proof. Let T be the type

$$\{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{S}] \Vdash\!\!\to \top \Vdash\!\!\to [\mathsf{hd}][\mathsf{tt}] \quad \wedge \quad [\mathsf{Z}] \Vdash\!\!\to [\mathsf{S}] \Vdash\!\!\to \bigcirc[\mathsf{hd}][\mathsf{tt}]\}$$

Note that

$$T \leq \mathsf{CoNat}^{\mathsf{g}} \longrightarrow \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\,[\mathsf{hd}][\mathsf{tt}]\}$$

Assume

$$g : \blacktriangleright T$$

Let

$$\begin{array}{rl} M(g,c,m) := & \mathsf{case}\ c\ \mathsf{of} \\ & \mid \mathsf{Z}^{\mathsf{g}} \ \mapsto\ \mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}^{\mathsf{g}}\ (\mathsf{next}\ m)) \\ & \mid \mathsf{S}^{\mathsf{g}} n \ \mapsto\ \mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) \end{array}$$

We show

$$\lambda c.\lambda m.M(g,c,m) : T$$

We consider each conjunct separately.

Case of $[\mathsf{S}] \Vert\!\!\to \top \Vert\!\!\to [\mathsf{hd}][\mathsf{tt}]$**.**
Assume

$$c : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\}$$

Applying the ($\textsc{Inj}_1$-E) rule, we are done since

$$\mathsf{tt} ::^{\mathsf{g}} g \circledast n \circledast (\mathsf{next}\ m) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{hd}][\mathsf{tt}]\}$$

assuming

$$n : \mathsf{CoNat}^{\mathsf{g}}$$

Case of $[\mathsf{Z}] \Vert\!\!\to [\mathsf{S}] \Vert\!\!\to \bigcirc[\mathsf{hd}][\mathsf{tt}]$**.**
Assume

$$\begin{array}{l} c\ \ : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{Z}]\} \\ m : \{\mathsf{CoNat}^{\mathsf{g}} \mid [\mathsf{S}]\} \end{array}$$

Applying the ($\textsc{Inj}_0$-E) rule, we are left with showing

$$\mathsf{ff} ::^{\mathsf{g}} g \circledast (\mathsf{next}\ m) \circledast \mathsf{next}(\mathsf{S}\ (\mathsf{next}\ m)) : \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid \bigcirc[\mathsf{hd}][\mathsf{tt}]\}$$

But the result is trivial since

$$g : \blacktriangleright \{\mathsf{CoNat}^{\mathsf{g}} \to \mathsf{CoNat}^{\mathsf{g}} \to \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \mid [\mathsf{S}] \Vert\!\!\to \top \Vert\!\!\to [\mathsf{hd}]\mathsf{tt}\}$$

□

A Scheduler

Example E.24.

$$\begin{array}{rl} \mathsf{sched} & : \ \ \mathsf{Str}\,\mathsf{Bool} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \mathsf{Str}(A+B) \\ & := \lambda b.\lambda s.\lambda t.\ \mathsf{box}_\iota(\mathsf{sched}^{\mathsf{g}}\ (\mathsf{unbox}\ b)\ (\mathsf{unbox}\ s)\ (\mathsf{unbox}\ t)) \end{array}$$

$$\begin{array}{rl} \mathsf{sched}^{\mathsf{g}} & : \ \ \mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \longrightarrow \mathsf{Str}^{\mathsf{g}}\,B \longrightarrow \mathsf{Str}^{\mathsf{g}}(A+B) \\ & := \mathsf{fix}(g).\lambda b.\lambda s.\lambda t.\ \mathsf{case}\ (\mathsf{hd}^{\mathsf{g}}\ b)\ \mathsf{of} \\ & \quad \mid \mathsf{tt}\ \mapsto\ (\mathsf{in}_0\ (\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t) \\ & \quad \mid \mathsf{ff}\ \mapsto\ (\mathsf{in}_1\ (\mathsf{hd}^{\mathsf{g}}\ t)) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t) \end{array}$$

Example E.25. We can give the following refinement types to sched :

$$\begin{array}{l}\{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{tt}]\} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \{\mathsf{Str}(A+B) \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_0]\top\}\\ \{\mathsf{Str}\,\mathsf{Bool} \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{ff}]\} \longrightarrow \mathsf{Str}\,A \longrightarrow \mathsf{Str}\,B \longrightarrow \{\mathsf{Str}(A+B) \mid [\mathsf{box}]\Box\Diamond[\mathsf{hd}][\mathsf{in}_1]\top\}\end{array}$$

Proof. Direct, using the following Ex. E.26. □

Example E.26. We can give the following refinement types to $\mathsf{sched}^{\mathsf{g}}$:

$$\begin{array}{l}\forall k\cdot\forall\ell\cdot\left(\left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{tt}]\right\} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \longrightarrow \mathsf{Str}^{\mathsf{g}}\,B \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{in}_0]\top\right\}\right)\\ \forall k\cdot\forall\ell\cdot\left(\left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{ff}]\right\} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \longrightarrow \mathsf{Str}^{\mathsf{g}}\,B \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{in}_1]\top\right\}\right)\end{array}$$

Proof. We only discuss the first type, since the second one is completely similar. Let $T(k,\ell)$ be the type

$$\left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{tt}]\right\} \longrightarrow \mathsf{Str}^{\mathsf{g}}\,A \longrightarrow \mathsf{Str}^{\mathsf{g}}\,B \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Box^k\Diamond^\ell[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

and assume

$$g : \blacktriangleright\forall k\cdot\forall\ell\cdot T(k,\ell)$$

Let

$$\begin{array}{rl}M(g,b,s,t) := & \mathsf{case}\ (\mathsf{hd}^{\mathsf{g}}\ b)\ \mathsf{of}\\ & \mid \mathsf{tt}\ \mapsto\ (\mathsf{in}_0\ (\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t)\\ & \mid \mathsf{ff}\ \mapsto\ (\mathsf{in}_1\ (\mathsf{hd}^{\mathsf{g}}\ t)) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t)\end{array}$$

We show

$$\lambda b.\lambda s.\lambda t.M(g,b,s,t) : \forall k\cdot\forall\ell\cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. In the case of $\forall\ell\cdot T(\mathsf{0},\ell)$, the result is trivial since

$$\Box^{\mathsf{0}}\Diamond^\ell[\mathsf{hd}][\mathsf{in}_0]\top \Leftrightarrow \top$$

As for $\forall\ell\cdot T(k{+}\mathsf{1},\ell)$, we apply the ($\forall$-CI) rule, this time on $\forall\ell$. In the case of $T(k{+}\mathsf{1},\mathsf{0})$, since

$$\begin{array}{rl} & \Box^{k+\mathsf{1}}\Diamond^{\mathsf{0}}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow \Diamond^{\mathsf{0}}[\mathsf{hd}][\mathsf{tt}] \quad\wedge\quad \bigcirc\,\Box^k\Diamond^{\mathsf{0}}[\mathsf{hd}][\mathsf{tt}]\\ \text{and} & \Diamond^{\mathsf{0}}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow \bot\end{array}$$

we get

$$\Box^{k+\mathsf{1}}\Diamond^{\mathsf{0}}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow \bot$$

and we can conclude using the (ExF) rule. It remains to deal with the case of $T(k{+}\mathsf{1},\ell{+}\mathsf{1})$. We have to show

$$M(g,b,s,t) : \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Box^{k+\mathsf{1}}\Diamond^{\ell+\mathsf{1}}[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

assuming

$$\begin{array}{l}b : \left\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{Bool} \;\middle|\; \Box^{k+\mathsf{1}}\Diamond^{\ell+\mathsf{1}}[\mathsf{hd}][\mathsf{tt}]\right\}\\ s : \mathsf{Str}^{\mathsf{g}}\,A\\ t : \mathsf{Str}^{\mathsf{g}}\,B\end{array}$$

We have

$$\Box^{k+\mathsf{1}}\Diamond^{\ell+\mathsf{1}}[\mathsf{hd}][\mathsf{in}_0]\top \Leftrightarrow \Diamond^{\ell+\mathsf{1}}[\mathsf{hd}][\mathsf{in}_0]\top \quad\wedge\quad \bigcirc\,\Box^k\Diamond^{\ell+\mathsf{1}}[\mathsf{hd}][\mathsf{in}_0]\top$$

and we consider each conjunct separately.

Case of $\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top$.

Since

$$\Box^{k+1}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow \Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}] \quad \wedge \quad \bigcirc\, \Box^{k}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]$$

we have

$$b : \left\{\mathsf{Str}^{\mathsf{g}}\, \mathsf{Bool} \;\middle|\; \Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]\right\}$$

Using

$$\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow [\mathsf{hd}][\mathsf{tt}] \quad \vee \quad \bigcirc\, \Diamond^{\ell}[\mathsf{hd}][\mathsf{tt}]$$

we reason by cases on the refinement type of b.

(Sub)Case of $[\mathsf{hd}][\mathsf{tt}]$.

We apply the (Inj$_0$-E) rule on b and we are done since

$$(\mathsf{in}_0\ (\mathsf{hd}^{\mathsf{g}}\ s)) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t) : \{\mathsf{Str}^{\mathsf{g}}(A+B) \mid [\mathsf{hd}][\mathsf{in}_0]\top\}$$

(Sub)Case of $\bigcirc\Diamond^{\ell}[\mathsf{hd}][\mathsf{tt}]$.

We have

$$\mathsf{tl}^{\mathsf{g}}\ b : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, \mathsf{Bool} \;\middle|\; \Diamond^{\ell}[\mathsf{hd}][\mathsf{tt}]\right\}$$

We apply the case-elimination rule on b. In both branches, since (by subtyping) g has type

$$\blacktriangleright \left(\left\{\mathsf{Str}^{\mathsf{g}}\, \mathsf{Bool} \;\middle|\; \Box^{1}\Diamond^{\ell}[\mathsf{hd}][\mathsf{tt}]\right\} \longrightarrow \mathsf{Str}^{\mathsf{g}}\, A \longrightarrow \mathsf{Str}^{\mathsf{g}}\, B \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Box^{1}\Diamond^{\ell}[\mathsf{hd}][\mathsf{in}_0]\top\right\}\right)$$

and since, according to Table 2,

$$\Box^{1}\theta \Leftrightarrow \theta$$

we get

$$g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \Diamond^{\ell}[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

so that

$$(-) ::^{\mathsf{g}} g \circledast (\mathsf{tl}^{\mathsf{g}}\ b) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) \circledast (\mathsf{tl}^{\mathsf{g}}\ t) : \left\{\mathsf{Str}^{\mathsf{g}}(A+B) \;\middle|\; \bigcirc\Diamond^{\ell}[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

and we are done since

$$\bigcirc\Diamond^{\ell}[\mathsf{hd}][\mathsf{in}_0]\top \Rightarrow \Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top$$

Case of $\bigcirc\Box^{k}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top$.

Since

$$\Box^{k+1}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}] \Leftrightarrow \Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}] \quad \wedge \quad \bigcirc\, \Box^{k}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]$$

we have

$$b : \left\{\mathsf{Str}^{\mathsf{g}}\, \mathsf{Bool} \;\middle|\; \bigcirc\Box^{k}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]\right\}$$

so that

$$\mathsf{tl}^{\mathsf{g}}\ b : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\, \mathsf{Bool} \;\middle|\; \Box^{k}\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]\right\}$$

We apply the case-elimination rule on b. In both branches, since (by subtyping) g has type

$$\blacktriangleright \left(\left\{\mathsf{Str^g\,Bool} \;\middle|\; \Box^k\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{tt}]\right\} \longrightarrow \mathsf{Str^g}\,A \longrightarrow \mathsf{Str^g}\,B \longrightarrow \left\{\mathsf{Str^g}(A+B) \;\middle|\; \Box^k\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top\right\}\right)$$

we get

$$g \circledast (\mathsf{tl^g}\ b) \circledast (\mathsf{tl^g}\ s) \circledast (\mathsf{tl^g}\ t) : \blacktriangleright \left\{\mathsf{Str^g}(A+B) \;\middle|\; \Box^k\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

so that

$$(-) ::^{\mathsf{g}} g \circledast (\mathsf{tl^g}\ b) \circledast (\mathsf{tl^g}\ s) \circledast (\mathsf{tl^g}\ t) : \left\{\mathsf{Str^g}(A+B) \;\middle|\; \bigcirc\Box^k\Diamond^{\ell+1}[\mathsf{hd}][\mathsf{in}_0]\top\right\}$$

□

E.6 Colists

We detail here the refinement types given to the guarded and coinductive append functions on colists in Table 4. We present some basic material in §E.6. The append function itself is detailed in §E.6, and we give sharper refinements with iteration terms in §E.6. We begin in §E.6 with an overview of the main examples on colists.

Overview The cases of

$$\begin{array}{l}\mathsf{append^g} : \{\mathsf{CoList^g}\,A \mid [\neg\mathsf{nil}]\} \longrightarrow \mathsf{CoList^g}\,A \longrightarrow \{\mathsf{CoList^g}\,A \mid [\neg\mathsf{nil}]\}\\ \mathsf{append^g} : \mathsf{CoList^g}\,A \longrightarrow \{\mathsf{CoList^g}\,A \mid [\neg\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList^g}\,A \mid [\neg\mathsf{nil}]\}\end{array}$$

are detailed in Ex. E.33.

We now discuss

$$\mathsf{append} : \{\mathsf{CoList}\,A \mid [\mathsf{box}][\mathrm{fin}]\} \longrightarrow \{\mathsf{CoList}\,A \mid [\mathsf{box}][\mathrm{fin}]\} \longrightarrow \{\mathsf{CoList}\,A \mid [\mathsf{box}][\mathrm{fin}]\}$$

which says that append takes finite colists to a finite colist. Recall that $[\mathrm{fin}] = \Diamond[\mathsf{nil}]$. Details are given in Ex. E.35. The other refinement types for append are detailed in Ex. E.36 and Ex. E.37.

We refer here to the code of the append function as defined in Table 3 and Ex. E.32. First, since $\Diamond[\mathsf{nil}]$ is smooth, we can apply the rule (μ-E) (Fig. 11) twice and reduce to

$$\mathcal{E} \vdash \mathsf{box}_\iota(\mathsf{append^g}\ (\mathsf{unbox}\ s)\ (\mathsf{unbox}\ t)) : \{\mathsf{CoList}\,A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\}$$

where $\mathcal{E}$ assumes s of type $\left\{\mathsf{CoList}\,A \;\middle|\; [\mathsf{box}]\Diamond^k[\mathsf{nil}]\right\}$ and t of type $\left\{\mathsf{CoList}\,A \;\middle|\; [\mathsf{box}]\Diamond^\ell[\mathsf{nil}]\right\}$. Using the derived rule (μ-I) (Ex. 6.10), we further reduce to

$$\mathcal{E} \vdash \mathsf{box}_\iota(\mathsf{append^g}\ (\mathsf{unbox}\ s)\ (\mathsf{unbox}\ t)) : \left\{\mathsf{CoList}\,A \;\middle|\; [\mathsf{box}]\Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

Now, since the formulae $\Diamond^{\mathsf{t}}[\mathsf{nil}]$ are safe, by subtyping (Fig. 11) we have

$$\mathcal{E} \vdash s : \blacksquare\left\{\mathsf{CoList}\,A \;\middle|\; \Diamond^k[\mathsf{nil}]\right\} \qquad \text{and} \qquad \mathcal{E} \vdash t : \blacksquare\left\{\mathsf{CoList}\,A \;\middle|\; \Diamond^\ell[\mathsf{nil}]\right\}$$

and we can reduce to showing that the *guarded* $\mathsf{append}^{\mathsf{g}}$ has type $\forall k \cdot \forall \ell \cdot T(k, \ell)$, where

$$T(k,\ell) := \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

Let $N(g,s,t)$ be such that $\mathsf{append}^{\mathsf{g}} = \mathsf{fix}(g).\lambda s.\lambda t.N(g,s,t)$. We show

$$\lambda s.\lambda t.N(g,s,t) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

in a typing context (leaved implicit) which assumes g of type $\blacktriangleright\forall k \cdot \forall \ell \cdot T(k,\ell)$. We apply the ($\forall$-CI) rule on $\forall k \cdot \forall \ell \cdot T(k,\ell)$. Since $\Diamond^{\mathsf{0}}[\mathsf{nil}] \Leftrightarrow \bot$, the branch of $\forall \ell \cdot T(\mathsf{0},\ell)$ can be dealt with using the (ExF) rule. In the branch of $\forall \ell \cdot T(k{+}\mathsf{1},\ell)$, we apply the ($\forall$-I) rule. We are thus left with showing

$$N(g,s,t) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell+\mathsf{1}}[\mathsf{nil}]\right\}$$

assuming further $s : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\mathsf{1}}[\mathsf{nil}]\right\}$ and $t : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\}$. We unfold $\Diamond^{k+\mathsf{1}}[\mathsf{nil}]$ as

$$\Diamond^{k+\mathsf{1}}[\mathsf{nil}] \Leftrightarrow [\mathsf{nil}] \quad \vee \quad \bigcirc\, \Diamond^{k}[\mathsf{nil}]$$

Using the ($\vee$-E) rule, we have two cases for the refinement type of s. In the case of $\{\mathsf{CoList}\, A \mid [\mathsf{nil}]\}$, since $[\mathsf{nil}] = [\mathsf{fold}][\mathsf{in}_0]\top$, we have $(\mathsf{unfold}\ s) : [\mathsf{in}_0]\top$. Thanks to the ($\textsc{Inj}_0$) rule, we are left with showing

$$t : \left\{\mathsf{CoList}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\} \vdash t : \left\{\mathsf{CoList}\, A \;\middle|\; \Diamond^{k+\mathsf{1}+\ell}[\mathsf{nil}]\right\}$$

But we are done since $[\![\ell]\!] \leq [\![k{+}\ell{+}\mathsf{1}]\!]$ so that

$$\Diamond^{\ell}[\mathsf{nil}] \Rightarrow \Diamond^{k+\mathsf{1}+\ell}[\mathsf{nil}]$$

Assume now that s has type $\left\{\mathsf{CoList}\, A \;\middle|\; \bigcirc\Diamond^{k}[\mathsf{nil}]\right\}$. By unfolding $\Diamond^{k+\ell+\mathsf{1}}[\mathsf{nil}]$ we reduce to showing

$$N(g,s,t) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

Since, on colists, $\bigcirc(-) = [\mathsf{fold}][\mathsf{in}_1][\pi_1][\mathsf{next}](-)$, we can apply the ($\textsc{Inj}_1$-E) rule on $(\mathsf{unfold}\ s)$. This amounts to showing

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{\mathsf{CoList}\, A \;\middle|\; \bigcirc\Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

where, since

$$(\mathsf{unfold}\ s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

we can assume $xs : \blacktriangleright\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\}$. By subtyping and ($\forall$-E) we have $g : \blacktriangleright T(k,\ell)$, so that

$$g \circledast xs \circledast (\mathsf{next}\ t) : \blacktriangleright\left\{\mathsf{CoList}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

and we conclude by the analogue of Ex. 5.3 for colists. The other typings for append are dealt with similarly. Let us finally just mention that the type of $\mathsf{append}^{\mathsf{g}}$ can be sharpened to

$$\forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+\mathsf{1}}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}\right)$$

reflecting that on finite colists, $\mathsf{append}^{\mathsf{g}}$ *removes* one constructor $\mathsf{Nil}^{\mathsf{g}}$ from its arguments (see Ex. E.38).

The Type of CoLists The type of colists is

$$\begin{aligned}\mathsf{CoList}\,A &:= \blacksquare\,\mathsf{CoList}^{\mathsf{g}}\,A\\ \mathsf{CoList}^{\mathsf{g}}\,A &:= \mathsf{Fix}(X).\mathbf{1} + A \times \blacktriangleright X\end{aligned}$$

Its usual guarded constructors are represented as

$$\begin{aligned}\mathsf{Nil}^{\mathsf{g}} &:= \mathsf{fold}(\mathsf{in}_0\langle\rangle) &&: \mathsf{CoList}^{\mathsf{g}}\,A\\ \mathsf{Cons}^{\mathsf{g}} &:= \lambda x.\lambda xs.\mathsf{fold}(\mathsf{in}_1\langle x, xs\rangle) &&: A \to \blacktriangleright\,\mathsf{CoList}^{\mathsf{g}}\,A \to \mathsf{CoList}^{\mathsf{g}}\,A\end{aligned}$$

Their coinductive (for A a constant type) variants are

$$\begin{aligned}\mathsf{Nil} &:= \mathsf{box}_\iota(\mathsf{Nil}^{\mathsf{g}}) &&: \mathsf{CoList}\,A\\ \mathsf{Cons} &:= \lambda x.\lambda xs.\mathsf{box}_\iota(\mathsf{Cons}^{\mathsf{g}}\ x\ (\mathsf{next}\ (\mathsf{unbox}\ xs))) &&: A \to \mathsf{CoList}\,A \to \mathsf{CoList}\,A\end{aligned}$$

Note E.27. Extending the notation for (guarded) streams, we often write

$$\begin{array}{lll}(x ::^{\mathsf{g}} xs) := \mathsf{Cons}^{\mathsf{g}}\ x\ xs & []^{\mathsf{g}} := \mathsf{Nil}^{\mathsf{g}} & [x_0, x_1, \dots, x_n]^{\mathsf{g}} := x_0 ::^{\mathsf{g}} [x_1, \dots, x_n]^{\mathsf{g}}\\ (x :: xs) := \mathsf{Cons}\ x\ xs & [] := \mathsf{Nil} & [x_0, x_1, \dots, x_n] := x_0 :: [x_1, \dots, x_n]\end{array}$$

Note E.28 (Syntactic Sugar for Pattern Matching). Assuming $s : \mathsf{CoList}^{\mathsf{g}}\,A$, we often write

$$\begin{array}{l}\mathsf{case}\ s\ \mathsf{of}\\ \mid \mathsf{Nil}^{\mathsf{g}}\ \mapsto\ N\\ \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs\ \mapsto\ M\end{array}$$

for

$$\begin{array}{l}\mathsf{case}\ (\mathsf{unfold}\ s)\ \mathsf{of}\\ \mid y.\ N[\langle\rangle/y]\\ \mid y.\ M[\pi_0(y)/x\,,\ \pi_1(y)/xs]\end{array}$$

Example E.29 (Formulae over $\mathsf{CoList}^{\mathsf{g}}$). Assuming $\psi : A$ and $\varphi : \mathsf{CoList}^{\mathsf{g}}\,A$,

$$\begin{array}{lll}[\mathsf{nil}] & := [\mathsf{fold}][\mathsf{in}_0]\top & : \mathsf{CoList}^{\mathsf{g}}\,A\\ [\neg\mathsf{nil}] & := [\mathsf{fold}][\mathsf{in}_1]\top & : \mathsf{CoList}^{\mathsf{g}}\,A\\ [\mathsf{hd}]\psi & := [\mathsf{fold}][\mathsf{in}_1][\pi_0]\varphi & : \mathsf{CoList}^{\mathsf{g}}\,A\\ \bigcirc\varphi & := [\mathsf{fold}][\mathsf{in}_1][\pi_1][\mathsf{next}]\varphi & : \mathsf{CoList}^{\mathsf{g}}\,A\\ \Diamond\varphi & := \mu\alpha.\ \varphi \vee \bigcirc\alpha & : \mathsf{CoList}^{\mathsf{g}}\,A\\ \Diamond^{\mathsf{t}}\varphi & := \mu^{\mathsf{t}}\alpha.\ \varphi \vee \bigcirc\alpha & : \mathsf{CoList}^{\mathsf{g}}\,A\\ \Box\varphi & := \nu\alpha.\ \varphi \wedge \bigcirc\alpha & : \mathsf{CoList}^{\mathsf{g}}\,A\\ \Box^{\mathrm{fin}}\varphi & := \nu\alpha.\ [\mathsf{nil}] \vee (\varphi \wedge \bigcirc\alpha) & : \mathsf{CoList}^{\mathsf{g}}\,A\\ [\mathsf{inf}] & := \Box[\neg\mathsf{nil}] & : \mathsf{CoList}^{\mathsf{g}}\,A\\ [\mathsf{fin}] & := \Diamond[\mathsf{nil}] & : \mathsf{CoList}^{\mathsf{g}}\,A\end{array}$$

Example E.30.

$$\begin{aligned}\mathsf{Cons}^{\mathsf{g}} &: A \longrightarrow \blacktriangleright\,\mathsf{CoList}^{\mathsf{g}}\,A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\neg\mathsf{nil}]\}\\ \mathsf{Cons}^{\mathsf{g}} &: A \longrightarrow \blacktriangleright\,\{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\mathsf{inf}]\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\mathsf{inf}]\}\\ \mathsf{Nil}^{\mathsf{g}} &: \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\mathsf{nil}]\}\end{aligned}$$

Note that

$$\vdash^{\mathsf{CoList}^{\mathsf{g}}\, A} [\mathsf{nil}] \Rightarrow \Box^{\mathrm{fin}}\varphi$$

Example E.31. Similarly as in §E.1 and §E.1, assuming $\varphi : A$ we have

$$\begin{array}{rl}
\mathsf{Cons}^{\mathsf{g}} & : \{A \mid \varphi\} \longrightarrow \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \\
\mathsf{Cons}^{\mathsf{g}} & : \{A \mid \varphi\} \longrightarrow \blacktriangleright \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{nil}]\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \\
\mathsf{Nil}^{\mathsf{g}} & : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}
\end{array}$$

$$\mathsf{Cons}^{\mathsf{g}} : \{A \mid \varphi\} \longrightarrow \blacktriangleright \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

The Append Function on Colists

Example E.32 (The Append Function on Colists).

$$\begin{array}{rcl}
\mathsf{append}^{\mathsf{g}} & : & \mathsf{CoList}^{\mathsf{g}}\, A \to \mathsf{CoList}^{\mathsf{g}}\, A \to \mathsf{CoList}^{\mathsf{g}}\, A \\
& := & \mathsf{fix}(g).\lambda s.\lambda t.\mathsf{case}\ s\ \mathsf{of} \\
& & \mid \mathsf{Nil}^{\mathsf{g}} \ \mapsto\ t \\
& & \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs \ \mapsto\ \mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) \\[1em]
\mathsf{append} & : & \mathsf{CoList}\, A \to \mathsf{CoList}\, A \to \mathsf{CoList}\, A \\
& := & \lambda s.\lambda t.\mathsf{box}_\iota(\mathsf{append}^{\mathsf{g}}\ (\mathsf{unbox}\ s)\ (\mathsf{unbox}\ t))
\end{array}$$

Example E.33 (Properties of Append).

$$\begin{array}{l}
\mathsf{append}^{\mathsf{g}} : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\} \longrightarrow \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\} \\
\mathsf{append}^{\mathsf{g}} : \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\neg\mathsf{nil}]\}
\end{array}$$

Example E.34. Assuming $\varphi : A$,

$$\mathsf{append}^{\mathsf{g}} : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

Proof. Let

$$T := \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

and assume

$$\begin{array}{rl}
g & : \blacktriangleright T \\
s & : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \\
t & : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}
\end{array}$$

Note that

$$\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi \Leftrightarrow [\mathsf{nil}] \vee \left([\mathsf{hd}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right)$$

We reason by cases on the refinement type of s, applying the ($\vee$-E) rule (Fig. 8).

Case of $[\mathsf{nil}]$**.**
We thus have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_0]\top\}$$

We apply the (Inj$_0$-E) rule and get the result by

$$t : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

Case of $[\mathsf{hd}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi$**.**
We thus have

$$s : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{hd}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

Since the modalities $[\mathsf{fold}]$ and $[\mathsf{in}_1]$ preserve $\wedge$ this gives

$$s : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{fold}][\mathsf{in}_1]\left([\pi_0]\varphi \wedge [\pi_1][\mathsf{next}]\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right)\right\}$$

so that

$$\mathsf{unfold}(s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1]\left([\pi_0]\varphi \wedge [\pi_1][\mathsf{next}]\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right)\right\}$$

We then apply the (Inj$_1$-E) rule. Assume

$$y : \left\{A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_0]\varphi \wedge [\pi_1][\mathsf{next}]\Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

and let

$$\begin{array}{lcl} x & := & \pi_0(y) : \{A \mid \varphi\} \\ xs & := & \pi_1(y) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\} \end{array}$$

Then Ex. E.31 easily gives

$$\mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\varphi\right\}$$

□

Example E.35.

$$\begin{array}{ll} \mathsf{append} & : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \\ \mathsf{append}^{\mathsf{g}} & : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}\right) \end{array}$$

Proof. Let

$$T(k,\ell) := \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}\right)$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot T(k,\ell)$$

Let

$$\begin{array}{lll} M(g,s,t) := & \mathsf{case}\; s\; \mathsf{of} & \\ & \mid \mathsf{Nil}^{\mathsf{g}} & \mapsto\; t \\ & \mid \mathsf{Cons}^{\mathsf{g}}\; x\; xs & \mapsto\; \mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) \end{array}$$

We show

$$\lambda s.\lambda t.M(g,s,t) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $\forall \ell \cdot T(0, \ell)$.

Apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$s : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{nil}]\}$$

Since

$$\Diamond^{0}[\mathsf{nil}] \Leftrightarrow \bot$$

the result follows using the rule (ExF).

Case of $\forall \ell \cdot T(k{+}1, \ell)$.

Apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$\begin{array}{l} s : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{nil}]\right\} \\ t : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{nil}]\right\} \end{array}$$

We have to show

$$M(g, s, t) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1+\ell}[\mathsf{nil}]\right\}$$

Using

$$\Diamond^{k+1}[\mathsf{nil}] \Leftrightarrow [\mathsf{nil}] \vee \bigcirc \Diamond^{k}[\mathsf{nil}]$$

we apply the ($\vee$-E) rule on the refinement type of s. This leads to two subcases.

(Sub)Case of $[\mathsf{nil}]$.

We have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_0]\top\}$$

Since $[\![\ell]\!] \leq [\![k{+}1 + \ell]\!]$, the result then follows by applying the (Inj$_0$-E) rule.

(Sub)Case of $\bigcirc \Diamond^{k}[\mathsf{nil}]$.

We have

$$\mathsf{unfold}(s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

Using the (Inj$_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{(k+\ell)+1}[\mathsf{nil}]\right\}$$

where

$$\begin{array}{l} x \;\; := \pi_0(y) : A \\ xs := \pi_1(y) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \end{array}$$

assuming

$$y : \left\{A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

We have

$$g \circledast xs \circledast (\mathsf{next}\; t) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

It follows that

$$\mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc \Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

and we are done since

$$\bigcirc \Diamond^{k+\ell}[\mathsf{nil}] \Rightarrow \Diamond^{(k+\ell)+1}[\mathsf{nil}]$$

$\square$

Example E.36. Assuming $\varphi : A$,

$$\mathsf{append} \ : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \longrightarrow \mathsf{CoList}\, A \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\}$$

$$\mathsf{append}^{\mathsf{g}} : \forall k \cdot \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\} \longrightarrow \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\}\right)$$

where, in the case of append, $\varphi : A$ is safe and smooth.

Proof. Let

$$T(k) := \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\} \longrightarrow \mathsf{CoList}^{\mathsf{g}}\, A \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{hd}]\varphi\right\}$$

and assume

$$g : \blacktriangleright\forall k \cdot T(k)$$

Let

$$\begin{aligned} M(g,s,t) := {} & \mathsf{case}\ s\ \mathsf{of} \\ & \mid \mathsf{Nil}^{\mathsf{g}} \ \mapsto\ t \\ & \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs \ \mapsto\ \mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) \end{aligned}$$

We show

$$\lambda s.\lambda t.M(g,s,t) : \forall k \cdot T(k)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $T(0)$.

Assume

$$s : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{hd}]\varphi\}$$

Since

$$\Diamond^{0}[\mathsf{hd}]\varphi \Leftrightarrow \bot$$

the result follows using the rule (ExF).

Case of $T(k+1)$.

Assume

$$\begin{aligned} s &: \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi\right\} \\ t &: \mathsf{CoList}^{\mathsf{g}}\, A \end{aligned}$$

Using

$$\Diamond^{k+1}[\mathsf{hd}]\varphi \Leftrightarrow [\mathsf{hd}]\varphi \vee \bigcirc\Diamond^{k}[\mathsf{hd}]\varphi$$

we apply the ($\vee$-E) rule on the refinement type of s. This leads to two subcases.

(Sub)Case of $[\mathsf{hd}]\varphi$.

We have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_1][\pi_0]\varphi\}$$

Using the (Inj$_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

where

$$\begin{aligned} x\ &:= \pi_0(y) : \{A \mid \varphi\} \\ xs &:= \pi_1(y) : \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \end{aligned}$$

assuming

$$y : \{A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\pi_0]\varphi\}$$

We have

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{hd}]\varphi\}$$

and we are done since

$$[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$$

(Sub)Case of $\bigcirc\Diamond^k[\mathsf{hd}]\varphi$.
We have

$$\mathsf{unfold}(s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^k[\mathsf{hd}]\varphi\right\}$$

Using the (Inj$_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{hd}]\varphi\right\}$$

where

$$\begin{array}{l} x \ := \pi_0(y) : A \\ xs := \pi_1(y) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\} \end{array}$$

assuming

$$y : \left\{A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\Diamond^k[\mathsf{hd}]\varphi\right\}$$

We have

$$g \circledast xs \circledast (\mathsf{next}\ t) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{hd}]\varphi\right\}$$

It follows that

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^k[\mathsf{hd}]\varphi\right\}$$

and we are done since

$$\bigcirc\Diamond^k[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1}[\mathsf{hd}]\varphi$$

□

Example E.37. Assuming $\varphi : A$, we have

$$\begin{array}{ll} \mathsf{append} & : \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{CoList}\, A \mid [\mathsf{box}]\Diamond[\mathsf{hd}]\varphi\} \\ \mathsf{append}^{\mathsf{g}} & : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^\ell[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi\right\}\right) \end{array}$$

where, in the case of append, $\varphi : A$ is safe and smooth.

Proof. Let

$$T(k,\ell) := \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi\right\}\right)$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot T(k,\ell)$$

Let

$$\begin{aligned} M(g,s,t) := {} & \mathsf{case}\ s\ \mathsf{of} \\ & \mid \mathsf{Nil}^{\mathsf{g}} \ \mapsto\ t \\ & \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs \ \mapsto\ \mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) \end{aligned}$$

We show

$$\lambda s.\lambda t.M(g,s,t) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $\forall \ell \cdot T(0,\ell)$.
We apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$s : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{nil}]\}$$

Since

$$\Diamond^{0}[\mathsf{nil}] \Leftrightarrow \bot$$

the result follows using the rule (ExF).

Case of $\forall \ell \cdot T(k{+}1,\ell)$.
We apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$\begin{aligned} s &: \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{nil}]\right\} \\ t &: \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell}[\mathsf{hd}]\varphi\right\} \end{aligned}$$

Using

$$\Diamond^{k+1}[\mathsf{nil}] \Leftrightarrow [\mathsf{nil}] \vee \bigcirc\Diamond^{k}[\mathsf{nil}]$$

we apply the ($\vee$-E) rule on the refinement type of s. This leads to two subcases.

(Sub)Case of $[\mathsf{nil}]$.
We have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_0]\top\}$$

Since $[\![\ell]\!] \leq [\![k+1+\ell]\!]$, the result then follows by applying the (Inj$_0$-E) rule.

(Sub)Case of $\bigcirc\Diamond^{k}[\mathsf{nil}]$.
We have

$$\mathsf{unfold}(s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

Using the (Inj$_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{(k+\ell)+1}[\mathsf{hd}]\varphi\right\}$$

where

$$\begin{aligned} x &:= \pi_0(y) : A \\ xs &:= \pi_1(y) : \blacktriangleright \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{nil}] \right\} \end{aligned}$$

assuming

$$y : \left\{ A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\Diamond^k[\mathsf{nil}] \right\}$$

We have

$$g \circledast xs \circledast (\mathsf{next}\ t) : \blacktriangleright \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi \right\}$$

It follows that

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k+\ell}[\mathsf{hd}]\varphi \right\}$$

and we are done since

$$\bigcirc\Diamond^{k+\ell}[\mathsf{hd}]\varphi \Rightarrow \Diamond^{(k+\ell)+1}[\mathsf{hd}]\varphi$$

□

Sharper Refinements for the Append Function on Colists

Example E.38.

$$\mathsf{append}^{\mathsf{g}} : \forall k \cdot \forall \ell \cdot \left(\left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{nil}] \right\} \longrightarrow \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{nil}] \right\} \longrightarrow \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}] \right\} \right)$$

Proof. Let

$$T(k,\ell) := \left(\left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{nil}] \right\} \longrightarrow \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{nil}] \right\} \longrightarrow \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}] \right\} \right)$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot T(k,\ell)$$

Let

$$\begin{aligned} M(g,s,t) := {}& \mathsf{case}\ s\ \mathsf{of} \\ & \mid \mathsf{Nil}^{\mathsf{g}} \ \mapsto\ t \\ & \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs \ \mapsto\ \mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) \end{aligned}$$

We show

$$\lambda s.\lambda t.M(g,s,t) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $\forall \ell \cdot T(0,\ell)$.

Apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$s : \{ \mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond^0[\mathsf{nil}] \}$$

Since

$$\Diamond^0[\mathsf{nil}] \Leftrightarrow \bot$$

the result follows using the rule (ExF).

Case of $\forall \ell \cdot T(k{+}1, \ell)$.

Apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$\begin{array}{r}s : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{nil}]\right\} \\ t : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{nil}]\right\}\end{array}$$

We have to show

$$M(g, s, t) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1+\ell}[\mathsf{nil}]\right\}$$

Using

$$\Diamond^{k+1}[\mathsf{nil}] \Leftrightarrow [\mathsf{nil}] \vee \bigcirc\Diamond^{k}[\mathsf{nil}]$$

we apply the ($\vee$-E) rule on the refinement type of s. This leads to two subcases.

(Sub)Case of $[\mathsf{nil}]$.

We have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_0]\top\}$$

Since $[\![\ell{+}1]\!] \leq [\![k{+}1{+}\ell]\!]$, the result then follows by applying the ($\textsc{Inj}_0$-E) rule.

(Sub)Case of $\bigcirc\Diamond^{k}[\mathsf{nil}]$.

We have

$$\mathsf{unfold}(s) : \left\{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

Using the ($\textsc{Inj}_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1+\ell}[\mathsf{nil}]\right\}$$

where

$$\begin{array}{ll}x &:= \pi_0(y) : A \\ xs &:= \pi_1(y) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\}\end{array}$$

assuming

$$y : \left\{A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\Diamond^{k}[\mathsf{nil}]\right\}$$

We have

$$g \circledast xs \circledast (\mathsf{next}\; t) : \blacktriangleright \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

It follows that

$$\mathsf{Cons}^{\mathsf{g}}\; x\; (g \circledast xs \circledast (\mathsf{next}\; t)) : \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k+\ell}[\mathsf{nil}]\right\}$$

and we are done since

$$\bigcirc\Diamond^{k+\ell}[\mathsf{nil}] \Rightarrow \Diamond^{k+1+\ell}[\mathsf{nil}]$$

$\square$

Example E.39. Assuming $\varphi : A$, we have

$$\mathsf{append}^{\mathsf{g}} : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi\right\}\right)$$

Proof. Let

$$T(k,\ell) := \left(\left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k}[\mathsf{nil}]\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{hd}]\varphi\right\} \longrightarrow \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi\right\}\right)$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot T(k,\ell)$$

Let

$$\begin{array}{rl} M(g,s,t) := & \mathsf{case}\ s\ \mathsf{of} \\ & \mid \mathsf{Nil}^{\mathsf{g}} \ \mapsto\ t \\ & \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs \ \mapsto\ \mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) \end{array}$$

We show

$$\lambda s.\lambda t.M(g,s,t) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. This leads to two cases.

Case of $\forall \ell \cdot T(0,\ell)$.

We apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$s : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond^{0}[\mathsf{nil}]\}$$

Since

$$\Diamond^{0}[\mathsf{nil}] \Leftrightarrow \bot$$

the result follows using the rule (ExF).

Case of $\forall \ell \cdot T(k{+}1,\ell)$.

We apply the ($\forall$-I) rule on $\forall \ell$ and assume

$$\begin{array}{rl} s : & \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1}[\mathsf{nil}]\right\} \\ t : & \left\{\mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell+1}[\mathsf{hd}]\varphi\right\} \end{array}$$

We have to show

$$M(g,s,t) : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Diamond k + 1 + \ell[\mathsf{hd}]\varphi\}$$

Using

$$\Diamond^{k+1}[\mathsf{nil}] \Leftrightarrow [\mathsf{nil}] \vee \bigcirc\Diamond^{k}[\mathsf{nil}]$$

we apply the ($\vee$-E) rule on the refinement type of s. This leads to two subcases.

(Sub)Case of [nil].

We have

$$\mathsf{unfold}(s) : \{\mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \mid [\mathsf{in}_0]\top\}$$

Since $[\![\ell{+}1]\!] \leq [\![k{+}1{+}\ell]\!]$, the result then follows by applying the (Inj$_0$-E) rule.

(Sub)Case of $\bigcirc\Diamond^k[\mathsf{nil}]$.
We have

$$\mathsf{unfold}(s) : \left\{ \mathbf{1} + A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\mathsf{in}_1][\pi_1][\mathsf{next}]\Diamond^k[\mathsf{nil}] \right\}$$

Using the (INJ$_1$-E) rule we are left with showing

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+1+\ell}[\mathsf{hd}]\varphi \right\}$$

where

$$\begin{aligned} x &:= \pi_0(y) : A \\ xs &:= \pi_1(y) : \blacktriangleright \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^k[\mathsf{nil}] \right\} \end{aligned}$$

assuming

$$y : \left\{ A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\Diamond^k[\mathsf{nil}] \right\}$$

We have

$$g \circledast xs \circledast (\mathsf{next}\ t) : \blacktriangleright \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{k+\ell}[\mathsf{hd}]\varphi \right\}$$

It follows that

$$\mathsf{Cons}^{\mathsf{g}}\ x\ (g \circledast xs \circledast (\mathsf{next}\ t)) : \left\{ \mathsf{CoList}^{\mathsf{g}}\, A \;\middle|\; \bigcirc\Diamond^{k+\ell}[\mathsf{hd}]\varphi \right\}$$

and we are done since

$$\bigcirc\Diamond^{k+\ell}[\mathsf{hd}]\varphi \Rightarrow \Diamond^{k+1+\ell}[\mathsf{hd}]\varphi$$

□

E.7 Resumptions

This example is adapted from [48]. Fix a constant type $\mathtt{O}$ and a *finite base type* $\mathtt{I}$. Let

$$\begin{aligned} \mathsf{Res}\, A &:= \blacksquare\, \mathsf{Res}^{\mathsf{g}}\, A \\ \mathsf{Res}^{\mathsf{g}}\, A &:= \mathsf{Fix}(X).A + (\mathtt{O} \times \blacktriangleright X)^{\mathtt{I}} \end{aligned}$$

and

$$\begin{aligned} \mathsf{Ret}^{\mathsf{g}} &:= \lambda a.\ \mathsf{fold}(\mathsf{in}_0\ a) : A \longrightarrow \mathsf{Res}^{\mathsf{g}}\, A \\ \mathsf{Cont}^{\mathsf{g}} &:= \lambda k.\ \mathsf{fold}(\mathsf{in}_1\ k) : (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \longrightarrow \mathsf{Res}^{\mathsf{g}}\, A \end{aligned}$$

Example E.40 (A Scheduler on Resumptions).

$$\begin{aligned} \mathsf{sched} \ :\ \ & \mathsf{Res}\, A \longrightarrow \mathsf{Res}\, A \longrightarrow \mathsf{Res}\, A \\ :=\ & \lambda p.\lambda q.\ \mathsf{box}_\iota(\mathsf{sched}^{\mathsf{g}}\ (\mathsf{unbox}\ p)\ (\mathsf{unbox}\ q)) \end{aligned}$$

$$\begin{aligned} \mathsf{sched}^{\mathsf{g}} :\ \ & \mathsf{Res}^{\mathsf{g}}\, A \longrightarrow \mathsf{Res}^{\mathsf{g}}\, A \longrightarrow \mathsf{Res}^{\mathsf{g}}\, A \\ :=\ & \mathsf{fix}(g).\lambda p.\lambda q.\ \mathsf{case}\ p\ \mathsf{of} \\ & \mid \mathsf{Ret}^{\mathsf{g}}\ a\ \mapsto\ \mathsf{Ret}^{\mathsf{g}}\ a \\ & \mid \mathsf{Cont}^{\mathsf{g}}\ k\ \mapsto \\ & \quad \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o, t\rangle = ki \\ & \quad \qquad\qquad\quad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ & \quad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{aligned}$$

Here, $\mathsf{Ret}^{\mathsf{g}}(a)$ represents a computation which returns the value $a : A$, while $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$ (with $\langle f, k\rangle : \mathtt{I} \to (\mathtt{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A))$ represents a computation which on input $\mathtt{i} : \mathtt{I}$ outputs $f\mathtt{i} : \mathtt{O}$ and continues with the computation $k\mathtt{i} : \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A$.

Provided with resumptions $p, q : \mathsf{Res}^{\mathsf{g}}\, A$, the scheduler ($\mathsf{sched}^{\mathsf{g}}\ p\ q$), adapted from [48], first evaluates p. If p returns, then the whole computation returns, with the same value. Otherwise, p evaluates to say $\mathsf{Cont}^{\mathsf{g}}\langle f, k\rangle$. Then ($\mathsf{sched}^{\mathsf{g}}\ p\ q$) produces a computation which on input $\mathtt{i} : \mathtt{I}$ outputs $f\mathtt{i}$ and continues with the computation ($\mathsf{sched}^{\mathsf{g}}\ q\ (k\mathtt{i})$), thus switching arguments.

Example E.41 (Formulae on $\mathsf{Res}^{\mathsf{g}}\, A$). Assuming $\psi : A$, $\varphi : \mathsf{Res}^{\mathsf{g}}\, A$, $\vartheta : \mathtt{O}$ and $\mathtt{i} \in \mathtt{I}$,

$$
\begin{array}{lll}
[\mathsf{Ret}] & := [\mathsf{fold}][\mathsf{in}_0]\top & : \mathsf{Res}^{\mathsf{g}}\, A \\
[\mathsf{Cont}] & := [\mathsf{fold}][\mathsf{in}_1]\top & : \mathsf{Res}^{\mathsf{g}}\, A \\
\\
[\mathsf{now}]\psi & := [\mathsf{fold}][\mathsf{in}_0]\psi & : \mathsf{Res}^{\mathsf{g}}\, A \\
[\mathsf{out}_{\mathtt{i}}]\vartheta & := [\mathsf{fold}][\mathsf{in}_1]\,([\mathtt{i}] \Vert\!\!\to [\pi_0]\vartheta) & : \mathsf{Res}^{\mathsf{g}}\, A \\
[\wedge\mathsf{out}]\vartheta & := \wedge_{\mathtt{i}\in\mathtt{I}}[\mathsf{out}_{\mathtt{i}}]\vartheta & : \mathsf{Res}^{\mathsf{g}}\, A \\
[\vee\mathsf{out}]\vartheta & := \vee_{\mathtt{i}\in\mathtt{I}}[\mathsf{out}_{\mathtt{i}}]\vartheta & : \mathsf{Res}^{\mathsf{g}}\, A \\
\\
\bigcirc_{\mathtt{i}}\varphi & := [\mathsf{fold}][\mathsf{in}_1]\,([\mathtt{i}] \Vert\!\!\to [\pi_1][\mathsf{next}]\varphi) & : \mathsf{Res}^{\mathsf{g}}\, A \\
\owedge\, \varphi & := \wedge_{\mathtt{i}\in\mathtt{I}} \bigcirc_{\mathtt{i}}\, \varphi & : \mathsf{Res}^{\mathsf{g}}\, A \\
\ovee\, \varphi & := \vee_{\mathtt{i}\in\mathtt{I}} \bigcirc_{\mathtt{i}}\, \varphi & : \mathsf{Res}^{\mathsf{g}}\, A \\
\\
\exists\Box\varphi & := \nu\alpha.\ \varphi \wedge \ovee\, \alpha & : \mathsf{Res}^{\mathsf{g}}\, A \\
\forall\Box\varphi & := \nu\alpha.\ \varphi \wedge \owedge\, \alpha & : \mathsf{Res}^{\mathsf{g}}\, A \\
\\
\exists\Diamond\varphi & := \mu\alpha.\ \varphi \vee \ovee\, \alpha & : \mathsf{Res}^{\mathsf{g}}\, A \\
\forall\Diamond\varphi & := \mu\alpha.\ \varphi \vee \owedge\, \alpha & : \mathsf{Res}^{\mathsf{g}}\, A
\end{array}
$$

We moreover let

$$
\begin{array}{ll}
\forall\Box^{\mathtt{t}}\psi := \nu^{\mathtt{t}}\alpha.\ \psi \wedge \owedge\, \alpha : \mathsf{Res}^{\mathsf{g}}\, A & \qquad \forall\Diamond^{\mathtt{t}}\psi := \mu^{\mathtt{t}}\alpha.\ \psi \vee \owedge\, \alpha : \mathsf{Res}^{\mathsf{g}}\, A \\
\exists\Box^{\mathtt{t}}\psi := \nu^{\mathtt{t}}\alpha.\ \psi \wedge \ovee\, \alpha : \mathsf{Res}^{\mathsf{g}}\, A & \qquad \exists\Diamond^{\mathtt{t}}\psi := \mu^{\mathtt{t}}\alpha.\ \psi \vee \ovee\, \alpha : \mathsf{Res}^{\mathsf{g}}\, A
\end{array}
$$

The formula $\exists\Diamond\varphi$ holds on a resumption if there is a finite sequence of inputs which leads to a resumption satisfying φ, while $\forall\Diamond\varphi$ holds on a resumption if φ holds at some point for any infinite sequence of inputs (this relies on Weak König Lemma). Moreover, $\exists\Box\varphi$ expresses that there is an infinite sequence of inputs in which the resumption never returns and along which φ always holds, while $\forall\Box\varphi$ expresses that for all infinite sequence of inputs, the resumption never returns and φ always holds. For instance, the composite formula $\exists\Box\exists\Diamond[\mathsf{Ret}]$ says that there is an infinite sequence of inputs along which (1) the resumption does not return and (2), at any point, there is a finite sequence of inputs which leads to a return.

Example E.42. Let $\psi : A$ be a *safe and smooth* formula and let $\varphi \in \{[\mathsf{Ret}], [\mathsf{now}]\psi\}$. We have

$$\begin{array}{l}\mathsf{sched} \;\; : \{\mathsf{Res}\,A \mid [\mathsf{box}]\exists\Diamond\varphi\} \longrightarrow \{\mathsf{Res}\,A \mid [\mathsf{box}]\exists\Diamond\varphi\} \longrightarrow \{\mathsf{Res}\,A \mid [\mathsf{box}]\exists\Diamond\varphi\} \\ \mathsf{sched} \;\; : \{\mathsf{Res}\,A \mid [\mathsf{box}]\forall\Diamond\varphi\} \longrightarrow \{\mathsf{Res}\,A \mid [\mathsf{box}]\forall\Diamond\varphi\} \longrightarrow \{\mathsf{Res}\,A \mid [\mathsf{box}]\forall\Diamond\varphi\}\end{array}$$

$$\begin{array}{l}\mathsf{sched}^{\mathsf{g}} : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \exists\Diamond^{k}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \exists\Diamond^{\ell}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \exists\Diamond^{k+\ell}\varphi\right\}\right) \\ \mathsf{sched}^{\mathsf{g}} : \forall k \cdot \forall \ell \cdot \left(\left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \forall\Diamond^{k}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \forall\Diamond^{\ell}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \forall\Diamond^{k+\ell}\varphi\right\}\right)\end{array}$$

Proof. Let $\Diamond \in \{\exists\Diamond, \forall\Diamond\}$ and

$$T(k,\ell) := \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{k}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{\ell}\varphi\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{k+\ell}\varphi\right\}$$

and assume

$$g : \blacktriangleright \forall k \cdot \forall \ell \cdot T(k,\ell)$$

Let

$$\begin{array}{l}M(g,p,q) := \mathsf{case}\ p\ \mathsf{of} \\ \qquad\qquad\qquad \mid \mathsf{Ret}^{\mathsf{g}}\ a \ \mapsto\ \mathsf{Ret}^{\mathsf{g}}\ a \\ \qquad\qquad\qquad \mid \mathsf{Cont}^{\mathsf{g}}\ k \ \mapsto \\ \qquad\qquad\qquad\quad \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o, t\rangle = ki \\ \qquad\qquad\qquad\qquad\qquad\qquad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \qquad\qquad\qquad\quad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h\end{array}$$

We show

$$\lambda p.\lambda q.M(g,p,q) : \forall k \cdot \forall \ell \cdot T(k,\ell)$$

We apply the ($\forall$-CI) rule on $\forall k$. In the case of $\forall \ell \cdot T(\mathsf{0},\ell)$, we get the result using the (ExF) rule since

$$\Diamond^{\mathsf{0}}\varphi \Leftrightarrow \bot$$

As for $\forall \ell \cdot T(k{+}\mathsf{1},\ell)$, we apply the ($\forall$-I) rule on $\forall \ell$. We have to show

$$M(g,p,q) : \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{k+\ell+\mathsf{1}}\varphi\right\}$$

assuming

$$\begin{array}{l}p : \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{k+\mathsf{1}}\varphi\right\} \\ q : \left\{\mathsf{Res}^{\mathsf{g}}\,A \;\middle|\; \Diamond^{\ell}\varphi\right\}\end{array}$$

Using

$$\begin{array}{l}\exists\Diamond^{k+\mathsf{1}}\varphi \Leftrightarrow \varphi \quad \vee \quad \textcircled{\scriptsize $\vee$}\,\exists\Diamond^{k}\varphi \\ \forall\Diamond^{k+\mathsf{1}}\varphi \Leftrightarrow \varphi \quad \vee \quad \textcircled{\scriptsize $\wedge$}\,\forall\Diamond^{k}\varphi\end{array}$$

we reason by cases on the refinement type of p.

Case of $[\mathsf{Ret}]$**.**

We have

$$\mathsf{unfold}\ p : \{A + (\mathsf{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\,A)^{\mathtt{I}} \mid [\mathsf{in}_0]\top\}$$

We apply the (Inj$_0$-E) rule on p and we are done since

$$\mathsf{Ret}^{\mathsf{g}}\ a : \{\mathsf{Res}^{\mathsf{g}}\,A \mid [\mathsf{Ret}]\}$$

assuming

$$a : A$$

Case of $[\mathsf{now}]\psi$.

We have

$$\mathsf{unfold}\ p : \{A + (\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \mid [\mathsf{in}_0]\psi\}$$

We apply the ($\textsc{Inj}_0$-E) rule on p and we are done since

$$\mathsf{Ret}^{\mathsf{g}}\ a : \{\mathsf{Res}^{\mathsf{g}}\, A \mid [\mathsf{now}]\psi\}$$

assuming

$$a : \{A \mid \psi\}$$

Case of $\circledcirc\, \exists\Diamond^k\varphi$.

We apply the ($\vee$-E) rule on the refinement type of p. So let $\mathtt{i} \in \mathtt{I}$ and assume

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\exists\Diamond^k\varphi\right\}$$

We have

$$\mathsf{unfold}\ p : \left\{A + (\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathsf{in}_1]\left([\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Diamond^k\varphi\right)\right\}$$

We apply the ($\textsc{Inj}_1$-E) rule on the refinement type of p. Let

$$\begin{aligned} N(g,k,q) := \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ &\langle o, t\rangle = ki \\ \mathsf{in}\ \ &\langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{aligned}$$

We show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\exists\Diamond^{k+\ell}\varphi\right\}$$

assuming

$$k : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Diamond^k\varphi\right\}$$

Assuming

$$i : \{\mathtt{I} \mid [\mathtt{i}]\}$$

we thus have

$$ki : \left\{\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\exists\Diamond^k\varphi\right\}$$

It follows that

$$\langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki))\rangle : \left\{\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\exists\Diamond^{k+\ell}\varphi\right\}$$

and thus

$$\lambda i.\ \langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki))\rangle : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Diamond^{k+\ell}\varphi\right\}$$

Now we are done since

$$\begin{array}{rl} & \bigcirc_{\mathtt{i}}\exists\Diamond^{k+\ell}\varphi = [\mathsf{fold}][\mathsf{in}_1]\left([\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Diamond^{k+\ell}\varphi\right) \\ \text{and} & \mathsf{Cont}^{\mathsf{g}} = \lambda h.\ \mathsf{fold}(\mathsf{in}_1\ h) \end{array}$$

Case of $\circledcirc\, \forall\Diamond^k\varphi$.
Using

$$\forall\Diamond^{k+\ell+1}\varphi \Leftrightarrow \varphi \quad \vee \quad \circledcirc\, \forall\Diamond^{k+\ell}\varphi$$

for each $\mathtt{i} \in \mathtt{I}$ we show

$$M(g,p,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\forall\Diamond^{k+\ell}\varphi\right\}$$

So let $\mathtt{i} \in \mathtt{I}$. Since

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \circledcirc\, \exists\Diamond^k\varphi\right\}$$

We have

$$\mathsf{unfold}\ p : \left\{A + (\mathsf{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathsf{in}_1]\left([\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Diamond^k\varphi\right)\right\}$$

and we conclude similarly as in the case of $\circledcirc\, \exists\Diamond^k\varphi$. $\square$

Example E.43. Let $\vartheta : \mathsf{O}$ be a *safe and smooth* formula. Furthermore, let $\square \in \{\forall\square, \exists\square\}$, $\Diamond \in \{\forall\Diamond, \exists\Diamond\}$ and $[\mathsf{out}] \in \{[\wedge\mathsf{out}], [\vee\mathsf{out}]\}$. We have

$$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\square\Diamond[\mathsf{out}]\vartheta\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\square\Diamond[\mathsf{out}]\vartheta\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\square\Diamond[\mathsf{out}]\vartheta\}$$

Proof. We show that we can give the following refinement type to $\mathsf{sched}^{\mathsf{g}}$:

$$\forall k\cdot\forall\ell_0\cdot\forall\ell_1\cdot\left(\left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_0}[\mathsf{out}]\vartheta\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_1}[\mathsf{out}]\vartheta\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}\right)$$

Let $T(k,\ell_0,\ell_1)$ be the type

$$\left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_0}[\mathsf{out}]\vartheta\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_1}[\mathsf{out}]\vartheta\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \square^k\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}$$

and assume

$$g : \blacktriangleright\forall k \cdot \forall\ell_0 \cdot \forall\ell_1 \cdot T(k,\ell_0,\ell_1)$$

Let

$$\begin{array}{rl} M(g,p,q) := & \mathsf{case}\ p\ \mathsf{of} \\ & \quad \mid \mathsf{Ret}^{\mathsf{g}}\ a \ \mapsto\ \mathsf{Ret}^{\mathsf{g}}\ a \\ & \quad \mid \mathsf{Cont}^{\mathsf{g}}\ k \ \mapsto \\ & \qquad \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o,t\rangle = ki \\ & \qquad\qquad\qquad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ & \qquad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{array}$$

We show

$$\lambda p.\lambda q.M(g,p,q) : \forall k \cdot \forall\ell_0 \cdot \forall\ell_1 \cdot T(k,\ell_0,\ell_1)$$

We apply the ($\forall$-CI) rule on $\forall k$. The case of $\forall\ell_0 \cdot \forall\ell_1 \cdot T(\mathsf{0},\ell_0,\ell_1)$ is trivial since

$$\square^{\mathsf{0}}\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta \Leftrightarrow \top$$

As for $\forall\ell_0 \cdot \forall\ell_1 \cdot T(k{+}\mathsf{1},\ell_0,\ell_1)$, we apply the ($\forall$-CI) rule, this time on $\forall\ell_0$. In the case of $\forall\ell_1 \cdot T(k{+}\mathsf{1},\mathsf{0},\ell_1)$, since $\square^{k+\mathsf{1}}\Diamond^{\mathsf{0}}[\mathsf{out}]\vartheta$ is of the form

$$\Diamond^{\mathsf{0}}[\mathsf{out}]\vartheta \wedge \psi$$

while

$$\Diamond^{0}[\mathsf{out}]\vartheta \Leftrightarrow \bot$$

we can conclude using the (ExF) rule. It remains to deal with the case of $\forall \ell_1 \cdot T(k{+}1, \ell_0{+}1, \ell_1)$. We apply the ($\forall$-I) rule on $\forall\ell_1$. We show

$$M(g,p,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right\}$$

assuming

$$\begin{array}{l} p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\} \\ q : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_1}[\mathsf{out}]\vartheta\right\} \end{array}$$

We will apply the (Inj_1-E) rule on ($\mathsf{unfold}\ p$) and show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right\}$$

where

$$\begin{array}{l} N(g,k,q) := \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o,t\rangle = ki \\ \qquad\qquad\qquad\qquad\qquad\quad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \qquad\qquad\quad\ \ \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{array}$$

and under suitable assumption on the refinement type of k. We have

$$\begin{array}{lll} \forall\Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta \Leftrightarrow \Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta & \wedge & \oslash\, \forall\Box^{k}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta \\ \exists\Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta \Leftrightarrow \Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta & \wedge & \oslash\, \exists\Box^{k}\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta \end{array}$$

and we consider each conjunct separately.

Cases of $\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta$.

We have

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

Using

$$\begin{array}{lll} \exists\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta \Leftrightarrow [\mathsf{out}]\vartheta & \vee & \oslash\, \exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta \\ \forall\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta \Leftrightarrow [\mathsf{out}]\vartheta & \vee & \oslash\, \forall\Diamond^{\ell_0}[\mathsf{out}]\vartheta \end{array}$$

we reason by cases on the refinement type of p.

(Sub)Cases of $[\mathsf{out}]\vartheta$.

We show

$$N(g,k,q) : \{\mathsf{Res}^{\mathsf{g}}\, A \mid [\mathsf{out}]\vartheta\}$$

We handle the cases of $[\vee\mathsf{out}]$ and $[\wedge\mathsf{out}]$ separately.

(SubSub)Case of $[\vee\mathsf{out}]$.

We apply the ($\vee$-E) rule on the refinement type of p. So let $\mathtt{i} \in \mathtt{I}$ and assume

$$p : \{\mathsf{Res}^{\mathsf{g}}\, A \mid [\mathsf{out}_{\mathtt{i}}]\vartheta\}$$

This amounts to

$$k : \{(\mathsf{O} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \mid [\mathtt{i}] \Vert\!\!\to [\pi_0]\vartheta\}$$

Hence assuming

$$i : \{A \mid [\mathtt{i}]\}$$

we have

$$\langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki)) \rangle : \{ \mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \mid [\pi_0]\vartheta \}$$

It follows that

$$\lambda i.\ \langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki)) \rangle : \{ (\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \mid [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_0]\vartheta \}$$

and we are done since

$$\mathsf{Cont}^{\mathsf{g}} = \lambda h.\ \mathsf{fold}(\mathsf{in}_1\ h)$$

(SubSub)Case of $[\wedge\mathsf{out}]$**.**
For each $\mathtt{i} \in \mathtt{I}$ we have to show

$$N(g,k,q) : \{ \mathsf{Res}^{\mathsf{g}}\, A \mid [\mathsf{out}_i]\vartheta \}$$

So let $\mathtt{i} \in \mathtt{I}$. Since

$$p : \{ \mathsf{Res}^{\mathsf{g}}\, A \mid [\mathsf{out}_{\mathtt{i}}]\vartheta \}$$

we have

$$k : \{ (\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \mid [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_0]\vartheta \}$$

and we conclude similarly as in the case of $[\vee\mathsf{out}]$.

(Sub)Case of $\circledcirc\, \exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta$**.**
We show

$$N(g,k,q) : \left\{ \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \circledcirc\, \exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta \right\}$$

We apply the ($\vee$-E) rule on the refinement type of p. So let $\mathtt{i} \in \mathtt{I}$ and assume

$$p : \left\{ \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}} \exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta \right\}$$

This amounts to

$$k : \left\{ (\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta \right\}$$

Assuming

$$i : \{ \mathtt{I} \mid [\mathtt{i}] \}$$

we thus have

$$ki : \left\{ \mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta \right\}$$

since (by subtyping) g has type

$$\blacktriangleright \left(\left\{ \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^1\exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta \right\} \longrightarrow \left\{ \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^1\exists\Diamond^{\ell_1}[\mathsf{out}]\vartheta \right\} \longrightarrow \left\{ \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^1\exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta \right\} \right)$$

and since, according to Table 2,

$$\Box^1\theta \Leftrightarrow \theta$$

it follows that

$$\langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki))\rangle : \left\{\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}$$

We thus get

$$\lambda i.\ \langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki))\rangle : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}$$

Now we are done since

$$\begin{array}{lrcl} & \bigcirc_{\mathtt{i}}\exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta &=& [\mathsf{fold}][\mathsf{in}_1]\left([\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\exists\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right) \\ \text{and} & \mathsf{Cont}^{\mathsf{g}} &=& \lambda h.\ \mathsf{fold}(\mathsf{in}_1\ h) \end{array}$$

(Sub)Case of $\owedge\, \forall\Diamond^{\ell_0}[\mathsf{out}]\vartheta$.

We show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \owedge\, \forall\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}$$

Hence, for each $\mathtt{i} \in \mathtt{I}$ we have to show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\forall\Diamond^{\ell_0+\ell_1}[\mathsf{out}]\vartheta\right\}$$

So let $\mathtt{i} \in \mathtt{I}$. Since

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\forall\Diamond^{\ell_0}[\mathsf{out}]\vartheta\right\}$$

we have

$$k : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\forall\Diamond^{\ell_0}[\mathsf{out}]\vartheta\right\}$$

and we conclude similarly as in the case of $\ovee\, \exists\Diamond^{\ell_0}[\mathsf{out}]\vartheta$.

Case of $\owedge\, \forall\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta$.

For each $\mathtt{i} \in \mathtt{I}$ we have to show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\forall\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right\}$$

So let $\mathtt{i} \in \mathtt{I}$. Since

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\forall\Box^k\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

we have

$$k : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\forall\Box^k\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

Assuming

$$i : \{\mathtt{I} \mid [\mathtt{i}]\}$$

we thus have

$$ki : \left\{\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; [\pi_1][\mathsf{next}]\forall\Box^k\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

and it follows that

$$\lambda i.\ \langle \pi_0(ki)\,,\, g \circledast (\mathsf{next}\ q) \circledast (\pi_1(ki))\rangle : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\forall\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right\}$$

Now we are done since

$$\begin{array}{lrcl} & \bigcirc_{\mathtt{i}}\forall\Box^k\exists\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta &=& [\mathsf{fold}][\mathsf{in}_1]\left([\mathtt{i}] \Vdash\!\!\rightarrow [\pi_1][\mathsf{next}]\forall\Box^k\exists\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right) \\ \text{and} & \mathsf{Cont}^{\mathsf{g}} &=& \lambda h.\ \mathsf{fold}(\mathsf{in}_1\ h) \end{array}$$

Case of $\circledcirc\, \exists\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta$.

We have to show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \circledcirc\, \exists\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta\right\}$$

We apply the ($\vee$-E) rule on the refinement type of p. So let $\mathtt{i} \in \mathtt{I}$ and assume

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \bigcirc_{\mathtt{i}}\exists\Box^k\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

We have

$$k : \left\{(\mathtt{0} \times \blacktriangleright \mathsf{Res}^{\mathsf{g}}\, A)^{\mathtt{I}} \;\middle|\; [\mathtt{i}] \Vdash\!\!\to [\pi_1][\mathsf{next}]\exists\Box^k\Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

and we conclude similarly as in the case of $\circledcirc\, \forall\Box^k\Diamond^{\ell_0+\ell_1+1}[\mathsf{out}]\vartheta$. $\Box$

Example E.44. Let $\Box \in \{\forall\Box, \exists\Box\}$ and $\Diamond \in \{\forall\Diamond, \exists\Diamond\}$. We have

$$\mathsf{sched} : \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\} \longrightarrow \{\mathsf{Res}\, A \mid [\mathsf{box}]\Box\Diamond[\mathsf{Ret}]\}$$

Proof. We show that we can give the following refinement type to $\mathsf{sched}^{\mathsf{g}}$:

$$\forall k\cdot\forall\ell_0\cdot\forall\ell_1\cdot\left(\left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_0}[\mathsf{Ret}]\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_1}[\mathsf{Ret}]\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_0+\ell_1}[\mathsf{Ret}]\right\}\right)$$

Let $T(k,\ell_0,\ell_1)$ be the type

$$\left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_0}[\mathsf{Ret}]\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_1}[\mathsf{Ret}]\right\} \longrightarrow \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^k\Diamond^{\ell_0+\ell_1}[\mathsf{Ret}]\right\}$$

and assume

$$g : \blacktriangleright\forall k\cdot\forall\ell_0\cdot\forall\ell_1\cdot T(k,\ell_0,\ell_1)$$

Let

$$\begin{array}{l} M(g,p,q) := \mathsf{case}\ p\ \mathsf{of} \\ \qquad\qquad\quad \mid \mathsf{Ret}^{\mathsf{g}}\ a \ \mapsto\ \mathsf{Ret}^{\mathsf{g}}\ a \\ \qquad\qquad\quad \mid \mathsf{Cont}^{\mathsf{g}}\ k \ \mapsto \\ \qquad\qquad\qquad \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o,t\rangle = ki \\ \qquad\qquad\qquad\qquad\qquad\quad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \qquad\qquad\qquad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{array}$$

We show

$$\lambda p.\lambda q.M(g,p,q) : \forall k\cdot\forall\ell_0\cdot\forall\ell_1\cdot T(k,\ell_0,\ell_1)$$

We apply the ($\forall$-CI) rule on $\forall k$. The case of $\forall\ell_0\cdot\forall\ell_1\cdot T(\mathtt{0},\ell_0,\ell_1)$ is trivial since

$$\Box^{\mathtt{0}}\Diamond^{\ell_0+\ell_1}[\mathsf{Ret}] \Leftrightarrow \top$$

As for $\forall\ell_0\cdot\forall\ell_1\cdot T(k{+}\mathtt{1},\ell_0,\ell_1)$, we apply the ($\forall$-CI) rule, this time on $\forall\ell_0$. In the case of $\forall\ell_1\cdot T(k{+}\mathtt{1},\mathtt{0},\ell_1)$, since $\Box^{k+\mathtt{1}}\Diamond^{\mathtt{0}}[\mathsf{Ret}]$ is of the form

$$\Diamond^{\mathtt{0}}[\mathsf{Ret}] \wedge \psi$$

while

$$\Diamond^{\mathtt{0}}[\mathsf{Ret}] \Leftrightarrow \bot$$

we can conclude using the (ExF) rule. It remains to deal with the case of $\forall \ell_1 \cdot T(k{+}1, \ell_0{+}1, \ell_1)$. We apply the ($\forall$-I) rule on $\forall \ell_1$. We show

$$M(g,p,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}]\right\}$$

assuming

$$\begin{array}{r} p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+1}[\mathsf{Ret}]\right\} \\ q : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_1}[\mathsf{Ret}]\right\} \end{array}$$

We have

$$\begin{array}{lllll} \forall\Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] & \Leftrightarrow & \Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] & \wedge & \textcircled{\forall}\, \forall\Box^{k}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] \\ \exists\Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] & \Leftrightarrow & \Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] & \wedge & \textcircled{\exists}\, \exists\Box^{k}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}] \end{array}$$

and we consider each conjunct separately.

Cases of $\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}]$.
We have

$$p : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell_0+1}[\mathsf{out}]\vartheta\right\}$$

Using

$$\begin{array}{lllll} \exists\Diamond^{\ell_0+1}[\mathsf{Ret}] & \Leftrightarrow & [\mathsf{Ret}] & \vee & \textcircled{\exists}\, \exists\Diamond^{\ell_0}[\mathsf{Ret}] \\ \forall\Diamond^{\ell_0+1}[\mathsf{Ret}] & \Leftrightarrow & [\mathsf{Ret}] & \vee & \textcircled{\forall}\, \forall\Diamond^{\ell_0}[\mathsf{Ret}] \end{array}$$

we reason by cases on the refinement type of p. In the case of $[\mathsf{Ret}]$, apply the (Inj_0-E) rule on ($\mathsf{unfold}\ p$), and we conclude similarly as in Ex. E.42. In the other cases, we apply the (Inj_1-E) rule on ($\mathsf{unfold}\ p$) and show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}]\right\}$$

where

$$\begin{array}{l} N(g,k,q) := \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o,t\rangle = ki \\ \qquad\qquad\qquad\qquad\qquad\qquad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \qquad\qquad\qquad\quad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{array}$$

and under suitable assumption on the refinement type of k. We can then conclude similarly as in Ex. E.43.

Cases of $\bigcirc\Box^{k}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}]$.
We apply the (Inj_1-E) rule on ($\mathsf{unfold}\ p$) and show

$$N(g,k,q) : \left\{\mathsf{Res}^{\mathsf{g}}\, A \;\middle|\; \Box^{k+1}\Diamond^{\ell_0+\ell_1+1}[\mathsf{Ret}]\right\}$$

where

$$\begin{array}{l} N(g,k,q) := \mathsf{let}\ \ h = \lambda i.\ \mathsf{let}\ \ \langle o,t\rangle = ki \\ \qquad\qquad\qquad\qquad\qquad\qquad \mathsf{in}\ \ \langle o, g \circledast (\mathsf{next}\ q) \circledast t\rangle \\ \qquad\qquad\qquad\quad \mathsf{in}\ \ \mathsf{Cont}^{\mathsf{g}}\ h \end{array}$$

and under suitable assumption on the refinement type of k. We can then conclude similarly as in Ex. E.43. $\Box$

E.8 Breadth-First Tree Traversal

Infinite Binary Trees The guarded recursive type of binary trees is

$$\begin{aligned}\mathsf{Tree}^{\mathsf{g}}\,A &:= \mathsf{Fix}(X).A \times (\blacktriangleright X \times \blacktriangleright X)\\ \mathsf{Tree}\,A &:= \blacksquare\,\mathsf{Tree}^{\mathsf{g}}\,A\end{aligned}$$

The usual guarded constructors and destructors on $\mathsf{Tree}^{\mathsf{g}}\,A$ are represented as

$$\begin{array}{lll}\mathsf{Node}^{\mathsf{g}} & := \lambda v.\lambda \ell.\lambda r.\mathsf{fold}(\langle v, \langle \ell, r\rangle\rangle) & : A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A \to \mathsf{Tree}^{\mathsf{g}}\,A\\ \mathsf{label}^{\mathsf{g}} & := \lambda t.\pi_0(\mathsf{unfold}\ t) & : \mathsf{Tree}^{\mathsf{g}}\,A \to A\\ \mathsf{son}^{\mathsf{g}}_{\ell} & := \lambda t.\pi_0(\pi_1(\mathsf{unfold}\ t)) & : \mathsf{Tree}^{\mathsf{g}}\,A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A\\ \mathsf{son}^{\mathsf{g}}_{r} & := \lambda t.\pi_1(\pi_1(\mathsf{unfold}\ t)) & : \mathsf{Tree}^{\mathsf{g}}\,A \to \blacktriangleright \mathsf{Tree}^{\mathsf{g}}\,A\end{array}$$

Their coinductive (for A a constant type) variants are

$$\begin{array}{lll}\mathsf{Node} & := \lambda v.\lambda \ell.\lambda r. & : A \to \mathsf{Tree}\,A \to \mathsf{Tree}\,A \to \mathsf{Tree}\,A\\ & \quad \mathsf{box}_{\iota}(\mathsf{Node}^{\mathsf{g}}\ v\ (\mathsf{next}\ (\mathsf{unbox}\ \ell))\ (\mathsf{next}\ (\mathsf{unbox}\ \ell))) & \\ \mathsf{label} & := \lambda t.\mathsf{label}^{\mathsf{g}}\ (\mathsf{unbox}\ t) & : \mathsf{Tree}\,A \to A\\ \mathsf{son}_{\ell} & := \lambda t.\mathsf{son}^{\mathsf{g}}_{\ell}\ (\mathsf{unbox}\ t) & : \mathsf{Tree}\,A \to \mathsf{Tree}^{\mathsf{g}}\,A\\ \mathsf{son}_{r} & := \lambda t.\mathsf{son}^{\mathsf{g}}_{r}\ (\mathsf{unbox}\ t) & : \mathsf{Tree}\,A \to \mathsf{Tree}\,A\end{array}$$

Example E.45 (Tree Formulae). Assuming $\varphi : \mathsf{Tree}^{\mathsf{g}}\,A$,

$$\begin{aligned}\forall\Box\varphi :&\quad \mathsf{Tree}^{\mathsf{g}}\,A\\ &:= \nu\alpha.\ \varphi \wedge (\bigcirc_{\ell}\alpha \wedge \bigcirc_{r}\alpha)\end{aligned}$$

$$\begin{aligned}\exists\Diamond\varphi :&\quad \mathsf{Tree}^{\mathsf{g}}\,A\\ &:= \mu\alpha.\ \varphi \vee (\bigcirc_{\ell}\alpha \vee \bigcirc_{r}\alpha)\end{aligned}$$

Example E.46. Assuming $\varphi : A$, we have

$$\mathsf{Node}^{\mathsf{g}} : \{A \mid \varphi\} \to \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \to \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \to \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\}$$

$$\mathsf{label}^{\mathsf{g}} : \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \longrightarrow \{A \mid \varphi\}$$

$$\mathsf{son}^{\mathsf{g}}_{\ell} : \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\}$$

$$\mathsf{son}^{\mathsf{g}}_{r} : \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\}$$

Breadth-First Traversal of Guarded Trees Using Forests

Example E.47.

$$\begin{array}{lll}
\mathsf{bft} & : & \mathsf{Tree}\,A \to \mathsf{CoList}\,A \\
 & := & \lambda t.\ \mathsf{box}_\iota(\mathsf{bft}^{\mathsf{g}}\ (\mathsf{unbox}\ t))
\end{array}$$

$$\begin{array}{lll}
\mathsf{bft}^{\mathsf{g}} & : & \mathsf{Tree}^{\mathsf{g}}\,A \to \mathsf{CoList}^{\mathsf{g}}\,A \\
 & := & \lambda t.\mathsf{bftaux}^{\mathsf{g}}\ [t]^{\mathsf{g}}
\end{array}$$

$$\begin{array}{lll}
\mathsf{bftaux}^{\mathsf{g}} & : & \mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A) \to \mathsf{CoList}^{\mathsf{g}}\,A \\
 & := & \mathsf{fix}(g).\lambda s.\ \mathsf{case}\ s\ \mathsf{of} \\
 & & \quad \mid \mathsf{Nil}^{\mathsf{g}}\ \mapsto\ \mathsf{Nil}^{\mathsf{g}} \\
 & & \quad \mid \mathsf{Cons}^{\mathsf{g}}\ x\ xs\ \mapsto\ (\mathsf{label}^{\mathsf{g}}\ x) ::^{\mathsf{g}} g \circledast \left(\mathsf{next}(\mathsf{append}^{\mathsf{g}}) \circledast xs \circledast [(\mathsf{son}^{\mathsf{g}}_{\ell}\ x), (\mathsf{son}^{\mathsf{g}}_{r}\ x)]^{\mathsf{g}\blacktriangleright}\right)
\end{array}$$

where

$$\begin{array}{ll}
[]^{\mathsf{g}\blacktriangleright} & := \mathsf{next}([]^{\mathsf{g}}) \\
[y_0, y_1, \dots, y_n]^{\mathsf{g}\blacktriangleright} & := \mathsf{next}(\mathsf{Cons}^{\mathsf{g}}) \circledast y_0 \circledast \mathsf{next}[y_1, \dots, y_n]^{\mathsf{g}\blacktriangleright}
\end{array}$$

Example E.48.

$$\mathsf{bft}^{\mathsf{g}} \quad : \mathsf{Tree}^{\mathsf{g}}\,A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\neg\mathsf{nil}]\}$$

$$\mathsf{bftaux}^{\mathsf{g}} : \{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A) \mid [\neg\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\neg\mathsf{nil}]\}$$

Example E.49.

$$\mathsf{bft}^{\mathsf{g}} \quad : \mathsf{Tree}\,A \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\mathsf{inf}]\}$$

$$\mathsf{bftaux}^{\mathsf{g}} : \{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}\,A) \mid [\neg\mathsf{nil}]\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid [\mathsf{inf}]\}$$

Example E.50. Assuming $\varphi : A$,

$$\mathsf{bft}^{\mathsf{g}} : \{\mathsf{Tree}^{\mathsf{g}}\,A \mid \forall\Box[\mathsf{lbl}]\varphi\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}$$

Proof. Thanks to Ex. E.30 and Ex. E.31, we can reduce to showing

$$\mathsf{bftaux}^{\mathsf{g}} : \left\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A) \;\middle|\; [\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\right\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}$$

Let

$$T := \left\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A) \;\middle|\; [\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\right\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\}$$

and assume

$$\begin{array}{l}
g : \blacktriangleright T \\
s : \left\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A) \;\middle|\; [\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\right\}
\end{array}$$

Note that we have, at type $\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\,A)$,

$$\begin{array}{rl}
[\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi & \Leftrightarrow [\neg\mathsf{nil}] \wedge \big([\mathsf{nil}] \vee \big([\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big)\big) \\
 & \Leftrightarrow \big([\neg\mathsf{nil}] \wedge [\mathsf{nil}]\big) \vee \big([\neg\mathsf{nil}] \wedge [\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big)
\end{array}$$

Since the modality $[\mathsf{fold}]$ preserves $\wedge$ and $\bot$ (Table 2), we have

$$\big([\neg\mathsf{nil}] \wedge [\mathsf{nil}]\big) \Rightarrow \bot$$

We apply the ($\vee$-E) rule on the refinement type of s. The branch of $[\neg\mathsf{nil}] \wedge [\mathsf{nil}]$ is dealt-with using the rule (ExF). It remains to handle the case of

$$s : \big\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\, A) \;\big|\; [\neg\mathsf{nil}] \wedge [\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi \wedge \bigcirc\Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big\}$$

Since the modalities $[\mathsf{fold}]$ and $[\mathsf{in}_1]$ preserve $\wedge$ we have

$$\mathsf{unfold}(s) : \big\{\mathbf{1} + \mathsf{Tree}^{\mathsf{g}}\, A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\, A) \;\big|\; [\mathsf{in}_1]\big([\pi_0]\varphi \wedge [\pi_1][\mathsf{next}]\Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big)\big\}$$

Using the typing rule (Inj$_1$-E) (Fig. 8) and Ex. E.46 we are left with showing

$$v ::^{\mathsf{g}} g \circledast \big(\mathsf{next}(\mathsf{append}^{\mathsf{g}}) \circledast xs \circledast [\ell, r]^{\mathsf{g}\blacktriangleright}\big) : \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

where

$$\begin{array}{lll}
xs & := \pi_1\ y & : \blacktriangleright \big\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\, A) \;\big|\; \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big\} \\
v & := \mathsf{label}^{\mathsf{g}}\ (\pi_0\ y) & : \{A \mid \varphi\} \\
\ell & := \mathsf{son}^{\mathsf{g}}_{\ell}\ (\pi_0\ y) & : \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\} \\
r & := \mathsf{son}^{\mathsf{g}}_{r}\ (\pi_0\ y) & : \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\}
\end{array}$$

assuming

$$y : \big\{\mathsf{Tree}^{\mathsf{g}}\, A \times \blacktriangleright \mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}^{\mathsf{g}}\, A) \;\big|\; [\pi_0]\varphi \wedge [\pi_1][\mathsf{next}]\Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big\}$$

It follows from Ex. E.30 and Ex. E.31 that

$$[\ell, r]^{\mathsf{g}\blacktriangleright} : \blacktriangleright \big\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}\, A) \;\big|\; [\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big\}$$

Hence, by Ex. E.33 and Ex. E.34 we obtain

$$\mathsf{next}(\mathsf{append}^{\mathsf{g}}) \circledast xs \circledast [\ell, r]^{\mathsf{g}\blacktriangleright} : \blacktriangleright \big\{\mathsf{CoList}^{\mathsf{g}}(\mathsf{Tree}\, A) \;\big|\; [\neg\mathsf{nil}] \wedge \Box^{\mathrm{fin}}[\mathsf{hd}]\forall\Box[\mathsf{lbl}]\varphi\big\}$$

and the result follows. $\Box$

Martin Hofmann's Algorithm We follow the presentation of [10] with some slight changes in terminology and notation. Consider the non-strictly positive type

$$\mathsf{Rou}^{\mathsf{g}}\, A := \mathsf{Fix}(X).\ \mathbf{1} + ((\blacktriangleright X \to \blacktriangleright A) \to A)$$

so that

$$\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) := \mathsf{Fix}(X).\ \mathbf{1} + ((\blacktriangleright X \to \blacktriangleright \mathsf{CoList}^{\mathsf{g}}\, A) \to \mathsf{CoList}^{\mathsf{g}}\, A)$$

The constructors of $\mathsf{Rou}^{\mathsf{g}}\, A$ are

$$\begin{array}{lll}
\mathsf{Over}^{\mathsf{g}} & := \mathsf{fold}(\mathsf{in}_0\langle\rangle) & : \mathsf{Rou}^{\mathsf{g}}\, A \\
\mathsf{Cont}^{\mathsf{g}} & := \lambda f.\mathsf{fold}(\mathsf{in}_1 f) & : \big((\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\, A \to \blacktriangleright A) \to A\big) \to \mathsf{Rou}^{\mathsf{g}}\, A
\end{array}$$

The following are two basic important functions on $\mathsf{Rou}^{\mathsf{g}}$:

$$\begin{array}{rl}\mathsf{unfold}\ : & \mathsf{Rou}^{\mathsf{g}}\,A \longrightarrow (\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\,A \to \blacktriangleright A) \longrightarrow \blacktriangleright A \\ := & \lambda c.\ \mathsf{case}\ c\ \mathsf{of} \\ & \quad \mid \mathsf{Over}^{\mathsf{g}}\ \mapsto\ \lambda k.\ k\ (\mathsf{next}\ \mathsf{Over}^{\mathsf{g}}) \\ & \quad \mid \mathsf{Cont}^{\mathsf{g}} f\ \mapsto\ \lambda k.\ \mathsf{next}(fk)\end{array}$$

$$\begin{array}{rl}\mathsf{extract}\ : & \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \longrightarrow \mathsf{CoList}^{\mathsf{g}}\,A \\ := & \mathsf{fix}(g).\lambda c.\ \mathsf{case}\ c\ \mathsf{of} \\ & \quad \mid \mathsf{Over}^{\mathsf{g}}\ \mapsto\ \mathsf{Nil}^{\mathsf{g}} \\ & \quad \mid \mathsf{Cont}^{\mathsf{g}} f\ \mapsto\ f g^{\circledast}\end{array}$$

where

$$g^{\circledast} := \lambda x.g \circledast x$$

We then let

$$\begin{array}{rl}\mathsf{bft}^{\mathsf{g}}\ : & \mathsf{Tree}^{\mathsf{g}}\,A \longrightarrow \mathsf{CoList}^{\mathsf{g}}\,A \\ := & \lambda t.\ \mathsf{extract}\ (\mathsf{bftaux}\ t\ \mathsf{Over}^{\mathsf{g}})\end{array}$$

$$\begin{array}{rl}\mathsf{bftaux}\ : & \mathsf{Tree}^{\mathsf{g}}\,A \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \\ := & \mathsf{fix}(g).\lambda t.\lambda c. \\ & \quad \mathsf{Cont}\left(\lambda k.\ (\mathsf{label}^{\mathsf{g}}\ t) ::^{\mathsf{g}} \mathsf{unfold}\ c\ \left(k \circ (g \circledast (\mathsf{son}^{\mathsf{g}}_{\ell} t))^{\circledast} \circ (g \circledast (\mathsf{son}^{\mathsf{g}}_{r} t))^{\circledast}\right)\right)\end{array}$$

Example E.51 ((Non) Emptiness).

$$\begin{array}{l}[\mathsf{ov}] := [\mathsf{fold}][\mathsf{in}_0]\top : \mathsf{Rou}^{\mathsf{g}}\,A \\ [\mathsf{ct}]\ := [\mathsf{fold}][\mathsf{in}_1]\top : \mathsf{Rou}^{\mathsf{g}}\,A\end{array}$$

Example E.52. Assuming $\varphi : A$, we let

$$[\mathsf{Rou}]\varphi := \nu\alpha.\ [\mathsf{fold}][\mathsf{in}_1](([\mathsf{next}]\alpha \mathrel{\|\!\!\to} [\mathsf{next}]\varphi) \mathrel{\|\!\!\to} \varphi) : \mathsf{Rou}^{\mathsf{g}}\,A$$

Then for $\varphi : \mathsf{CoList}^{\mathsf{g}}\,A$ we have

$$\mathsf{extract} : \{\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \mid [\mathsf{Rou}]\varphi\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid \varphi\}$$

Proof. Assume

$$\begin{array}{l}g : \blacktriangleright (\{\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \mid [\mathsf{Rou}]\varphi\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\,A \mid \varphi\}) \\ c : \{\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\,A) \mid [\mathsf{Rou}]\varphi\}\end{array}$$

and let

$$B := \mathsf{CoList}^{\mathsf{g}}\,A$$

Since

$$[\mathsf{Rou}]\varphi = \nu\alpha.\ [\mathsf{fold}][\mathsf{in}_1](([\mathsf{next}]\alpha \mathrel{\|\!\!\to} [\mathsf{next}]\varphi) \mathrel{\|\!\!\to} \varphi)$$

we have

$$(\mathsf{unfold}\ c) : \{\mathbf{1} + (\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\,B \to \blacktriangleright B) \to B \mid [\mathsf{in}_1](([\mathsf{next}][\mathsf{Rou}]\varphi \mathrel{\|\!\!\to} [\mathsf{next}]\varphi) \mathrel{\|\!\!\to} \varphi)\}$$

We can thus apply the (INJ$_1$-E) rule, which leads us to showing

$$f\ (\lambda x.\ g \circledast x) : \{B \mid \varphi\}$$

assuming

$$f : \{(\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\, B \to \blacktriangleright B) \to B \mid ([\mathsf{next}][\mathsf{Rou}]\varphi \Vdash\!\!\to [\mathsf{next}]\varphi) \Vdash\!\!\to \varphi\}$$

that is

$$f : (\blacktriangleright \{\mathsf{Rou}^{\mathsf{g}}\, B \mid [\mathsf{Rou}]\varphi\} \to \blacktriangleright \{B \mid \varphi\}) \longrightarrow \{B \mid \varphi\}$$

But this is trivial, by assumption on the type of g. □

Example E.53. Assuming $\varphi : A$ we have

$$\mathsf{unfold} : \mathsf{Rou}^{\mathsf{g}}\, A \longrightarrow \big(\blacktriangleright \mathsf{Rou}^{\mathsf{g}}\, A \longrightarrow \blacktriangleright \{A \mid \varphi\}\big) \longrightarrow \blacktriangleright \{A \mid \varphi\}$$

Proof. Assume

$$\begin{aligned} c &: \mathsf{Rou}^{\mathsf{g}}\, A \\ k &: \blacktriangleright \mathsf{Rou}^{\mathsf{g}}\, A \longrightarrow \blacktriangleright \{A \mid \varphi\} \\ f &: \big(\blacktriangleright \{\mathsf{Rou}^{\mathsf{g}}\, A \mid [\mathsf{Rou}]\varphi\} \longrightarrow \blacktriangleright \{A \mid \varphi\}\big) \longrightarrow \{A \mid \varphi\} \end{aligned}$$

Then we have

$$k\ (\mathsf{next}\ \mathsf{Over}^{\mathsf{g}}) : \blacktriangleright \{A \mid \varphi\}$$

Moreover, by subtyping we have

$$k : \blacktriangleright \{\mathsf{Rou}^{\mathsf{g}}\, A \mid [\mathsf{Rou}]\varphi\} \longrightarrow \blacktriangleright \{A \mid \varphi\}$$

so that

$$\mathsf{next}(f k) : \blacktriangleright \{A \mid \varphi\}$$

□

Example E.54. Assuming $\varphi : A$ we have

$$\mathsf{bft}^{\mathsf{g}} : \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\} \longrightarrow \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

Proof. It follows from the type of $\mathsf{extract}$ in Ex. E.52 that we are done if we show

$$\mathsf{bftaux} : \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\psi\} \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) \longrightarrow \{\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) \mid [\mathsf{Rou}]\Box[\mathsf{hd}]\psi\}$$

Let

$$T := \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\psi\} \longrightarrow \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) \longrightarrow \{\mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) \mid [\mathsf{Rou}]\Box[\mathsf{hd}]\psi\}$$

and assume

$$\begin{aligned} g &: \blacktriangleright T \\ t &: \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\} \\ c &: \mathsf{Rou}^{\mathsf{g}}(\mathsf{CoList}^{\mathsf{g}}\, A) \end{aligned}$$

Using Ex. E.46, let

$$\begin{array}{l} \ell := \mathsf{son}^{\mathsf{g}}_{\ell}\ t : \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\} \\ r := \mathsf{son}^{\mathsf{g}}_{r}\ t : \blacktriangleright \{\mathsf{Tree}^{\mathsf{g}}\, A \mid \forall\Box[\mathsf{lbl}]\varphi\} \end{array}$$

Since $(\mathsf{label}^{\mathsf{g}}\ t) : \{A \mid \varphi\}$, it follows from Ex. E.31 that we are done if we show

$$\mathsf{unfold}\ c\ \left(k \circ (g \circledast \ell)^{\circledast} \circ (g \circledast r)^{\circledast}\right) : \blacktriangleright \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

assuming

$$k : \blacktriangleright \{\mathsf{Rou}^{\mathsf{g}}\ (\mathsf{CoList}^{\mathsf{g}}\, A) \mid [\mathsf{Rou}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \blacktriangleright \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

But by Ex. E.53 we are done since

$$k \circ (g \circledast \ell)^{\circledast} \circ (g \circledast r)^{\circledast} : \blacktriangleright \mathsf{Rou}^{\mathsf{g}}\ (\mathsf{CoList}\, A) \longrightarrow \blacktriangleright \{\mathsf{CoList}^{\mathsf{g}}\, A \mid \Box[\mathsf{hd}]\varphi\}$$

□

F Proofs of §7

Note F.1. In §F.1–F.3 we assume formulae to have no free iteration variables. Free iteration variables in types are then always instantiated in the Adequacy Theorem F.16 (Thm. D.29, Thm. 7.7).

F.1 Correctness of the External and Internal Semantics

Proof of Lem. D.13.(1) (Lem. 7.2)

Lemma F.2. *If $\vdash^{A}_{\mathrm{c}} \varphi$ in full modal theory of Def. 6.2, then $\{\!|\varphi|\!\} = \boldsymbol{\Gamma}[\![A]\!]$.*

Lemma D.19 gives almost all the axioms and rules of Table 2 and Fig. 6, but for the $[\mathsf{ev}(-)]$ modality that we treat separately. We first treat the axioms of Table 2.

Lemma F.3. *If $\varphi : A$ is an axiom of Table 2, then $\{\!|\varphi|\!\}^{A} = [\![A]\!]$.*

Proof. Most of the axioms follow from Lem. D.19. Following Def. 4.4, we include the axioms marked **(C)** in Table 2. The cases of $[\mathsf{box}]$ are trivial and omitted.

Case of (C)**.** Since in each case, the map $\{\!|[\triangle]|\!\}$ preserves $\wedge$.

The case of $[\mathsf{ev}(-)]$ is treated directly:

$$\frac{}{\vdash^{B\to A} \left([\mathsf{ev}(\phi)]\psi \wedge [\mathsf{ev}(\phi)]\varphi\right) \quad\Longrightarrow\quad [\mathsf{ev}(\phi)](\psi \wedge \varphi)}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$ and assume that $x \in \{\!|[\mathsf{ev}(\phi)]\psi|\!\} \cap \{\!|[\mathsf{ev}(\phi)]\varphi|\!\}$. Let now $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y \in \{\!|\phi|\!\}$. We then have $\mathsf{ev} \circ \langle x, y\rangle \in \{\!|\psi|\!\} \cap \{\!|\varphi|\!\}$.

Case of (N)**.** Since $\{|[\pi_i]|\}$, $\{|[\mathsf{next}]|\}$ and $\{|[\mathsf{fold}]|\}$ are maps of Heyting algebras. The case of $[\mathsf{ev}(-)]$ is treated directly:

$$\frac{}{\vdash^{B\to A} [\mathsf{ev}(\phi)]\top}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$. Given $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y \in \{|\phi|\}$, we have $\mathsf{ev} \circ \langle x, y\rangle \in \boldsymbol{\Gamma}[\![A]\!] = \{|\top|\}$.

Case of (P)**.** Since $\{|[\pi_i]|\}$, $\{|[\mathsf{next}]|\}$ and $\{|[\mathsf{fold}]|\}$ are maps of Heyting algebras. As for $[\mathsf{in}_i]$, this follows from Lem. D.19.

Case of $(\mathsf{C}_\vee)$**.** By Lem. D.19.

Case of $(\mathsf{C}_\Rightarrow)$**.** Since $\{|[\pi_i]|\}$, $\{|[\mathsf{next}]|\}$ and $\{|[\mathsf{fold}]|\}$ are maps of Heyting algebras. ☐

In order to handle fixpoints, we have the usual monotonicity lemma w.r.t. set inclusion.

Lemma F.4. *Consider, for a formula* $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi$*, the map*

$$\{|\varphi|\} : \mathcal{P}(\boldsymbol{\Gamma}[\![A_1]\!]) \times \cdots \times \mathcal{P}(\boldsymbol{\Gamma}[\![A_k]\!]) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma}[\![A]\!]),\ v \longmapsto \{|\varphi|\}_v$$

For $i \in \{1, \dots, k\}$*, if* α_i Pos φ *(resp.* α_i Neg φ*), then w.r.t. set inclusion,* $\{|\varphi|\}$ *is monotone (resp. anti-monotone) in its ith argument.*

We can now turn to the proof of Lemma F.2.

Proof (Proof of Lemma F.2). By induction on $\vdash^A \varphi$. The rules of intuitionistic propositional logic (Fig. 16) as well as of (CL) are trivial and omitted.

Case of

$$(\mathsf{RM})\ \frac{\vdash \psi \Rightarrow \varphi}{\vdash [\triangle]\psi \Rightarrow [\triangle]\varphi}$$

By Lem. D.19, this holds for $[\pi_i]$, $[\mathsf{next}]$ and $[\mathsf{fold}]$ since $\{|[\pi_i]|\}$, $\{|[\mathsf{next}]|\}$ and $\{|[\mathsf{fold}]|\}$ are maps of Heyting algebras. As for $[\mathsf{in}_i]$, this follows from the fact that $\{|[\mathsf{in}_i]|\}$ preserves implications as it preserves $\vee$.
The case of $[\mathsf{ev}(-)]$ is treated directly:

$$\frac{\vdash^A \psi \ \Rightarrow\ \varphi}{\vdash^{B\to A} [\mathsf{ev}(\phi)]\psi \ \Rightarrow\ [\mathsf{ev}(\phi)]\varphi}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$. Given $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y \in \{|\phi|\}$, we have $\mathsf{ev} \circ \langle x, y\rangle \in \{|\psi|\}$, so that $\mathsf{ev} \circ \langle x, y\rangle \in \{|\varphi|\}$ since $\{|\psi|\} \subseteq \{|\varphi|\}$.

Case of

$$\frac{\vdash^A_{\mathsf{c}} \varphi}{\vdash^{\blacksquare A} [\mathsf{box}]\varphi}$$

Trivial.

Case of

$$\frac{\vdash^B \psi \Rightarrow \phi \qquad \vdash \varphi : A}{\vdash^{B \to A} [\mathsf{ev}(\phi)]\varphi \Rightarrow [\mathsf{ev}(\psi)]\varphi}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$ and assume that $x \in \{\![[\mathsf{ev}(\phi)]\varphi]\!\}$. Let furthermore $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y \in \{\!|\psi|\!\}$. We have to show $\mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}$. By induction hypothesis we have $y \in \{\!|\psi \Rightarrow \phi|\!\}$, so that $y \in \{\!|\phi|\!\}$. But this implies $\mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}$ since $x \in \{\!|[\mathsf{ev}(\phi)]\varphi|\!\}$.

Case of

$$\frac{}{\vdash^{B \to A} ([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi) \Rightarrow [\mathsf{ev}(\psi_0 \vee \psi_1)]\varphi}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$ and assume that $x \in \{\!|([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi)|\!\}$. Let furthermore $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y \in \{\!|\psi_0 \vee \psi_1|\!\}$. We have to show $\mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}$. But if $y \in \{\!|\psi_0|\!\}$ then we are done since $x \in \{\!|[\mathsf{ev}(\psi_0)]\varphi|\!\}$, and similarly if $y \in \{\!|\psi_1|\!\}$.

Case of

$$\frac{}{\vdash^{A_0 + A_1} \big([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\big) \quad \wedge \quad \neg\big([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\big)}$$

Consider $x \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \simeq \boldsymbol{\Gamma}[\![A_0]\!] + \boldsymbol{\Gamma}[\![A_1]\!]$ (via Lem. D.2). Hence $x = \mathsf{in}_i(y)$ for some $y \in \boldsymbol{\Gamma}[\![A_i]\!]$ and we have $x \in \{\!|[\mathsf{in}_i]\top|\!\}$. Moreover, since the injections in_0 and in_1 have disjoint images, we have $\{\!|[\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top|\!\} = \emptyset$ so $x \in \{\!|\neg([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top)|\!\}$.

Case of

$$\frac{}{\vdash^{A_0 + A_1} [\mathsf{in}_i]\top \quad \Rightarrow \quad (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)}$$

Let $x \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \simeq \boldsymbol{\Gamma}[\![A_0]\!] + \boldsymbol{\Gamma}[\![A_1]\!]$, and assume $x \in \{\!|[\mathsf{in}_i]\top|\!\}$, so that $x = \mathsf{in}_i(y)$ for some (unique) $y \in \boldsymbol{\Gamma}[\![A_i]\!]$. We show

$$x \in \{\!|\neg[\mathsf{in}_i]\varphi \;\Rightarrow\; [\mathsf{in}_i]\neg\varphi|\!\} \qquad \text{and} \qquad x \in \{\!|[\mathsf{in}_i]\neg\varphi \;\Rightarrow\; \neg[\mathsf{in}_i]\varphi|\!\}$$

For the former, assume $x \notin \{\!|[\mathsf{in}_i]\varphi|\!\}$. Since y is unique such that $x = \mathsf{in}_i(y)$, we have $y \notin \{\!|\varphi|\!\}$. But this implies $y \in \{\!|\neg\varphi|\!\}$ and we are done.
For the latter, assume $x \in \{\!|[\mathsf{in}_i]\neg\varphi|\!\}$. Assume toward a contradiction that $x \in \{\!|[\mathsf{in}_i]\varphi|\!\}$. Since y is unique such that $x = \mathsf{in}_i(y)$, we have both $y \notin \{\!|\varphi|\!\}$ and $y \in \{\!|\varphi|\!\}$, a contradiction.

Cases of

$$\frac{}{\vdash^A \nu^{\mathtt{0}}\alpha\varphi \;\Leftrightarrow\; \top} \qquad \frac{}{\vdash^A \nu^{\mathtt{t}+\mathtt{1}}\alpha\varphi \;\Leftrightarrow\; \varphi[\nu^{\mathtt{t}}\alpha\varphi/\alpha]} \qquad \frac{}{\vdash^A \mu^{\mathtt{0}}\alpha\varphi \;\Leftrightarrow\; \bot} \qquad \frac{}{\vdash^A \mu^{\mathtt{t}+\mathtt{1}}\alpha\varphi \;\Leftrightarrow\; \varphi[\mu^{\mathtt{t}}\alpha\varphi/\alpha]}$$

By definition of $\{\!|\theta^{\mathtt{t}}\alpha\varphi|\!\}$.

Cases of

$$\frac{[\![\mathtt{t}]\!] \geq [\![\mathtt{u}]\!]}{\vdash^A \nu^{\mathtt{t}}\alpha\varphi \;\Rightarrow\; \nu^{\mathtt{u}}\alpha\varphi} \qquad \frac{[\![\mathtt{t}]\!] \leq [\![\mathtt{u}]\!]}{\vdash^A \mu^{\mathtt{t}}\alpha\varphi \;\Rightarrow\; \mu^{\mathtt{u}}\alpha\varphi}$$

These cases follows from Lem. F.4 (in $\theta^{\mathtt{t}}\alpha\varphi$ we assume that α is positive in φ) and the definition of $\{\!|\theta^{\mathtt{t}}\alpha\varphi|\!\}$.

Cases of

$$\frac{}{\vdash^A \nu\alpha\varphi \;\Rightarrow\; \varphi[\nu\alpha\varphi/\alpha]} \qquad \frac{\vdash^A \psi \;\Rightarrow\; \varphi[\psi/\alpha]}{\vdash^A \psi \;\Rightarrow\; \nu\alpha\varphi} \qquad \frac{}{\vdash^A \varphi[\mu\alpha\varphi/\alpha] \Rightarrow \mu\alpha\varphi} \qquad \frac{\vdash^A \varphi[\psi/\alpha] \Rightarrow \psi}{\vdash^A \mu\alpha\varphi \Rightarrow \psi}$$

By Lem. F.4 and the Knaster-Tarski Theorem.

Cases of

$$\frac{}{\vdash^A \mu^{\mathtt{t}}\alpha\varphi(\alpha) \;\Rightarrow\; \mu\alpha\varphi(\alpha)} \qquad \frac{}{\vdash^A \nu\alpha\varphi(\alpha) \;\Rightarrow\; \nu^{\mathtt{t}}\alpha\varphi(\alpha)}$$

We show by induction on $m \in \mathbb{N}$ that

$$\{|\mu^{\mathtt{m}}\alpha\varphi(\alpha)|\} \subseteq \{|\mu\alpha\varphi(\alpha)|\} \qquad \text{and} \qquad \{|\nu\alpha\varphi(\alpha)|\} \subseteq \{|\nu^{\mathtt{m}}\alpha\varphi(\alpha)|\}$$

The base case $m = 0$ is trivial since

$$\{|\mu^0\alpha\varphi(\alpha)|\} = \{|\bot|\} \qquad \text{and} \qquad \{|\nu^0\alpha\varphi(\alpha)|\} = \{|\top|\}$$

For the induction step we have

$$\{|\mu^{\mathtt{m}+1}\alpha\varphi(\alpha)|\} = \{|\varphi(\mu^{\mathtt{m}}\alpha\varphi(\alpha))|\} \qquad \text{and} \qquad \{|\nu^{\mathtt{m}+1}\alpha\varphi(\alpha)|\} = \{|\varphi(\nu^{\mathtt{m}}\alpha\varphi(\alpha)|\}$$

So the induction hypothesis together with Lem. F.4 gives

$$\{|\mu^{\mathtt{m}+1}\alpha\varphi(\alpha)|\} \subseteq \{|\varphi(\mu\alpha\varphi(\alpha))|\} \qquad \text{and} \qquad \{|\varphi(\nu\alpha\varphi(\alpha))|\} \subseteq \{|\varphi(\nu^{\mathtt{m}}\alpha\varphi(\alpha))|\}$$

and we are done since by the Knaster-Tarski Theorem, we have

$$\{|\varphi(\mu\alpha\varphi(\alpha))|\} = \{|\mu\alpha\varphi(\alpha)|\} \qquad \text{and} \qquad \{|\varphi(\nu\alpha\varphi(\alpha))|\} = \{|\nu\alpha\varphi(\alpha)|\}$$

$\square$

Proof of Lem. D.13.(2) (Lem. 7.2)

Lemma F.5. *If* $\vdash^A \varphi$ *in full modal theory of Def. 6.2, then* $[\![\varphi]\!] = [\![A]\!]$.

Corollary D.17 gives almost everything we need for the semantic correctness of the modal theory. We begin with the axioms of Table 2.

Lemma F.6. *If* $\varphi : A$ *is an axiom of Table 2, then* $[\![\varphi]\!]^A = [\![A]\!]$.

Proof. Most of the axioms follow from Cor. D.17.

Case of (C)**.** Since in each case, the map $[\![[\triangle]]\!]$ preserves $\wedge$.

Case of (N)**.** Since in each case, the map $[\![[\triangle]]\!]$ preserves $\top$ (recall that axiom is *not* assumed for $[\mathsf{in}_i]$).

Case of (P)**.** The result for $[\pi_i]$, $[\mathsf{fold}]$ and $[\mathsf{box}]$ follows from the fact that $[\![[\pi_i]]\!]$, $[\![[\mathsf{fold}]]\!]$ and $[\![[\mathsf{box}]]\!]$ are maps of Heyting algebras.

As for $[\mathsf{in}_i]$, it follows from the fact that $[\![[\mathsf{in}_i]]\!]$ preserves $\bot$ (Cor. D.17).

Case of ($\mathsf{C}_\vee$)**.** By Cor. D.17.

Case of $(\mathsf{C}_{\Rightarrow})$**.** Since $[\![[\pi_i]]\!]$, $[\![[\mathsf{fold}]]\!]$ and $[\![[\mathsf{box}]]\!]$ are maps of Heyting algebras. □

In order to handle fixpoints, we have the usual monotonicity property w.r.t. subobject posets.

Lemma F.7. *Consider, for a formula* $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi$*, the map*

$$[\![\varphi]\!] : \mathrm{Sub}([\![A_1]\!]) \times \dots \times \mathrm{Sub}([\![A_k]\!]) \longrightarrow \mathrm{Sub}([\![A]\!]),\ v \longmapsto [\![\varphi]\!]_v$$

For $i \in \{1, \dots, k\}$*, if* α_i Pos φ *(resp.* α_i Neg φ*), then w.r.t. subobjects posets,* $[\![\varphi]\!]$ *is monotone (resp. anti-monotone) in its ith argument.*

We can now turn to the proof of Lemma F.5.

Proof (Proof of Lemma F.5). By induction on $\vdash^A \varphi$. The rules of Fig. 16 follow from the fact that in a topos, the subobjects of a given object form a Heyting algebra.

Case of

$$(\mathsf{RM})\ \frac{\vdash \psi \Rightarrow \varphi}{\vdash [\triangle]\psi \Rightarrow [\triangle]\varphi}$$

The result holds for $[\pi_i]$, $[\mathsf{fold}]$ and $[\mathsf{box}]$ since $[\![[\pi_i]]\!]$, $[\![[\mathsf{fold}]]\!]$ and $[\![[\mathsf{box}]]\!]$ are maps of Heyting algebras.
As for $[\mathsf{in}_i]$, $[\mathsf{next}]$ and $[\mathsf{ev}(-)]$, this follows from the fact that the maps $[\![[\mathsf{in}_i]]\!]$, $[\![[\mathsf{next}]]\!]$ and $[\![[\mathsf{ev}(-)]]\!]$ preserve implications since they preserve $\wedge$.

Case of

$$\frac{\vdash^A_c \varphi}{\vdash^{\blacksquare A} [\mathsf{box}]\varphi}$$

By Cor. D.17.

Case of

$$\frac{\vdash^B \psi \Rightarrow \phi \qquad \vdash \varphi : A}{\vdash^{B \to A} [\mathsf{ev}(\phi)]\varphi \Rightarrow [\mathsf{ev}(\psi)]\varphi}$$

This case can be seen as following (via Lem. D.15) from the definition of $[\![[\mathsf{ev}(-)]]\!]$. A direct argument is nevertheless possible. Let $t \in [\![B \to A]\!](n)$. Let $k \leq n$ such that $t{\uparrow}k \Vdash_k [\mathsf{ev}(\phi)]\varphi$. Let furthermore $\ell \leq k$ and $u \in [\![B]\!](\ell)$ such that $u \Vdash^B_\ell \psi$. We have to show $\mathsf{ev} \circ \langle t{\uparrow}\ell, u\rangle \Vdash^A_\ell \varphi$. By induction hypothesis we have $u \Vdash^B_\ell \psi \Rightarrow \phi$, so that $u \Vdash^B_\ell \phi$. But this implies $\mathsf{ev} \circ \langle t{\uparrow}\ell, u\rangle \Vdash^A_\ell \varphi$ since $t{\uparrow}k \Vdash_k [\mathsf{ev}(\phi)]\varphi$.

Case of

$$\frac{}{\vdash^{B \to A} ([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi) \Rightarrow [\mathsf{ev}(\psi_0 \vee \psi_1)]\varphi}$$

Let $t \in [\![B \to A]\!](n)$. Let $k \leq n$ such that $t{\uparrow}k \Vdash_k ([\mathsf{ev}(\psi_0)]\varphi \wedge [\mathsf{ev}(\psi_1)]\varphi)$. Let furthermore $\ell \leq k$ and $u \in [\![B]\!](\ell)$ such that $u \Vdash^B_\ell \psi_0 \vee \psi_1$. We have to show $\mathsf{ev} \circ \langle t{\uparrow}\ell, u\rangle \Vdash^A_\ell \varphi$. If $u \Vdash^B_\ell \psi_0$, then we are done since $t \Vdash_k [\mathsf{ev}(\psi_0)]\varphi$, and similarly if $u \Vdash^B_\ell \psi_1$.

Case of

$$\overline{\vdash^{A_0+A_1} \big([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\big) \quad\wedge\quad \neg\big([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\big)}$$

Write $A = A_0 + A_1$ and consider $t \in [\![A_0 + A_1]\!](n)$. Hence $t = \mathsf{in}_i(u)$ for some $u \in [\![A_i]\!](n)$ and we have $t \Vdash_n [\mathsf{in}_i]\top$. Moreover, since the injections in_0 and in_1 have disjoint images, we have $[\![[\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top]\!](k) = \emptyset$ for all $k > 0$ so $t \Vdash_n \neg([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top)$.

Case of

$$\overline{\vdash^{A_0+A_1} [\mathsf{in}_i]\top \quad\Rightarrow\quad (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)}$$

Write $A = A_0 + A_1$. Let $t \in [\![A_0 + A_1]\!](n)$, and let $k \leq n$ such that $t{\uparrow}k \Vdash_k [\mathsf{in}_i]\top$, so that we have $t{\uparrow}k = \mathsf{in}_i(u)$ for some (unique) $u \in [\![A_i]\!](k)$. We show

$$t \Vdash_k^{A_0+A_1} \neg[\mathsf{in}_i]\varphi \;\Rightarrow\; [\mathsf{in}_i]\neg\varphi \qquad\text{and}\qquad t \Vdash_k^{A_0+A_1} [\mathsf{in}_i]\neg\varphi \;\Rightarrow\; \neg[\mathsf{in}_i]\varphi$$

For the former, let $\ell \leq k$ such that $t{\uparrow}\ell = (t{\uparrow}k){\uparrow}\ell \Vdash_\ell \neg[\mathsf{in}_i]\varphi$, that is such that $t{\uparrow}m \nVdash_m [\mathsf{in}_i]\varphi$ for all $m \leq \ell$. We show $t{\uparrow}\ell \Vdash_\ell [\mathsf{in}_i]\neg\varphi$. Hence we are done if $u{\uparrow}m \nVdash_m \varphi$ for all $m \leq \ell$. But if $u{\uparrow}m \Vdash_m \varphi$, then we would have $t{\uparrow}m = \mathsf{in}_i(u{\uparrow}m) \Vdash_m [\mathsf{in}_i]\varphi$, a contradiction.
For the latter, let $\ell \leq k$ such that $t{\uparrow}\ell \Vdash_\ell [\mathsf{in}_i]\neg\varphi$. We have to show $t{\uparrow}\ell \Vdash_\ell \neg[\mathsf{in}_i]\varphi$, that is $t{\uparrow}m \nVdash_m [\mathsf{in}_i]\varphi$ for all $m \leq \ell$. So assume $t{\uparrow}\tilde{m} \Vdash_{\tilde{m}} [\mathsf{in}_i]\varphi$ for some $\tilde{m} \leq \ell$. Hence, there is $u' \in [\![A_i]\!](\tilde{m})$ such that $t{\uparrow}\tilde{m} = \mathsf{in}_i(u')$ and $u' \Vdash_{\tilde{m}} \varphi$. But we have $u' = u{\uparrow}\tilde{m}$. On the other hand, since $t{\uparrow}\ell \Vdash_\ell [\mathsf{in}_i]\neg\varphi$, there is some $u'' \in [\![A_i]\!](\ell)$ such that $t{\uparrow}\ell = \mathsf{in}_i(u'')$ and $u''{\uparrow}m \nVdash_m \varphi$ for all $m \leq \ell$. But we also have $u''{\uparrow}\tilde{m} = u{\uparrow}\tilde{m}$, thus contradicting $u{\uparrow}\tilde{m} \Vdash_{\tilde{m}} \varphi$.

Cases of

$$\overline{\vdash^A \nu^0\alpha\varphi \;\Leftrightarrow\; \top} \qquad \overline{\vdash^A \nu^{\mathtt{t}+1}\alpha\varphi \;\Leftrightarrow\; \varphi[\nu^{\mathtt{t}}\alpha\varphi/\alpha]} \qquad \overline{\vdash^A \mu^0\alpha\varphi \;\Leftrightarrow\; \bot} \qquad \overline{\vdash^A \mu^{\mathtt{t}+1}\alpha\varphi \;\Leftrightarrow\; \varphi[\mu^{\mathtt{t}}\alpha\varphi/\alpha]}$$

By definition of $[\![\theta^{\mathtt{t}}\alpha\varphi]\!]$.

Cases of

$$\frac{[\![\mathtt{t}]\!] \geq [\![\mathtt{u}]\!]}{\vdash^A \nu^{\mathtt{t}}\alpha\varphi \;\Rightarrow\; \nu^{\mathtt{u}}\alpha\varphi} \qquad \frac{[\![\mathtt{t}]\!] \leq [\![\mathtt{u}]\!]}{\vdash^A \mu^{\mathtt{t}}\alpha\varphi \;\Rightarrow\; \mu^{\mathtt{u}}\alpha\varphi}$$

These cases follows from Lem. F.7 (in $\theta^{\mathtt{t}}\alpha\varphi$ we assume that α is positive in φ) and the definition of $[\![\theta^{\mathtt{t}}\alpha\varphi]\!]$.

Cases of

$$\overline{\vdash^A \nu\alpha\varphi \quad\Rightarrow\quad \varphi[\nu\alpha\varphi/\alpha]} \qquad \frac{\vdash^A \psi \quad\Rightarrow\quad \varphi[\psi/\alpha]}{\vdash^A \psi \quad\Rightarrow\quad \nu\alpha\varphi} \qquad \overline{\vdash^A \varphi[\mu\alpha\varphi/\alpha] \Rightarrow \mu\alpha\varphi} \qquad \frac{\vdash^A \varphi[\psi/\alpha] \Rightarrow \psi}{\vdash^A \mu\alpha\varphi \Rightarrow \psi}$$

By Lem. F.7 and the Knaster-Tarski Theorem, since subobject lattices of $\mathcal{S}$ are complete ([52, Prop. I.8.5]).

Cases of

$$\overline{\vdash^A \mu^{\mathtt{t}}\alpha\varphi(\alpha) \;\Rightarrow\; \mu\alpha\varphi(\alpha)} \qquad \overline{\vdash^A \nu\alpha\varphi(\alpha) \;\Rightarrow\; \nu^{\mathtt{t}}\alpha\varphi(\alpha)}$$

Similar to the same case in the proof of Lem. F.2. $\square$

F.2 The Safe Fragment

Lemma F.8 (Lem. D.21). *The greatest fixpoint of a Scott cocontinuous function $f : L \to L$ is given by*

$$\nu(f) := \bigwedge_{n\in\mathbb{N}} f^n(\top)$$

Proof. That $\nu(f)$ is a fixpoint of f follows from the continuity of f and the fact that the set $\{f^n(\top) \mid \in \mathbb{N}\}$ is codirected, which in turn follows from the fact that f is monotone. In order to show that $\nu(f)$ is the greatest fixpoint of f, recall that the greatest fixpoint of f is in any case given by

$$b := \bigvee \{a \in L \mid a \leq f(a)\}$$

We trivially have $\nu(f) \leq b$ as $\nu(f)$ is a fixpoint of f. For the revere inequality, for all a such that $a \leq f(a)$, it follows by induction on $n \in \mathbb{N}$ and from the monotony of f that we have $a \leq f^n(\top)$ for all $n \in \mathbb{N}$. Hence $a \leq \nu(f)$ for all a such that $a \leq f(a)$, which in turn gives $b \leq \nu(f)$. □

Lemma F.9 (Lem. D.22). *Consider a safe formula $\alpha_1 : P_1^+, \dots, \alpha_k : P_k^+ \vdash \varphi : P^+$. The following two functions are Scott-cocontinuous:*

$$\begin{array}{c} [\![\varphi]\!] : \mathrm{Sub}([\![P_1^+]\!]) \times \dots \times \mathrm{Sub}([\![P_k^+]\!]) \longrightarrow \mathrm{Sub}([\![P^+]\!]),\ v \longmapsto [\![\varphi]\!]_v \\ \{\![\varphi]\!\} : \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]) \times \dots \times \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!]) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]),\ v \longmapsto \{\![\varphi]\!\}_v \end{array}$$

Proof. In both cases, monotony w.r.t. lattice order follows by an easy induction from the positivity of safe formulae. We now turn to preservation of codirected meets. We first consider the case of $\{\![\varphi]\!\}$. We reason by induction on φ.

Cases of α, $\top$, $\bot$.
Trivial.

Case of $\varphi \wedge \psi$.
Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$\{\![\varphi \wedge \psi]\!\}\left(\bigcap D_1, \dots, \bigcap D_k\right) \quad = \quad \bigcap \{\![\varphi]\!\}(D_1, \dots, D_k) \cap \bigcap \{\![\psi]\!\}(D_1, \dots, D_k)$$

and the result is trivial.

Case of $\varphi \vee \psi$.
This is the interesting case. Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$\{\![\varphi \wedge \psi]\!\}\left(\bigcap D_1, \dots, \bigcap D_k\right) \quad = \quad \bigcap \{\![\varphi]\!\}(D_1, \dots, D_k) \cup \bigcap \{\![\psi]\!\}(D_1, \dots, D_k)$$

We then trivially get

$$\bigcap \{\![\varphi]\!\}(D_1, \dots, D_k) \cup \bigcap \{\![\psi]\!\}(D_1, \dots, D_k) \quad \subseteq \quad \bigcap \{\![\varphi \vee \psi]\!\}(D_1, \dots, D_k)$$

It remains to show the converse direction

$$\bigcap \{|\varphi \vee \psi|\} (D_1, \dots, D_k) \quad \subseteq \quad \bigcap \{|\varphi|\} (D_1, \dots, D_k) \cup \bigcap \{|\psi|\} (D_1, \dots, D_k)$$

So let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ such that $x \in \{|\varphi \vee \psi|\} (S_1, \dots, S_k)$ for every $S_1 \in D_1, \dots, S_k \in D_k$. Assume toward a contradiction that there are $S_1 \in D_1, \dots, S_k \in D_k$ such that $x \notin \{|\varphi|\} (S_1, \dots, S_k)$ and that there are $S'_1 \in D_1, \dots, S'_k \in D_k$ such that $x \notin \{|\psi|\} (S'_1, \dots, S'_k)$. Since the D_i's are codirected for inclusion, there are $S''_1 \in D_1, \dots, S''_k \in D_k$ such that $S''_i \subseteq S_i \cap S'_i$ for $i = 1, \dots, k$. By monotonicity w.r.t. inclusion, we have $x \notin \{|\varphi|\} (S''_1, \dots, S''_k)$ and $x \notin \{|\psi|\} (S''_1, \dots, S''_k)$. But this implies $x \notin \{|\varphi \vee \psi|\} (S''_1, \dots, S''_k)$, a contradiction.

Case of $[\pi_i]\varphi$.

Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = Q_0^+ \times Q_1^+$. Then we are done since by induction hypothesis

$$\begin{array}{l} \quad x \in \{|[\pi_i]\varphi|\} (\bigcap D_1, \dots, \bigcap D_k) \\ \text{iff } \pi_i \circ x \in \{|\varphi|\} (\bigcap D_1, \dots, \bigcap D_k) \\ \text{iff } \pi_i \circ x \in \bigcap \{|\varphi|\} (D_1, \dots, D_k) \\ \text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k, \quad \pi_i \circ x \in \{|\varphi|\} (D_1, \dots, D_k) \\ \text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k, \quad x \in \{|[\pi_i]\varphi|\} (D_1, \dots, D_k) \\ \text{iff } x \in \bigcap \{|[\pi_i]\varphi|\} (D_1, \dots, D_k) \end{array}$$

Case of $[\mathsf{in}_i]\varphi$.

Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = Q_0^+ + Q_1^+$. By Lem. D.2, we have $x = \mathsf{in}_j \circ y$ for some unique $j \in \{0, 1\}$ and $y \in \boldsymbol{\Gamma}[\![Q_j^+]\!]$. Then we are done since by induction hypothesis we have $x \in \{|[\mathsf{in}_i]\varphi|\} (\bigcap D_1, \dots, \bigcap D_k)$

$$\begin{array}{ll} \text{iff } j = i \text{ and } y \in \{|\varphi|\} (\bigcap D_1, \dots, \bigcap D_k) & \\ \text{iff } j = i \text{ and } y \in \bigcap \{|\varphi|\} (D_1, \dots, D_k) & \\ \text{iff } j = i \text{ and } \forall S_1 \in D_1, \dots, S_k \in D_k, \quad y \in \{|\varphi|\} (D_1, \dots, D_k) & \\ \text{iff} \qquad\qquad \forall S_1 \in D_1, \dots, S_k \in D_k, \quad x \in \{|[\mathsf{in}_i]\varphi|\} (D_1, \dots, D_k) & \\ \text{iff} \qquad\qquad x \in \bigcap \{|[\mathsf{in}_i]\varphi|\} (D_1, \dots, D_k) & \end{array}$$

Case of $[\mathsf{next}]\varphi$.

Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = \blacktriangleright Q^+$. By Lem. D.2, we have $x = \mathsf{next} \circ y$ for some unique $y \in \boldsymbol{\Gamma}[\![Q^+]\!]$. Then we are done since by induction hypothesis we have

$$\begin{array}{l} \quad x \in \{|[\mathsf{next}]\varphi|\} (\bigcap D_1, \dots, \bigcap D_k) \\ \text{iff } y \in \{|\varphi|\} (\bigcap D_1, \dots, \bigcap D_k) \\ \text{iff } y \in \bigcap \{|\varphi|\} (D_1, \dots, D_k) \\ \text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k, \quad y \in \{|\varphi|\} (D_1, \dots, D_k) \\ \text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k, \quad x \in \{|[\mathsf{next}]\varphi|\} (D_1, \dots, D_k) \\ \text{iff } x \in \bigcap \{|[\mathsf{next}]\varphi|\} (D_1, \dots, D_k) \end{array}$$

Case of $[\mathsf{fold}]\varphi$.

This case is dealt-with similarly as that of $[\pi_i]$.

Case of $[\mathsf{box}]\varphi$.
Trivial since φ is required to be closed.

Case of $[\mathsf{ev}(\psi)]\varphi$.
Note that ψ is assumed to be closed since $[\mathsf{ev}(\psi)]\varphi$ is safe. Let $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = R^+ \to Q^+$. Then we are done since by induction hypothesis we have

$$\begin{array}{l}
x \in \{\!|[\mathsf{ev}(\psi)]\varphi|\!\}\,(\bigcap D_1, \dots, \bigcap D_k) \\
\text{iff } \forall y \in \{\!|\psi|\!\}\,,\ \mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}\,(\bigcap D_1, \dots, \bigcap D_k) \\
\text{iff } \forall y \in \{\!|\psi|\!\}\,,\ \mathsf{ev} \circ \langle x, y\rangle \in \bigcap \{\!|\varphi|\!\}\,(D_1, \dots, D_k) \\
\text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k,\ \forall y \in \{\!|\psi|\!\}\,,\ \mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}\,(S_1, \dots, S_k) \\
\text{iff } \forall S_1 \in D_1, \dots, S_k \in D_k,\ x \in \{\!|[\mathsf{ev}(\psi)]\varphi|\!\}\,(S_1, \dots, S_k) \\
\text{iff } x \in \bigcap \{\!|[\mathsf{ev}(\psi)]\varphi|\!\}\,(D_1, \dots, D_k)
\end{array}$$

Cases of $\theta^{\mathsf{t}}\alpha\varphi$.
By induction hypothesis, the function

$$\{\!|\varphi|\!\} \quad : \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]) \times \cdots \times \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!]) \times \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \quad \longrightarrow \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]), \quad v, S \longmapsto \{\!|\varphi|\!\}_{v[S/\alpha]}$$

is Scott-cocontinuous. Hence by Lem. F.8, for $S_1 \in \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, S_k \in \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ we have

$$\{\!|\nu^{\mathtt{m}}\alpha\varphi|\!\}\,(S_1, \dots, S_k) \quad = \quad (\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^m(\top)$$

where

$$(\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^{m+1}(\top) \quad := \quad \{\!|\varphi|\!\}\,\big(S_1, \dots, S_k, (\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^m(\top)\big)$$

and where $(\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^0(\top) := \top$ and $(\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^0(\bot) := \bot$. An easy induction on $m \in \mathbb{N}$ then shows that each function

$$(\{\!|\varphi|\!\}\,(-, \dots, -))^m(\top) : \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]) \times \cdots \times \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!]) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!])$$

is Scott-cocontinuous.

Case of $\nu\alpha\varphi$.
By induction hypothesis, the function

$$\{\!|\varphi|\!\} \quad : \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]) \times \cdots \times \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!]) \times \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \quad \longrightarrow \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]), \quad v, S \longmapsto \{\!|\varphi|\!\}_{v[S/\alpha]}$$

is Scott-cocontinuous. Hence by Lem. F.8, for $S_1 \in \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, S_k \in \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$ we have

$$\{\!|\nu\alpha.\varphi|\!\}\,(S_1, \dots, S_k) \quad = \quad \bigcap_{n \in \mathbb{N}} (\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^n(\top)$$

where $(\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^0(\top) := \top$ and

$$(\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^{n+1}(\top) \quad := \quad \{\!|\varphi|\!\}\,\big(S_1, \dots, S_k, (\{\!|\varphi|\!\}\,(S_1, \dots, S_k))^n(\top)\big)$$

An easy induction on n shows that each function

$$(\{|\varphi|\}(-,\dots,-))^n(\top) \quad : \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]) \times \cdots \times \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!]) \quad \longrightarrow \quad \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!])$$

is Scott-cocontinuous.

Consider now codirected $D_1 \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![P_k^+]\!])$. Then we are done since

$$\begin{aligned}
\{|\nu\alpha.\varphi|\}(\textstyle\bigcap D_1,\dots,\bigcap D_k) &= \textstyle\bigcap_{n\in\mathbb{N}}(\{|\varphi|\}(\bigcap D_1,\dots,\bigcap D_k))^n(\top) \\
&= \textstyle\bigcap_{n\in\mathbb{N}}\bigcap(\{|\varphi|\}(D_1,\dots,D_k))^n(\top) \\
&= \textstyle\bigcap\bigcap_{n\in\mathbb{N}}(\{|\varphi|\}(D_1,\dots,D_k))^n(\top) \\
&= \textstyle\bigcap\{|\nu\alpha.\varphi|\}(D_1,\dots,D_k)
\end{aligned}$$

Case of $\mu\alpha\varphi$.

This case cannot occur since $\mu\alpha\varphi$ is not safe.

We now turn to the case of $[\![\varphi]\!]$. Most of cases are similar to those for $\{|\varphi|\}$. Also, note that

$$[\![\varphi]\!] \quad : \quad \mathrm{Sub}([\![P_1^+]\!]) \times \cdots \times \mathrm{Sub}([\![P_k^+]\!]) \quad \longrightarrow \quad \mathrm{Sub}([\![P^+]\!])$$

being Scott-continuous means that for $D_1 \subseteq \mathrm{Sub}([\![P_1^+]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P_k^+]\!])$ codirected w.r.t. subobject lattice orders, we have

$$[\![\varphi]\!](\textstyle\bigwedge D_1,\dots,\bigwedge D_k) \quad = \quad \textstyle\bigwedge[\![\varphi]\!](D_1,\dots,D_k)$$

But since meets in subobject lattices of $\mathcal{S}$ are pointwise, the above is equivalent to have, for all $n > 0$ that

$$[\![\varphi]\!](\textstyle\bigwedge D_1,\dots,\bigwedge D_k)(n) \quad = \quad \textstyle\bigcap[\![\varphi]\!](D_1,\dots,D_k)(n)$$

Cases of α, $\top$, $\bot$.

Trivial.

Case of $\varphi \wedge \psi$.

Let $D_1 \subseteq \mathrm{Sub}([\![P_1^+]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$[\![\varphi\wedge\psi]\!](\textstyle\bigwedge D_1,\dots,\bigwedge D_k) \quad = \quad \textstyle\bigwedge[\![\varphi]\!](D_1,\dots,D_k) \;\wedge\; \bigwedge[\![\psi]\!](D_1,\dots,D_k)$$

and the result is trivial.

Case of $\varphi \vee \psi$.

Let $D_1 \subseteq \mathrm{Sub}([\![P_1^+]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$[\![\varphi\wedge\psi]\!](\textstyle\bigwedge D_1,\dots,\bigwedge D_k) \quad = \quad \textstyle\bigwedge[\![\varphi]\!](D_1,\dots,D_k) \;\vee\; \bigwedge[\![\psi]\!](D_1,\dots,D_k)$$

By monotonicity w.r.t. subobject lattice orders, we trivially get

$$\textstyle\bigwedge[\![\varphi]\!](D_1,\dots,D_k) \;\vee\; \bigwedge[\![\psi]\!](D_1,\dots,D_k) \quad \subseteq \quad \bigwedge[\![\varphi\vee\psi]\!](D_1,\dots,D_k)$$

It remains to show the converse direction

$$\bigwedge [\![\varphi \vee \psi]\!](D_1, \dots, D_k) \quad \subseteq \quad \bigwedge [\![\varphi]\!](D_1, \dots, D_k) \quad \vee \quad \bigwedge [\![\psi]\!](D_1, \dots, D_k)$$

Since meets and joins are computed pointwise in subobject lattices, we are done if for each $n > 0$ we show

$$\bigcap [\![\varphi \vee \psi]\!](D_1, \dots, D_k)(n) \quad \subseteq \quad \bigcap [\![\varphi]\!](D_1, \dots, D_k)(n) \cup \bigcap [\![\psi]\!](D_1, \dots, D_k)(n)$$

We can then conclude as in the case of $\{\!|-|\!\}$. Fix $n > 0$ and let $t \in [\![P^+]\!]$ such that $t \in [\![\varphi \vee \psi]\!](A_1, \dots, A_k)(n)$ for every $A_1 \in D_1, \dots, A_k \in D_k$. Assume toward a contradiction that there are $A_1 \in D_1, \dots, A_k \in D_k$ such that $t \notin [\![\varphi]\!](A_1, \dots, A_k)(n)$ and that there are $A'_1 \in D_1, \dots, A'_k \in D_k$ such that $t \notin [\![\psi]\!](A'_1, \dots, A'_k)(n)$. Since the D_i's are codirected for inclusion, there are $A''_1 \in D_1, \dots, A''_k \in D_k$ such that $A''_i \leq A_i \wedge A'_1$ for $i = 1, \dots, k$. By monotonicity w.r.t. subobject lattice orders, we have $t \notin [\![\varphi]\!](A''_1, \dots, A''_k)(n)$ and $t \notin [\![\psi]\!](A''_1, \dots, A''_k)(n)$. But this implies $t \notin [\![\varphi \vee \psi]\!](A''_1, \dots, A''_k)(n)$, a contradiction.

Case of $[\pi_i]\varphi$.
Let $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. We show that for all $n > 0$ we have

$$[\![[\pi_i]\varphi]\!](\bigwedge D_1, \dots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\pi_i]\varphi]\!](D_1, \dots, D_k)(n)$$

and this goes similarly as for $\{\!|-|\!\}$.

Case of $[\mathsf{in}_i]\varphi$.
Let $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. We show that for all $n > 0$ we have

$$[\![[\mathsf{in}_i]\varphi]\!](\bigwedge D_1, \dots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\mathsf{in}_i]\varphi]\!](D_1, \dots, D_k)(n)$$

and this goes similarly as for $\{\!|-|\!\}$ since the pointwise maps $(\mathsf{in}_j)_n : [\![Q^+_j]\!](n) \to [\![Q^+_0]\!](n) + [\![Q^+_1]\!](n)$ are injective.

Case of $[\mathsf{next}]\varphi$.
Let $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \dots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. Write $P^+ = \blacktriangleright Q^+$. We show that for all $n > 0$ we have

$$[\![[\mathsf{next}]\varphi]\!](\bigwedge D_1, \dots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\mathsf{next}]\varphi]\!](D_1, \dots, D_k)(n)$$

The result is trivial if $n = 1$. For $n > 1$, it reduces to

$$[\![\varphi]\!](\bigwedge D_1, \dots, \bigwedge D_k)(n-1) \quad = \quad \bigcap [\![\varphi]\!](D_1, \dots, D_k)(n-1)$$

which follows from the induction hypothesis.

Case of $[\mathsf{fold}]\varphi$.
This case is handled similarly as that of $[\pi_i]$.

Case of $[\mathsf{box}]\varphi$.
Trivial since φ is required to be closed.

Case of $[\mathsf{ev}(\psi)]\varphi$.

Note that ψ is assumed to be closed since $[\mathsf{ev}(\psi)]\varphi$ is safe. Let $D_1 \subseteq \mathrm{Sub}(\llbracket P_1^+ \rrbracket), \dots, D_k \subseteq \mathrm{Sub}(\llbracket P_k^+ \rrbracket)$ be codirected. Write $P^+ = R^+ \to Q^+$. We show that for all $n > 0$ we have

$$\llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket(\bigwedge D_1, \dots, \bigwedge D_k)(n) \quad = \quad \bigcap \llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket(D_1, \dots, D_k)(n)$$

Let $n > 0$ and $t \in \llbracket P^+ \rrbracket(n)$. Then we are done since by induction hypothesis we have:

$$\begin{aligned}
& t \in \llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket(\bigwedge D_1, \dots, \bigwedge D_k)(n) \\
\text{iff } & \forall \ell \leq n,\ \forall u \in \llbracket \psi \rrbracket(\ell),\ \mathsf{ev} \circ \langle t{\uparrow}\ell, u \rangle \in \llbracket \varphi \rrbracket(\bigwedge D_1, \dots, \bigwedge D_k)(\ell) \\
\text{iff } & \forall \ell \leq n,\ \forall u \in \llbracket \psi \rrbracket(\ell),\ \mathsf{ev} \circ \langle t{\uparrow}\ell, u \rangle \in \bigcap \llbracket \varphi \rrbracket(D_1, \dots, D_k)(\ell) \\
\text{iff } & \forall S_1 \in D_1, \dots, S_k \in D_k,\ \forall \ell \leq n,\ \forall u \in \llbracket \psi \rrbracket(\ell),\ \mathsf{ev} \circ \langle t{\uparrow}\ell, u \rangle \in \llbracket \varphi \rrbracket(S_1, \dots, S_k)(\ell) \\
\text{iff } & \forall S_1 \in D_1, \dots, S_k \in D_k,\ t \in \llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket(S_1, \dots, S_k)(n) \\
\text{iff } & t \in \bigcap \llbracket [\mathsf{ev}(\psi)]\varphi \rrbracket(D_1, \dots, D_k)(n)
\end{aligned}$$

Cases of $\theta^{\mathsf{t}}\alpha\varphi$ and $\nu\alpha\varphi$.

These cases are handled exactly as for $\{\!|-|\!\}$.

Case of $\mu\alpha\varphi$.

This case cannot occur since $\mu\alpha\varphi$ is not safe. □

Proposition F.10 (Prop. 7.3). *Let $\alpha_1 : P_1^+, \dots, \alpha_k : P_k^+ \vdash \varphi : P^+$ be a safe formula. Given $S_1 \in \mathrm{Sub}(\llbracket P_1^+ \rrbracket), \dots, S_k \in \mathrm{Sub}(\llbracket P_k^+ \rrbracket)$, we have*

$$\{\!|\varphi|\!\}\,(\boldsymbol{\Gamma}(S_1), \dots, \boldsymbol{\Gamma}(S_k)) = \boldsymbol{\Gamma}\big(\llbracket \varphi \rrbracket(S_1, \dots, S_k)\big)$$

Proof. We reason by induction on the derivation of $\alpha_1 : P_1^+, \dots, \alpha_k : P_k^+ \vdash \varphi : P^+$. In all cases but $\theta^{\mathsf{t}}\alpha\varphi$ and $\nu\alpha\varphi$, the parameters are irrelevant and we omit them.

Cases of α, $\top$ and $\bot$.

Trivial.

Case of $\varphi \wedge \psi$.

Let $x \in \boldsymbol{\Gamma}\llbracket P^+ \rrbracket$. Then we are done since by induction hypothesis we have

$$\begin{aligned}
x \in \{\!|\varphi \wedge \psi|\!\} & \text{ iff } x \in \{\!|\varphi|\!\} \text{ and } x \in \{\!|\psi|\!\} \\
& \text{ iff } (\forall n > 0,\ x_n(\bullet) \in \llbracket \varphi \rrbracket(n)) \text{ and } (\forall n > 0,\ x_n(\bullet) \in \llbracket \psi \rrbracket(n)) \\
& \text{ iff } \forall n > 0,\ x_n(\bullet) \in \llbracket \varphi \rrbracket(n) \text{ and } x_n(\bullet) \in \llbracket \psi \rrbracket(n) \\
& \text{ iff } \forall n > 0,\ x_n(\bullet) \in \llbracket \varphi \wedge \psi \rrbracket(n)
\end{aligned}$$

Case of $\varphi \vee \psi$.

Let $x \in \boldsymbol{\Gamma}\llbracket P^+ \rrbracket$. Assume first that $x \in \{\!|\varphi \vee \psi|\!\}$. If (say) $x \in \{\!|\varphi|\!\}$, then by induction hypothesis we get $x_n(\bullet) \in \llbracket \varphi \rrbracket(n)$ for all $n > 0$, which implies $x_n(\bullet) \in \llbracket \varphi \vee \psi \rrbracket(n)$ for all $n > 0$.

Conversely, assume that $x_n(\bullet) \in \llbracket \varphi \vee \psi \rrbracket(n)$ for all $n > 0$. Assume toward a contradiction that there are $k, \ell > 0$ with (say) $k \leq \ell$ such that $x_k(\bullet) \notin \llbracket \varphi \rrbracket(n)$ and $x_\ell(\bullet) \notin \llbracket \psi \rrbracket(n)$. Since $k \leq \ell$, by Lem. D.16 we have $x_k(\bullet) \notin \llbracket \psi \rrbracket(n)$, but this contradicts $x_k(\bullet) \in \llbracket \varphi \vee \psi \rrbracket(n)$. Hence, we have either $x_n(\bullet) \in \llbracket \varphi \rrbracket(n)$ for all $n > 0$ or $x_n(\bullet) \in \llbracket \psi \rrbracket(n)$ for all $n > 0$, and the result follows by induction hypothesis.

Case of $\psi \Rightarrow \varphi$.
This case cannot occur since $\psi \Rightarrow \varphi$ is not safe.

Case of $[\pi_i]\varphi$.
Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = Q_0^+ \times Q_1^+$. Then we are done since $(\pi_i \circ x)_n(\bullet) = \pi_i(x_n(\bullet))$ so that by induction hypothesis we have

$$\begin{aligned} x \in \{\![\pi_i]\varphi]\!\} &\text{ iff } \pi_i \circ x \in \{\![\varphi]\!\} \\ &\text{ iff } \forall n > 0, \quad (\pi_i \circ x)_n(\bullet) \in [\![\varphi]\!](n) \\ &\text{ iff } \forall n > 0, \quad x_n(\bullet) \in [\![[\pi_i]\varphi]\!](n) \end{aligned}$$

Case of $[\mathsf{in}_i]\varphi$.
Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = Q_0^+ + Q_1^+$. By Lem. D.2, we have $x = \mathsf{in}_j \circ y$ for some unique $j \in \{0,1\}$ and $y \in \boldsymbol{\Gamma}[\![Q_j^+]\!]$. Then we are done since $x_n(\bullet) = (\mathsf{in}_j \circ y)_n(\bullet) = \mathsf{in}_j(y_n(\bullet))$ so that by induction hypothesis we have

$$\begin{aligned} x \in \{\![\mathsf{in}_i]\varphi]\!\} &\text{ iff } j = i \text{ and } y \in \{\![\varphi]\!\} \\ &\text{ iff } j = i \text{ and } \forall n > 0, \quad y_n(\bullet) \in [\![\varphi]\!](n) \\ &\text{ iff } \qquad\qquad \forall n > 0, \quad x_n(\bullet) \in [\![[\mathsf{in}_i]\varphi]\!](n) \end{aligned}$$

Case of $[\mathsf{next}]\varphi$.
Let $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and write $P^+ = \blacktriangleright Q^+$. By Lem. D.2, we have $x = \mathsf{next} \circ y$ for some unique $y \in \boldsymbol{\Gamma}[\![Q^+]\!]$. Assume first $x \in \{\![\mathsf{next}]\varphi]\!\}$. Hence we have $y \in \{\![\varphi]\!\}$, which by induction hypothesis implies $y_n(\bullet) \in [\![\varphi]\!](n)$ for all $n > 0$. Now, we trivially have $x_1(\bullet) \in [\![[\mathsf{next}]\varphi]\!](1)$. Moreover, for $n > 1$, we have $x_n(\bullet) = y_{n-1}(\bullet)$, so that $x_n(\bullet) \in [\![[\mathsf{next}]\varphi]\!](n) = [\![\varphi]\!](n-1)$.
Assume conversely that $x_n(\bullet) \in [\![[\mathsf{next}]\varphi]\!](n)$ for all $n > 0$. This implies $x_n(\bullet) \in [\![\varphi]\!](n-1)$ for all $n > 1$, which in turn implies $y_{n-1}(\bullet) \in [\![\varphi]\!](n-1)$ for all $n > 1$. But by induction hypothesis this implies $y \in \{\![\varphi]\!\}$ so that $x \in \{\![\mathsf{next}]\varphi]\!\}$.

Case of $[\mathsf{fold}]\varphi$.
This case is handled similarly as that of $[\pi_i]$.

Case of $[\mathsf{box}]\varphi$.
Recall that φ is required to be closed. Also, by definition we have

$$\begin{aligned} [\![[\mathsf{box}]\varphi]\!]^{\blacksquare A}(n) &:= \left\{ t \in [\![\blacksquare A]\!](n) = \boldsymbol{\Gamma}[\![A]\!] \;\middle|\; t \in \{\![\varphi]\!\}^A \right\} \\ \{\![\mathsf{box}]\varphi]\!\}^{\blacksquare A} &:= \left\{ x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!] \;\middle|\; x_1(\bullet) \in \{\![\varphi]\!\}^A \right\} \end{aligned}$$

It follows that given $x \in \boldsymbol{\Gamma}[\![\blacksquare A]\!]$, we have

$$\begin{aligned} x \in \{\![\mathsf{box}]\varphi]\!\}^{\blacksquare A} &\text{ iff } x_1(\bullet) \in \{\![\varphi]\!\}^A \\ &\text{ iff } \forall n > 0, \; x_n(\bullet) \in \{\![\varphi]\!\}^A \\ &\text{ iff } \forall n > 0, \; x_n(\bullet) \in [\![[\mathsf{box}]\varphi]\!]^{\blacksquare A}(n) \end{aligned}$$

Case of $[\mathsf{ev}(\psi)]\varphi$.
This case cannot occur since P^+ is assumed to be strictly positive.

Case of $[\mathsf{ev}(\psi)]\varphi$.
Since $[\mathsf{ev}(\psi)]\varphi$ is smooth, the formula ψ is closed and we have $Q^+ = B \to R^+$ where B is constant. Since B is constant, by Lem. D.4 there is a set A such that $[\![B]\!] \simeq \boldsymbol{\Delta} A$, so that $\boldsymbol{\Gamma}[\![B]\!] \simeq A$ by Lem. D.2. Moreover, it follows from Lem. D.24 that $[\![\psi]\!]$ is also constant, so there is a set S such that $[\![\psi]\!] \simeq \boldsymbol{\Delta} S$. Now, by induction hypothesis we have $\boldsymbol{\Gamma}[\![\psi]\!] = \{\!|\psi|\!\}$. Since $\boldsymbol{\Gamma}\boldsymbol{\Delta} \simeq \mathrm{Id}_{\mathbf{Set}}$ (Lem. D.2), it follows that $[\![\psi]\!] \simeq \boldsymbol{\Delta}\,\{\!|\psi|\!\}$. We then have

$$x \in \{\!|[\mathsf{ev}(\psi)]\varphi|\!\} \text{ iff } \forall y \in \boldsymbol{\Gamma}[\![B]\!]\,(y \in \{\!|\psi|\!\} \implies \mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\})$$

and

$$\begin{aligned} t \in [\![[\mathsf{ev}(\psi)]\varphi]\!](n) &\text{ iff } \forall k \leq n,\ \forall u \in A\,(u \in \{\!|\psi|\!\} \implies (t{\uparrow}k)(u) \in [\![\varphi]\!](k)) \\ &\text{ iff } \forall u \in A\,(u \in \{\!|\psi|\!\} \implies \forall k \leq n,\ (t{\uparrow}k)(u) \in [\![\varphi]\!](k)) \end{aligned}$$

Given $x \in \boldsymbol{\Gamma}[\![B \to R^+]\!]$ and $y \in \boldsymbol{\Gamma}[\![B]\!]$, for all $0 < k \leq n$ we have

$$(\mathsf{ev} \circ \langle x, y\rangle)_n(\bullet){\uparrow}k = (x_n(\bullet){\uparrow}k)(y_k(\bullet))$$

Since $\{\!|\varphi|\!\} \simeq \boldsymbol{\Gamma}[\![\varphi]\!]$ by induction hypothesis, we are done with

$$\begin{aligned} x \in \{\!|[\mathsf{ev}(\psi)]\varphi|\!\} &\text{ iff } \forall y \in \boldsymbol{\Gamma}[\![B]\!]\,(y \in \{\!|\psi|\!\} \implies \mathsf{ev} \circ \langle x, y\rangle \in \{\!|\varphi|\!\}) \\ &\text{ iff } \forall y \in \boldsymbol{\Gamma}[\![B]\!]\,(y \in \{\!|\psi|\!\} \implies \forall n > 0,\ (\mathsf{ev} \circ \langle x, y\rangle)_n(\bullet) \in [\![\varphi]\!](n)) \\ &\text{ iff } \forall y \in \boldsymbol{\Gamma}[\![B]\!]\,(y \in \{\!|\psi|\!\} \implies \forall n > 0,\ \forall k \leq n,\ ((\mathsf{ev} \circ \langle x, y\rangle)_n(\bullet)){\uparrow}k \in [\![\varphi]\!](k)) \\ &\text{ iff } \forall y \in \boldsymbol{\Gamma}[\![B]\!]\,(y \in \{\!|\psi|\!\} \implies \forall n > 0,\ \forall k \leq n,\ (x_n(\bullet){\uparrow}k)(y_k(\bullet)) \in [\![\varphi]\!](k)) \\ &\text{ iff } \forall u \in A\,(u \in \{\!|\psi|\!\} \implies \forall n > 0,\ \forall k \leq n,\ (x_n(\bullet){\uparrow}k)(u) \in [\![\varphi]\!](k)) \\ &\text{ iff } \forall n > 0,\ \forall u \in A\,(u \in \{\!|\psi|\!\} \implies \forall k \leq n,\ (x_n(\bullet){\uparrow}k)(u) \in [\![\varphi]\!](k)) \\ &\text{ iff } \forall n > 0,\ x_n(\bullet) \in [\![[\mathsf{ev}(\psi)]\varphi]\!] \end{aligned}$$

Cases of $\theta^{\mathsf{t}}\alpha\varphi(\alpha)$.
Assume $\alpha_1 : P_1^+, \ldots, \alpha_k : P_k^+, \alpha : P^+ \vdash \varphi(\alpha) : P^+$, and let $S_1 \in \mathrm{Sub}([\![P_1^+]\!]), \ldots, S_k \in \mathrm{Sub}([\![P_k^+]\!])$. Using the induction hypothesis on φ, an easy induction on $m \in \mathbb{N}$ shows that

$$\begin{aligned} &\{\!|\varphi^m|\!\}\,(\boldsymbol{\Gamma}(S_1), \ldots, \boldsymbol{\Gamma}(S_k), \top) = \boldsymbol{\Gamma}\big([\![\varphi]\!]^m(S_1, \ldots, S_k, \top)\big) \\ \text{and}\quad &\{\!|\varphi^m|\!\}\,(\boldsymbol{\Gamma}(S_1), \ldots, \boldsymbol{\Gamma}(S_k), \bot) = \boldsymbol{\Gamma}\big([\![\varphi]\!]^m(S_1, \ldots, S_k, \bot)\big) \end{aligned}$$

Case of $\nu\alpha\varphi$.
Assume $\alpha_1 : P_1^+, \ldots, \alpha_k : P_k^+, \alpha : P^+ \vdash \varphi(\alpha) : P^+$, and let $S_1 \in \mathrm{Sub}([\![P_1^+]\!]), \ldots, S_k \in \mathrm{Sub}([\![P_k^+]\!])$. Similarly as above, for all $m \in \mathbb{N}$ we have

$$\{\!|\varphi^m|\!\}\,(\boldsymbol{\Gamma}(S_1), \ldots, \boldsymbol{\Gamma}(S_k), \top) = \boldsymbol{\Gamma}\big([\![\varphi]\!]^m(S_1, \ldots, S_k, \top)\big)$$

It then directly follows that for all $x \in \boldsymbol{\Gamma}[\![P^+]\!]$, we have

$$\begin{gathered} x \in \textstyle\bigcap_{m \in \mathbb{N}} \{\!|\varphi^m|\!\}\,(\boldsymbol{\Gamma}(S_1), \ldots, \boldsymbol{\Gamma}(S_k), \top) \\ \text{iff } \forall n > 0,\ x_n(\bullet) \in \textstyle\bigcap_{m \in \mathbb{N}} [\![\varphi]\!]^m(S_1, \ldots, S_k, \top)(n) \end{gathered}$$

and we conclude by Lem. F.9 and Lem. F.8.

Case of $\mu\alpha\varphi$.
This case cannot occur since $\mu\alpha\varphi$ is not safe. $\square$

F.3 The Smooth Fragment

Assume for this §F.3 that the set of propositional variables is partitionned into two infinite sets $\{\alpha^\nu, \beta^\nu, \dots\}$ and $\{\alpha^\mu, \beta^\mu, \dots\}$ of respectively *gfp* (or ν) and *lfp* (or μ) propositional variables. Write Σ^ν (resp. Σ^μ) if the context Σ only declares gfp (resp. lfp) propositional variables.

Lemma F.11. *If φ is alternation-free, then φ can be formed with the rules of Fig. 5 and Fig. 9, but with the rules* (ν-F) *and* (μ-F) *replaced respectively by*

$$\frac{\Sigma^\nu, \alpha^\nu : A \vdash \varphi : A}{\Sigma^\nu \vdash \nu\alpha^\nu\varphi : A} \qquad \frac{\Sigma^\mu, \alpha^\mu : A \vdash \varphi : A}{\Sigma^\mu \vdash \mu\alpha^\mu\varphi : A}$$

where in both cases α^θ is guarded in φ, and α^θ as well as all variables of Σ^θ are positive in φ.

Proof. By induction on φ. The only relevant cases are $\theta\alpha\varphi$. Since the two cases are similar, we only discuss that of $\Sigma \vdash \nu\alpha\varphi : A$. First, since $\nu\alpha\varphi$ is alternation-free, we can assume that all variables declared in Σ are positive in φ. Moreover, since $\nu\alpha\varphi$ is alternation-free, then so is φ. By induction hypothesis Σ can be split into Σ^μ, Σ^ν and we have

$$\Sigma^\mu,\ \Sigma^\nu,\ \alpha : A \vdash \varphi : A$$

Assume toward a contradiction that Σ^μ cannot be made empty. This means that there is some variable β^μ which does occur in φ, and such that β^μ must occur in the context of a μ rule for some subformula of φ. But then β^μ occurs free in $\nu\alpha\varphi$ under two fixpoints of different kinds, a contradiction. It follows that we can assume Σ^μ empty. Similarly, α can be assumed to be gfp variable, since otherwise it would occur free under a lfp in $\nu\alpha\varphi$. □

Lemma F.12 (Lem. 7.4). *Let $\alpha_1 : P_1^+, \dots, \alpha_k : P_k^+, \alpha : Q^+ \vdash \varphi : P^+$ be a smooth formula and let v be a valuation taking each propositional variable α_i for $i = 1, \dots, k$ to a set $v(\alpha_i) \in \mathcal{P}(\boldsymbol{\Gamma}[\![P_i^+]\!])$. Consider the function*

$$\{|\varphi|\} : \mathcal{P}(\boldsymbol{\Gamma}[\![Q^+]\!]) \longrightarrow \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]),\ S \longmapsto \{|\varphi|\}_{v[S/\alpha]}$$

Then,

- *if α is positive in φ (i.e. α* Pos *φ):*
  - *if α is a gfp variable, then $\{|\varphi|\}$ is Scott-cocontinuous,*
  - *if α is a lfp variable, then $\{|\varphi|\}$ is Scott-continuous,*
- *if α is negative in φ (i.e. α* Neg *φ), then $\{|\varphi|\}$ is antimonotone and*
  - *takes meets of codirected sets to joins of directed sets if α is a gfp variable,*
  - *takes joins of directed sets to meets of codirected sets if α is a lfp variable.*

Proof. The proof is by induction on formation of formulae $\alpha_1 : P_1^+, \dots, \alpha_k : P_k^+, \alpha : Q^+ \vdash \varphi : P^+$. Monotonicity and antimonotonicity follow from Lem. F.4. Note that since formulae of the form $[\mathsf{box}]\varphi$ are necessarily closed, nothing has to be proved for these. Some cases are already handled by Lem. D.22 (Lem. F.9), and we do not repeat them. We omit the valuation v when possible.

Cases of $\alpha, \top, \bot$.
Trivial.

Case of $\varphi \wedge \psi$ (monotone).
Preservation of codirected meets is trivial (see Lem. D.22 (Lem. F.9)). As for the preservation of directed joins, let $D \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![Q^+]\!])$ be directed. Then by induction hypothesis we have

$$\{\!|\varphi \wedge \psi|\!\}\,(\bigcup D) \quad = \quad \bigcup \{\!|\varphi|\!\}\,(D) \;\cap\; \bigcup \{\!|\psi|\!\}\,(D) \quad \supseteq \quad \bigcup \{\!|\varphi \wedge \psi|\!\}\,(D)$$

For the converse inclusion, consider some x both in $\bigcup \{\!|\varphi|\!\}\,(D)$ and $\bigcup \{\!|\psi|\!\}\,(D)$. Hence there are $S, S' \in D$ such that $x \in \{\!|\varphi|\!\}\,(S)$ and $x \in \{\!|\psi|\!\}\,(S')$. Now since D is directed and by monotonicity, there is some $S'' \in D$ such that $x \in \{\!|\varphi|\!\}\,(S'') \cap \{\!|\psi|\!\}\,(S'')$.

Case of $\varphi \wedge \psi$ (antimonotone).
That $\{\!|\varphi \wedge \psi|\!\}$ turns directed joins into codirected meets is trivial (as codirected meets commute over binary meets) and omitted. Let us show that $\{\!|\varphi \wedge \psi|\!\}$ turns codirected meets into directed joins. So let $D \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![Q^+]\!])$ be codirected. Then by induction hypothesis we have

$$\{\!|\varphi \wedge \psi|\!\}\,(\bigcap D) \quad = \quad \bigcup \{\!|\varphi|\!\}\,(D) \;\cap\; \bigcup \{\!|\psi|\!\}\,(D) \quad \supseteq \quad \bigcup \{\!|\varphi \wedge \psi|\!\}\,(D)$$

We then conclude as for preservation of directed joins in the monotone case. Given x both in $\bigcup \{\!|\varphi|\!\}\,(D)$ and $\bigcup \{\!|\psi|\!\}\,(D)$, there are $S, S' \in D$ such that $x \in \{\!|\varphi|\!\}\,(S)$ and $x \in \{\!|\psi|\!\}\,(S')$. Now since D is codirected there is some $S'' \in D$ such that $S'' \subseteq S \cap S'$, and by antimonotonicity we have $x \in \{\!|\varphi|\!\}\,(S'') \cap \{\!|\psi|\!\}\,(S'')$.

Case of $\varphi \vee \psi$ (monotone).
Preservation of codirected meets is handled in Lem. D.22 (Lem. F.9) while preservation of directed join is trivial.

Case of $\varphi \vee \psi$ (antimonotone).
That $\{\!|\varphi \vee \psi|\!\}$ turns codirected meets into directed joins is trivial (as directed joins commute over binary joins) and omitted. Let us show that $\{\!|\varphi \vee \psi|\!\}$ turns directed joins into codirected meets. So let $D \subseteq \mathcal{P}(\boldsymbol{\Gamma}[\![Q^+]\!])$ be directed. By induction hypothesis we have

$$\{\!|\varphi \vee \psi|\!\}\,(\bigcup D) \quad = \quad \bigcap \{\!|\varphi|\!\}\,(D) \;\cup\; \bigcap \{\!|\psi|\!\}\,(D) \quad \subseteq \quad \bigcap \{\!|\varphi \vee \psi|\!\}\,(D)$$

We can then conclude similarly as in Lem. D.22 (Lem. F.9). Let $x \in \bigcap \{\!|\varphi \vee \psi|\!\}\,(D)$ and assume toward a contradiction that there are $S, S' \in D$ such that $x \notin \{\!|\varphi|\!\}\,(S)$ and $x \notin \{\!|\psi|\!\}\,(S')$. Then since D is directed, there is some $S'' \in D$ such that $S \cup S' \subseteq S''$, and by antimonotonicity we get $x \notin \{\!|\varphi \vee \psi|\!\}\,(S'')$, a contradiction.

Case of $\psi \Rightarrow \varphi$.
With the classical semantics, the interpretation of $\Rightarrow$ can be decomposed into $\vee$ and $\neg$, where $\{\!|\neg\varphi|\!\}$ is the complement of $\{\!|\varphi|\!\}$ (at the appropriate type). Let α be positive in φ and negative in ψ, with $\alpha : Q^+ \vdash \varphi, \psi : P^+$,

and let furthermore by D and D' (of the appropriate type) be resp. directed and codirected. We then trivially have

$$\begin{aligned}\{|\neg\varphi|\}\left(\bigcup D\right) &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\varphi|\}\left(\bigcup D\right) \\ &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \bigcup \{|\varphi|\}(D) \\ &= \bigcap \left(\mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\varphi|\}(D)\right)\end{aligned} \qquad \begin{aligned}\{|\neg\varphi|\}\left(\bigcap D'\right) &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\varphi|\}\left(\bigcap D'\right) \\ &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \bigcap \{|\varphi|\}(D') \\ &= \bigcup \left(\mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\varphi|\}(D')\right)\end{aligned}$$

$$\begin{aligned}\{|\neg\psi|\}\left(\bigcup D\right) &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\psi|\}\left(\bigcup D\right) \\ &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \bigcap \{|\psi|\}(D) \\ &= \bigcup \left(\mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\psi|\}(D)\right)\end{aligned} \qquad \begin{aligned}\{|\neg\psi|\}\left(\bigcap D'\right) &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\psi|\}\left(\bigcap D'\right) \\ &= \mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \bigcup \{|\psi|\}(D') \\ &= \bigcap \left(\mathcal{P}(\boldsymbol{\Gamma}[\![P^+]\!]) \setminus \{|\psi|\}(D')\right)\end{aligned}$$

Cases of $[\pi_i]\varphi$, $[\mathsf{in}_i]\varphi$, $[\mathsf{next}]\varphi$ and $[\mathsf{fold}]\varphi$.
These modalities are handled similarly as in Lem. D.22 (Lem. F.9).

Case of $[\mathsf{ev}(\psi)]\varphi$.
Since $[\mathsf{ev}(\psi)]\varphi$ is smooth, the formula ψ is closed and we have $Q^+ = B \to R^+$ with B a finite base type. Since B is constant, by Lem. D.4 there is a *finite* set A such that $[\![B]\!] \simeq \boldsymbol{\Delta}A$, so that $\boldsymbol{\Gamma}[\![B]\!] \simeq A$ by Lem. D.2. Now, given $x \in \boldsymbol{\Gamma}[\![P^+]\!]$ and $S \subseteq \boldsymbol{\Gamma}[\![Q^+]\!]$ we have

$$x \in \{|[\mathsf{ev}(\psi)]\varphi|\}(S) \text{ iff } \forall y \in A\, (y \in \{|\psi|\} \implies \mathsf{ev} \circ \langle x, y\rangle \in \{|\varphi|\}(S))$$

Since A is finite, we can then reason similarly as in the cases of conjunction ($\wedge$) above.

Cases of $\theta^{\mathtt{t}}\beta\varphi$.
We have $\alpha_1 : P_1^+, \ldots, \alpha_k : P_k^+, \alpha : Q^+, \beta : P^+ \vdash \varphi : P^+$ with β Pos φ. Let v be a valuation. Since for $S \subseteq \boldsymbol{\Gamma}[\![Q^+]\!]$ and $m \in \mathbb{N}$ we have

$$\{|\theta^{\mathtt{m}+1}\beta\varphi|\}_v(S) = \{|\varphi[\theta^{\mathtt{m}}\beta\varphi/\beta]|\}_v(S)$$

it follows from Lem. D.22 (Lem. F.9), that the function $\{|\theta^{\mathtt{t}}\beta\varphi|\}_v$ is monotone (resp. antimonotone) if α Pos φ (resp. α Neg φ). We can then reason as in Lem. D.22 (Lem. F.9).

Case of $\nu\beta\varphi$.
We have $\alpha_1 : P_1^+, \ldots, \alpha_k : P_k^+, \alpha : Q^+, \beta : P^+ \vdash \varphi : P^+$ where the involved variables are gfp variables and are positive in φ. The result is then proved exactly the same way as in Lem. D.22 (Lem. F.9).

Case of $\mu\beta\varphi$.
The result is proved the same way as in Lem. F.9 (replacing codirected meets by directed joins and Scott cocontinuity by Scott continuity). ☐

F.4 Realizability

Lemma F.13 (Monotonicity of Realizability (Lem. D.25)). *Let T be a type without free iteration variables. If $x \Vdash_n T$ then $x \Vdash_k T$ for all $k \leq n$.*

Proof. By induction on the definition of $\Vdash$.

Case of a refinement type $\{A \mid \varphi\}$.
The result follows from monotony of forcing (*i.e.* that $[\![\varphi]\!]$ is a subobject of $[\![A]\!]$) .

Case of 1.
The result is trivial as $x \Vdash_n \mathbf{1}$ for all $n > 0$.

Case of $T_0 + T_1$.
Assume $x \Vdash_n T_0 + T_1$ and let $k \leq n$. Then we have $x = \mathsf{in}_i \circ y$ for some $i = 0, 1$ and some $y \in \boldsymbol{\Gamma}[\![|T_i|]\!]$ such that $y \Vdash_n T_i$. By induction hypothesis we get $y \Vdash_k T_i$, so that $x \Vdash_k T_0 + T_1$.

Case of $T_0 \times T_1$.
Assume $x \Vdash_n T_0 \times T_1$ and let $k \leq n$. Then for each $i = 0, 1$ we have $\pi_i \circ x \Vdash_n T_i$, so that $\pi_i \circ x \Vdash_k T_i$ by induction hypothesis, and it follows that $x \Vdash_k T_0 \times T_1$.

Case of $U \to T$.
Assume $x \Vdash_n U \to T$ and let $k \leq n$. But given $\ell \leq k$ and $y \in \boldsymbol{\Gamma}[\![|U|]\!]$ such that $y \Vdash_\ell U$ we have $\mathsf{ev} \circ \langle x, y\rangle \Vdash_\ell T$ since $\ell \leq n$.

Case of $\blacktriangleright T$.
Assume $x \Vdash_n \blacktriangleright T$ and let $k \leq n$. If $k = 1$ then we are done since always $x \Vdash_1 \blacktriangleright T$. Otherwise, $k = \ell + 1$, so that $n = m + 1$ with $\ell \leq m$. Moreover, there is $y \in \boldsymbol{\Gamma}[\![T]\!]$ such that $x = \mathsf{next} \circ y$ and $y \Vdash_m T$. We get $y \Vdash_\ell T$ by induction hypothesis, so that $x \Vdash_k \blacktriangleright T$.

Case of $\mathsf{Fix}(X).A$.
Assume $x \Vdash_n \mathsf{Fix}(X).A$ and let $k \leq n$. We have $\mathsf{unfold} \circ x \Vdash_n A[\mathsf{Fix}(X).A/X]$, so that $\mathsf{unfold} \circ x \Vdash_k A[\mathsf{Fix}(X).A/X]$ by induction hypothesis and thus $x \Vdash_k \mathsf{Fix}(X).A$.

Case of $\blacksquare T$.
Trivial. □

Lemma F.14 (Lem. D.26). *For a pure type A and $x \in \boldsymbol{\Gamma}[\![A]\!]$, we have $x \Vdash_n A$ for all $n > 0$.*

Proof. The proof is by induction on pairs (n, A), using implicitly Lem. D.2 whenever required.

Case of 1.
Trivial.

Case of $A_0 + A_1$.
Given $x \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \simeq \boldsymbol{\Gamma}[\![A_0]\!] + \boldsymbol{\Gamma}[\![A_1]\!]$, we have $x = \mathsf{in}_i \circ y$ for some $y \in \boldsymbol{\Gamma}[\![A_i]\!]$. Then we are done since $y \Vdash_n A_i$ by induction hypothesis.

Case of $A_0 \times A_1$.
Given $x \in \boldsymbol{\Gamma}[\![A_0 \times A_1]\!] \simeq \boldsymbol{\Gamma}[\![A_0]\!] \times \boldsymbol{\Gamma}[\![A_1]\!]$, we have $\pi_0 \circ x \Vdash_n A_0$ and $\pi_1 \circ x \Vdash_n A_1$ by induction hypothesis, and the result follows.

Case of $B \to A$.
Fix $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$. Given $y \in \boldsymbol{\Gamma}[\![B]\!]$ and $k \leq n$, we have $y \Vdash_k B$ by induction hypothesis, so that $\mathsf{ev} \circ \langle x, y\rangle \Vdash_k A$. Hence $x \Vdash_n B \to A$.

Case of $\blacktriangleright A$.
The result is trivial if $n = 1$, so assume $n > 1$. Given $x \in \boldsymbol{\Gamma}[\![\blacktriangleright A]\!]$, we have

$x = \mathsf{next} \circ y$ for some $y \in \boldsymbol{\Gamma}[\![A]\!]$. But then $y \Vdash_{n-1} A$ by induction hypothesis, so that $x \Vdash_n \blacktriangleright A$.

Case of $\mathsf{Fix}(X).A$.

Let $x \in \boldsymbol{\Gamma}[\![\mathsf{Fix}(X).A]\!]$. It follows by induction on A from the induction hypothesis on n and the guardedness of X in A that $\mathsf{unfold} \circ x \Vdash_n A[\mathsf{Fix}(X).A/X]$, and we are done.

Case of $\blacksquare T$.

Let $x \in \boldsymbol{\Gamma}[\![\blacksquare T]\!]$. Given $n > 0$, we have $x_n(\bullet) \in \boldsymbol{\Gamma}[\![T]\!]$, so that $x_n(\bullet) \Vdash_m T$ for all $m > 0$ by induction hypothesis. But this implies $x \Vdash_n \blacksquare T$. □

Lemma F.15 (Correctness of Subtyping (Lem. D.28)). *Given types T, U without free iteration variable, if $x \Vdash_n U$ and $U \leq T$ then $x \Vdash_n T$.*

Proof. By induction on $U \leq T$.

Cases of

$$\frac{}{T \leq T} \qquad \frac{T \leq U \qquad U \leq V}{T \leq V}$$

Trivial.

Cases of

$$\frac{T_0 \leq U_0 \qquad T_1 \leq U_1}{T_0 \times T_1 \leq U_0 \times U_1} \qquad \frac{T_0 \leq U_0 \qquad T_1 \leq U_1}{T_0 + T_1 \leq U_0 + U_1} \qquad \frac{U_0 \leq T_0 \qquad T_1 \leq U_1}{T_0 \to T_1 \leq U_0 \to U_1}$$

$$\frac{T \leq U}{\blacktriangleright T \leq \blacktriangleright U}$$

Trivial

Case of

$$\frac{U \leq T}{\blacksquare U \leq \blacksquare T}$$

Let $x : \mathbf{1} \to_{\mathcal{S}} \boldsymbol{\Delta\Gamma}[\![U]\!]$ such that $x \Vdash_n \blacksquare U$, so that $x_n(\bullet) \Vdash_m U$ for all $m > 0$. By induction hypothesis we get $x_n(\bullet) \Vdash_m T$ for all $m > 0$ and we are done.

Case of

$$\frac{}{T \leq |T|}$$

By Lem. D.26.

Case of

$$\frac{}{A \leq \{A \mid \top\}}$$

Trivial

Case of

$$\frac{\vdash^A \varphi \Rightarrow \psi}{\{A \mid \varphi\} \leq \{A \mid \psi\}}$$

By Lem. F.5 (Lem. D.13.(2)).

Case of

$$\overline{\{B \to A \mid [\mathsf{ev}(\psi)]\varphi\} \leq \{B \mid \psi\} \to \{A \mid \varphi\}}$$

Let $x \in \boldsymbol{\Gamma}[\![B \to A]\!]$ and $n > 0$. Assume $x \Vdash_n \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}$, that is $x_n(\bullet) \in [\![[\mathsf{ev}(\psi)]\varphi]\!](n)$. Let further $y \in \boldsymbol{\Gamma}[\![B]\!]$ and $k \leq n$ such that $y \Vdash_k \{B \mid \psi\}$, that is $y_k(\bullet) \in [\![\psi]\!](k)$. Then by monotonicity of $[\![-]\!]$ (Lem. D.16) we have $x_k(\bullet) \in [\![[\mathsf{ev}(\psi)]\varphi]\!](k)$, from which it follows that $(x_k(\bullet))(y_k(\bullet)) \in [\![\varphi]\!](k)$. But this means $\mathsf{ev} \circ \langle x, y\rangle \Vdash_k \{A \mid \varphi\}$ and we are done.

Case of

$$\overline{\{B \mid \psi\} \to \{A \mid \varphi\} \leq \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}}$$

Let $x \in \boldsymbol{\Gamma}[\![B]\!] \to A$ and $n > 0$. Assume $x \Vdash_n \{B \mid \psi\} \to \{A \mid \varphi\}$. Let furthermore $k \leq n$ and $u \in [\![\psi]\!](k)$. By Lem. D.27 ([20, Cor. 3.8]) there is some $y \in \boldsymbol{\Gamma}[\![B]\!]$ such that $y_k(\bullet) = u$. We thus have $y \Vdash_k \{B \mid \psi\}$, and it follows that $\mathsf{ev} \circ \langle x, y\rangle \Vdash_k \{A \mid \varphi\}$, that is $x_k(\bullet)(y_k(\bullet)) \in [\![\varphi]\!](k)$, and we are done.

Case of

$$\overline{\blacktriangleright \{A \mid \varphi\} \equiv \{\blacktriangleright A \mid [\mathsf{next}]\varphi\}}$$

Let $x \in \boldsymbol{\Gamma}[\![\blacktriangleright A]\!]$. First, we always have $x \Vdash_1 \blacktriangleright A$, as well as $x_1 \in [\![[\mathsf{next}]\varphi]\!]^{\blacktriangleright A}$. Let now $n > 1$. By Lem. D.2 we have $x = \mathsf{next} \circ y$ for some $y \in \boldsymbol{\Gamma}[\![A]\!]$. Since $x_n(\bullet) = y_{n-1}(\bullet)$, we have

$$\begin{aligned} x \Vdash_n \blacktriangleright \{A \mid \varphi\} & \text{ iff } y \Vdash_{n-1} \{A \mid \varphi\} \\ & \text{ iff } y_{n-1}(\bullet) \in [\![\varphi]\!]^{A}(n-1) \\ & \text{ iff } x_n(\bullet) = y_{n-1}(\bullet) \in [\![[\mathsf{next}]\varphi]\!]^{\blacktriangleright A}(n) \\ & \text{ iff } x \Vdash_n \{\blacktriangleright A \mid [\mathsf{next}]\varphi\}\,. \end{aligned}$$

Case of

$$\overline{\forall k \cdot \blacktriangleright T \equiv \blacktriangleright \forall k \cdot T}$$

Let $x \in \boldsymbol{\Gamma}[\![\blacktriangleright |T|]\!]$.
Assume first that $x \Vdash_n \forall k \cdot \blacktriangleright T$. We have to show $x \Vdash_n \blacktriangleright \forall k \cdot T$. The result is trivial if $n = 1$. So assume $n > 1$. By Lem. D.2, there some unique $y \in \boldsymbol{\Gamma}[\![|T|]\!]$ such that $x = \mathsf{next} \circ y$. We have to show $y \Vdash_{n-1} T[\mathtt{m}/k]$ for all $m \in \mathbb{N}$. But by assumption we have $x \Vdash_n \blacktriangleright T[\mathtt{m}/k]$, so that by uniqueness of y we get $y \Vdash_{n-1} T[\mathtt{m}/k]$.
Conversely, assume that $x \Vdash_n \blacktriangleright \forall k \cdot T$. We have to show $x \Vdash_n \forall k \cdot \blacktriangleright T$. Let $m \in \mathbb{N}$. If $n = 1$, then we trivially have $x \Vdash_n \blacktriangleright T[\mathtt{m}/k]$. Otherwise, by Lem. D.2 let $y \in \boldsymbol{\Gamma}[\![|T|]\!]$ such that $x = \mathsf{next} \circ y$. But since $x \Vdash_n \blacktriangleright \forall k \cdot T$, we get $y \Vdash_{n-1} T[\mathtt{m}/k]$, so that $x \Vdash_n \blacktriangleright T[\mathtt{m}/k]$ and we are done.

Case of

$$\frac{\varphi \text{ safe}}{\blacksquare \{A \mid \varphi\} \equiv \{\blacksquare A \mid [\mathsf{box}]\varphi\}}$$

Let $x : \mathbf{1} \to_{\mathcal{S}} \boldsymbol{\Delta\Gamma}[\![A]\!]$. Since φ is safe we have $\{|\varphi|\}^A = \mathrm{Clos}([\![\varphi]\!]^A)$ by Prop. F.10 (Prop. 7.3). Then we are done since:

$$\begin{aligned} x \Vdash_n \blacksquare\{A \mid \varphi\} &\text{ iff } x_n(\bullet) \Vdash_m \{A \mid \varphi\} \text{ for all } m > 0 \\ &\text{ iff } (x_n(\bullet))_m(\bullet) \in [\![\varphi]\!]^A(m) \text{ for all } m > 0 \\ &\text{ iff } x_n(\bullet) \in \{|\varphi|\}^A \\ &\text{ iff } x_n(\bullet) \in [\![[\mathsf{box}]\varphi]\!]^{\blacksquare A}(n) \\ &\text{ iff } x \Vdash_n \{\blacksquare A \mid [\mathsf{box}]\varphi\} \end{aligned}$$

Case of

$$\frac{\vdash^A_{\mathsf{c}} \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathsf{box}]\varphi\} \leq \{\blacksquare A \mid [\mathsf{box}]\psi\}}$$

By Lem. F.2 (Lem. D.13.(1)). ☐

Theorem F.16 (Adequacy (Thm. D.29)). *Let $\mathcal{E}, T$ have free iteration variables among $\overline{\ell}$, and let $\overline{m} \in \mathbb{N}$. If $\mathcal{E} \vdash M : T$ and $\rho \models \mathcal{E}$, then*

$$\forall n > 0, \quad \rho \Vdash_n \mathcal{E}[\overline{\ell}/\overline{m}] \quad \Longrightarrow \quad [\![M]\!]_\rho \Vdash_n T[\overline{\ell}/\overline{m}]$$

Proof. The proof is by induction on typing derivations. We implicitly use Lem. D.2 whenever required. We omit iteration variables when possible.

Case of

$$\frac{\mathcal{E}, x : \blacktriangleright T \vdash M : T}{\mathcal{E} \vdash \mathsf{fix}(x).M : T}$$

Let $\rho \models \mathcal{E}$ and write $y := [\![\mathsf{fix}(x).M]\!]_\rho \in \boldsymbol{\Gamma}[\![T]\!]$. Note that

$$y \quad = \quad [\![M[\mathsf{next}(\mathsf{fix}(x).M)/x]]\!]_\rho \quad = \quad [\![M]\!]_{\rho[\mathsf{next} \circ y/x]}$$

We show by induction on $n > 0$ that $\rho \Vdash_n \mathcal{E}$ implies $y \Vdash_n T$. In the base case $n = 1$, since $\mathsf{next} \circ y \Vdash_1 \blacktriangleright T$, we have $\rho[\mathsf{next} \circ y/x] \Vdash_1 \mathcal{E}, x : \blacktriangleright T$, so that the induction hypothesis on typing derivations gives $y = [\![M]\!]_{\rho[\mathsf{next} \circ y/x]} \Vdash_1 T$. As for induction step, assume $\rho \Vdash_{n+1} \mathcal{E}$. By Monotonicity of Realizability (Lem. F.13), we have $\rho \Vdash_n \mathcal{E}$, and the induction hypothesis on n gives $y \Vdash_n T$. It follows that $\mathsf{next} \circ y \Vdash_{n+1} \blacktriangleright T$, so that $\rho[\mathsf{next} \circ y/x] \Vdash_{n+1} \mathcal{E}, x : \blacktriangleright T$ and the induction hypothesis on typing derivations gives $y = [\![M]\!]_{\rho[\mathsf{next} \circ y/x]} \Vdash_{n+1} T$.

Case of

$$\frac{\mathcal{E} \vdash M : T}{\mathcal{E} \vdash \mathsf{next}(M) : \blacktriangleright T}$$

Let $\rho \models \mathcal{E}$ and write $x := [\![\mathsf{next}(M)]\!]_\rho \in \boldsymbol{\Gamma}[\![\blacktriangleright T]\!]$. Let $n > 0$ such that $\rho \Vdash_n T$. If $n = 1$ then we trivially have $x \Vdash_1 \blacktriangleright T$. Assume $n > 1$. Write $y := [\![M]\!]_\rho$, so that $x = \mathsf{next} \circ y$. By Monotonicity of Realizability (Lem. F.13), we have $\rho \Vdash_{n-1} \mathcal{E}$, so that the induction hypothesis on typing derivations gives $y \Vdash_{n-1} T$ and we are done.

Case of

$$\frac{x_1 : T_1, \ldots, x_k : T_k \vdash M : T \qquad \mathcal{E} \vdash M_1 : T_1 \quad \ldots \quad \mathcal{E} \vdash M_k : T_k}{\mathcal{E} \vdash \mathsf{box}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : \blacksquare T} \ (T_1, \ldots, T_k \text{ constant})$$

Let $\rho \models \mathcal{E}$ and write $x := [\![\mathsf{box}_\sigma(M)]\!]_\rho$ where $\sigma = [x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. We show $x \Vdash_n \blacksquare T$, *i.e.* that $x_m(\bullet) \Vdash_m T$ for all $m > 0$. Fix $m > 0$. We have by definition

$$x_m(\bullet) \quad : \quad \ell \quad \longmapsto \quad [\![M]\!]_\ell\Big([\![M_1]\!]_m(\rho_m(\bullet))\,,\, \ldots\,,\, [\![M_k]\!]_m(\rho_m(\bullet))\Big)$$

For $i = 1, \ldots, k$, since the type T_i is constant, we have by Lem. D.24 that $[\![M_i]\!]_m(\rho_m(\bullet)) = [\![M_i]\!]_\ell(\rho_\ell(\bullet))$ for all $\ell > 0$, so that

$$x_m(\bullet) \quad = \quad \ell \longmapsto [\![M]\!]_\ell\Big([\![M_1]\!]_\ell(\rho_\ell(\bullet))\,,\, \ldots\,,\, [\![M_k]\!]_\ell(\rho_\ell(\bullet))\Big)$$

Now, by induction hypothesis, since $\rho \Vdash_n \mathcal{E}$ by assumption, for each $i = 1, \ldots, k$ we have $[\![M_i]\!]_\rho \Vdash_n T_i$ and since T_i is constant, by Lem. D.24 this implies $[\![M_i]\!]_\rho \Vdash_\ell T_i$ for all $\ell > 0$. By induction hypothesis again, this in turn gives $[\![M]\!] \circ \langle [\![M_1]\!]_\rho, \ldots, [\![M_k]\!]_\rho \rangle \Vdash_\ell T$ for each $\ell > 0$. But then we are done since

$$\begin{aligned} x_m(\bullet) &= \ell \longmapsto [\![M]\!]_\ell\Big([\![M_1]\!]_\ell(\rho_\ell(\bullet))\,,\, \ldots\,,\, [\![M_k]\!]_\ell(\rho_\ell(\bullet))\Big) \\ &= [\![M]\!] \circ \langle [\![M_1]\!]_\rho, \ldots, [\![M_k]\!]_\rho \rangle \end{aligned}$$

Case of

$$\frac{\mathcal{E} \vdash M : \blacksquare T}{\mathcal{E} \vdash \mathsf{unbox}(M) : T}$$

Let $\rho \models \mathcal{E}$ and write $x := [\![\mathsf{unbox}(M)]\!]_\rho$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis we get $[\![M]\!]_\rho \Vdash_n \blacksquare T$, that is $([\![M]\!]_\rho)_m(\bullet) \Vdash_m T$ for all $m > 0$, so in particular $([\![M]\!]_\rho)_n(\bullet) \Vdash_n T$. But now we are done since $x_m(\bullet) = ([\![M]\!]_\rho)_n(\bullet)_m(\bullet)$ for each $m > 0$.

Case of

$$\frac{x_1 : T_1, \ldots, x_k : T_k \vdash M : \blacktriangleright T \qquad \mathcal{E} \vdash M_1 : T_1 \quad \ldots \quad \mathcal{E} \vdash M_k : T_k}{\mathcal{E} \vdash \mathsf{prev}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : T} \ (T_1, \ldots, T_k \text{ constant})$$

Let $\rho \models \mathcal{E}$ and write $x := [\![\mathsf{box}_\sigma(M)]\!]_\rho$ where $\sigma = [x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. We show $x \Vdash_n \blacktriangleright T$. If $n = 1$ then the result trivially holds. Assume $n > 1$. For each $m > 0$, we have by definition

$$x_m(\bullet) \quad = \quad [\![M]\!]_{m+1}\Big([\![M_1]\!]_m(\rho_m(\bullet))\,,\, \ldots\,,\, [\![M_k]\!]_m(\rho_m(\bullet))\Big)$$

For $i = 1, \ldots, k$, since the type T_i is constant, we have by Lem. D.24 that $[\![M_i]\!]_m(\rho_m(\bullet)) = [\![M_i]\!]_{m+1}(\rho_{m+1}(\bullet))$, so that

$$x_m(\bullet) \quad = \quad [\![M]\!]_{m+1}\Big([\![M_1]\!]_{m+1}(\rho_{m+1}(\bullet))\,,\, \ldots\,,\, [\![M_k]\!]_{m+1}(\rho_{m+1}(\bullet))\Big)$$

and it follows that

$$x \quad = \quad \mathsf{next} \circ [\![M]\!] \circ \langle [\![M_1]\!]_\rho, \dots, [\![M_k]\!]_\rho \rangle$$

Now, by induction hypothesis, since $\rho \Vdash_n \mathcal{E}$ by assumption, for each $i = 1, \dots, k$ we have $[\![M_i]\!]_\rho \Vdash_n T_i$ and since T_i is constant, by Lem. D.24 this implies $[\![M_i]\!]_\rho \Vdash_{n-1} T_i$. By induction hypothesis again, this in turn gives $[\![M]\!] \circ \langle [\![M_1]\!]_\rho, \dots, [\![M_k]\!]_\rho \rangle \Vdash_{n-1} T$ and we are done.

Case of

$$\frac{\mathcal{E} \vdash M : T \qquad T \leq U}{\mathcal{E} \vdash M : U}$$

By Lem. D.28 (Lem. F.15).

Case of

$$\frac{\mathcal{E} \vdash M : \{A \mid \psi \Rightarrow \varphi\} \qquad \mathcal{E} \vdash M : \{A \mid \psi\}}{\mathcal{E} \vdash M : \{A \mid \varphi\}}$$

Let $\rho \models \mathcal{E}$ and write $x := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A]\!]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis, the right premise gives $x_n(\bullet) \in [\![\psi]\!]^A(n)$ and the left premise implies $x_n(\bullet) \in [\![\varphi]\!]^A(n)$.

Case of

$$\frac{\mathcal{E} \vdash M : \{A \mid \varphi_0 \vee \varphi_1\} \qquad \begin{array}{l}\text{for } i \in \{0,1\}, \\ \mathcal{E}, x : \{A \mid \varphi_i\} \vdash N : U\end{array}}{\mathcal{E} \vdash N[M/x] : U}$$

Let $\rho \models \mathcal{E}$ and write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A]\!]$ and $z := [\![N]\!]_{\rho[y/x]} \in \boldsymbol{\Gamma}[\![|U|]\!]$. Let $n > 0$ and assume $\rho \Vdash_n \mathcal{E}$. By induction hypothesis we have $y \in [\![\varphi_i]\!]$ for some $i \in \{0, 1\}$. It follows that $\rho[y/x] \Vdash_n \mathcal{E}, x : \{A \mid \varphi_i\}$, from which we get $z \Vdash_n B$ by induction hypothesis.

Case of

$$\frac{\mathcal{E} \vdash M : \{A \mid \bot\} \qquad \mathcal{E} \vdash N : |U|}{\mathcal{E} \vdash N : U}$$

Let $\rho \models \mathcal{E}$ and write $x := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A]\!]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis, the left premise gives $x_n(\bullet) \in [\![\bot]\!](n) = \emptyset$, a contradiction. Hence $\rho \not\Vdash_n \mathcal{E}$, and the result follows.

Case of

$$\frac{\mathcal{E} \vdash M_i : \{A_i \mid \varphi\} \qquad \mathcal{E} \vdash M_{1-i} : A_{1-i}}{\mathcal{E} \vdash \langle M_0, M_1 \rangle : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y_0 := [\![M_0]\!]_\rho \in \boldsymbol{\Gamma}[\![A_0]\!]$, $y_1 := [\![M_1]\!]_\rho \in \boldsymbol{\Gamma}[\![A_1]\!]$, and $x := [\![\langle M_0, M_1 \rangle]\!]_\rho = \langle y_0, y_1 \rangle$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis on typing derivations we have $(y_i)_n(\bullet) \in [\![\varphi]\!]$. But since $\pi_i(x_n(\bullet)) = (y_i)_n(\bullet)$, this gives $x_n(\bullet) \in [\![[\pi_i]\varphi]\!]$.

Case of

$$\frac{\mathcal{E} \vdash M : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}{\mathcal{E} \vdash \pi_i(M) : \{A_i \mid \varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A_0 \times A_1]\!]$ and $x := [\![\pi_i(M)]\!]_\rho = \pi_i \circ y$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![[\pi_i]\varphi]\!]$, so that $\pi_i(y_n(\bullet)) \in [\![\varphi]\!]$. But then we are done since $x_n(\bullet) = \pi_i(y_n(\bullet))$.

Case of

$$\frac{\mathcal{E} \vdash M : \{A_i \mid \varphi\}}{\mathcal{E} \vdash \mathsf{in}_i(M) : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A_i]\!]$, and $x := [\![\mathsf{in}_i(M)]\!]_\rho = \mathsf{in}_i \circ y$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. Hence by induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![\varphi]\!]$. But since $x_n(\bullet) = \mathsf{in}_i(y_n(\bullet))$, this implies $x_n(\bullet) \in [\![[\mathsf{in}_i]\varphi]\!]$.

Case of

$$\frac{\mathcal{E} \vdash M : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\} \qquad \mathcal{E}, x : \{A_i \mid \varphi\} \vdash N_i : U \qquad \mathcal{E}, x : A_{1-i} \vdash N_{1-i} : U}{\mathcal{E} \vdash \mathsf{case}\, M \text{ of } (x.N_0 | x.N_1) : U}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A_0 + A_1]\!] \simeq \boldsymbol{\Gamma}[\![A_0]\!] + \boldsymbol{\Gamma}[\![A_1]\!]$. Hence $y = \mathsf{in}_j \circ z$ for some (unique) $j \in \{0, 1\}$ and $z \in \boldsymbol{\Gamma}[\![A_j]\!]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis, the left premise gives $y_n(\bullet) \in [\![[\mathsf{in}_i]\varphi]\!](n)$, so that $y_n(\bullet) = \mathsf{in}_i(u)$ for some $u \in [\![\varphi]\!](n)$. But this implies $j = i$ and $u = z_n(\bullet)$, so that $z \Vdash_n \{A_i \mid \varphi\}$. It follows that $\rho[z/x] \Vdash_n \mathcal{E}, x : \{A_i \mid \varphi\}$, and the induction hypothesis on typing derivations gives $[\![N_i]\!]_{\rho[z/x]} \Vdash_n U$. But then we are done since

$$[\![\mathsf{case}\, M \text{ of } (x.N_0 | x.N_1)]\!]_\rho \quad = \quad [\![N_i]\!]_{\rho[z/x]}$$

Case of

$$\frac{\mathcal{E}, x : \{B \mid \psi\} \vdash M : \{A \mid \varphi\}}{\mathcal{E} \vdash \lambda x.M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![\lambda x.M]\!]_\rho \in \boldsymbol{\Gamma}[\![B \to A]\!]$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. We show $y_n(\bullet) \in [\![[\mathsf{ev}(\psi)]\varphi]\!](n)$. So let $k \leq n$ and $u \in \boldsymbol{\Gamma}[\![B]\!](k)$ such that $u \in [\![\psi]\!](k)$. By [20, Cor. 3.8] there is some $z \in \boldsymbol{\Gamma}[\![B]\!]$ such that $z_k(\bullet) = t$. By Monotonicity of Realizability (Lem. F.13), we have $\rho \Vdash_k \mathcal{E}$, so that $\rho[z/x] \Vdash_k \mathcal{E}, x : \{B \mid \psi\}$. The induction hypothesis on typing derivations thus gives $([\![M]\!]_{\rho[z/x]})_k(\bullet) \in [\![\varphi]\!]$, and we are done since $(y_k(\bullet))(z_k(\bullet)) = ([\![M]\!]_{\rho[z/x]})_k(\bullet)$.

Case of

$$\frac{\mathcal{E} \vdash M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\} \qquad \mathcal{E} \vdash N : \{B \mid \psi\}}{\mathcal{E} \vdash MN : \{A \mid \varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![B \to A]\!]$, $z := [\![N]\!]_\rho \in \boldsymbol{\Gamma}[\![B]\!]$ and $x := [\![MN]\!]_\rho = \mathsf{ev} \circ \langle y, z\rangle$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction on typing derivations, the right premise gives $z_n(\bullet) \in [\![\psi]\!](n)$, so that the left premise gives $(y_n(\bullet))(z_n(\bullet)) \in [\![\varphi]\!](n)$. But then we are done since $x_n(\bullet) = (y_n(\bullet))(z_n(\bullet))$.

Case of

$$\frac{\mathcal{E} \vdash M : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}{\mathcal{E} \vdash \mathsf{fold}(M) : \{\mathsf{Fix}(X).A \mid [\mathsf{fold}]\varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![A[\mathsf{Fix}(X).A/X]]\!]$ and $x := [\![\mathsf{fold}(M)]\!]_\rho = \mathsf{fold} \circ y$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![\varphi]\!]$. But then we are done since $\mathsf{unfold}_n(x_n(\bullet)) = y_n(\bullet)$.

Case of

$$\frac{\mathcal{E} \vdash M : \{\mathsf{Fix}(X).A \mid [\mathsf{fold}]\varphi\}}{\mathcal{E} \vdash \mathsf{unfold}(M) : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}$$

Let $\rho \models \mathcal{E}$. Write $y := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![\mathsf{Fix}(X).A]\!]$ and $x := [\![\mathsf{unfold}(M)]\!]_\rho = \mathsf{unfold} \circ y$. Let $n > 0$ such that $\rho \Vdash_n \mathcal{E}$. By induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![[\mathsf{fold}]\varphi]\!]$. Hence $\mathsf{unfold}_n(y_n(\bullet)) \in [\![\varphi]\!]$ and we are done since $x_n(\bullet) = \mathsf{unfold}_n(y_n(\bullet))$.

Cases of

$$\frac{\mathcal{E} \vdash M : T[\mathtt{0}/\ell] \qquad \mathcal{E} \vdash M : T[\ell{+}\mathtt{1}/\ell]}{\mathcal{E} \vdash M : \forall\ell \cdot T} \ (\ell \text{ not free in } \mathcal{E}) \qquad \frac{\mathcal{E} \vdash M : T}{\mathcal{E} \vdash M : \forall\ell \cdot T} \ (\ell \text{ not free in } \mathcal{E})$$

Let $\rho \models \mathcal{E}$ and write $x := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![|T|]\!]$. Let $n > 0$ and assume $\rho \Vdash_n \mathcal{E}$. Let $m \in \mathbb{N}$. We have to show $M \Vdash_n T[\mathtt{m}/\ell]$. Since ℓ does not occur free in $\mathcal{E}$, we have $\rho \Vdash_n \mathcal{E}[\mathtt{m}'/\ell]$ for all $m' \in \mathbb{N}$. For both rules we can conclude from the induction hypothesis.

Case of

$$\frac{\mathcal{E} \vdash M : \forall\ell \cdot T}{\mathcal{E} \vdash M : T[\mathtt{t}/\ell]}$$

Let $\rho \models \mathcal{E}$ and write $x := [\![M]\!]_\rho \in \boldsymbol{\Gamma}[\![|T|]\!]$. Let $n > 0$ and assume $\rho \Vdash_n \mathcal{E}$. By induction hypothesis we have $x \Vdash_n T[\mathtt{m}/\ell]$ for $m = [\![\mathtt{t}]\!]$ and the result follows.

Cases of

$$\frac{\mathcal{E} \vdash M : \left\{\blacksquare A \;\middle|\; [\mathsf{box}]\gamma[\nu^\ell\alpha\varphi/\beta]\right\} \qquad \beta \text{ Pos } \gamma}{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\nu\alpha\varphi/\beta]\}}$$

$$\frac{\mathcal{E} \vdash M : \{\blacksquare A \mid [\mathsf{box}]\gamma[\mu\alpha\varphi/\beta]\} \qquad \mathcal{E}, x : \left\{\blacksquare A \;\middle|\; [\mathsf{box}]\gamma[\mu^\ell\alpha\varphi/\beta]\right\} \vdash N : U \qquad \beta \text{ Pos } \gamma}{\mathcal{E} \vdash N[M/x] : U}$$

where ℓ is not free in $\mathcal{E}, U, \gamma$, and γ, φ are smooth. First, since φ is smooth by Lem. 7.4 we have

$$\begin{array}{rl} & \{\!|\nu\alpha\varphi(\alpha)|\!\} = \bigcap_{m\in\mathbb{N}} \{\!|\varphi^m(\top)|\!\} \\ \text{and} & \{\!|\mu\alpha\varphi(\alpha)|\!\} = \bigcup_{m\in\mathbb{N}} \{\!|\varphi^m(\top)|\!\} \end{array}$$

Moreover, since β is positive in γ and γ is smooth, it follows from Lem. F.12 (Lem. 7.4) that $\{\!|\gamma|\!\}$ is continuous and cocontinuous in β. We thus get

$$\begin{array}{rl} & \{\!|\gamma[\nu\alpha\varphi(\alpha)/\beta]|\!\} = \bigcap_{m\in\mathbb{N}} \{\!|\gamma[\varphi^m(\top)/\beta]|\!\} \\ \text{and} & \{\!|\gamma[\mu\alpha\varphi(\alpha)/\beta]|\!\} = \bigcup_{m\in\mathbb{N}} \{\!|\gamma[\varphi^m(\top)/\beta]|\!\} \end{array}$$

and the result follows. □

Table of Contents