Temporal Refinements for Guarded Recursive Types

Guilhem Jaber, Colin Riba

Temporal Refinements for Guarded Recursive Types

Guilhem Jaber*
guilhem.jaber@univ-nantes.fr

Colin Riba†
colin.riba@ens-lyon.fr

Abstract

We propose a framework to reason on temporal properties of higher-order programs with coinductive types. It extends guarded recursive types with temporal refinements, which are formulae of the modal μ-calculus. Its semantics is given inside the topos of trees, and corresponds to the standard semantics for safety properties (defined as greatest fixpoints). For more general properties involving least fixpoints, we accommodate an external semantics, whose interaction with the internal one is regulated when restricting to the flat μ-calculus, in which fixpoints can be computed by iteration over $\mathbb{N}$, and thus can be unfolded syntactically.

Keywords guarded recursive types, μ-calculus, refinement types

1 Introduction

Programming on infinite objects like streams is crucial to represent reactive systems. In such settings, programs in general do not terminate, but always compute a part of their output in a finite amount of time. For example, if a program is expected to generate a stream, it should always be able to produce the next element in finite time: it is *productive*.

Functional programming offers high-level abstractions to handle infinite data, with declarative definitions and equational reasoning. This is exemplified by functional reactive programming [16], in which datatypes formed of infinite objects are represented as coinductive types.

The goal of this paper is to be able to specify temporal properties of higher-order programs that handle coinductive types. Temporal logics like LTL, CTL or the modal μ-calculus are widely used to formulate, on infinite objects, specifications like safety, liveness or fairness properties (see e.g. [6]). 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 introduce temporal refinement types $\{A \mid \varphi\}$, where A is a standard type of our programming language, (e.g. the type of streams Str), and φ is a formula of the (flat) μ-calculus. Using refinements [17], 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 map function on streams can have the following two types:

$$(\{\mathsf{B} \mid \psi\} \to \{\mathsf{A} \mid \varphi\}) \to \{\mathrm{Str}\,\mathsf{B} \mid \Box[\psi]\} \to \{\mathrm{Str}\,\mathsf{A} \mid \Box[\varphi]\}$$
$$(\{\mathsf{B} \mid \psi\} \to \{\mathsf{A} \mid \varphi\}) \to \{\mathrm{Str}\,\mathsf{B} \mid \Diamond[\psi]\} \to \{\mathrm{Str}\,\mathsf{A} \mid \Diamond[\varphi]\}$$

These types are intended to mean that given $f : B \to A$ s.t. $f(b)$ satisfies φ whenever b satisfies ψ, the function $\mathrm{map} f$ takes a stream whose elements all (resp. at least one) satisfy ψ to one whose elements all (resp. at least one) satisfy φ.

Having a type system enables to reason compositionally on programs, by decomposing a specification to the various components of a program and pick the right temporal refinements for each component in order to prove the global specification.

Our system is built on top of Nakano's guarded recursive types [42]. Guarded recursive types use a type modality $\blacktriangleright T$, called "later", to indicate that a value of type T is not available now but only after one "time-step", that could correspond to performing some computations like unfolding a recursive definition. Using this modality, one can then have fixpoint combinators for both terms and types, while ensuring productivity of programs by enforcing that recursive definitions are guarded with $\blacktriangleright$ in the type system.

The programming language we consider is the guarded λ-calculus [13], a higher-order programming language over both guarded and coinductive types, that uses a modality $\blacksquare$ to transform guarded recursive types into coinductive types. The adequacy of our modal refinements is proved w.r.t. a denotational semantics of this language in the topos of trees.

Our main challenge is that the topos of trees has unique guarded fixpoints [8], and that only safety properties (e.g. $\Box[\varphi]$) can be correctly represented. In order to correctly handle liveness properties (e.g. $\Diamond[\varphi]$), that are defined as least fixpoints, one needs to escape the topos of trees and go to the standard world of sets.

This leads to a two level type system: 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 modal fixpoints are correctly handled, but without direct access to guarded recursion. By restricting to *flat* modal fixpoints [47] (e.g. $\Box$, $\Diamond$), which can always be computed in ω-steps, one can syntactically reason on finite unfoldings of least fixpoints, thus allowing for crossing the safety barrier.

Organization of the paper. We first give an overview of our approach in §2, and describe related work in §3. Then §4 presents the syntax of the guarded λ-calculus. Our temporal

*Université de Nantes, LS2N CNRS, Inria, France
†Univ Lyon, EnsL, UCBL, CNRS, LIP, F-69342, LYON Cedex 07, France

Conference'17, July 2017, Washington, DC, USA
2020. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00

$$\begin{array}{rcll} \mathsf{cons}^{\mathsf{g}} & := & \lambda x.\lambda s.\mathsf{fd}(\langle x, s\rangle) & : \quad \mathsf{A} \to \blacktriangleright\, \mathrm{Str}^{\mathsf{g}}\,\mathsf{A} \to \mathrm{Str}^{\mathsf{g}}\,\mathsf{A} \\ \mathsf{hd}^{\mathsf{g}} & := & \lambda s.\pi_0(\mathsf{ufd}\ s) & : \quad \mathrm{Str}^{\mathsf{g}}\,\mathsf{A} \to \mathsf{A} \\ \mathsf{tl}^{\mathsf{g}} & := & \lambda s.\pi_1(\mathsf{ufd}\ s) & : \quad \mathrm{Str}^{\mathsf{g}}\,\mathsf{A} \to \blacktriangleright\, \mathrm{Str}^{\mathsf{g}}\,\mathsf{A} \\ \mathsf{map}^{\mathsf{g}} & := & \lambda f.\mathsf{fix}(g).\lambda s.\mathsf{cons}^{\mathsf{g}}\ (f(\mathsf{hd}^{\mathsf{g}}\ s))\ (g \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) & \\ & : & (B \to A) \to \mathrm{Str}^{\mathsf{g}}\,B \to \mathrm{Str}^{\mathsf{g}}\,A & \end{array}$$

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

logic is introduced in §5, and it is used to define our temporally refined type system (§6). Its semantics, inside the topos of trees, is defined in §7. Finally, we discuss future possible work in §8. Full proofs are available in the Appendices.

2 Outline

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

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

With this syntax, the basic destructors and the constructor on guarded streams are given in Figure 1. where $\mathsf{fd}(-)$ and $\mathsf{ufd}(-)$ are explicit term constructor for folding and unfolding guarded recursive types. In the following, we use the infix notation $a :: s$ for $\mathsf{cons}^{\mathsf{g}}\ a\ s$. Using the fact that the type modality $\blacktriangleright$ is an applicative functor [38], we can distribute $\blacktriangleright$ over the arrow type. This is represented in the programming language by the applicative construction $\circledast$. With it, one can define the usual map function on guarded streams.

The Semantics of Guarded Recursive Types in the Topos of Trees. The types of this language can be interpreted as sequences of indexed sets $(X(n))_{n>0}$ where $X(n)$ represents the values available "at time n". To navigate through time via the type modality $\blacktriangleright$ and the term construction next, one also needs to have access to functions $r_n^X : X(n+1) \to X(n)$. This means that the objects used to represent types are in fact *presheaves* over the poset $(\mathbb{N} \setminus \{0\}, \leq)$, the functions r_n^X being the so-called *restriction morphisms*.

The category $\mathcal{S}$ of such presheaves is called the *topos of trees* [8]. The type modality $\blacktriangleright$ is interpreted by the endofunctor on $\mathcal{S}$ that maps $X(n+1)$ to $X(n)$ (for $n > 1$) and $X(1)$ to the singleton set $\mathbf{1}$.

Considering a guarded recursive type $\mathsf{Fix}(X).A$ where X is the only free type variable of A, and whose occurrences are guarded by a $\blacktriangleright$ modality, the open type A is interpreted as an endofunctor F_A over $\mathcal{S}$. This functor has a unique fixpoint in $\mathcal{S}$, which interprets $\mathsf{Fix}(X).A$.

The guarded streams $\mathrm{Str}^{\mathsf{g}}\,\mathsf{B}$ over a finite base type B are then interpreted as the indexed sequences of sets $(\mathsf{B}^n)_{n\in\mathbb{N}_*}$ with the restriction morphism r_n mapping $(\mathsf{a}_1, \ldots, \mathsf{a}_n, \mathsf{a}_{n+1})$ to $(\mathsf{a}_1, \ldots, \mathsf{a}_n)$.

Compositional Safety Reasoning on Streams. Given a property φ on a type A, we would like to consider a subtype of $\mathrm{Str}^{\mathsf{g}}\,A$ that selects those streams whose elements all satisfy φ. To do so, we introduce a temporal modality "always φ", written $\Box[\varphi]$, and consider the refinement type $\{\mathrm{Str}^{\mathsf{g}}\,A \mid \Box[\varphi]\}$. Suppose for now that we can give the following refinement types to the basic stream operations:

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

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

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

A Coalgebraic Temporal Logic. Our temporal modal logic is many-sorted, so that in a refinement type $\{A \mid \varphi\}$ the formula φ talks about elements of type A. To do so, following intuitions of [23], we use basic modalities $[\pi_i]$, $[\mathsf{fd}]$ and $[\mathsf{next}]$ to navigate between guarded recursive types.

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. So given a formula $\vdash \varphi : A$, one can define its "current lift" $[\mathsf{hd}]\varphi$ of type $\mathrm{Str}^{\mathsf{g}}\,A$, that enforces φ to be satisfied on the head of the provided stream. Also, one can define the "next-step" modality $\bigcirc$ such that given a formula $\vdash \psi : \mathrm{Str}^{\mathsf{g}}\,A$, the formula $\bigcirc\psi : \mathrm{Str}^{\mathsf{g}}\,A$ enforces ψ to be satisfied on the tail of the provided stream. These modalities are obtained as

$$[\mathsf{hd}]\varphi := [\mathsf{fd}][\pi_0]\varphi \qquad \bigcirc\varphi := [\mathsf{fd}][\pi_1][\mathsf{next}]\varphi$$

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, so that $\{A \mid \varphi\} \leq \{A \mid \psi\}$ when $\vdash^A \varphi \Rightarrow \psi$. The subtyping relation is thus crucial in order to incorporate logical reasoning in our type system.

In addition, we have greatest fixpoints predicates $\nu\alpha.\varphi$, with Kozen-style ([31]) reasoning principles. Using them, we can form the "always" modality $\Box$, as, for $\varphi : \mathrm{Str}^{\mathsf{g}}\,A$,

$$\Box\varphi := \nu\alpha.\varphi \wedge \bigcirc\alpha \quad : \quad \mathrm{Str}^{\mathsf{g}}\,A$$

which intuitively holds on a stream s iff φ holds on every substream $s[n\ldots)$ for $n \in \mathbb{N}$. If we rather start with $\psi : A$, one then need to lift it to $\mathrm{Str}^{\mathsf{g}}\,A$. This is what we have written $[\psi]$ in the previous paragraph. It can simply be defined as

$[\mathsf{hd}]\psi$. One can then check that $\Box[\mathsf{hd}]\psi$ indeed means that all the elements of the stream satisfies ψ, since all its suffixes satisfies $[\mathsf{hd}]\psi$.

Beyond Safety Reasoning: The Failure of the Internal Semantics. One would also want to define least fixpoints predicates $\mu\alpha.\varphi$. For example, one could consider the modality $\Diamond\varphi$ defined as the least fixpoint $\mu\alpha.\varphi \vee \bigcirc\alpha$. One could then give the following two types to the guarded stream constructor $\mathsf{cons}^{\mathsf{g}}$:

- $\mathsf{cons}^{\mathsf{g}} \ : \ \{A \mid \varphi\} \to \blacktriangleright \mathrm{Str}^{\mathsf{g}}\, A \to \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Diamond[\varphi]\}$;
- $\mathsf{cons}^{\mathsf{g}} \ : \ A \to \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Diamond\varphi\} \to \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Diamond[\varphi]\}$.

But consider a finite base type A with two distinguished elements a, b, and suppose that we have access to a modality $[\mathsf{a}]$ on A so that terms inhabiting $\{\mathsf{A} \mid [\mathsf{a}]\}$ must be equal to a. Using the second least fixpoint rule, we could type the stream with constant value b, defined as $\mathrm{fix}(s).\mathsf{b} :: s$, with the type $\{\mathrm{Str}^{\mathsf{g}}\, \mathsf{A} \mid \Diamond[\mathsf{a}]\}$ that is supposed to enforce the existence of an occurrence of a in the stream. It is clearly problematic!

This comes from the fact that inside the topos of trees the recursive definitions that one can compute satisfy a unique fixpoint theorem [8].

To avoid this problem, one needs to compute least fixpoints externally, directly on the sets of global elements. But in general one cannot transform back such sets of global elements into subobjects of the topos of trees. This is apparent with this property $\Diamond\mathsf{a}$. It is interpreted externally as the set of streams that contain at least an occurrence of a. There is no subobject of $\mathrm{Str}^{\mathsf{g}}\, \mathsf{A}$ that correspond correctly to this set of streams, since the only possible one would be $\mathrm{Str}^{\mathsf{g}}\, A$. Indeed, such a subobject would be a collection $(C_n)_{n\in\mathbb{N}_*}$ of subsets of A^n. But since for any $n \in \mathbb{N}_*$, any element of A^n can be extended into a stream that contains an occurrence of a, necessarily C_n would be equal to A^n.

For safety properties, it is still possible to transform their external semantics, defined as sets of global elements, into subobjects of the topos of trees, simply because safety properties represent topologically *closed* sets.

The Necessity of an External Semantics. As shown above, we have a formal system with least and greatest fixpoints that has a semantics inside the topos of trees. However, this system does not correspond to the standard way to reason on least fixpoints. It is thus important to relate the semantics of our system to a standard **Set**-based semantics of the coalgebraic μ-calculus. To do so, we need to restrict ourselves to polynomial types, for which it is possible to represent guarded recursive types as **Set**-based final coalgebra. In this setting, Møgelberg [40], has been able to prove a correspondence between the final coalgebras computed inside the topos of trees and the **Set**-based ones.

The Constant Modality. To define correctly least fixpoints of temporal predicates over a type A we have seen that we need to access the global elements of A. However, the internal semantics is still necessary to handle definitions by guarded recursion. We thus need to have available in our logic a way to navigate between the internal and the external semantics. To do so, we use the constant modality $\blacksquare$ introduced in [13]. It was used in this paper to transform guarded recursive types into coinductive types, in order to define programs that are productive but not causal.

To be able to build predicates over $\blacksquare T$, we also use a modality $[\mathrm{bx}]\varphi$. We permit to navigate between $\blacksquare\, \{A \mid \varphi\}$ and $\{\blacksquare A \mid [\mathrm{bx}]\varphi\}$ via the subtyping relation, but only when φ is safe. Indeed, for safety properties, one can transform their external semantics into a subobject, which is equal to their internal semantics inside $\mathcal{S}$.

Approximating Least Fixpoints. In order to reason on unsafe properties such as $\Diamond\varphi$, one introduces finite approximation of these properties, that is finite unfolding. Approximating fixpoints with finite unfolding, à la Kleene, is possible because we restrict to *flat* fixpoints [47]. We consider finite iterations $\mu\alpha^k\varphi$ of least fixpoints, with k an "iteration variable". We can then define approximations of $\Diamond\varphi$ as

$$\Diamond^k\varphi \quad := \quad \mu\alpha^k.\varphi \vee \bigcirc\alpha$$

The approximations $\Diamond^k\varphi$ are safe for φ safe. We can type $\mathrm{map}^{\mathsf{g}}$ with

$$(\{B \mid \varphi\} \to \{A \mid \psi\}) \to \left\{\mathrm{Str}^{\mathsf{g}}\, B \,\middle|\, \Diamond^k[\varphi]\right\} \to \left\{\mathrm{Str}^{\mathsf{g}}\, A \,\middle|\, \Diamond^k[\psi]\right\}$$

From it, one can prove that the map function, lifted to coinductive streams Str defined as $\blacksquare\, \mathrm{Str}^{\mathsf{g}}$, has type

$$(\{\mathsf{B} \mid \psi\} \to \{\mathsf{A} \mid \varphi\}) \longrightarrow \{\mathrm{Str}\,\mathsf{B} \mid [\mathrm{bx}]\Diamond[\mathsf{hd}]\psi\} \longrightarrow \{\mathrm{Str}\,\mathsf{A} \mid [\mathrm{bx}]\Diamond[\mathsf{hd}]\varphi\}$$

One can even go further, by replacing $\Diamond$ with $\Diamond\Box$ or $\Box\Diamond$.

3 Related Work

Using guarded recursive types, type systems have been designed to enforce good properties of programs handling coinductive types, like causality [33], productivity [4, 40, 13, 19] or the absence of space leaks [32] and time leaks [5].

Guarded Dependent Type Theory [9, 7], combine dependent types with guarded recursive types. One can thus use dependent type to give precise specifications. It should thus be possible to prove safety properties in these theories. However, it does not seem possible to do the same for liveness properties, as they do not have access to least fixpoints.

In a different line of work, temporal logics have been used as type systems for functional reactive programs, starting from LTL[25, 26] to the intuitionistic modal μ-calculus [11]. These works follow the "proof-as-programs" motto, and reflect in the programming languages the constructions of the temporal logic. In particular, temporal operators are wired into the structure of types, so that different temporal specifications for the same program may lead to differences in the actual code, contrary to our work.

$$
\begin{array}{rcl@{\quad}rcl@{\quad}rcl}
v & ::= & & M,N & ::= & v \mid x & E & ::= & \bullet \\
& \mid & \lambda x.M & & \mid & MN & & \mid & EM \\
& \mid & \langle M_0, M_1\rangle & & \mid & \pi_0(M) & & \mid & \pi_0(E) \\
& \mid & \langle\rangle & & \mid & \pi_1(M) & & \mid & \pi_1(E) \\
& \mid & \mathsf{in}_0(M) & & \mid & \mathsf{case}\ M\ \mathsf{of} & & \mid & \mathsf{case}\ E\ \mathsf{of} \\
& \mid & \mathsf{in}_1(M) & & & (x.N_0|x.N_1) & & & (x.N_0|x.N_1) \\
& \mid & \mathsf{fd}(M) & & \mid & \mathsf{ufd}(M) & & \mid & \mathsf{ufd}(E) \\
& \mid & \mathsf{bx}_\sigma(M) & & \mid & \mathsf{ubx}(M) & & \mid & \mathsf{ubx}(E) \\
& \mid & \mathsf{next}(M) & & \mid & \mathsf{prev}_\sigma(M) & & \mid & \mathsf{prev}_{[]}(E) \\
& & & & \mid & M \circledast N & & \mid & E \circledast M \\
& & & & \mid & \mathsf{fix}(x).M & & \mid & v \circledast E
\end{array}
$$

Figure 2. Values, Terms and Evaluation Contexts.

$$
\begin{array}{rcll}
(\lambda x.M)N & \rightsquigarrow & M[N/x] & \\
\pi_i(\langle M_0, M_1\rangle) & \rightsquigarrow & M_i & \\
\mathsf{case}\ \mathsf{in}_i(M)\ \mathsf{of}\ (x.N_0|x.N_1) & \rightsquigarrow & N_i[M/x] & \\
\mathsf{ufd}(\mathsf{fd}(M)) & \rightsquigarrow & M & \\
\mathsf{fix}(x).M & \rightsquigarrow & M[\mathsf{next}(\mathsf{fix}(x).M)/x] & \\
\mathsf{next}(M) \circledast \mathsf{next}(N) & \rightsquigarrow & \mathsf{next}(MN) & \\
\mathsf{ubx}(\mathsf{bx}_{[x_1\mapsto M_1,\ldots,x_n\mapsto M_n]}(M)) & \rightsquigarrow & M[M_1/x_1,\ldots,M_n/x_n] & \\
\mathsf{prev}(\mathsf{next}(M)) & \rightsquigarrow & M & \\
\mathsf{prev}_{[x_1\mapsto M_1,\ldots,x_n\mapsto M_n]}(M) & \rightsquigarrow & \mathsf{prev}(M[M_1/x_1,\ldots,M_n/x_n]) & (n \geq 1)
\end{array}
$$

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

Figure 3. Operational Semantics.

More generally, verification of higher-order programs has a vast literature. Higher-order model checking [43, 29] 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 formulas. Automatic verification of higher-order programs with infinite data-types (integers) has been explored for safety [30, 27], termination [34], and more generally ω-regular [41] properties. In this setting, the combination of refinement types with automatic techniques like predicate abstraction [46] or SMT solvers [50, 49] has been particularly successful. However, none of these works has considered coinductive types.

4 The Pure Calculus

This Section presents the guarded λ-calculus of [13], with an emphasis on the examples relevant to our framework.

Terms. We consider values and terms from the grammar given in Fig. 2. In both $\mathsf{bx}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$, σ is a *delayed substitution* of the form $\sigma = [x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$ and such that $\mathsf{bx}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$ bind $x_1, \ldots, x_k$ in M. We use the convention of [13] that $\mathsf{bx}(M)$ and $\mathsf{prev}(M)$ (without indicated substitution) stand resp. for $\mathsf{bx}_{[]}(M)$ and $\mathsf{prev}_{[]}(M)$ *i.e.* bind no variable of M.

We consider a weak call-by-name reduction, defined in Fig. 3. The productivity of the operational semantics is ensured by the insertion of next in the reduction rule of fix.

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

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

where, (1) in the case $\mathsf{Fix}(X).A$, X does occur in A and 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.

We could actually have included primitive infinite base types (say a type of natural numbers as in [13]), but we refrain to do so in order to keep the system not too complex.

Example 4.1. Thanks to sum types, we can code a finite base type $\mathsf{B} = \{\mathsf{b}_1, \ldots, \mathsf{b}_n\}$ 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 b_i of B. At the term level, the elements of B are represented as compositions of injections $\mathsf{in}_{j_1}(\mathsf{in}_{j_2}(\ldots \mathsf{in}_{j_i}\langle\rangle))$,

Example 4.2. Guarded recursive definitions are formalized using the fixpoint constructor $\mathsf{Fix}(X).A$ on types, which allows for X to appear in A both at positive and negative positions, but only under a $\blacktriangleright$. Then one can define the type $\mathsf{Str}^{\mathsf{g}}\, A$ of guarded streams of A as $\mathsf{Fix}(X).A \times \blacktriangleright X$ and the type $\mathsf{Tree}^{\mathsf{g}}\, A$ of infinite binary trees over A as $\mathsf{Fix}(X).A \times (\blacktriangleright X \times \blacktriangleright X)$.

Definition 4.3. *A pure type A is* constant *if each occurrence of $\blacktriangleright$ in A is guarded by a $\blacksquare$ modality.*

The typing rules of the pure calculus are given in Fig. 4.

Positive and Polynomial Pure Types. A (pure) type is *positive* (notation P^+, Q^+, etc.) if each arrow ($\to$) is guarded by a $\blacksquare$ modality. So positive types are defined by the grammar

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

Positive types are a convenient generalization of *polynomial types*. In the context of this paper, we say that a guarded recursive type $\mathsf{Fix}(X).P(X)$ is *polynomial* if $P(X)$ is induced by the grammar

$$P(X) ::= \mathbf{1} \mid \blacktriangleright X \mid P(X) + P(X) \mid P(X) \times P(X) \mid \blacksquare A$$

For Q^+ a constant positive type, $\mathsf{Str}^{\mathsf{g}}\, Q^+$ and $\mathsf{Tree}^{\mathsf{g}}\, Q^+$ are polynomial types. More generally, polynomial types include all recursive types $\mathsf{Fix}(X).P(X)$ for $P(X)$ of the form

$$\sum_{i=0}^{n} a_i \blacktriangleright X^i$$

where X^i is the product of i copies of X and $a_i X^i$ (for $a_i \in \mathbb{N}$) is the sum of a_i copies of X^i.

Examples. We have seen in Fig. 1 how to define constructor, destructors and the map function over guarded streams. One can also define a merge function that takes two guarded

$$\frac{(x:A)\in\Gamma}{\Gamma\vdash x:A} \qquad \frac{\Gamma,x:B\vdash M:A}{\Gamma\vdash\lambda x.M:B\to A} \qquad \frac{\Gamma\vdash M:B\to A \quad \Gamma\vdash N:B}{\Gamma\vdash MN:A}$$

$$\frac{}{\Gamma\vdash\langle\rangle:\mathbf{1}} \qquad \frac{\Gamma\vdash M_0:A_0 \qquad \Gamma\vdash M_1:A_1}{\Gamma\vdash\langle M_0,M_1\rangle:A_0\times A_1} \qquad \frac{\Gamma\vdash M:A_0\times A_1}{\Gamma\vdash\pi_i(M):A_i}$$

$$\frac{\Gamma\vdash M:A_i}{\Gamma\vdash \mathsf{in}_i(M):A_0+A_1} \qquad \frac{\Gamma\vdash M:A_0+A_1 \qquad \text{for } i\in\{0,1\},\ \Gamma,x:A_i\vdash N_i:B}{\Gamma\vdash \mathsf{case}\,M\,\mathsf{of}\,(x.N_0|x.N_1):B}$$

$$\frac{\Gamma\vdash M:A[\mathsf{Fix}(X).A/X]}{\Gamma\vdash \mathsf{fd}(M):\mathsf{Fix}(X).A} \qquad \frac{\Gamma\vdash M:\mathsf{Fix}(X).A}{\Gamma\vdash \mathsf{ufd}(M):A[\mathsf{Fix}(X).A/X]}$$

$$\frac{x_1:A_1,\dots,x_k:A_k\vdash M:A \qquad \text{for } 1\le i\le k,\ \Gamma\vdash M_i:A_i \text{ with } A_i \text{ const.}}{\Gamma\vdash \mathsf{bx}_{[x_1\mapsto M_1,\dots,x_k\mapsto M_k]}(M):\blacksquare A}$$

$$\frac{\Gamma\vdash M:\blacksquare A}{\Gamma\vdash \mathsf{ubx}(M):A} \qquad \frac{\Gamma\vdash M:A}{\Gamma\vdash \mathsf{next}(M):\blacktriangleright A}$$

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

$$\frac{\Gamma\vdash M:\blacktriangleright(B\to A) \qquad \Gamma\vdash N:\blacktriangleright B}{\Gamma\vdash M\circledast N:\blacktriangleright A} \qquad \frac{\Gamma,x:\blacktriangleright A\vdash M:A}{\Gamma\vdash \mathsf{fix}(x).M:A}$$

Figure 4. Typing Rules of the Pure Calculus.

streams and interleaves them:

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

Coinductive streams are guarded streams under a $\blacksquare$:

$$\mathsf{Str}\,A \quad := \quad \blacksquare\,\mathsf{Str}^{\mathsf{g}}A$$

The basic operations on guarded streams lift to coinductive ones (for A a constant type):

$$\begin{array}{rcll}\mathsf{cons} & := & \lambda x.\lambda s.\mathsf{bx}\big(x::^{\mathsf{g}}(\mathsf{ubx}\ s)\big) & : \ A\to\mathsf{Str}\,A\to\mathsf{Str}\,A\\ \mathsf{hd} & := & \lambda s.\mathsf{hd}^{\mathsf{g}}\ (\mathsf{ubx}\ s) & : \ \mathsf{Str}\,A\to A\\ \mathsf{tl} & := & \lambda s.\mathsf{bx}\big(\mathsf{prev}\ (\mathsf{tl}^{\mathsf{g}}\ (\mathsf{ubx}\ s))\big) & : \ \mathsf{Str}\,A\to\mathsf{Str}\,A\end{array}$$

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

$$\begin{array}{rcl}\mathsf{map} & : & (B\to A)\longrightarrow\mathsf{Str}\,B\longrightarrow\mathsf{Str}\,A\\ & := & \lambda f.\lambda s.\mathsf{bx}\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{ubx}\ s)\big)\end{array}$$

Example 4.4 (The Diagonal Stream Function). Coalgebraic streams allow for more functions than guarded streams, as for instance the following diagonal stream function

$$\begin{array}{rcl}\mathsf{diag} & : & \mathsf{Str}(\mathsf{Str}\,A)\longrightarrow\mathsf{Str}\,A\\ & := & \lambda s.\mathsf{bx}\big(\mathsf{diag}^{\mathsf{g}}\ (\mathsf{ubx}\ s)\big)\end{array}$$

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

$$\begin{array}{rcl}\mathsf{diagaux}^{\mathsf{g}} & : & (\mathsf{Str}\,A\to\mathsf{Str}\,A)\to\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A)\to\mathsf{Str}^{\mathsf{g}}\,A\\ & := & \mathsf{fix}(f).\lambda g.\lambda s.\ (\mathsf{hd}\circ g)(\mathsf{hd}^{\mathsf{g}}\ s)::^{\mathsf{g}}\\ & & \qquad f\circledast\mathsf{next}(g\circ\mathsf{tl})\circledast(\mathsf{tl}^{\mathsf{g}}\ s)\end{array}$$

The auxiliary higher-order function $\mathsf{diagaux}^{\mathsf{g}}$ iterates coinductive tl functions over the head of the stream of streams s.

5 A Temporal Modal Logic

This Section presents our logic of (modal) temporal specifications. We focus on syntactic aspects. The semantics is discussed in §7.

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

Manysorted Modal Temporal Formulae. Our logical language, that we took with minor adaptations from [23], is *manysorted*: for each pure type A we have formulae *of type* A (notation $\vdash\varphi:A$) as defined in Fig. 5. For every pure type A, formulae of type A are closed under usual propositional connectives. Moreover (and that is the key ingredient we took from [23]), formulae of compound types (say $A_0\times A_1$ or A_0+A_1) may be obtained from formulae of the component types. 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 selects those inhabitants of $A_0\times A_1$ whose first component satisfies φ.

Example 5.1. Given a finite base type $\mathsf{B}=\{\mathsf{b}_1,\dots,\mathsf{b}_n\}$ as in Ex. 4.1, with element 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 $\{\mathsf{b}_k\}$ of B.

Example 5.2. (a) On guarded streams, have the modalities $[\mathsf{hd}]$ and $\bigcirc$ mentioned in §2, with $[\mathsf{hd}]\varphi:\mathsf{Str}^{\mathsf{g}}A$ and $\bigcirc\psi:\mathsf{Str}^{\mathsf{g}}A$ provided $\varphi:A$ and $\psi:\mathsf{Str}^{\mathsf{g}}A$:

$$[\mathsf{hd}]\varphi\ (=\ [\varphi])\ :=\ [\mathsf{fd}][\pi_0]\varphi \qquad \bigcirc\psi\ :=\ [\mathsf{fd}][\pi_1][\mathsf{next}]\psi$$

(b) On (guarded) infinite binary trees over A, we also have a modality $[\mathsf{rt}]\varphi:=[\mathsf{fd}][\pi_0]\varphi:\mathsf{Tree}^{\mathsf{g}}A$ (provided $\varphi:A$). Moreover, we have modalities $\bigcirc_0$ and $\bigcirc_1$ defined on formulae $\varphi:\mathsf{Tree}^{\mathsf{g}}A$ as $\bigcirc_i\varphi\ :=\ [\mathsf{fd}][\pi_1][\pi_i][\mathsf{next}]\varphi$. Intuitively, $[\mathsf{rt}]\varphi$ should hold on a tree t over A iff the root label of t satisfies φ, and $\bigcirc_i\varphi$ should hold on t iff φ holds on the ith son of t.

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

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

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

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

$$\frac{\alpha : A \vdash \varphi : A \qquad \alpha \text{ Pos } \varphi}{\vdash \nu\alpha^{\mathtt{t}_\omega}\varphi : A} \ (\alpha \text{ guarded in } \varphi,\ \mathtt{t}_\omega \text{ iteration term or } \omega)$$

$$\frac{\alpha : A \vdash \varphi : A \qquad \alpha \text{ Pos } \varphi}{\vdash \mu\alpha^{\mathtt{t}_\omega}\varphi : A} \ (\alpha \text{ guarded in } \varphi,\ \mathtt{t}_\omega \text{ iteration term or } \omega)$$

Figure 5. Formation Rules of Flat Formulae.

Our logic has greatest and least *flat* fixpoints, notation $\nu\alpha^{\omega}\varphi$ and $\mu\alpha^{\omega}\varphi$. The rules of Fig. 5 thus allow for the formation of formulae with free typed propositional variables (ranged over by $\alpha, \beta, \dots$), and thus 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 [next] modality. We assume a usual positivity condition of α in φ, represented as usual by an inductive predicate α Pos φ.

Remark 5.3. Note that formulae $[\mathsf{bx}]\varphi$ and $[\mathsf{ev}(\psi)]\varphi$ can only be formed for *closed* formulae φ, ψ.

Example 5.4. The modality $\Box$ makes it possible to express a range of safety properties. For instance, assuming $\varphi, \psi : \mathrm{Str}^{\mathrm{g}} A$, the formula $\Box(\psi \Rightarrow \bigcirc\varphi)$ is intended to hold on a stream s iff, for all $n \in \mathbb{N}$, if the substream $s(n).s(n+1).\cdots$ satisfies ψ, then $s(n+1).s(n+2).\cdots$ satisfies φ.

Example 5.5. The modality $\Box$ extends to infinite binary trees over A, with $\Box\varphi := \nu\alpha.\varphi \wedge (\bigcirc_0\alpha \wedge \bigcirc_1\alpha) : \mathrm{Tree}^{\mathrm{g}} A$. For e.g. $\psi : A$, $\Box[\mathsf{rt}]\psi$ is intended to hold on a tree t over A iff all node-labels of t satisfy ψ.

The restriction to *flat* fixpoints [47] means that greatest (resp. least) fixpoints $\nu\alpha^{\omega}\varphi(\alpha)$ (resp. $\mu\alpha^{\omega}\varphi(\alpha)$) have no free propositional variable (*i.e.* $\varphi(\alpha)$ has at most α free). This implies that greatest (resp. least) fixpoints can be thought about as

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

Iteration terms allow for formal reasoning about such iterations. Assuming $[\![\mathtt{t}]\!] = m \in \mathbb{N}$, the formula $\nu\alpha^{\mathtt{t}}\varphi(\alpha)$ (resp. $\mu\alpha^{\mathtt{t}}\varphi(\alpha)$) can be read as $\varphi^m(\top)$ (resp. $\varphi^m(\bot)$).

Modal Theories. Formulae are equipped with a modal deduction system which enters the type system via a subtyping relation (§6). For each pure type A, we have an intuitionistic theory $\vdash^A$ (the general case) and a classical theory $\vdash^A_{\mathrm{c}}$ (which is only assumed under $\blacksquare$/[bx]), summarized in Fig. 6 and Table 1. The atomic modalities $[\pi_i]$, [fd], [next], $[\mathsf{in}_i]$ and [bx] have unbouded deterministic branching (see Fig. 9, §7). In any case, $\vdash^A_{(\mathrm{c})} \varphi$ is only defined when $\vdash \varphi : A$ (and so when φ has no free propositional variable).

We can get the axioms of the intuitionistic (normal) modal logic **IK** [45] (see also e.g. [48, 37]) for $[\pi_i]$, [fd] and [bx] but not for $[\mathsf{in}_i]$ nor for the intuitionistic [next]. For [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 in particular allows to derive, for a finite base type B

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

This implies that the necessitation rule (see Rem. 5.7) does not hold for $[\mathsf{in}_i]$.

Fixpoints $\nu\alpha^{\omega}\varphi$ and $\mu\alpha^{\omega}\varphi$ are equipped with their usual Kozen axioms [31]. In addition, iteration formulae $\nu\alpha^{\mathtt{t}}\varphi(\alpha)$ and $\mu\alpha^{\mathtt{t}}\varphi(\alpha)$ have axioms expressing that they are indeed iterations of $\varphi(\alpha)$ from resp. $\top$ and $\bot$.

Definition 5.6 (Modal Theories)**.** *For each pure type A, the* intuitionistic *and* classical *modal theories $\vdash^A$ and $\vdash^A_{\mathrm{c}}$ are defined by mutual induction as follows:*

- *The theory $\vdash^A$ is deduction for intuitionistic propositional logic augmented with the checkmarked (✓) axioms and rules of Table 1 and the rules of Fig. 6 (for $\vdash^A$).*
- *The theory $\vdash^A_{\mathrm{c}}$ is $\vdash^A$ augmented with the axioms* (P) *and* ($\mathsf{C}_{\Rightarrow}$) *for* [next] *and with the axiom* (CL) *(Fig. 6).*

In any case, $\vdash^A \varphi$ and $\vdash^A_{\mathrm{c}} \varphi$ are only defined when $\vdash \varphi : A$.

Remark 5.7. All modalities ($[\pi_i]$, [fd], [next], $[\mathsf{in}_i]$, $[\mathsf{ev}(\psi)]$ and [bx]) satisfy the *monotonicity rule* (RM) and are thus monotone in the sense of [12], from which we borrowed the terminology used in Table 1 (see also [20, 18]). With our adaptation to unbounded deterministic branching, the normal intuitionistic modal logic **IK** of [45] is (RM) + (C) + (N) + (P) + ($\mathsf{C}_{\vee}$) + ($\mathsf{C}_{\Rightarrow}$), while the normal modal logic **K** is **IK** + (CL) (see e.g. [10]).

Example 5.8. Using the rules to reason on greatest fixpoints, one can prove the following implications:

$$\vdash^{\mathrm{Str}^{\mathrm{g}} A} \Box\psi \Rightarrow \psi \wedge \bigcirc\Box\psi \qquad \vdash^{\mathrm{Str}^{\mathrm{g}} A} (\psi \wedge \bigcirc\Box\psi) \Rightarrow \Box\psi$$

The Safe Fragment. The safe fragment plays a crucial role, because it reconciliates the internal and external semantics of our system (see §7). The safe fragment impacts the subytping relation (Fig. 7, §6).

Definition 5.9 (Safe Formula)**.** *A formula $\alpha_1 : A_1, \dots, \alpha_n : A_n \vdash \varphi : A$ is* safe *if $A_1, \dots, A_n, A$ are positive types and if moreover all occurrences in φ of least fixpoints ($\mu\alpha^{\omega}(-)$) and implications ($\Rightarrow$) are guarded by* [bx].

Name	Formulation	$[\pi_i]$	[fd]	[next]	$[\mathsf{in}_i]$	[ev(ψ)]	[bx]	[hd]	○
(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)**
($C_\vee$)	$[\triangle](\varphi \vee \psi) \implies [\triangle]\varphi \vee [\triangle]\psi$	✓	✓	✓	✓		✓	✓	✓
($C_\Rightarrow$)	$([\triangle]\psi \Rightarrow [\triangle]\varphi) \implies [\triangle](\psi \Rightarrow \varphi)$	✓	✓	**(C)**			✓	✓	**(C)**

Table 1. Modal Axioms and Rules (with types omitted in $\vdash$ and where **(C)** marks axioms assumed for $\vdash_c$ but not for $\vdash$).

$$\frac{}{\vdash_c^A ((\varphi \Rightarrow \psi) \Rightarrow \varphi) \Rightarrow \varphi}\ (\mathsf{CL})$$

$$\frac{\vdash_c^A \varphi}{\vdash^{\blacksquare A} [\mathsf{bx}]\varphi} \qquad \frac{\vdash^B \psi \Rightarrow \phi \qquad \vdash \varphi : A}{\vdash^{B \to A} [\mathsf{ev}(\phi)]\varphi \Rightarrow [\mathsf{ev}(\psi)]\varphi}$$

$$\frac{}{\vdash^{A_0+A_1} \left([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\right) \wedge \neg\left([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\right)}$$

$$\frac{}{\vdash^{A_0+A_1} ([\mathsf{in}_i]\top) \Rightarrow (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)}$$

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

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

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

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

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

Figure 6. Modal Axioms and Rules.

Recalling that the theory under a [bx] is $\vdash_c^A$, the only propositional connectives accessible to $\vdash^A$ in safe formulae are those on which $\vdash^A$ and $\vdash_c^A$coincide.

Example 5.10. Any formula without fixpoint is equivalent in $\vdash_c$ to a safe formulae. Given safe formulae $\psi : A$ and $\varphi : \mathrm{Str}^g A$, the formulae $\Box[\mathsf{hd}]\psi$ and $\Box\varphi$ are both safe.

6 A Temporally Refined Type System

Temporal Refinement Types. Temporal refinement types (or simply *types*), ranged over by T, U, V, etc., are defined by the grammar:

$$T ::= A \mid \{A \mid \varphi\} \mid \forall k \cdot T \mid T + T \mid T \times T \mid T \to T \mid \blacktriangleright T \mid \blacksquare T$$

So types are built from (closed) pure types A and temporal refinements $\{A \mid \varphi\}$, where $\vdash \varphi : A$. They allow all the type constructors of pure types (where T has no free type variables in $\blacksquare T$). Types furthermore allow for universal quantifications over iteration variables with $\forall k \cdot T$.

Subtyping. As a refined 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 refined 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 an intuitionistic modal theory (notation $\vdash^A \varphi$ for provability of a formula φ of type A), discussed in §5.

The subtyping rules for 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 Figure 12 in the Appendix B. Notice that we do not incorporate folding and unfolding of guarded recursive types in subtyping.

Typing with Temporal Refinement Types. Typing for refined types is given by the rules of Fig. 8, together with the rules of Fig. 4 *extended to refinement types*, where T is *constant* if $|T|$ is constant. Modalities $[\pi_i]$, $[\mathsf{in}_i]$, [fd] and [ev(−)] (but [next]) have introduction rules extending those of the corresponding term formers.

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

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

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

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

Figure 7. Subtyping Rules (excerpt).

Example 6.1. Using the fact that $\varphi \Rightarrow \psi \Rightarrow (\varphi \wedge \psi)$ and two times the rule (MP), one gets the derived rule:

$$\frac{\Gamma \vdash M : \{A \mid \varphi\} \qquad \Gamma \vdash M : \{A \mid \psi\}}{\Gamma \vdash M : \{A \mid \varphi \wedge \psi\}}$$

from which one can deduce the rule:

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

Example 6.2 (Operations on Guarded Streams). The following typings, mentioned in §2, are easy to derive:

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

For e.g. $\mathsf{cons}^{\mathsf{g}}$, direct applications of the rules give

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

where $\Gamma = x : \{A \mid \varphi\}, s : \blacktriangleright \{\mathsf{Str}^{\mathsf{g}} A \mid \Box[\mathsf{hd}]\varphi\}$. We conclude with Ex. 6.1 and Ex. 5.8. The cases of hd^{g} and tl^{g} are similar and simpler. One can then type $\mathsf{map}^{\mathsf{g}}$ with

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

Indeed, the above types for $\mathsf{cons}^{\mathsf{g}}$, hd^{g} and tl^{g} give

$$\Gamma' \;\vdash\; \mathsf{cons}^{\mathsf{g}}\,(f(\mathsf{hd}^{\mathsf{g}}\,s))\,(g \circledast (\mathsf{tl}^{\mathsf{g}}\,s)) \;:\; \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Box[\mathsf{hd}]\psi\}$$

with $\Gamma' := f : \{A \mid \varphi\} \to \{B \mid \psi\}, g : \blacktriangleright(\{\mathsf{Str}^{\mathsf{g}} A \mid \Box[\varphi]\} \to \{\mathsf{Str}^{\mathsf{g}} B \mid \Box[\psi]\}), s : \{\mathsf{Str}^{\mathsf{g}} A \mid \Box[\varphi]\}$.

Similarly, one can type the function $\mathsf{merge}^{\mathsf{g}}$ with

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

Example 6.3. For a *safe* $\varphi : A$, we can type map with

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

with $\triangle \in \{\Diamond, \Diamond\Box, \Box\Diamond\}$. In the case of $\Diamond$, one starts, using the rules (μ-E) and (μ-E), to reduce to a typing of the form

$$\Gamma_f,\; s : \left\{\mathsf{Str}\,B \;\middle|\; [\mathsf{bx}]\Diamond^k[\psi]\right\} \vdash \mathsf{bx}(\mathsf{map}^{\mathsf{g}}\; f\; (\mathsf{ubx}\; s)) : \left\{\mathsf{Str}\,A \;\middle|\; [\mathsf{bx}]\Diamond^k[\varphi]\right\}$$

Since $\Diamond^k[\varphi]$ and $\Diamond^k[\psi]$ are safe, one can apply the subtyping rule for $\Box$ to get the type $\blacksquare\left\{\mathsf{Str}^{\mathsf{g}} A \;\middle|\; \Diamond^k[\varphi]\right\}$. Then we apply the typing rule for bx presentend in Figure 4 (and extended to refinement types), so that one can conclude by typing *guarded* $\mathsf{map}^{\mathsf{g}}$ as

$$(\{\mathsf{B} \mid \psi\} \to \{\mathsf{A} \mid \varphi\}) \to \forall k \cdot (\{\mathsf{Str}^{\mathsf{g}}\,\mathsf{B} \mid \Box[\mathsf{hd}]\psi\} \to \{\mathsf{Str}^{\mathsf{g}}\,\mathsf{A} \mid \Box[\mathsf{hd}]\varphi\})$$

Using the rules ($\forall$-CI) and (ExF), we are left with

$$\Gamma \;\vdash\; \mathsf{cons}^{\mathsf{g}}\,(f(\mathsf{hd}^{\mathsf{g}}\,s))\,(g \circledast (\mathsf{tl}^{\mathsf{g}}\,s)) \;:\; \{\mathsf{Str}^{\mathsf{g}}\,B \mid \Box[\mathsf{hd}]\psi\}$$

where Γ is $f : \{A \mid \varphi\} \to \{B \mid \psi\}$, $s : \left\{\mathsf{Str}^{\mathsf{g}} A \;\middle|\; \Diamond^{k+1}[\varphi]\right\}$, $g : \blacktriangleright\forall\ell \cdot (\left\{\mathsf{Str}^{\mathsf{g}} A \;\middle|\; \Diamond^{\ell}[\varphi]\right\} \to \left\{\mathsf{Str}^{\mathsf{g}} B \;\middle|\; \Diamond^{\ell}[\psi]\right\})$. Using subtyping, one can instantiate ℓ with k. Unfolding $\Diamond^{k+1}[\varphi]$ and then reasoning by cases with ($\vee$-E) gives the result.

The case of $\Diamond\Box$ is similar, but the type of $\mathsf{map}^{\mathsf{g}}$ has to be strengthened. Since [next] (and thus $\bigcirc$) do not satisfy axiom (P) of Table 1 (see §7), giving g the type, say,

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

in the branch of $s : \{\mathsf{Str}^{\mathsf{g}} A \mid \Box[\varphi]\}$ is not sufficient. The solution is provided by the $[\mathsf{ev}(-)]$ modality, used to encode a kind of "intersection" on arrow types, to type $\mathsf{map}^{\mathsf{g}}$ with

$$(\{\mathsf{B} \mid \psi\} \to \{\mathsf{A} \mid \varphi\}) \to \forall k \cdot \{\mathsf{Str}^{\mathsf{g}} B \to \mathsf{Str}^{\mathsf{g}} A \mid \theta(k) \;\wedge\; [\mathsf{ev}(\Box[\psi])]\Box[\varphi]\}$$

where $\theta(k)$ is $[\mathsf{ev}(\Diamond^k\Box[\psi])]\Diamond^k\Box[\varphi]$. The case of $\Box\Diamond$ is more intricate. See App. D.2 for details.

Remark 6.4. The $[\mathsf{ev}(-)](-)$ modalities provide a mean to incorporate properties of functions. This is instrumental in giving good refined typings with a $\Diamond$ modality. As we shall see in §7, the $[\mathsf{ev}(-)](-)$ modalities can be seen as a form of internalized *logical predicates* in the sense of [22, §9.2].

Example 6.5 (The Diagonal Stream Function). For a *safe* $\varphi : A$, we have the following (see App. D.3):

$$\begin{array}{rcl} \mathsf{diag}^{\mathsf{g}} & : & \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{bx}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\mathsf{hd}]\varphi\} \\ \mathsf{diag} & : & \{\mathsf{Str}(\mathsf{Str}\,A) \mid [\mathsf{bx}]\Box[\mathsf{hd}][\mathsf{bx}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}\,A \mid [\mathsf{bx}]\Box[\mathsf{hd}]\varphi\} \\ \mathsf{diag} & : & \{\mathsf{Str}(\mathsf{Str}\,A) \mid [\mathsf{bx}]\Diamond\Box[\mathsf{hd}][\mathsf{bx}]\Box[\mathsf{hd}]\varphi\} \longrightarrow \{\mathsf{Str}\,A \mid [\mathsf{bx}]\Diamond\Box[\mathsf{hd}]\varphi\} \end{array}$$

7 Semantics

The Section progressively presents 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, that we briefly sketch.

$$(\textsc{Sub})\ \frac{\Gamma \vdash M : T \qquad T \leq U}{\Gamma \vdash M : U} \qquad (\text{MP})\ \frac{\Gamma \vdash M : \{A \mid \psi \Rightarrow \varphi\} \qquad \Gamma \vdash M : \{A \mid \psi\}}{\Gamma \vdash M : \{A \mid \varphi\}}$$

$$(\vee\text{-E})\ \frac{\Gamma \vdash M : \{A \mid \varphi_0 \vee \varphi_1\} \qquad \Gamma, x : \{A \mid \varphi_i\} \vdash N : U \quad \text{for } i \in \{0,1\},}{\Gamma \vdash N[M/x] : U} \qquad (\text{ExF})\ \frac{\Gamma \vdash M : \{A \mid \bot\} \qquad \Gamma \vdash N : |U|}{\Gamma \vdash N : U}$$

$$(\textsc{Pr}_i\text{-I})\ \frac{\Gamma \vdash M_i : \{A_i \mid \varphi\} \quad \Gamma \vdash M_{1-i} : A_{1-i}}{\Gamma \vdash \langle M_0, M_1\rangle : \{A_0 \times A_1 \mid [\pi_i]\varphi\}} \qquad (\textsc{Pr}_i\text{-E})\ \frac{\Gamma \vdash M : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}{\Gamma \vdash \pi_i(M) : \{A_i \mid \varphi\}} \qquad (\textsc{Inj}_i\text{-I})\ \frac{\Gamma \vdash M : \{A_i \mid \varphi\}}{\Gamma \vdash \mathsf{in}_i(M) : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\}}$$

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

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

$$(\textsc{Fd}\text{-I})\ \frac{\Gamma \vdash M : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}{\Gamma \vdash \mathsf{fd}(M) : \{\mathsf{Fix}(X).A \mid [\mathsf{fd}]\varphi\}} \qquad (\textsc{Fd}\text{-E})\ \frac{\Gamma \vdash M : \{\mathsf{Fix}(X).A \mid [\mathsf{fd}]\varphi\}}{\Gamma \vdash \mathsf{ufd}(M) : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}$$

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

$$(\nu\text{-I})\ \frac{\Gamma \vdash M : \left\{\blacksquare A \,\middle|\, [\mathrm{bx}]\gamma[\nu\alpha^k\varphi/\beta]\right\}}{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\gamma[\nu\alpha^\omega\varphi/\beta]\}} \qquad (\nu\text{-E})\ \frac{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\gamma[\nu\alpha^\omega\varphi/\beta]\}}{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\gamma[\nu\alpha^{\mathtt{t}}\varphi/\beta]\}} \qquad (\mu\text{-I})\ \frac{\Gamma \vdash M : \left\{\blacksquare A \,\middle|\, [\mathrm{bx}]\gamma[\mu\alpha^{\mathtt{t}}\varphi/\beta]\right\}}{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\gamma[\mu\alpha^\omega\varphi/\beta]\}}$$

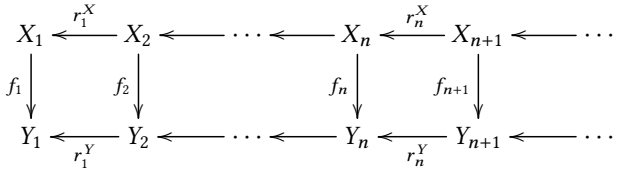
$$(\mu\text{-E})\ \frac{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\gamma[\mu\alpha^\omega\varphi/\beta]\} \qquad \Gamma, x : \left\{\blacksquare A \,\middle|\, [\mathrm{bx}]\gamma[\mu\alpha^k\varphi/\beta]\right\} \vdash N : U}{\Gamma \vdash N[M/x] : U}$$

Figure 8. Typing Rules for Refined Modal Types, (where k is fresh and β is positive in γ).

Denotational Semantics in the Topos of Trees. The *topos of trees* [8] provides a natural model of guarded recursion.

Definition 7.1 (The Topos of Trees). *The* topos of trees $\mathcal{S}$ *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* $r_n^X : X(n+1) \to X(n)$. Intuitively, $X(n)$ represents the values available "at time n", and r_n^X tells how values "at $n+1$" can be restricted (actually most often truncated) to values "at n". Excluding 0 from the indexes is a customary notational convenience [8]. The morphisms from X to Y are families of functions $f = (f_n : X(n) \to Y(n))_{n>0}$ which commute with restriction:



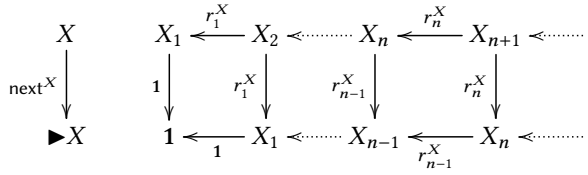
As any presheaf category, $\mathcal{S}$ has (pointwise) limits and colimits, and is Cartesian closed (see e.g. [36, §I.6]). We write $\Gamma : \mathcal{S} \to \mathbf{Set}$ for the *global section functor*, which takes X to $\mathcal{S}[\mathbf{1}, X]$, the set of $\mathcal{S}$ morphisms $\mathbf{1} \longrightarrow X$, where $\mathbf{1} = (\{\bullet\})_{n>0}$ is the terminal object of $\mathcal{S}$.

A typed term $\Gamma \vdash M : T$ is to be interpreted as a morphism

$$[\![M]\!] \ : \ [\![|\Gamma|]\!] \longrightarrow_{\mathcal{S}} [\![|T|]\!]$$

where $[\![|\Gamma|]\!] = [\![|T_1|]\!] \times \cdots \times [\![|T_n|]\!]$ for $\Gamma = x_1 : T_1, \ldots, x_n : T_n$. In particular, a closed term $M : T$ is to be interpreted as a global section $[\![M]\!] \in \Gamma[\![|T|]\!]$. 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 [8]. 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:



The guarded fixpoint combinator fix is interpreted by the morphism $\mathsf{fix}^X : X^{\blacktriangleright X} \to X$, natural in X, such that 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 s.t.:

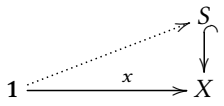
$$Y \xrightarrow{\langle \text{next fix } f^t,\ \mathrm{id}\rangle} \blacktriangleright X \times Y \xrightarrow{f} X \quad = \quad Y \xrightarrow{\text{fix } f^t} X$$

Together with an interpretation of guarded recursive types (see [8]) this gives an denotational semantics of the whole calculus but for the ■ modality. See [8, 13] for details.

We write $\mathsf{fd} : [\![A[\mathsf{Fix}(X).A/X]]\!] \to [\![\mathsf{Fix}(X).A]\!]$ and $\mathsf{ufd} : [\![\mathsf{Fix}(X).A]\!] \to [\![A[\mathsf{Fix}(X).A/X]]\!]$ for the two isomorphisms of $[\![\mathsf{Fix}(X).A]\!] \simeq [\![A[\mathsf{Fix}(X).A/X]]\!]$.

Internal Semantics of Formulae. Each formula φ over A has a $\mathcal{S}$ interpretation, in the form of a subobject $[\![\varphi]\!]$ of $[\![A]\!]$.

A *subobject* S of a $\mathcal{S}$ object X, notation $S \hookrightarrow X$, is a family of subsets $S(n) \subseteq X(n)$ such that $r_n^X(t) \in S(n)$ whenever $t \in S(n+1)$. The set of subobjects of a $\mathcal{S}$ object X, denoted $\mathrm{Sub}(X)$, is a complete lattice w.r.t. pointwise inclusions (see e.g. [36, Prop. I.8.5]), and in particular a (complete) Heyting algebra. Following e.g. [36, 35], we say that $x \in \Gamma X$ *satisfies* a property $S \in \mathrm{Sub}(X)$ if x factors through S, as in



Note that this means

$$\forall n > 0, \quad x_n(\bullet) \in S(n)$$

By *adequacy* of the $\mathcal{S}$ semantics, we mean that for each closed term $M : \{A \mid \varphi\}$, the global section $[\![M]\!] \in \Gamma[\![A]\!]$ satisfies the property $[\![\varphi]\!] \in \mathrm{Sub}([\![A]\!])$.

Formulae without free iteration variables are interpreted by induction as expected. The propositional connectives are interpreted by the Heyting algebra structure on subobjects. This validates the rules of intuitionistic logic.

We now turn to the interpretation of modalities. Let $[\triangle]$ be a modality of the form $[\pi_i]$, $[\mathsf{in}_i]$, [next] or [fd], and assume $[\triangle]\varphi : B$ whenever $\varphi : A$. Standard topos theoretic constructions give posets morphisms

$$[\![[\triangle]]\!] \quad : \quad \mathrm{Sub}([\![A]\!]) \longrightarrow \mathrm{Sub}([\![B]\!])$$

such that:

- $[\![[\pi_i]]\!]$ and $[\![[\mathsf{fd}]]\!]$ are maps of Heyting algebras,
- $[\![[\mathsf{in}_i]]\!]$ preserves $\vee$, $\bot$ and $\wedge$,
- $[\![[\mathsf{next}]]\!]$ preserves $\wedge$, $\top$ and $\vee$.

With $[\![[\triangle]\varphi]\!] := [\![[\triangle]]\!]([\![\varphi]\!])$, all the axioms and rules of Table 1 are validated for these modalities. To handle guarded recursion, it is crucial to have

$$[\![[\mathsf{next}]\varphi]\!] \quad := \quad \blacktriangleright([\![\varphi]\!])$$

with $[\![[\mathsf{next}]\varphi]\!]$ true at time 1, independently from φ. As consequence, [next] and $\bigcirc$ do not validate axiom (P) (Table 1), and $\Diamond[\mathsf{hd}]\varphi$ can "lie" about the next time step.

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 [22, §9.2 & Prop. 9.2.4]. The idea is

$$\begin{array}{lcl}
\wr[\pi_i]\varphi\wr & := & \{x \in \Gamma[\![A_0 \times A_1]\!] \mid \pi_i \circ x \in \wr\varphi\wr\} \\
\wr[\mathsf{next}]\varphi\wr & := & \{\mathsf{next} \circ x \in \Gamma[\![\blacktriangleright A]\!] \mid x \in \wr\varphi\wr\} \\
\wr[\mathsf{fd}]\varphi\wr & := & \{x \in \Gamma[\![\mathsf{Fix}(X).A]\!] \mid \mathsf{ufd} \circ x \in \wr\varphi\wr\} \\
\wr[\mathsf{in}_i]\varphi\wr & := & \\
\multicolumn{3}{l}{\quad \{x \in \Gamma[\![A_0 + A_1]\!] \mid \exists y \in \Gamma[\![A_i]\!] (x = \mathsf{in}_i \circ y \text{ and } y \in \wr\varphi\wr)\}} \\
\wr[\mathsf{ev}(\psi)]\varphi\wr & := & \\
\multicolumn{3}{l}{\{x \in \Gamma[\![B \to A]\!] \mid \forall y \in \Gamma[\![B]\!],\ y \in \wr\psi\wr \implies \mathsf{ev} \circ \langle x, y\rangle \in \wr\varphi\wr\}}
\end{array}$$

Figure 9. External Semantics (■-free formulae).

that for a term $M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\}$, the global section $\mathsf{ev} \circ \langle [\![M]\!], x\rangle \in \Gamma[\![A]\!]$ should satisfy φ whenever $x \in \Gamma[\![B]\!]$ satisfies ψ. We refer to App. C for details.

The interpretations of $\nu\alpha^{\mathsf{t}}\varphi(\alpha)$ and $\mu\alpha^{\mathsf{t}}\varphi(\alpha)$ (for t closed) are defined to be the interpretations resp. of $\varphi^{[\![\mathsf{t}]\!]}(\top)$ and $\varphi^{[\![\mathsf{t}]\!]}(\bot)$, where e.g. $\varphi^0(\top) := \top$ and $\varphi^{n+1}(\top) := \varphi(\varphi^n(\top))$.

We turn to fixpoints $\nu\alpha^{\omega}\varphi(\alpha)$ and $\mu\alpha^{\omega}\varphi(\alpha)$. A naive possibility would be to rely on Kaster-Tarski Fixpoint Theorem and the fact that when α is positive in φ (*i.e.* α Pos φ), the typing $\alpha : A \vdash \varphi : A$ induces a poset morphism

$$[\![\varphi]\!] \quad : \quad \mathrm{Sub}([\![A]\!]) \longrightarrow \mathrm{Sub}([\![A]\!])$$

This, however, is to some extent meaningless in our setting, because $\mathcal{S}$ has *unique* guarded fixpoints [8, §2.5].

Proposition 7.2. *Given $\alpha : A \vdash \varphi(\alpha) : A$ with α positive and guarded by $\blacktriangleright$ in φ, there is a* unique $[\![\nu\alpha^{\omega}\varphi(\alpha)]\!] \in \mathrm{Sub}([\![A]\!])$ *such that* $[\![\nu\alpha^{\omega}\varphi(\alpha)]\!] = [\![\varphi(\nu\alpha^{\omega}\varphi(\alpha))]\!]$.

In particular, the typing $\mathsf{fix}(s).\mathsf{cons}^{\mathrm{g}}\ a\ s : \{\mathrm{Str}^{\mathrm{g}}\ A \mid \Diamond[\varphi]\}$ for arbitrary $a : A$ and $\varphi : \mathrm{Str}^{\mathrm{g}}\ A$ of §2 is not problematic w.r.t. the $\mathcal{S}$ semantics $[\![-]\!]$!

The External Semantics. The above issue suggests to look for semantics closer to the intended meaning of the logic. Møgelberg [40] has shown that for polynomial types such as $\mathrm{Str}^{\mathrm{g}}\ \mathsf{B}$ with B a finite base type, the set of global sections $\Gamma[\![\mathrm{Str}^{\mathrm{g}}\ \mathsf{B}]\!]$ is equipped with the usual final coalgebra structure of streams over B in **Set**.

This suggests, for a formula $\varphi : A$, to devise a proper **Set** interpretation $\wr\varphi\wr \in \mathcal{P}(\Gamma[\![A]\!])$. For propositional connectives and fixpoints, this interpretation is defined similarly as the $\mathcal{S}$ interpretation, but using the Boolean algebra structure of powersets rather than the Heyting algebra structure of subobjects. We give the cases of the modalities $[\pi_i]$, $[\mathsf{in}_i]$, [next] and [fd] in Fig. 9 (where for simplicity we assume formulae to be closed). It can be checked that, when restricting to polynomial functors, one recovers the expected coalgebraic semantics of [23] (with sums treated as in [24]) extended with fixpoints.

The Safe Fragment. We would like to have adequacy w.r.t. the **Set** semantics, namely that given $M : \{A \mid \varphi\}$, the global section $[\![M]\!] \in \Gamma[\![A]\!]$ satisfies $\wr\varphi\wr \in \mathcal{P}(\Gamma[\![A]\!])$ in the sense

that $[\![M]\!] \in \wr\varphi\wr$. The odd typing of §2 tells us that this is impossible in general. But this is possible for *safe* formulae since in this case we have:

$$\wr\varphi\wr \quad = \quad \Gamma[\![\varphi]\!]$$

Let us sketch the key ingredients for this property. First note that on $\blacksquare$-free types, safe formulae do not contain implications ($\Rightarrow$). For this fragment, intuitionistic and classical logic coincide, making $\wr\varphi\wr = \Gamma[\![\varphi]\!]$ plausible.

Second, for a safe formula $\alpha : A \vdash \varphi : A$, the poset morphisms

$$\begin{array}{rcccc} [\![\varphi]\!] & : & \mathrm{Sub}([\![A]\!]) & \longrightarrow & \mathrm{Sub}([\![A]\!]) \\ \wr\varphi\wr & : & \mathcal{P}(\Gamma[\![A]\!]) & \longrightarrow & \mathcal{P}(\Gamma[\![A]\!]) \end{array}$$

are *Scott cocontinuous*, in the sense that they preserve codirected meets. As a consequence, greatest fixpoints $\nu\alpha^\omega\varphi(\alpha)$ can be interpreted, *both in* **Set** *and* $\mathcal{S}$, as the meets of the interpretations of

$$\top\,, \quad \varphi(\top)\,, \quad \varphi(\varphi(\top))\,, \quad \cdots \quad \varphi^n(\top)\,, \quad \varphi^{n+1}(\top)\,, \quad \cdots$$

This leads to the expected coincidence of the two semantics. In particular, the **Set** semantics is adequate for safe formulae.

Let us step back to the cases of $\Box[\varphi]$ and $\Diamond[\varphi]$ on guarded streams $\mathrm{Str}^{\mathsf{g}}\,\mathsf{B}$. Assume that φ is safe. The equality

$$\wr\Box[\varphi]\wr \quad = \quad \Gamma[\![\Box[\varphi]]\!]$$

implies that the usual **Set** semantics of $\Box[\varphi]$ is in the image of Γ. But a subset of $\Gamma[\![\mathrm{Str}^{\mathsf{g}}\,\mathsf{B}]\!]$ which is in the image of Γ 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 $\Box[\varphi]$ do define safety properties on streams. On the other hand, liveness properties of the form $\Diamond[\varphi]$ are not closed (for non-trivial φ), and as such cannot be in the image of Γ.

The Constant Modality. In order to safely handle unsafe formulae, we rely on the *constant* type modality $\blacksquare$ of [13]. At the semantic level, $\blacksquare$ is interpreted as the composite functor $\Delta\Gamma : \mathcal{S} \to \mathcal{S}$, where the *constant object functor* $\Delta : \mathbf{Set} \to \mathcal{S}$ takes a set S to the constant family $(S)_{n>0}$. In words, all components $[\![\blacksquare A]\!](n)$ are equal to $\Gamma[\![A]\!]$, and the restriction maps of $[\![\blacksquare A]\!]$ are identities. In particular, a global section $x \in \Gamma[\![\blacksquare A]\!]$ is a constant family $(x_n)_n$ describing a unique global section $x_{n+1}(\bullet) = x_n(\bullet) \in \Gamma[\![A]\!]$. We refer to [13] and App. C for the interpretation of the term constructors prev, bx and ubx.

Consider now an arbitrary formula φ over A. In order to accommodate its **Set** semantics $\wr\varphi\wr$ within $\mathcal{S}$, we can syntactically lift φ to the formula $[\mathrm{bx}]\varphi$ over $\blacksquare A$ and impose

$$[\![[\mathrm{bx}]\varphi]\!] \quad := \quad \Delta\left(\wr\varphi\wr\right)$$

This definition is justified by simple and standard facts of topos theory,[1] namely that for each set S, the functor Δ induces a map of (complete) Heyting algebras

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

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

On the other hand, for the interpretation of [bx] in the external semantics we can trivially let

$$\wr[\mathrm{bx}]\varphi\wr \quad := \quad \left\{x \in \Gamma[\![\blacksquare A]\!] \;\middle|\; x_1(\bullet) \in \wr\varphi\wr\right\}$$

We can now state the correctness of our semantics w.r.t. the modal theories of Def. 5.6.

Lemma 7.3. *(1) If* $\vdash_{\mathrm{c}}^{A} \varphi$ *then* $\wr\varphi\wr = \Gamma[\![A]\!]$.
(2) If $\vdash^{A} \varphi$ *then* $[\![\varphi]\!] = [\![A]\!]$.

Safe Formulae: The General Case. The property we use on safe formulae, seen as lattice operators, is the following.

Definition 7.4 (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 meets 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 $L^{\mathrm{op}} \to L^{\mathrm{op}}$. Dually as with Scott continuity, we have the following.

Lemma 7.5. *The greatest fixpoint of a Scott cocontinuous function $f : L \to L$ is given by*

$$\nu(f) \quad := \quad \bigwedge_{m\in\mathbb{N}} f^m(\top)$$

Safe formulae indeed induce Scott cocontinuous operators.

Lemma 7.6. *Given a* safe *formula $\alpha : A \vdash \varphi(\alpha) : A$, the functions*

$$\begin{array}{rcccc} [\![\varphi]\!] & : & \mathrm{Sub}([\![A]\!]) & \longrightarrow & \mathrm{Sub}([\![A]\!]) \\ \wr\varphi\wr & : & \mathcal{P}(\Gamma[\![A]\!]) & \longrightarrow & \mathcal{P}(\Gamma[\![A]\!]) \end{array}$$

are Scott cocontinuous.

The key for Lem. 7.6 is the usual fact that codirected meets commute with finite joins and meets.

Proposition 7.7. *If $\varphi : A$ is safe then $\wr\varphi\wr = \Gamma[\![\varphi]\!]$.*

Recall that in safe formulae, implications can only occur under a [bx] modality and thus in *closed* subformulae. It is crucial for Prop. 7.7 that meets and joins 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. [36, §VI.7]). This of course does not hold for implications!

[1] Namely, Δ is left adjoint to Γ and the pair $\Delta \dashv \Gamma : \mathcal{S} \to \mathbf{Set}$ is an *open geometric morphism* (see e.g. [36, 28]).

The key case of Prop. 7.7 is that of $\nu\alpha^\omega\varphi(\alpha) : A$. We have

$$\wr\nu\alpha^\omega\varphi(\alpha)\wr = \bigcap_{m\in\mathbb{N}} \wr\varphi^m(\top)\wr \qquad [\![\nu\alpha^\omega\varphi(\alpha)]\!] = \bigwedge_{m\in\mathbb{N}} [\![\varphi^m(\top)]\!]$$

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

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

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

Flat Fixpoints. The situation due to *flat* fixpoints generalizes the safe case. Recall that a Scott continuous function $L \longrightarrow L$ is a Scott cocontinuous function $L^{\mathrm{op}} \longrightarrow L^{\mathrm{op}}$.

Lemma 7.8. *Given $\alpha : A \vdash \varphi(\alpha) : A$ with α positive in φ, the function $\wr\varphi\wr : \mathcal{P}(\Gamma[\![A]\!]) \longrightarrow \mathcal{P}(\Gamma[\![A]\!])$ is Scott continuous as well as cocontinuous.*

Dually as in the cocontinuous case, the least fixpoint of a Scott continuous function $f : L \longrightarrow L$ can be computed as

$$\mu(f) \quad = \quad \bigvee_{m\in\mathbb{N}} f^m(\bot)$$

Corollary 7.9. *Given $\nu\alpha^\omega\varphi(\alpha) : A$ and $\mu\alpha^\omega\varphi(\alpha) : A$ we have*

$$\wr\nu\alpha^\omega\varphi(\alpha)\wr = \bigcap_{n\in\mathbb{N}} \wr\varphi^n(\top)\wr \qquad \wr\mu\alpha^\omega\varphi(\alpha)\wr = \bigcup_{n\in\mathbb{N}} \wr\varphi^n(\bot)\wr$$

Corollary 7.9 implies the correctness of the typing rules (ν-I) and (μ-E) of Fig. 8.

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

Definition 7.10 (Realizability). *Given a type T without free iteration variable, a global section $x \in \Gamma[\![|T|]\!]$ and $n > 0$, we define the realizability relation $x \Vdash_n T$ by induction on lexicographicaly ordered pairs (n, T) as follows:*

- $x \Vdash_n \{A \mid \varphi\}$ *iff* $x_n(\bullet) \in [\![\varphi]\!]^A(n)$.
- $x \Vdash_n \mathbf{1}$.
- $x \Vdash_n T_0 + T_1$ *iff there are some* $i \in \{0,1\}$ *and* $y \in \Gamma[\![|T_i|]\!]$ *s.t.* $x = \mathsf{in}_i \circ y$ *and* $y \Vdash_n T_i$.
- $x \Vdash_n T_0 \times T_1$ *iff* $\pi_0 \circ x \Vdash_n T_0$ *and* $\pi_1 \circ x \Vdash_n T_1$.
- $x \Vdash_n U \longrightarrow T$ *iff for all* $k \le n$ *and for all* $y \in \Gamma[\![|U|]\!]$ *such that* $y \Vdash_k U$, *we have* $\mathsf{ev} \circ \langle x, y\rangle \Vdash_k T$.
- $x \Vdash_1 \blacktriangleright T$.
- $x \Vdash_{n+1} \blacktriangleright T$ *iff there is* $y \in \Gamma[\![|T|]\!]$ *such that* $x = \mathsf{next} \circ y$ *and* $y \Vdash_n T$.
- $x \Vdash_n \mathsf{Fix}(X).A$ *iff* $\mathsf{ufd} \circ x \Vdash_n A[\mathsf{Fix}(X).A/A]$.
- $x \Vdash_n \blacksquare T$ *iff* $x_n(\bullet) \Vdash_m T$ *for all* $m > 0$ *(where* $x \in \Gamma[\![|\blacksquare T|]\!]$*).*
- $x \Vdash_n \forall k \cdot T$ *iff* $x \Vdash_n T[\mathtt{t}/k]$ *for all* $\mathtt{t}$.

Note that we have $x \Vdash_n A$ for $x \in \Gamma A$. It is easy to see that if $x \Vdash_n T$, then $x \Vdash_k T$ for all $k \le n$. Moreover, the subtyping relation is correct in the following sense.

Lemma 7.11. *Given types T, U without free iteration variable, if $x \Vdash_n U$ and $U \le T$ then $x \Vdash_n T$.*

The correctness of typing is the following.

Theorem 7.12 (Adequacy). *If $\vdash M : T$ where T has no free iteration variable, then $[\![M]\!] \Vdash_n T$ for all $n > 0$.*

A closed term $M : \{A \mid \varphi\}$ for φ safe thus induces a global section $[\![M]\!] \in \Gamma[\![A]\!]$ which satisfies $\wr\varphi\wr$. Moreover a function, say $M : \{B \mid \psi\} \longrightarrow \{A \mid \varphi\}$ with ψ, φ safe, induces by composition a **Set**-function

$$\Gamma[\![M]\!] : \Gamma[\![B]\!] \longrightarrow \Gamma[\![A]\!], \quad x \mapsto [\![M]\!] \circ x$$

such that $\Gamma[\![M]\!](x)$ satisfies $\wr\varphi\wr$ whenever x satisfies $\wr\psi\wr$.

Polynomial Types. We give the statement of Møgelberg's Theorem [40] for our context. To each polynomial recursive type $\mathsf{Fix}(X).P(X)$, we associate a polynomial functor $P_{\mathbf{Set}}$ in the obvious way: $\mathbf{1}_{\mathbf{Set}}$ is $\{\bullet\}$, $(-)_{\mathbf{Set}}$ commutes over $\times$ and $+$, $(\blacktriangleright X)_{\mathbf{Set}}$ is the identity and $(\blacksquare A)_{\mathbf{Set}}$ is the constant functor with value $\Gamma[\![A]\!]$. It is well-known that each polynomial functor F has a final coalgebra (see e.g. [24]).

Theorem 7.13 ([40] (see also [13])). *Given a polynomial type $\mathsf{Fix}(X).P(X)$, the pair $(\Gamma[\![\mathsf{Fix}(X).P(X)]\!], \Gamma[\![\mathsf{ufd}]\!])$ is a final* **Set***-coalgebra for the polynomial functor $P_{\mathbf{Set}}$.*

Let φ, ψ be safe. Then $\mathsf{map} : (\mathsf{B} \longrightarrow \mathsf{A}) \longrightarrow \mathsf{Str}\,\mathsf{B} \longrightarrow \mathsf{Str}\,\mathsf{A}$ induces a standard stream function which, when provided with some $f : \mathsf{B} \longrightarrow \mathsf{A}$ taking $\mathsf{b} \in \mathsf{B}$ satisfying ψ to $f(y) \in \mathsf{A}$ satisfying φ, gives a stream with all (resp. some, almost all, infinitely many) elements satisfying φ whenever its stream argument has all (resp. some, almost all, infinitely many) elements satisfying ψ. Similarly, $\mathsf{diag} : \mathsf{Str}(\mathsf{Str}\,\mathsf{B}) \longrightarrow \mathsf{Str}\,\mathsf{B}$ induces a function which gives a stream with all (resp. almost all) elements satisfying φ whenever its argument has all (resp. almost all) elements whose elements all satisfy φ.

8 Conclusion

Guarded recursion has been used as an abstraction of the step-indexing techniques [2], used to define realizability and logical relations for programming languages [3, 1]. In this setting, logics have been defined to reason over of such step-indexed Kripke logical relations (LSLR [14], LADR [15]). We would like to explore extention of our framework to define such logics, particularly modalities used in LADR to reason about the evolution of worlds (defined as transition systems of heap invariants).

We also want to explore application of our refinement types to reasoning over coinductively defined *resumption monads* [44], which formalizes the notion of resumption [39] used to reason on interaction agents in concurrency theory. We would be particularly interested by applying our framework to reason over recently introduced interaction trees [51], that generalize resumption monads. General theory of weak bisimulation for them is defined using parametric coinduction (Paco) [21, 52], it would be a good opportunity to compare it to guarded recursion.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. nnnnnnn and Grant No. mmmmmmm. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

References

[1] A. Ahmed. 2006. Step-indexed syntactic logical relations for recursive and quantified types. In *European Symposium on Programming*. Springer, 69–83.

[2] A. Appel, P.-A. Melliès, C. Richards, and J. Vouillon. 2007. A Very Modal Model of a Modern, Major, General Type System. *SIGPLAN Not.* 42, 1 (Jan. 2007), 109?122. https://doi.org/10.1145/1190215.1190235

[3] Andrew W. Appel and David McAllester. 2001. An Indexed Model of Recursive Types for Foundational Proof-Carrying Code. *ACM Trans. Program. Lang. Syst.* 23, 5 (2001), 657?683. https://doi.org/10.1145/504709.504712

[4] R. Atkey and C. McBride. 2013. Productive Coprogramming with Guarded Recursion. In *Proceedings of the 18th ACM SIGPLAN International Conference on Functional Programming (ICFP '13)*. ACM, New York, NY, USA, 197–208. https://doi.org/10.1145/2500365.2500597

[5] P. Bahr, C. Graulund, and R. Møgelberg. 2019. Simply RaTT: A Fitch-style Modal Calculus for Reactive Programming. *arXiv preprint arXiv:1903.05879* (2019).

[6] C. Baier and J.-P. Katoen. 2008. *Principles of Model Checking*. MIT Press.

[7] L. Birkedal, A. Bizjak, R. Clouston, H. B. Grathwohl, B. Spitters, and A. Vezzosi. 2019. Guarded Cubical Type Theory. *Journal of Automated Reasoning* 63, 2 (01 Aug 2019), 211–253. https://doi.org/10.1007/s10817-018-9471-7

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

[9] A. Bizjak, H. B. Grathwohl, R. Clouston, R. E. Møgelberg, and L. Birkedal. 2016. Guarded Dependent Type Theory with Coinductive Types. In *Foundations of Software Science and Computation Structures*, Bart Jacobs and Christof Löding (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 20–35.

[10] P. Blackburn, M. de Rijke, and Y. Venema. 2002. *Modal Logic*. Cambridge University Press.

[11] A. Cave, F. Ferreira, P. Panangaden, and B. Pientka. 2014. Fair Reactive Programming. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '14)*. ACM, New York, NY, USA, 361–372.

[12] B. F. Chellas. 1980. *Modal Logic: An Introduction*. Cambridge University Press.

[13] R. Clouston, A. Bizjak, H. Bugge Grathwohl, and L. Birkedal. 2016. The Guarded Lambda-Calculus: Programming and Reasoning with Guarded Recursion for Coinductive Types. *Logical Methods in Computer Science* 12, 3 (2016).

[14] D. Dreyer, A. Ahmed, and L Birkedal. 2011. 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

[15] D. Dreyer, G. Neis, A. Rossberg, and L. Birkedal. 2010. A Relational Modal Logic for Higher-order Stateful ADTs. In *Proceedings POPL'10*. ACM, 185–198.

[16] C. Elliott and P. Hudak. 1997. Functional Reactive Animation. In *Proceedings of the Second ACM SIGPLAN International Conference on Functional Programming (ICFP '97)*. ACM, New York, NY, USA, 263–273. https://doi.org/10.1145/258948.258973

[17] T. Freeman and F. Pfenning. 1991. Refinement Types for ML. In *Proceedings of the ACM SIGPLAN 1991 Conference on Programming Language Design and Implementation (PLDI ?91)*. Association for Computing Machinery, New York, NY, USA, 268?277. https://doi.org/10.1145/113445.113468

[18] S. Frittella. 2014. *Monotone Modal Logics & Friends*. Ph.D. Dissertation. Aix-Marseille Univ.

[19] A. Guatto. 2018. A Generalized Modality for Recursion. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS '18)*. ACM, New York, NY, USA, 482–491. https://doi.org/10.

1145/3209108.3209148

[20] H. H. Hansen. 2003. *Monotonic Modal Logics*. Master's thesis. ILLC, Amsterdam.

[21] C.-K. Hur, G. Neis, D. Dreyer, and V. Vafeiadis. 2013. The Power of Parameterization in Coinductive Proof. In *Proceedings of the 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL ?13)*. Association for Computing Machinery, New York, NY, USA, 193?206. https://doi.org/10.1145/2429069.2429093

[22] B. Jacobs. 2001. *Categorical Logic and Type Theory*. Elsevier.

[23] B. Jacobs. 2001. Many-Sorted Coalgebraic Modal Logic: a Model-theoretic Study. *ITA* 35, 1 (2001), 31–59.

[24] B. Jacobs. 2016. *Introduction to Coalgebra: Towards Mathematics of States and Observation*. Cambridge University Press.

[25] A. Jeffrey. 2012. 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 (PLPV '12)*. ACM, New York, NY, USA, 49–60. https://doi.org/10.1145/2103776.2103783

[26] W. Jeltsch. 2014. An Abstract Categorical Semantics for Functional Reactive Programming with Processes. In *Proceedings of the ACM SIGPLAN 2014 Workshop on Programming Languages Meets Program Verification (PLPV '14)*. ACM, New York, NY, USA, 47–58. https://doi.org/10.1145/2541568.2541573

[27] Ranjit Jhala, Rupak Majumdar, and Andrey Rybalchenko. 2011. HMC: Verifying functional programs using abstract interpreters. In *International Conference on Computer Aided Verification*. Springer, 470–485.

[28] P.T. Johnstone. 2002. *Sketches of an Elephant: A Topos Theory Compendium*. Clarendon Press.

[29] N. Kobayashi and C-H L. Ong. 2009. 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*. IEEE, 179–188.

[30] N. Kobayashi, R. Sato, and H. Unno. 2011. Predicate abstraction and CEGAR for higher-order model checking. In *ACM SIGPLAN Notices*, Vol. 46. ACM, 222–233.

[31] D. Kozen. 1983. Results on the propositional μ-calculus. *Theoretical Computer Science* 27, 3 (1983), 333 – 354. Special Issue Ninth International Colloquium on Automata, Languages and Programming (ICALP) Aarhus, Summer 1982.

[32] N. R. Krishnaswami. 2013. Higher-order Functional Reactive Programming Without Spacetime Leaks. In *Proceedings of ICFP'13*. ACM, New York, NY, USA, 221–232.

[33] N. R. Krishnaswami and N. Benton. 2011. Ultrametric Semantics of Reactive Programs. In *2011 IEEE 26th Annual Symposium on Logic in Computer Science*. 257–266. https://doi.org/10.1109/LICS.2011.38

[34] T. Kuwahara, T. Terauchi, H. Unno, and N. Kobayashi. 2014. Automatic termination verification for higher-order functional programs. In *European Symposium on Programming Languages and Systems*. Springer, 392–411.

[35] J. Lambek and P. J. Scott. 1986. *Introduction to Higher Order Categorical Logic*. CUP.

[36] S. Mac Lane and I. Moerdijk. 1992. *Sheaves in geometry and logic: A first introduction to topos theory*. Springer.

[37] S. Marin. 2018. *Modal proof theory through a focused telescope*. PhD Thesis. Université Paris Saclay. https://hal.archives-ouvertes.fr/tel-01951291

[38] C. McBride and R. Paterson. 2008. Applicative programming with effects. *Journal of Functional Programming* 18, 1 (2008), 1?13. https://doi.org/10.1017/S0956796807006326

[39] R. Milner. 1975. Processes: a mathematical model of computing agents. In *Studies in Logic and the Foundations of Mathematics*. Vol. 80. Elsevier, 157–173.

[40] R. E. Møgelberg. 2014. A Type Theory for Productive Coprogramming via Guarded Recursion. In *Proceedings of CSL-LICS 2014 (CSL-LICS '14)*. ACM.

[41] A. Murase, T. Terauchi, N. Kobayashi, R. Sato, and H. Unno. 2016. Temporal Verification of Higher-Order Functional Programs. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL ?16)*. Association for Computing Machinery, New York, NY, USA, 57?68. https://doi.org/10.1145/2837614.2837667

[42] H. Nakano. 2000. A Modality for Recursion. In *Proceedings of LICS'00*. IEEE Computer Society, 255–266.

[43] C.-H. L. Ong. 2006. On Model-Checking Trees Generated by Higher-Order Recursion Schemes. In *Proceedings of LICS 2006*. IEEE Computer Society, 81–90.

[44] M. Piróg and J. Gibbons. 2014. The coinductive resumption monad. *Electronic Notes in Theoretical Computer Science* 308 (2014), 273–288.

[45] G. Plotkin and C. Stirling. 1986. A Framework for Intuitionistic Modal Logics: Extended Abstract. In *Proceedings of the 1986 Conference on Theoretical Aspects of Reasoning About Knowledge (TARK '86)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 399–406.

[46] Patrick M. Rondon, Ming Kawaguci, and Ranjit Jhala. 2008. Liquid Types. In *Proceedings of the 29th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI ?08)*. Association for Computing Machinery, New York, NY, USA, 159?169. https://doi.org/10.1145/1375581.1375602

[47] L. Santocanale and Y. Venema. 2010. Completeness for flat modal fixpoint logics. *Ann. Pure Appl. Logic* 162, 1 (2010), 55–82.

[48] A. K. Simpson. 1994. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD Thesis. University of Edinburgh. https://www.era.lib.ed.ac.uk/handle/1842/407

[49] Niki Vazou. 2016. *Liquid Haskell: Haskell as a theorem prover*. Ph.D. Dissertation. UC San Diego.

[50] Niki Vazou, Eric L. Seidel, Ranjit Jhala, Dimitrios Vytiniotis, and Simon Peyton-Jones. 2014. Refinement Types for Haskell. In *Proceedings of the 19th ACM SIGPLAN International Conference on Functional Programming (ICFP ?14)*. Association for Computing Machinery, New York, NY, USA, 269?282. https://doi.org/10.1145/2628136.2628161

[51] L.-Y. Xia, Y. Zakowski, P. He, C.-K. Hur, G. Malecha, B. C. Pierce, and S. Zdancewic. 2019. Interaction Trees: Representing Recursive and Impure Programs in Coq. *Proc. ACM Program. Lang.* 4, POPL, Article Article 51 (Dec. 2019), 32 pages. https://doi.org/10.1145/3371119

[52] Y. Zakowski, P. He, C.-K. Hur, and S. Zdancewic. [n. d.]. An Equational Theory for Weak Bisimulation via Generalized Parameterized Coinduction. ([n. d.]).

A Additional Material for Section 5

The full definition of the variance predicates α Pos φ and α Neg φ is given in Fig. 10. The intuitionistic propositional deduction rules are given in Fig. 11.

Remark A.1 (Rem. 5.7). All modalities ($[\pi_i]$, [fd], [next], $[\mathsf{in}_i]$, [ev(ψ)] and [bx]) satisfy the *monotonicity rule* (RM) and are thus monotone in the sense of [12], from which we borrowed the terminology used in Table 1 (see also [20, 18]). Assuming the rule (RM), we easily get the following:

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

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

Proof. Indeed, one can derive

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

□

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

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

Proof. Indeed, one has

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

□

(3) We have the monotonicity axioms

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

Hence, with our adaptation to unbounded linear branching, the normal intuitionistic modal logic **IK** of [45] is (RM) + (C) + (N) + (P) + ($\mathsf{C}_\vee$) + ($\mathsf{C}_\Rightarrow$), while the normal modal logic **K** is **IK** + (CL) (see e.g. [10]).

B Additional Material for Section 6

The full definition of the subtyping relation $\leq$ is given in Fig. 12.

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

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

C Additional Material for Section 7

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

C.1 The Topos of Trees (Basic Structure)

Notation C.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 [8, 13] for details.

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

$$\begin{array}{rcl} (X + Y)(n) & = & X(n) + Y(n) \\ (X \times Y)(n) & = & X(n) \times Y(n) \end{array}$$

Moreover, exponentials are induced by the Yoneda Lemma see e.g. [36, §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

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

Since we do not require the explicit constructions, we refer to [8] for the interpretation of guarded recursive types $\mathsf{Fix}(X).A(X)$ and for the definition of the isos

$$\begin{array}{rcccl} \mathsf{fd} & : & [\![A(\mathsf{Fix}(X).A(X))]\!] & \longrightarrow & [\![\mathsf{Fix}(X).A(X)]\!] \\ \mathsf{ufd} & : & [\![\mathsf{Fix}(X).A(X)]\!] & \longrightarrow & [\![A(\mathsf{Fix}(X).A(X))]\!] \end{array}$$

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

C.2 Global Sections and Constant Objects

As for any presheaf topos, the global section functor $\mathbf{\Gamma} : \mathcal{S} \to \mathbf{Set}$ is right adjoint to the constant object functor $\mathbf{\Delta} : \mathbf{Set} \to$

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

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

$$\frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\pi_i]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{in}_i]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{fd}]\varphi} \qquad \frac{\alpha \text{ Pos } \varphi}{\alpha \text{ Pos } [\mathsf{next}]\varphi}$$

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

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

$$\frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\pi_i]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{in}_i]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{fd}]\varphi} \qquad \frac{\alpha \text{ Neg } \varphi}{\alpha \text{ Neg } [\mathsf{next}]\varphi}$$

Figure 10. Positive and Negative Occurrences in a Formula.

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

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

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

Figure 11. Intuitionistic Propositional Deduction Rules.

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

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

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

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

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

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

Figure 12. Subtyping Rules (full version).

$\mathcal{S}$ (see e.g. [36, §I.6]):

$$\mathcal{S} \underset{\Delta}{\overset{\Gamma}{\underset{\top}{\rightleftarrows}}} \mathbf{Set}$$

We state the following for the record.

Lemma C.2. *For X, Y objects of $\mathcal{S}$, we have $\mathbf{\Gamma}(X + Y) \simeq \mathbf{\Gamma}X + \mathbf{\Gamma}Y$, $\mathbf{\Gamma}(X \times Y) \simeq \mathbf{\Gamma}X \times \mathbf{\Gamma}Y$ and $\mathbf{\Gamma}(\blacktriangleright X) \simeq \mathbf{\Gamma}X$ (via $\mathbf{\Gamma}(\mathsf{next})$).*

Following [13], for a (closed) pure type A, we have

$$[\![\blacksquare A]\!] \quad := \quad \mathbf{\Delta}\mathbf{\Gamma}[\![A]\!]$$

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

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

$$[\![\Gamma]\!] \quad \xrightarrow{[\![M]\!]} \quad [\![\blacksquare A]\!] = \mathbf{\Delta}\mathbf{\Gamma}[\![A]\!] \quad \xrightarrow{\varepsilon} \quad [\![A]\!]$$

The term constructors bx and prev rely on a strong semantic property of constant types, namely that their interpretation lie in the image of the constant object functor $\mathbf{\Delta}$.

Definition C.3. *An object X of $\mathcal{S}$ is* constant *if $X = \mathbf{\Delta}S$ for some set S.*

Lemma C.4 ([13, 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 $\mathsf{bx}_\sigma(M)$ and $\mathsf{prev}_\sigma(M)$ (where σ stands for $[x_1 \mapsto M_1, \dots, x_k \mapsto M_k]$). Assuming in both cases $[\![M]\!]$ to be defined, for $n > 0$ we let

$$\begin{array}{rcccl} [\![\mathsf{bx}_\sigma(M)]\!](n) & : & [\![\Gamma]\!](n) & \longrightarrow & \Delta\Gamma[\![A]\!](n) = \Gamma[\![A]\!] \\ \gamma & \longmapsto & \Big(m \mapsto [\![M]\!]_m\Big([\![M_1]\!]_n(\gamma), \dots, [\![M_k]\!]_n(\gamma)\Big)\Big) & & \end{array}$$

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

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

C.3 External and Internal Semantics: Global Definitions

We can now give the full **Set** and $\mathcal{S}$ interpretations of the logical language. In contrast with §7, we discuss the external semantics $(\!|-|\!)$ in **Set** before the internal semantics $[\![-]\!]$ in $\mathcal{S}$. In both cases, for $\alpha : A \vdash \varphi : A(\alpha)$, we let

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

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

Definition C.5 (External Semantics)**.** *Consider a formula $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi : A$ without free iteration variable. Assume given a valuation v taking each propositional variable α_i for $i = 1, \dots, k$ to a set $v(\alpha_i) \in \mathcal{P}(\Gamma[\![A_i]\!])$. We define $(\!|\varphi|\!)^A_v \in \mathcal{P}(\Gamma[\![A]\!])$ by induction on φ in Fig. 13.*

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

Definition C.6 (Internal Semantics)**.** *Consider a formula $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi : A$ without free iteration variable. Assume given a valuation v taking each propositional variable α_i for $i = 1, \dots, k$ to a subobject $v(\alpha_i)$ of $[\![A_i]\!]$. The subobject $[\![\varphi]\!]^A_v$ of $[\![A]\!]$ is defined by induction on φ in Fig. 14.*

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

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

- $t \not\Vdash^A_n \bot$.
- $t \Vdash^A_n \top$.
- $t \Vdash^A_n \varphi \vee \psi$ iff $t \Vdash^A_n \varphi$ or $t \Vdash^A_n \psi$.
- $t \Vdash^A_n \varphi \wedge \psi$ iff $t \Vdash^A_n \varphi$ and $t \Vdash^A_n \psi$.
- $t \Vdash^A_n \psi \Rightarrow \varphi$ iff for all $k \le n$, $t{\uparrow}k \Vdash^A_k \varphi$ whenever $t{\uparrow}k \Vdash^A_k \psi$.
- $t \Vdash^{A_0 \times A_1}_n [\pi_i]\varphi$ iff $\pi_i(t) \Vdash^{A_i}_n \varphi$.
- $t \Vdash^{A_0 + A_1}_n [\mathsf{in}_i]\varphi$ iff there is $u \in [\![A_i]\!](n)$ such that $t = \mathsf{in}_i(u)$ and $u \Vdash^{A_i}_n \varphi$.
- $t \Vdash^{B \to A}_n [\mathsf{ev}(\psi)]\varphi$ iff for all $k \le n$ and all $u \in [\![B]\!](k)$, $(t{\uparrow}k)(u) \Vdash^A_k \varphi$ whenever $u \Vdash^B_k \psi$.
- $t \Vdash^{\mathsf{Fix}(X).A}_n [\mathsf{fd}]\varphi$ iff $\mathsf{ufd} \circ t \Vdash^{A[\mathsf{Fix}(X).A/X]}_n \varphi$.
- $t \Vdash^{\blacktriangleright A}_0 [\mathsf{next}]\varphi$.
- $t \Vdash^{\blacktriangleright A}_{n+1} [\mathsf{next}]\varphi$ iff $t \Vdash^A_n \varphi$.
- $t \Vdash^{\blacksquare A}_n [\mathsf{bx}]\varphi$ iff $t \in (\!|\varphi|\!)^A$.

C.4 An Open Geometric Morphism

Key properties of the internal semantics of [bx] rely on some further facts on the adjunction $\Delta \dashv \Gamma$. We refer to [36, 28].

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

$$A \in \mathcal{P}(S) \quad \longmapsto \quad \Delta A \in \mathsf{Sub}(\Delta S)$$

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

$$f_! \quad : \quad \mathsf{Sub}(\Delta S) \quad \longrightarrow \quad \mathcal{P}(S)$$

Proof. A subobject A of ΔS 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 $a \in (\Delta B)_n$ and thus $A \le \Delta B$. Conversely, if $A \le \Delta B$, then for every $a \in f_!(A)$, since $a \in A_n$ for some $n > 0$, we must have $a \in (\Delta B)_n = B$, so that $f_!(A) \subseteq B$. □

As a consequence, the adjoint pair $\Delta \dashv \Gamma : \mathcal{S} \to \mathbf{Set}$ is an *open geometric morphism* (in the sense of [36, Def. IX.6.2]), from which it follows that Δ induces maps of (complete) Heyting algebras $\mathcal{P}(S) \to \mathsf{Sub}(\Delta S)$ (see e.g. [36, Thm. X.3.1 & Lem. X.3.2]). We state this for later use.

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

C.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 C.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*

$$\begin{array}{ccc} A' & \longrightarrow & A \\ {\scriptstyle k^*(g)}\downarrow & \lrcorner & \downarrow{\scriptstyle g} \\ X & \xrightarrow[k]{} & Y \end{array}$$

- *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.

$$
\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl}
\wr \bot \wr_v^A & := & \emptyset & \wr \top \wr_v^A & := & \Gamma[\![A]\!] & \wr \alpha_i \wr_v^A & := & v(\alpha_i) \\
\wr \varphi \vee \psi \wr_v^A & := & \wr \varphi \wr_v^A \cup \wr \psi \wr_v^A & \wr \varphi \wedge \psi \wr_v^A & := & \wr \varphi \wr_v^A \cap \wr \psi \wr_v^A & & & \\
\wr \psi \Rrightarrow \varphi \wr_v^A & := & (\Gamma[\![A]\!] \setminus \wr \psi \wr_v^A) \cup \wr \varphi \wr_v^A & & & & & & \\
\wr [\pi_i]\varphi \wr_v^{A_0 \times A_1} & := & \left\{ x \in \Gamma[\![A_0 \times A_1]\!] \;\middle|\; \pi_i \circ x \in \wr \varphi \wr_v^{A_i} \right\} & & & & & & \\
\wr [\mathsf{in}_i]\varphi \wr_v^{A_0 + A_1} & := & \left\{ x \in \Gamma[\![A_0 + A_1]\!] \;\middle|\; \exists y \in \Gamma[\![A_i]\!] \big(x = \mathsf{in}_i \circ y \text{ and } y \in \wr \varphi \wr_v^{A_i} \big) \right\} & & & & & & \\
\wr [\mathsf{fd}]\varphi \wr_v^{\mathsf{Fix}(X).A} & := & \left\{ x \in \Gamma[\![\mathsf{Fix}(X).A]\!] \;\middle|\; \mathsf{ufd} \circ x \in \wr \varphi \wr_v^{A[\mathsf{Fix}(X).A/X]} \right\} & & & & & & \\
\wr [\mathsf{ev}(\psi)]\varphi \wr^{B \to A} & := & \left\{ x \in \Gamma[\![B \to A]\!] \;\middle|\; \forall y \in \Gamma[\![B]\!],\ y \in \wr \psi \wr^B \implies \mathsf{ev} \circ \langle x, y \rangle \in \wr \varphi \wr^A \right\} & & & & & & \\
\wr [\mathsf{bx}]\varphi \wr^{\blacksquare A} & := & \left\{ x \in \Gamma[\![\blacksquare A]\!] \;\middle|\; x_1(\bullet) \in \wr \varphi \wr^A \right\} & & & & & & \\
\wr [\mathsf{next}]\varphi \wr_v^{\blacktriangleright A} & := & \left\{ \mathsf{next} \circ x \in \Gamma[\![\blacktriangleright A]\!] \;\middle|\; x \in \wr \varphi \wr_v^A \right\} & & & & & & \\
\wr \nu\alpha^{\mathsf{t}}\varphi(\alpha) \wr^A & := & \wr \varphi^m(\top) \wr^A \qquad ([\![\mathsf{t}]\!] = m) & & & & & & \\
\wr \mu\alpha^{\mathsf{t}}\varphi(\alpha) \wr^A & := & \wr \varphi^m(\bot) \wr^A \qquad ([\![\mathsf{t}]\!] = m) & & & & & & \\
\wr \nu\alpha^{\omega}\varphi \wr^A & := & \bigcup \left\{ S \;\middle|\; S \in \mathcal{P}(\Gamma[\![A]\!]) \text{ and } S \subseteq \wr \varphi \wr_{[S/\alpha]}^A \right\} & & & & & & \\
\wr \mu\alpha^{\omega}\varphi \wr^A & := & \bigcap \left\{ S \;\middle|\; S \in \mathcal{P}(\Gamma[\![A]\!]) \text{ and } \wr \varphi \wr_{[S/\alpha]}^A \subseteq S \right\} & & & & & &
\end{array}
$$

Figure 13. External Semantics.

$$
\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl}
[\![\bot]\!]_v^A(n) & := & \emptyset & [\![\top]\!]_v^A & := & [\![A]\!] & [\![\alpha_i]\!]_v^A & := & v(\alpha_i) \\
[\![\varphi \vee \psi]\!]_v^A(n) & := & [\![\varphi]\!]_v^A(n) \cup [\![\psi]\!]_v^A(n) & [\![\varphi \wedge \psi]\!]_v^A(n) & := & [\![\varphi]\!]_v^A(n) \cap [\![\psi]\!]_v^A(n) & & & \\
[\![\psi \Rrightarrow \varphi]\!]_v^A(n) & := & \left\{ t \in [\![A]\!](n) \;\middle|\; \forall k \le n,\ t{\uparrow}k \in [\![\psi]\!]_v^A(k) \implies t{\uparrow}k \in [\![\varphi]\!]_v^A(k) \right\} & & & & & & \\
[\![[\pi_i]\varphi]\!]_v^{A_0 \times A_1}(n) & := & \left\{ t \in [\![A_0 \times A_1]\!](n) \;\middle|\; \pi_i(t) \in [\![\varphi]\!]_v^{A_i}(n) \right\} & & & & & & \\
[\![[\mathsf{in}_i]\varphi]\!]_v^{A_0 + A_1}(n) & := & \left\{ t \in [\![A_0 + A_1]\!](n) \;\middle|\; \exists u \in [\![A_i]\!](n),\ t = \mathsf{in}_i(u) \text{ and } u \in [\![\varphi]\!]_v^{A_i}(n) \right\} & & & & & & \\
[\![[\mathsf{fd}]\varphi]\!]_v^{\mathsf{Fix}(X).A}(n) & := & \left\{ t \in [\![\mathsf{Fix}(X).A]\!](n) \;\middle|\; \mathsf{ufd}_n(t) \in [\![\varphi]\!]_v^{A[\mathsf{Fix}(X).A/X]}(n) \right\} & & & & & & \\
[\![[\mathsf{ev}(\psi)]\varphi]\!]^{B \to A}(n) & := & \left\{ t \in [\![B \to A]\!](n) \;\middle|\; \forall k \le n,\ \forall u \in [\![B]\!](k),\ u \in [\![\psi]\!]^B(k) \implies (t{\uparrow}k)(u) \in [\![\varphi]\!]^A(k) \right\} & & & & & & \\
[\![[\mathsf{bx}]\varphi]\!]^{\blacksquare A}(n) & := & \left\{ t \in [\![\blacksquare A]\!](n) = \Gamma[\![A]\!] \;\middle|\; t \in \wr \varphi \wr^A \right\} & & & & & & \\
[\![[\mathsf{next}]\varphi]\!]_v^{\blacktriangleright A}(1) & := & \mathbf{1} & & & & & & \\
[\![[\mathsf{next}]\varphi]\!]_v^{\blacktriangleright A}(n) & := & [\![\varphi]\!]_v^A(n-1) \qquad (n > 1) & & & & & & \\
[\![\nu\alpha^{\mathsf{t}}\varphi(\alpha)]\!]^A & := & [\![\varphi^m(\top)]\!]^A \qquad ([\![\mathsf{t}]\!] = m) & & & & & & \\
[\![\mu\alpha^{\mathsf{t}}\varphi(\alpha)]\!]^A & := & [\![\varphi^m(\bot)]\!]^A \qquad ([\![\mathsf{t}]\!] = m) & & & & & & \\
[\![\nu\alpha^{\omega}\varphi]\!]^A & := & \bigvee \left\{ S \;\middle|\; S \in \mathrm{Sub}([\![A]\!]) \text{ and } S \le [\![\varphi]\!]_{[S/\alpha]}^A \right\} & & & & & & \\
[\![\mu\alpha^{\omega}\varphi]\!]^A & := & \bigwedge \left\{ S \;\middle|\; S \in \mathrm{Sub}([\![A]\!]) \text{ and } [\![\varphi]\!]_{[S/\alpha]}^A \le S \right\} & & & & & &
\end{array}
$$

Figure 14. Internal Semantics.

Lemma C.10 ([36, Thm. IV.7.2])**.** *Let $\mathcal{E}$ be a topos and fix a map $k : X \to_{\mathcal{E}} Y$. The functor $(\exists k)$ is left adjoint to $k^* : \mathcal{E}/Y \to \mathcal{E}/X$. Moreover, k^* has a right adjoint $(\forall k)$ and preserves exponentials, and thus preserves subobjects.*

Lemma C.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. □

Lemma C.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 ([8, §2.1]). It thus follows that $\blacktriangleright$ preserves monos. □

C.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 C.13 (Lem. 7.3)**.**

(1) If $\vdash_{\mathsf{c}}^{A} \varphi$ then $\lceil \varphi \rfloor = \mathbf{\Gamma}[\![A]\!]$.
(2) If $\vdash^{A} \varphi$ then $[\![\varphi]\!] = [\![A]\!]$.

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

C.6.1 Internal Semantics

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

Definition C.14.

(1) 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.
(2) 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.
(3) Given a locally contractive functor T on $\mathcal{S}$, define $[\![[\mathsf{fd}]]\!] : \mathrm{Sub}(T(\mathsf{Fix}(T))) \to \mathrm{Sub}(\mathsf{Fix}(T))$ as ufd^*, where we have $\mathsf{ufd} : \mathsf{Fix}(T) \to_{\mathcal{S}} T(\mathsf{Fix}(T))$.
(4) Given a $\mathcal{S}$-object X, define $[\![[\mathsf{next}]]\!] : \mathrm{Sub}(X) \to \mathrm{Sub}(\blacktriangleright X)$ as $\blacktriangleright(-)$.
(5) Given a set S, define $[\![[\mathsf{bx}]]\!] : \mathcal{P}(S) \to \mathrm{Sub}(\Delta S)$ as $\Delta(-)$.

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 [22, §9.2 & Prop. 9.2.4]. We follow here [36, 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. [36, Prop. I.8.5]).

- Second, it follows from Lem. C.10 that for objects X, Y of $\mathcal{S}$, taking the pullback of the evaluation map $\mathrm{ev} : X^Y \times Y \to X$ gives a map of subobjects, as in

$$\begin{array}{ccc} \mathrm{ev}^*(A) & \longrightarrow & A \\ \downarrow & \lrcorner & \uparrow \\ X^Y \times Y & \xrightarrow[\mathrm{ev}]{} & X \end{array}$$

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. C.10) by the right adjoint $\forall_Y := \forall(\pi)$ to π^*, where π is the projection $X \times Y \to X$ ([36, §VI.5, p. 300]). Moreover, via the Kripke-Joyal semantics for a presheaf topos ([36, §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 $S' \in \mathrm{Sub}([\![B]\!])$ to

$$[\![[\mathsf{ev}(S')]]\!] \;:=\; S \in \mathrm{Sub}([\![A]\!]) \;\longmapsto\; \forall_{[\![B]\!]}\Big(\pi^*(S') \Rightarrow_{[\![A]\!]^{[\![B]\!]} \times [\![B]\!]} \mathrm{ev}^*(S)\Big)$$

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

Now, note that we actually have

Lemma C.15. *Consider a formula $\Sigma \vdash \varphi : A$ and v as in Def. C.6, such that $[\![\varphi]\!]_v \in \mathrm{Sub}([\![A]\!])$. We have*

(a) $[\![[\pi_i]\varphi]\!]_v = [\![[\pi_i]]\!]([\![\varphi]\!]_v)$
(b) $[\![[\mathsf{in}_i]\varphi]\!]_v = [\![[\mathsf{in}_i]]\!]([\![\varphi]\!]_v)$
(c) $[\![[\mathsf{fd}]\varphi]\!]_v = [\![[\mathsf{fd}]]\!]([\![\varphi]\!]_v)$
(d) $[\![[\mathsf{next}]\varphi]\!]_v = [\![[\mathsf{next}]]\!]([\![\varphi]\!]_v)$
(e) $[\![[\mathsf{bx}]\varphi]\!] = [\![[\mathsf{bx}]]\!]([\![\varphi]\!])$
(f) $[\![[\mathsf{ev}(\psi)]\varphi]\!] = [\![[\mathsf{ev}([\![\psi]\!]_v)]]\!]([\![\varphi]\!]_v)$ for each $\vdash \psi : B$ such that $[\![\psi]\!] \in \mathrm{Sub}([\![B]\!])$.

Proof.

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

$$[\![[\pi_i]]\!]([\![\varphi]\!]^{A_i})(n) = \big\{(t,u) \in [\![A_0 \times A_1]\!](n) \times [\![\varphi]\!](n) \;\big|\; u = \pi_i(t)\big\}$$

which is clearly in bijection with $[\![[\pi_i]\varphi]\!]^{A_0 \times A_1}(n)$.
(b) Trivial.
(c) Similar to the case of $[\pi_i]$.
(d) Trivial.
(e) Trivial.
(f) Immediate from the above discussion. □

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

Lemma C.16. *Given $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi : A$, and v taking α_i for $i = 1, \dots, k$ to $v(\alpha_i) \in \mathrm{Sub}([\![A_i]\!])$, we have $[\![\varphi]\!]^A_v \in \mathrm{Sub}([\![A]\!])$.*

Proof. The proof is by induction on formulae. The interpretation of the propositional connectives follows the corresponding structures in presheaf toposes [36, Prop. I.8.5]. The cases of the modalities $[\triangle]$ follow from the induction hypothesis and Lem. C.15. The cases of $\theta\alpha^{\omega}\varphi$ simply amount to the fact that for presheaf toposes, subobjects lattices are complete ([36, Prop. I.8.5]). The cases of $\theta\alpha^{\mathtt{t}}\varphi$ for $\mathtt{t}$ an iteration term are trivial. □

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

Corollary C.17.

(a) The maps $[\![[\pi_i]]\!]$, $[\![[\mathsf{fd}]]\!]$ and $[\![[\mathsf{bx}]]\!]$ are maps of Heyting algebras.
(b) The maps $[\![[\mathsf{in}_i]]\!]$ preserve $\vee, \bot$ and $\wedge$.
(c) The maps $[\![[\mathsf{next}]]\!]$ preserve $\wedge, \top$ and $\vee$.
(d) For each object X of $\mathcal{S}$ and each fixed $S \in \mathrm{Sub}(X)$, the map $[\![[\mathsf{ev}(S)]]\!]$ preserves $\wedge, \top$.

Proof.

(a) This directly follows from Lem. C.10 and Lem. C.8.

(b) Preservation of $\vee, \bot$ follows from that fact that $[\![[\mathsf{in}_i]]\!]$ is a left adjoint by Lem. C.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

$$\begin{array}{ccc} A \wedge B & \longrightarrow & B \\ \downarrow & \lrcorner & \downarrow \\ A & \longrightarrow & X_i \end{array}$$

(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 $\mathrm{Sub}(X_0 + X_1)$:

$$\begin{array}{ccccc} A \wedge B & \longrightarrow & B & & \\ \downarrow & \lrcorner & \downarrow & & \\ & & X_i & & \\ & & \downarrow{\scriptstyle \mathsf{in}_i} & & \\ A & \longrightarrow & X_i & \xrightarrow[\mathsf{in}_i]{} & X_0 + X_1 \end{array}$$

(c) Preservation of $\wedge, \top$ follows from the fact that $\blacktriangleright(-)$ is a right adjoint ([8, §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

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

and

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

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

C.6.2 External Semantics

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

Definition C.18.

(1) Given sets S_0 and S_1, define $\wr[\pi_i]\wr : \mathcal{P}(S_i) \to \mathcal{P}(S_0 \times S_1)$ as π_i^*, where $\pi_i : S_0 \times S_1 \to S_i$ is the ith projection.
(2) Given sets S_0 and S_1, define $\wr[\mathsf{in}_i]\wr : \mathcal{P}(S_i) \to \mathcal{P}(S_0 + S_1)$ as $(\exists \mathsf{in}_i)$, where $\mathsf{in}_i : S_i \to S_0 + S_1$ is the ith injection.
(3) Given a $\mathcal{S}$ object X, define $\wr[\mathsf{next}]\wr : \mathcal{P}(\Gamma X) \to \mathcal{P}(\Gamma \blacktriangleright X)$ as $((\Gamma\mathsf{next})^{-1})^*$, where $(\Gamma\mathsf{next})^{-1} : \Gamma(\blacktriangleright X) \to \Gamma X$ is the inverse of $\Gamma(\mathsf{next})$ (Lem. C.2).
(4) Given a locally contractive functor T on $\mathcal{S}$, define $\wr[\mathsf{fd}]\wr : \mathcal{P}(\Gamma(T(\mathsf{Fix}(T)))) \to \mathcal{P}(\Gamma\mathsf{Fix}(T))$ as $\Gamma(\mathsf{ufd})^*$, where $\mathsf{ufd} : \mathsf{Fix}(T) \to_{\mathcal{S}} T(\mathsf{Fix}(T))$.

We trivially have (at appropriate types):

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

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

Lemma C.19.

(a) The functions $\wr[\pi_i]\wr$, $\wr[\mathsf{next}]\wr$, $\wr[\mathsf{fd}]\wr$ are maps of Boolean algebras.
(b) The function $\wr[\mathsf{in}_i]\wr$ preserves $\vee, \bot$ and $\wedge$.

C.7 The Safe Fragment

The proofs of Lem. 7.5, Lem. 7.6 and Prop. 7.7 are deferred to App. E.2.

C.8 Flat Fixpoints

The proof of Lem. 7.8 is deferred to App. E.3.

C.9 Constant Objects, Again

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

Definition C.20. *For T is a type without free iteration variables, we define $[\![T]\!]$ by induction as follows:*

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

We can now extend Lem. C.4. We crucially rely on the fact that Δ preserves limits (see e.g. [28, Ex. 4.1.4]).

Lemma C.21. *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 [13, Lem. 2.6]. The case of $\blacksquare T$ is trivial. As for $\forall k \cdot T$, assuming by induction that for each $n \in \mathbb{N}$ we have $[\![T[\mathsf{n}/k]]\!] = \Delta S_n$ for some S_n, since Δ preserves limits we get

$$\Delta\left(\bigcap_n S_n\right) \quad = \quad \bigwedge_n \Delta S_n \quad = \quad [\![\forall k \cdot T]\!]$$

As for refined 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 Δ induces maps of Heyting algebras on subobject lattices (Lem. C.8).

Case of $[\mathrm{bx}]\varphi$.
Trivial, since $[\![[\mathrm{bx}]\varphi]\!]$ is in the image of Δ.

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

Case of $[\mathrm{fd}]\varphi$.
In this case, we must have $A = \mathsf{Fix}(X).B(X)$. Since X is guarded in $B(X)$, it must not occur in $B(X)$ (recall that $\blacksquare T$ is only allowed for a *closed* type T). But this is forbidden.

Case of $[\pi_i]\varphi$.
We rely on the description of $[\![[\pi_i]\varphi]\!]$ as $[\![[\pi_i]]\!]([\![\varphi]\!])$ in §C.6. By induction hypothesis and recalling that Δ preserves finite products, consider the pullback

$$\begin{array}{ccc} \pi^*([\![\varphi]\!]) \simeq [\![[\pi_i]\varphi]\!] & \longrightarrow & [\![\varphi]\!] \simeq \Delta(S) \\ \downarrow & & \downarrow \\ \Delta(S_0) \times \Delta(S_1) & \xrightarrow[\pi_i]{} & \Delta(S_i) \end{array}$$

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

$$\begin{array}{ccc} S' & \longrightarrow & S \\ \downarrow & & \downarrow \\ S_0 \times S_1 & \xrightarrow[\pi_i]{} & S_i \end{array}$$

and this implies that $[\![[\pi_i]\varphi]\!] \simeq \Delta(S')$ since Δ preserves finite limits.

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

$$[\![\varphi]\!] \simeq \Delta(S) \hookrightarrow \Delta(S_i) \xrightarrow{\Delta(\mathsf{in}_i)=\mathsf{in}_i} \Delta(S_0) + \Delta(S_1)$$

Case of $[\mathrm{ev}(\psi)]\varphi$.
We rely on the description of $[\![[\mathrm{ev}(\psi)]\varphi]\!]$ in §C.6, that is

$$[\![[\mathrm{ev}(\psi)]\varphi]\!] \;=\; \forall_{[\![B]\!]} \left(\pi^*([\![\psi]\!]) \Longrightarrow_{[\![A]\!]^{[\![B]\!]}\times[\![B]\!]} \mathrm{ev}^*([\![\varphi]\!])\right)$$

The result then follows from Lem. C.8 and the fact that Δ thus preserves universal quantifications (see e.g. [36, Thm. X.3.1 & Lem. X.3.2]).

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

C.10 Realizability

We detail the steps toward the Adequacy Theorem 7.12. Full proofs are deferred to App. E.4. The first basic result we need about our notion of realizability is that it is monotone w.r.t. step indexes.

Lemma C.22 (Monotonicity of Realizability)**.** *If $x \Vdash_n T$ then $x \Vdash_k T$ for all $k \le n$.*

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

$$\frac{}{T \le |T|}$$

Lemma C.23. *For a pure type A and $x \in \Gamma[\![A]\!]$, we have $x \Vdash_n A$ for all $n > 0$.*

Second, we need a result of [13] for the correctness of the subtyping rules

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

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

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 C.24 ([13, Cor. 3.8])**.** *For a pure type A, the object $[\![A]\!]$ is total.*

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

$$\frac{\vdash^A \varphi \Rightarrow \psi}{\{A \mid \varphi\} \le \{A \mid \psi\}} \qquad \frac{\vdash_{\mathrm{c}}^A \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathrm{bx}]\varphi\} \le \{\blacksquare A \mid [\mathrm{bx}]\psi\}}$$

rely on Lem. C.13 (Lem. 7.3), while

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

is given by Prop. 7.7.

Lemma C.25 (Correctness of Subtyping (Lem. 7.11))**.** *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 7.12. As usual it requires a stronger inductive invariant than the statement of Thm. 7.12. Given a typed term

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

and global sections $u_1 \in \mathbf{\Gamma}[\![|T_1|]\!], \dots, u_k \in \mathbf{\Gamma}[\![|T_k|]\!]$, 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 $\Gamma = x_1 : T_1, \dots, x_k : T_k$ we write $\rho \models \Gamma$ if ρ takes each x_i for $i = 1, \dots, k$ to some $\rho(x_i) \in \mathbf{\Gamma}[\![|T_i|]\!]$. Given a typing judgment $\Gamma \vdash M : T$, we let

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

Given $\rho \models \Gamma$ and $n > 0$, write $\rho \Vdash_n \Gamma$ if $\rho(x_i) \Vdash_n T_i$ for all $i = 1, \dots, k$. Thm. 7.12 is proved under the following form.

Theorem C.26 (Adequacy (Thm. 7.12))**.** *Let Γ, T have free iteration variables among $\overline{\ell}$, and let $\overline{m} \in \mathbb{N}$. If $\Gamma \vdash M : T$ and $\rho \models \Gamma$, then*

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

Corollary C.27. *(a) Consider a closed term $\vdash M : \{A \mid \varphi\}$ with φ safe. Then $[\![M]\!] : \mathbf{1} \to_{\mathcal{S}} [\![A]\!] \in \wr\varphi\wr$.*

(b) Consider a closed term $\vdash M : \{A \mid \psi\} \to \{A \mid \varphi\}$, with φ, ψ safe. Then $[\![M]\!]$ induces a function $\mathbf{\Gamma}[\![M]\!]$ taking $x \in \wr\psi\wr$ to $\mathbf{\Gamma}[\![M]\!] = [\![M]\!] \circ x \in \wr\varphi\wr$.

Corollary C.27 of course extends to any arity. As a consequence of Cor. C.27, a closed term $M : \{P \mid \varphi\}$ for P polynomial recursive and φ safe induces a global section $[\![M]\!] : \mathbf{1} \to_{\mathcal{S}} [\![P]\!]$ which satisfies φ is the standard sense. Moreover a function, say $M : \{Q \mid \psi\} \to \{P \mid \varphi\}$ with Q, P polynomial recursive and ψ, φ safe, induces by composition a **Set**-function

$$\mathbf{\Gamma}[\![M]\!] : \mathbf{\Gamma}[\![Q]\!] \to \mathbf{\Gamma}[\![P]\!], \quad x \mapsto [\![M]\!] \circ x$$

such that, in the standard sense, $\mathbf{\Gamma}[\![M]\!](x)$ satisfies φ whenever x satisfies ψ.

C.11 A Galois Connection

In §7, we indicated that safe formulae over $\mathrm{Str}^{\mathrm{g}}\, A$ are safety (*i.e.* topologically closed) properties. In view of Møgelberg's Theorem [40] (Thm. 7.13), this generalizes to polynomial recursive types: safe formulae on polynomial recursive types define closed sets for the usual tree (or stream) topology.

We briefly elaborate on this. Fix an object X of $\mathcal{S}$. There is a Galois connection between the subobjects of X in $\mathcal{S}$ and the subsets of $\mathbf{\Gamma}X$ in **Set**:

$$\mathrm{Pref} \dashv [-] \;:\; \mathrm{Sub}(X) \to \mathcal{P}(\mathbf{\Gamma}X)$$

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

$$\begin{array}{rcl} \mathrm{Pref}(S) & : & n \longmapsto \{x_n(\bullet) \mid x \in S\} \\ [B] & := & \{x \in \mathbf{\Gamma}X \mid \forall n \in \mathbb{N}_*,\ x_n(\bullet) \in B(n)\} \end{array}$$

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

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

$$\begin{array}{rcccc} \mathrm{Pref} & : & \mathcal{P}(\mathbf{\Gamma}X) & \longrightarrow & \mathrm{Sub}(X) \\ [-] & : & \mathrm{Sub}(X) & \longrightarrow & \mathcal{P}(\mathbf{\Gamma}X) \end{array}$$

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

Lemma C.28. *We have*

(i) $S \subseteq [\mathrm{Pref}(S)]$ for $S \in \mathcal{P}(\mathbf{\Gamma}X)$.

(ii) $\mathrm{Pref}([B]) \subseteq B$ 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 $x \in [\mathrm{Pref}(S)]$.

(ii) Given $a \in \mathrm{Pref}([B])(n)$, there is some $x \in [B]$ such that $a = x_n(\bullet)$. But $x \in [B]$ means $x_k(\bullet) \in B(k)$ for all $k > 0$, so that $a = x_n(\bullet) \in B(n)$. □

As usual, we trivially get

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

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

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

When A is a polynomial recursive type, Thm. 7.13 thus says that S is closed if and only if S is closed for the corresponding usual tree (or stream) topology. Since Prop. 7.7 can be formulated as

$$\wr\varphi\wr \;=\; [[\![\varphi]\!]]$$

it indeed says that $\wr\varphi\wr$ is closed for the usual topology.

D Details of the Examples

D.1 Guarded Streams

D.1.1 The Later Modality on Guarded Streams

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

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

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

$$\dfrac{\dfrac{\dfrac{}{x : A,\ s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\}}}{x : A,\ s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash s : \{\blacktriangleright \mathrm{Str}^{\mathsf{g}}\, A \mid [\mathsf{next}]\varphi\}}}{x : A,\ s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash \langle x, s\rangle : \{A \times \blacktriangleright \mathrm{Str}^{\mathsf{g}}\, A \mid [\pi_1][\mathsf{next}]\varphi\}}}{x : A,\ s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\} \vdash \mathsf{fd}\langle x, s\rangle : \{\mathrm{Str}^{\mathsf{g}}\, A \mid [\mathsf{fd}][\pi_1][\mathsf{next}]\varphi\}}$$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid [\mathsf{fd}][\pi_1][\mathsf{next}]\varphi\}}}{s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \mathsf{ufd}\ s : \{A \times \blacktriangleright \mathrm{Str}^{\mathsf{g}}\, A \mid [\pi_1][\mathsf{next}]\varphi\}}}{s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \pi_1(\mathsf{ufd}\ s) : \{\blacktriangleright \mathrm{Str}^{\mathsf{g}}\, A \mid [\mathsf{next}]\varphi\}}}{s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \bigcirc\varphi\} \vdash \pi_1(\mathsf{ufd}\ s) : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \varphi\}}$$

□

D.1.2 Destructors of Guarded Streams

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

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

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

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

We use $\vdash^{\mathrm{Str}^{\mathsf{g}}\, A} \Box[\varphi] \Rightarrow [\varphi]$ (Ex. 5.8).

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

We continue with the typing of

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

We use $\vdash^{\mathrm{Str}^{\mathsf{g}}\, A} \Box[\varphi] \Rightarrow \bigcirc\Box[\varphi]$ (Ex.5.8). Recall that $\bigcirc\varphi = [\mathsf{fd}][\pi_1][\mathsf{next}]\varphi$.

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

□

D.1.3 Constructor of Guarded Streams

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

$$\mathsf{cons}^{\mathsf{g}} \quad : \quad \{A \mid \varphi\} \longrightarrow \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\} \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\}$$

Proof. We show

$$\mathsf{cons}^{\mathsf{g}} \quad := \quad \lambda x.\lambda s.\mathsf{fd}\langle x, s\rangle \quad : \quad \{A \mid \varphi\} \longrightarrow \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\} \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\}$$

To this end, we use the following derived rule (see Ex. 6.1):

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

Consider the typing context

$$\Gamma \quad := \quad x : \{A \mid \varphi\}\,,\ s : \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\}$$

We know from §D.1.1 that

$$\Gamma \vdash \mathsf{fd}\langle x, s\rangle : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \bigcirc\Box[\varphi]\}$$

Since $\vdash^{\mathrm{Str}^{\mathsf{g}}\, A} ([\varphi] \wedge \bigcirc\Box[\varphi]) \Rightarrow \Box[\varphi]$ (Ex. 5.8), we are done if we show

$$\Gamma \vdash \mathsf{fd}\langle x, s\rangle : \{\mathrm{Str}^{\mathsf{g}}\, A \mid [\varphi]\}$$

But this is trivial:

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

□

D.1.4 Map over Guarded Streams

Example D.4. We have the following:

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

Proof. We proceed as follows, using §D.1.2 and §D.1.3:

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

where

$$\begin{array}{rcl} T & := & (\{A \mid \varphi\} \to \{B \mid \psi\}) \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\} \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\, B \mid \Box[\psi]\} \\ \Gamma & := & f : \{A \mid \varphi\} \to \{B \mid \psi\}\,,\ g : \blacktriangleright(\{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\} \to \{\mathrm{Str}^{\mathsf{g}}\, B \mid \Box[\psi]\}),\ s : \{\mathrm{Str}^{\mathsf{g}}\, A \mid \Box[\varphi]\} \end{array}$$

□

D.1.5 Merge over Guarded Streams

Example D.5. We have the following:

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

Proof. Let Γ be the context

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

We have

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

We thus get

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

and we are done since using subtyping we have

$$\begin{array}{rcl} \mathsf{cons}^{\mathsf{g}} & : & \{A \mid \varphi_0\} \longrightarrow \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\ A \mid \Box([\varphi_0] \vee [\varphi_1])\} \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\ A \mid \Box([\varphi_0] \vee [\varphi_1])\} \\ \mathsf{cons}^{\mathsf{g}} & : & \{A \mid \varphi_1\} \longrightarrow \blacktriangleright \{\mathrm{Str}^{\mathsf{g}}\ A \mid \Box([\varphi_0] \vee [\varphi_1])\} \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\ A \mid \Box([\varphi_0] \vee [\varphi_1])\} \end{array}$$

□

D.2 Map over Coinductive Streams

D.2.1 The Case of *Eventually* ($\Diamond[\varphi]$)

Example D.6. We have the following, for *safe* φ and ψ:

$$\begin{array}{rcl} \mathsf{map} & : & (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathrm{Str}\ B \mid [\mathsf{bx}]\Diamond[\psi]\} \longrightarrow \{\mathrm{Str}\ A \mid [\mathsf{bx}]\Diamond[\varphi]\} \\ & = & \lambda f.\lambda s.\mathsf{bx}\big(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{ubx}\ s)\big) \end{array}$$

Proof. We first reduce to

$$\Gamma_f,\ s : \left\{\mathrm{Str}\ B \,\middle|\, [\mathsf{bx}]\Diamond^k[\psi]\right\} \quad \vdash \quad \mathsf{bx}(\mathsf{map}^{\mathsf{g}}\ f\ (\mathsf{ubx}\ s)) \quad : \quad \left\{\mathrm{Str}\ A \,\middle|\, [\mathsf{bx}]\Diamond^k[\varphi]\right\}$$

where

$$\Gamma_f \quad := \quad f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

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

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

Let

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

We show

$$\Gamma \quad \vdash \quad M \quad : \quad \forall k \cdot T(k)$$

We reason by cases on k with the rule

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

Case of $T(\mathtt{0})$**.** We show

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathsf{g}}\ B \,\middle|\, \Diamond^{\mathtt{0}}[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathsf{g}}\ A \,\middle|\, \Diamond^{\mathtt{0}}[\varphi]\right\}$$

Since $\vdash \Diamond^{\mathtt{0}}[\psi] \Leftrightarrow \bot$, we conclude with the *Ex Falso* rule

$$\frac{\Gamma,\ s : \left\{\mathrm{Str}^{\mathsf{g}}\ B \,\middle|\, \Diamond^{\mathtt{0}}[\psi]\right\} \vdash s : \{\mathrm{Str}^{\mathsf{g}}\ B \mid \bot\} \qquad \Gamma,\ s : \left\{\mathrm{Str}^{\mathsf{g}}\ B \,\middle|\, \Diamond^{\mathtt{0}}[\psi]\right\} \vdash N : \mathrm{Str}^{\mathsf{g}}\ A}{\Gamma,\ s : \{\mathrm{Str}^{\mathsf{g}}\ B \mid \Diamond^{\mathtt{0}}[\psi]\} \vdash N : \{\mathrm{Str}^{\mathsf{g}}\ A \mid \Diamond^{\mathtt{0}}[\varphi]\}}$$

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

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathsf{g}}\ B \,\middle|\, \Diamond^{k+1}[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathsf{g}}\ A \,\middle|\, \Diamond^{k+1}[\varphi]\right\}$$

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

Subcase of $[\psi]$**.** Since $\vdash [\varphi] \Rightarrow \Diamond^{k+1}[\varphi]$, we reduce to showing

$$\Gamma,\ s : \{\mathrm{Str}^{\mathsf{g}}\ B \mid [\psi]\} \quad \vdash \quad N \quad : \quad \{\mathrm{Str}^{\mathsf{g}}\ A \mid [\varphi]\}$$

By §D.1.2 we have

$$\Gamma,\ s : \{\mathrm{Str}^{\mathsf{g}}\ B \mid [\psi]\} \quad \vdash \quad \mathsf{hd}^{\mathsf{g}}\ s \quad : \quad \{B \mid \psi\}$$

But we are done since

$$\mathsf{cons}^{\mathsf{g}} \quad : \quad \{A \mid \varphi\} \longrightarrow \blacktriangleright \mathrm{Str}^{\mathsf{g}}\ A \longrightarrow \{\mathrm{Str}^{\mathsf{g}}\ A \mid [\varphi]\}$$

Subcase of $\bigcirc\Diamond^k[\psi]$. Since $\vdash \bigcirc\Diamond^k[\varphi] \Rightarrow \Diamond^{k+1}[\varphi]$, we reduce to showing

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k[\psi]\right\} \quad\vdash\quad N \quad:\quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \bigcirc\Diamond^k[\varphi]\right\}$$

By §D.1.1 we have

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k[\psi]\right\} \quad\vdash\quad \mathrm{tl}^{\mathrm{g}}\ s \quad:\quad \blacktriangleright \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^k[\psi]\right\}$$

Since

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

we have

$$\Gamma \quad\vdash\quad g \quad:\quad \blacktriangleright\left(\left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^k[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^k[\varphi]\right\}\right)$$

Since moreover by §D.1.1 we have

$$\mathrm{cons}^{\mathrm{g}} \quad:\quad A \longrightarrow \blacktriangleright \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^k[\varphi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \bigcirc\Diamond^k[\varphi]\right\}$$

we deduce that

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k[\psi]\right\} \quad\vdash\quad N \quad:\quad \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k[\psi]\right\}$$

□

D.2.2 The Case of *Eventually Always* ($\Diamond\Box[\varphi]$)

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

$$\begin{array}{rcl} \mathrm{map} & : & (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathrm{Str}\, B \mid [\mathrm{bx}]\Diamond\Box[\psi]\} \longrightarrow \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Diamond\Box[\varphi]\} \\ & = & \lambda f.\lambda s.\mathrm{bx}(\mathrm{map}^{\mathrm{g}}\ f\ (\mathrm{ubx}\ s)) \end{array}$$

Proof. We first reduce to

$$\Gamma_f,\ s : \left\{\mathrm{Str}\, B \,\middle|\, [\mathrm{bx}]\Diamond^k\Box[\psi]\right\} \quad\vdash\quad \mathrm{bx}(\mathrm{map}^{\mathrm{g}}\ f\ (\mathrm{ubx}\ s)) \quad:\quad \left\{\mathrm{Str}\, A \,\middle|\, [\mathrm{bx}]\Diamond^k\Box[\varphi]\right\}$$

where

$$\Gamma_f \quad:=\quad f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

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

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

Let

$$\begin{array}{rcl} N & := & (f(\mathrm{hd}^{\mathrm{g}}\ s)) ::^{\mathrm{g}} (g \circledast (\mathrm{tl}^{\mathrm{g}}\ s)) \\ M & := & \lambda s.N \\ T(k) & := & \left\{\mathrm{Str}^{\mathrm{g}}\, B \to \mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, [\mathrm{ev}(\Diamond^k\Box[\psi])]\Diamond^k\Box[\varphi] \ \wedge\ [\mathrm{ev}(\Box[\psi])]\Box[\varphi]\right\} \\ \Gamma & := & \Gamma_f,\ g : \blacktriangleright\forall k \cdot T(k) \end{array}$$

We show

$$\Gamma \quad\vdash\quad M \quad:\quad \forall k \cdot T(k)$$

We reason by cases on k with the rule

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

Case of $T(0)$. We have to show

$$\begin{array}{rcl} & \Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \Box[\psi]\} \quad\vdash\quad N \quad:\quad \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Box[\varphi]\} \\ \text{and} \quad & \Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^0\Box[\psi]\right\} \quad\vdash\quad N \quad:\quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^0\Box[\varphi]\right\} \end{array}$$

We only detail the latter since the former can be dealt-with as in §D.1.5. Since $\vdash \Diamond^0\Box[\psi] \Leftrightarrow \bot$, we conclude with the *Ex Falso* rule

$$\frac{\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^0\Box[\psi]\right\} \vdash s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \bot\} \qquad \Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^0\Box[\psi]\right\} \vdash N : \mathrm{Str}^{\mathrm{g}}\, A}{\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \Diamond^0\Box[\psi]\} \vdash N : \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Diamond^0\Box[\varphi]\}}$$

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

$$\begin{array}{rcl} & \Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \Box[\psi]\} \quad\vdash\quad N \quad:\quad \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Box[\varphi]\} \\ \text{and} \quad & \Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^{k+1}\Box[\psi]\right\} \quad\vdash\quad N \quad:\quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k+1}\Box[\varphi]\right\} \end{array}$$

We only detail the latter since the former can be dealt-with as in §D.1.5. Using $\vdash \Diamond^{k+1}\Box[\psi] \ \Leftrightarrow\ (\Box[\psi] \vee \bigcirc\Diamond^k\Box[\psi])$, we do a case analysis on the refinement type of s.

Subcase of $\Box[\psi]$. We show

$$\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \Box[\psi]\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k+1}\Box[\varphi]\right\}$$

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

$$\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \Box[\psi]\} \quad \vdash \quad N \quad : \quad \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Box[\varphi]\}$$

and we can conclude as in §D.1.5.

Subcase of $\bigcirc\Diamond^k\Box[\psi]$. Since $\vdash \bigcirc\Diamond^k\Box[\varphi] \Rightarrow \Diamond^{k+1}\Box[\varphi]$, we reduce to showing

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k\Box[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \bigcirc\Diamond^k\Box[\varphi]\right\}$$

By §D.1.1 we have

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k\Box[\psi]\right\} \quad \vdash \quad \mathrm{tl}^{\mathrm{g}}\ s \quad : \quad \blacktriangleright \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^k\Box[\psi]\right\}$$

Since

$$\Gamma \quad \vdash \quad g \quad : \quad \forall k \cdot \blacktriangleright \left(\left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^k\Box[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^k\Box[\varphi]\right\}\right)$$

we have

$$\Gamma \quad \vdash \quad g \quad : \quad \blacktriangleright \left(\left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^k\Box[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^k\Box[\varphi]\right\}\right)$$

Since moreover by §D.1.1 we have

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

we deduce that

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k\Box[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^k\Box[\psi]\right\}$$

□

D.2.3 The Case of *Always Eventually* ($\Box\Diamond[\varphi]$)

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

$$\begin{array}{rcl} \mathrm{map} & : & (\{B \mid \psi\} \to \{A \mid \varphi\}) \longrightarrow \{\mathrm{Str}\, B \mid [\mathrm{bx}]\Box\Diamond[\psi]\} \longrightarrow \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box\Diamond[\varphi]\} \\ & := & \lambda f.\lambda s.\mathrm{bx}\big(\mathrm{map}^{\mathrm{g}}\ f\ (\mathrm{ubx}\ s)\big) \end{array}$$

Notation D.9. We let

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

Proof. We start in the same spirit as in §D.2.1 and §D.2.2 but we now use the rules

$$\frac{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\psi[\mu\alpha^{\omega}\varphi/\beta]\} \qquad \Gamma, x : \left\{\blacksquare A \,\middle|\, [\mathrm{bx}]\psi[\mu\alpha^{k}\varphi/\beta]\right\} \vdash N : U \qquad \beta \text{ Pos } \psi}{\Gamma \vdash N[M/x] : U} \ (k \text{ not free in } \Gamma, U)$$

$$\frac{\Gamma \vdash M : \left\{\blacksquare A \,\middle|\, [\mathrm{bx}]\psi[\mu\alpha^{\mathrm{t}}\varphi/\beta]\right\} \qquad \beta \text{ Pos } \psi}{\Gamma \vdash M : \{\blacksquare A \mid [\mathrm{bx}]\psi[\mu\alpha^{\omega}\varphi/\beta]\}}$$

with the non-trivial context

$$\psi(\beta) \quad := \quad \Box\beta$$

We then similarly unfold the $\Box$. We are thus led to deriving

$$\Gamma_f,\ s : \left\{\mathrm{Str}\, B \,\middle|\, [\mathrm{bx}]\Box^{\ell}\Diamond^{k}[\psi]\right\} \quad \vdash \quad \mathrm{bx}(\mathrm{map}^{\mathrm{g}}\ f\ (\mathrm{ubx}\ s)) \quad : \quad \left\{\mathrm{Str}\, A \,\middle|\, [\mathrm{bx}]\Box^{\ell}\Diamond^{k}[\varphi]\right\}$$

where

$$\Gamma_f \quad := \quad f : \{B \mid \psi\} \to \{A \mid \varphi\}$$

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

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

Let

$$\begin{array}{rcl} N & := & (f(\mathrm{hd}^{\mathrm{g}}\ s)) ::^{\mathrm{g}} (g \circledast (\mathrm{tl}^{\mathrm{g}}\ s)) \\ M & := & \lambda s.N \\ T(k,\ell) & := & \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell}\Diamond^{k}[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Box^{\ell}\Diamond^{k}[\varphi]\right\} \\ \Gamma & := & \Gamma_f,\ g : \blacktriangleright\forall k \cdot \forall \ell \cdot T(k,\ell) \end{array}$$

We show

$$\Gamma \quad \vdash \quad M \quad : \quad \forall k \cdot \forall \ell \cdot T(k,\ell)$$

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

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

Cases of $T(\mathsf{u},0)$**.** We have $\vdash \Box^0\theta \Leftrightarrow \top$, and we are done since

$$\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \top\} \quad \vdash \quad N \quad : \quad \{\mathrm{Str}^{\mathrm{g}}\, A \mid \top\}$$

Case of $T(0,\ell{+}1)$**.** We have $\vdash \Diamond^0[\theta] \Leftrightarrow \bot$, and we reduce to showing

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\bot\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Box^{\ell+1}\bot\right\}$$

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

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\bot\right\} \quad \vdash \quad s \quad : \quad \{\mathrm{Str}^{\mathrm{g}}\, B \mid \bot\}$$

and we conclude with the *Ex Falso* rule

$$\frac{\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\bot\right\} \vdash s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid \bot\} \qquad \Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\bot\right\} \vdash N : \mathrm{Str}^{\mathrm{g}}\, A}{\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\bot\right\} \vdash N : \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Box^{\ell+1}\bot\right\}}$$

Case of $T(k{+}1,\ell{+}1)$**.** Using $\vdash^{\mathrm{Str}^{\mathrm{g}}\, A} \Box^{\ell+1}\theta \ \Leftrightarrow\ (\theta \wedge \bigcirc\Box^{\ell}\theta)$, we show

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\Diamond^{k+1}[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k+1}[\varphi] \ \wedge\ \bigcirc\Box^{\ell}\Diamond^{k+1}[\varphi]\right\}$$

We consider each conjunct separately.

(Sub)Case of $\Diamond^{k+1}[\varphi]$**.** We show

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\Diamond^{k+1}[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k+1}[\varphi]\right\}$$

Using

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{\ell+1}\Diamond^{k+1}[\psi]\right\} \quad \vdash \quad s \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^{k+1}[\psi]\right\}$$

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

(SubSub)Case of $[\psi]$**.** Since (by §D.1.1)

$$\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid [\psi]\} \quad \vdash \quad \mathrm{hd}^{\mathrm{g}}\, s \quad : \quad \{\mathrm{Str}^{\mathrm{g}}\, B \mid \psi\}$$

we easily deduce that

$$\Gamma,\ s : \{\mathrm{Str}^{\mathrm{g}}\, B \mid [\psi]\} \quad \vdash \quad N \quad : \quad \{\mathrm{Str}^{\mathrm{g}}\, A \mid [\varphi]\}$$

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

(SubSub)Case of $\bigcirc\Diamond^{k}[\psi]$**.** By §D.1.1 we have

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^{k}[\psi]\right\} \quad \vdash \quad \mathrm{tl}^{\mathrm{g}}\, s \quad : \quad \blacktriangleright \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^{k}[\psi]\right\}$$

Since

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

we have

$$\Gamma \quad \vdash \quad g \quad : \quad \blacktriangleright \left(\left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Box^{1}\Diamond^{k}[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Box^{1}\Diamond^{k}[\varphi]\right\}\right)$$

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

$$\Gamma \quad \vdash \quad g \quad : \quad \blacktriangleright \left(\left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \Diamond^{k}[\psi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k}[\varphi]\right\}\right)$$

Since moreover by §D.1.1 we have

$$\mathrm{cons}^{\mathrm{g}} \quad : \quad A \longrightarrow \blacktriangleright \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \Diamond^{k}[\varphi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\, A \,\middle|\, \bigcirc\Diamond^{k}[\varphi]\right\}$$

we deduce that

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^{k}[\psi]\right\} \quad \vdash \quad N \quad : \quad \left\{\mathrm{Str}^{\mathrm{g}}\, B \,\middle|\, \bigcirc\Diamond^{k}[\psi]\right\}$$

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

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

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

Since

$$\Gamma,\ s : \left\{\mathrm{Str}^{\mathrm{g}}\ B \,\middle|\, \Box^{\ell+1}\Diamond^{k+1}[\psi]\right\} \ \vdash\ s\ :\ \left\{\mathrm{Str}^{\mathrm{g}}\ B \,\middle|\, \bigcirc\Box^{\ell}\Diamond^{k+1}[\psi]\right\}$$

by §D.1.1 we have

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

But now since

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

we have

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

and we conclude with §D.1.1, namely

$$\mathrm{cons}^{\mathrm{g}}\ :\ A \longrightarrow \blacktriangleright\left\{\mathrm{Str}^{\mathrm{g}}\ A \,\middle|\, \Box^{\ell}\Diamond^{k+1}[\varphi]\right\} \longrightarrow \left\{\mathrm{Str}^{\mathrm{g}}\ A \,\middle|\, \bigcirc\Box^{\ell}\Diamond^{k+1}[\varphi]\right\}$$

□

D.3 The Diagonal Function

D.3.1 Operations on Coinductive Streams

Example D.10 (Operations on Coinductive Streams). For a *safe* φ of the appropriate type, we have

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

Proof.

Case of hd. Recall that

$$\begin{array}{rcl} \mathsf{hd} & : & \mathrm{Str}\ A \longrightarrow A \\ & := & \lambda s.\mathsf{hd}^{\mathrm{g}}\ (\mathrm{ubx}\ s) \end{array}$$

We have

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\}}\quad \Box[\varphi]\ \mathrm{safe}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash s : \blacksquare\{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathrm{ubx}\ s : \{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathsf{hd}^{\mathrm{g}}(\mathrm{ubx}\ s) : \{A \mid \varphi\}}}{\vdash \lambda s.\mathsf{hd}^{\mathrm{g}}\ (\mathrm{ubx}\ s)\ :\ \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{A \mid \varphi\}}$$

Cases of tl. Recall that

$$\begin{array}{rcl} \mathsf{tl} & : & \mathrm{Str}\ A \longrightarrow \mathrm{Str}\ A \\ & := & \lambda s.\mathrm{bx}(\mathrm{prev}(\mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s))) \end{array}$$

We have

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\}}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathrm{ubx}\ s : \{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s)\ :\ \blacktriangleright\{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}\quad \mathrm{Str}\ A\ \mathrm{constant}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathrm{prev}(\mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s))\ :\ \{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathrm{bx}(\mathrm{prev}(\mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s)))\ :\ \blacksquare\{\mathrm{Str}^{\mathrm{g}}\ A \mid \Box[\varphi]\}}\quad \Box[\varphi]\ \mathrm{safe}}{s : \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \vdash \mathrm{bx}(\mathrm{prev}(\mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s)))\ :\ \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\}}}{\vdash \lambda s.\mathrm{bx}(\mathrm{prev}(\mathsf{tl}^{\mathrm{g}}\ (\mathrm{ubx}\ s)))\ :\ \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}\ A \mid [\mathrm{bx}]\Box[\varphi]\}}$$

and

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\}}}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash \mathrm{ubx}\, s : \{\mathrm{Str}^{\mathrm{g}}\, A \mid \bigcirc\varphi\}}}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash \mathrm{tl}^{\mathrm{g}}\, (\mathrm{ubx}\, s) \ : \ \blacktriangleright \{\mathrm{Str}^{\mathrm{g}}\, A \mid \varphi\}} \quad \mathrm{Str}\, A \text{ constant}}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash \mathrm{prev}(\mathrm{tl}^{\mathrm{g}}\, (\mathrm{ubx}\, s)) \ : \ \{\mathrm{Str}^{\mathrm{g}}\, A \mid \varphi\}}}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash \mathrm{bx}(\mathrm{prev}(\mathrm{tl}^{\mathrm{g}}\, (\mathrm{ubx}\, s))) \ : \ \blacksquare \{\mathrm{Str}^{\mathrm{g}}\, A \mid \varphi\}} \quad \varphi \text{ safe}}{s : \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \vdash \mathrm{bx}(\mathrm{prev}(\mathrm{tl}^{\mathrm{g}}\, (\mathrm{ubx}\, s))) \ : \ \{\mathrm{Str}\, A \mid [\mathrm{bx}]\varphi\}}}{\vdash \lambda s.\mathrm{bx}(\mathrm{prev}(\mathrm{tl}^{\mathrm{g}}\, (\mathrm{ubx}\, s))) \ : \ \{\mathrm{Str}\, A \mid [\mathrm{bx}] \bigcirc \varphi\} \ \longrightarrow \ \{\mathrm{Str}\, A \mid [\mathrm{bx}]\varphi\}}$$

□

D.3.2 The Guarded Diagonal Function

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

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

Recall that

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

$$\begin{array}{rcl} \mathrm{diagaux}^{\mathrm{g}} & : & (\mathrm{Str}\, A \to \mathrm{Str}\, A) \longrightarrow \mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \longrightarrow \mathrm{Str}^{\mathrm{g}}\, A \\ & := & \mathrm{fix}(f).\lambda g.\lambda s.(\mathrm{hd} \circ g)(\mathrm{hd}^{\mathrm{g}}\, s) ::^{\mathrm{g}} (f \circledast \mathrm{next}(g \circ \mathrm{tl}) \circledast (\mathrm{tl}^{\mathrm{g}}\, s)) \end{array}$$

Proof. We reduce to

$$\mathrm{diagaux}^{\mathrm{g}} \ : \ \big(\{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \to \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\}\big) \longrightarrow \{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \mid \Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Box[\varphi]\}$$

Let Γ be the context

$$\begin{array}{rcl} f & : & \blacktriangleright T\,, \\ g & : & \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\}\,, \\ s & : & \{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \mid \Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\} \end{array}$$

where T is the type

$$\big(\{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \to \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\}\big) \longrightarrow \{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \mid \Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}^{\mathrm{g}}\, A \mid \Box[\varphi]\}$$

The result directly follows from the following typings, which are themselves given by §D.1.2, §D.1.3 and §D.3.1:

$$\begin{array}{rcl} \Gamma & \vdash & \mathrm{hd} \circ g \ : \ \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{A \mid \varphi\} \\ \Gamma & \vdash & \mathrm{hd}^{\mathrm{g}}\, s \ : \ \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \\ \Gamma & \vdash & g \circ \mathrm{tl} \ : \ \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \\ \Gamma & \vdash & \mathrm{tl}^{\mathrm{g}}\, s \ : \ \blacktriangleright \{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \mid \Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\} \end{array}$$

□

D.3.3 The Coinductive Diagonal Function

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

$$\begin{array}{rcl} \mathrm{diag} & : & \{\mathrm{Str}(\mathrm{Str}\, A) \mid [\mathrm{bx}]\Diamond\Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\} \longrightarrow \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Diamond\Box[\varphi]\} \\ & := & \lambda s.\mathrm{bx}(\mathrm{diag}^{\mathrm{g}}\, (\mathrm{ubx}\, s)) \end{array}$$

Proof. We first reduce to

$$s : \big\{\mathrm{Str}(\mathrm{Str}\, A) \,\big|\, [\mathrm{bx}]\Diamond^k\Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\big\} \ \vdash \ \mathrm{bx}(\mathrm{diag}^{\mathrm{g}}\, (\mathrm{ubx}\, s)) \ : \ \big\{\mathrm{Str}\, A \,\big|\, [\mathrm{bx}]\Diamond^k\Box[\varphi]\big\}$$

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

$$\mathrm{diag}^{\mathrm{g}} \ : \ \big\{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \,\big|\, \Diamond^k\Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi]\big\} \longrightarrow \big\{\mathrm{Str}^{\mathrm{g}}\, A \,\big|\, \Diamond^k\Box[\varphi]\big\}$$

Consider the types

$$\begin{array}{rcl} U(k) & := & \big\{\mathrm{Str}^{\mathrm{g}}(\mathrm{Str}\, A) \to \mathrm{Str}^{\mathrm{g}}\, A \,\big|\, [\mathrm{ev}(\Diamond^k\Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi])]\Diamond^k\Box[\varphi] \ \wedge \ [\mathrm{ev}(\Box[\mathrm{hd}][\mathrm{bx}]\Box[\varphi])]\Box[\varphi]\big\} \\ T(k) & := & \big(\{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\} \to \{\mathrm{Str}\, A \mid [\mathrm{bx}]\Box[\varphi]\}\big) \longrightarrow U(k) \end{array}$$

We show

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

Let

$$\begin{array}{lcl} N & := & (\mathsf{hd} \circ g)(\mathsf{hd}^{\mathsf{g}}\ s) ::^{\mathsf{g}} (f \circledast \mathsf{next}(g \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) \\ M & := & \lambda g.\lambda s.N \\ \Gamma & := & f : \blacktriangleright \forall k \cdot T(k) \end{array}$$

We reason by cases on k with the rule

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

Let

$$\Gamma' \quad := \quad \Gamma,\ g : \{\mathsf{Str}\,A \mid [\mathsf{bx}]\Box[\varphi]\} \longrightarrow \{\mathsf{Str}\,A \mid [\mathsf{bx}]\Box[\varphi]\}$$

We omit the proof of

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

since it follows that of §D.3.2.

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

$$\Gamma \quad \vdash \quad \lambda g.\lambda s.N \quad : \quad \big(\{\mathsf{Str}\,A \mid [\mathsf{bx}]\Box[\varphi]\} \to \{\mathsf{Str}\,A \mid [\mathsf{bx}]\Box[\varphi]\}\big) \longrightarrow \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \bot\} \longrightarrow \left\{\mathsf{Str}^{\mathsf{g}}\,A \,\middle|\, \Diamond^{\mathtt{0}}\Box[\varphi]\right\}$$

and we conclude using the *Ex Falso* rule.

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

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

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.

Subcase of $\Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]$**.** We show

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

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

$$\Gamma',\ s : \{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \mid \Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]\} \quad \vdash \quad N \quad : \quad \{\mathsf{Str}^{\mathsf{g}}\,A \mid \Box[\varphi]\}$$

which is proved as in §D.3.2.

Subcase of $\bigcirc\Diamond^{k}\Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]$**.** We show

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

Let

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

Note that $\Gamma'' \vdash f : \blacktriangleright T(k)$, so that by §D.3.1 we have

$$\Gamma'' \quad \vdash \quad f \circledast \mathsf{next}(g \circ \mathsf{tl}) \quad : \quad \blacktriangleright\left(\left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \,\middle|\, \Diamond^{k}\Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]\right\} \to \left\{\mathsf{Str}^{\mathsf{g}}\,A \,\middle|\, \Diamond^{k}\Box[\varphi]\right\}\right)$$

Using §D.1.1, we derive

$$\dfrac{\dfrac{\dfrac{}{\Gamma'' \vdash s : \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \,\middle|\, \bigcirc\Diamond^{k}\Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]\right\}}}{\Gamma'' \vdash \mathsf{tl}^{\mathsf{g}}\ s : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}(\mathsf{Str}\,A) \,\middle|\, \Diamond^{k}\Box[\mathsf{hd}][\mathsf{bx}]\Box[\varphi]\right\}}}{\Gamma'' \vdash f \circledast \mathsf{next}(g \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s) : \blacktriangleright \left\{\mathsf{Str}^{\mathsf{g}}\,A \,\middle|\, \Diamond^{k}\Box[\varphi]\right\}}$$

$$\Gamma'' \vdash (\mathsf{hd} \circ g)(\mathsf{hd}^{\mathsf{g}}\ s) ::^{\mathsf{g}} (f \circledast \mathsf{next}(g \circ \mathsf{tl}) \circledast (\mathsf{tl}^{\mathsf{g}}\ s)) : \left\{\mathsf{Str}^{\mathsf{g}}\,A \,\middle|\, \bigcirc\Diamond^{k}\Box[\varphi]\right\}$$

□

E Proofs of Section 7

E.1 Correctness of the External and Internal Semantics

E.1.1 Proof of Lem. C.13.(1) (Lem. 7.3.(1))

Lemma E.1. *If* $\vdash_c^A \varphi$ *then* $\wr\varphi\wr = \Gamma[\![A]\!]$.

Lemma C.19 gives almost all the axioms and rules of Table 1 and Fig. 6, but for the $[\mathsf{ev}(-)]$ modality that we treat separately. We first treat the axioms of Table 1.

Lemma E.2. *If* $\varphi : A$ *is an axiom of Table 1, then* $\wr\varphi\wr^A = [\![A]\!]$.

Proof. Most of the axioms follow from Lem. C.19. Following Def. 5.6, we include the axioms marked **(C)** in Table 1. The cases of [bx] are trivial and omitted.

Case of (C)**.** Since in each case, the map $\wr[\triangle]\wr$ preserves $\wedge$.
The case of $[\mathsf{ev}(-)]$ is treated directly:

$$\vdash^{B\to A} ([\mathsf{ev}(\phi)]\psi \wedge [\mathsf{ev}(\phi)]\varphi) \implies [\mathsf{ev}(\phi)](\psi \wedge \varphi)$$

Let $x \in \Gamma[\![B \to A]\!]$ and assume that $x \in \wr[\mathsf{ev}(\phi)]\psi\wr \cap \wr[\mathsf{ev}(\phi)]\varphi\wr$. Let now $y \in \Gamma[\![B]\!]$ such that $y \in \wr\phi\wr$. We then have $\mathsf{ev} \circ \langle x, y\rangle \in \wr\psi\wr \cap \wr\varphi\wr$.

Case of (N)**.** Since $\wr[\pi_i]\wr$, $\wr[\mathsf{next}]\wr$ and $\wr[\mathsf{fd}]\wr$ are maps of Heyting algebras.
The case of $[\mathsf{ev}(-)]$ is treated directly:

$$\vdash^{B\to A} [\mathsf{ev}(\phi)]\top$$

Let $x \in \Gamma[\![B \to A]\!]$. Given $y \in \Gamma[\![B]\!]$ such that $y \in \wr\phi\wr$, we have $\mathsf{ev} \circ \langle x, y\rangle \in \Gamma[\![A]\!] = \wr\top\wr$.

Case of (P)**.** Since $\wr[\pi_i]\wr$, $\wr[\mathsf{next}]\wr$ and $\wr[\mathsf{fd}]\wr$ are maps of Heyting algebras. As for $[\mathsf{in}_i]$, this follows from Lem. C.19.

Case of ($\mathsf{C}_\vee$)**.** By Lem. C.19.

Case of ($\mathsf{C}_\Rightarrow$)**.** Since $\wr[\pi_i]\wr$, $\wr[\mathsf{next}]\wr$ and $\wr[\mathsf{fd}]\wr$ are maps of Heyting algebras. □

In order to handle fixpoints, we have the usual monotonicity lemma w.r.t. set inclusion.

Lemma E.3. *Consider, for a formula* $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi$*, the map*

$$\wr\varphi\wr \quad : \quad \mathcal{P}(\Gamma[\![A_1]\!]) \times \cdots \times \mathcal{P}(\Gamma[\![A_k]\!]) \quad \longrightarrow \quad \mathcal{P}(\Gamma[\![A]\!]), \quad v \longmapsto \wr\varphi\wr_v$$

For $i \in \{1, \dots, k\}$*, if* α_i Pos φ *(resp.* α_i Neg φ*), then w.r.t. set inclusion,* $\wr\varphi\wr$ *is monotone (resp. anti-monotone) in its* i*th argument.*

We can now turn to the proof of Lemma E.1.

Proof of Lemma E.1. By induction on $\vdash^A \varphi$. The rules of intuitionistic propositional logic (Fig. 11) 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. C.19, this holds for $[\pi_i]$, [next] and [fd] since $\wr[\pi_i]\wr$, $\wr[\mathsf{next}]\wr$ and $\wr[\mathsf{fd}]\wr$ are maps of Heyting algebras. As for $[\mathsf{in}_i]$, this follows from the fact that $\wr[\mathsf{in}_i]\wr$ 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 $x \in \Gamma[\![B \to A]\!]$. Given $y \in \Gamma[\![B]\!]$ such that $y \in \wr\phi\wr$, we have $\mathsf{ev} \circ \langle x, y\rangle \in \wr\psi\wr$, so that $\mathsf{ev} \circ \langle x, y\rangle \in \wr\varphi\wr$ since $\wr\psi\wr \subseteq \wr\varphi\wr$.

Case of

$$\frac{\vdash_c^A \varphi}{\vdash^{\blacksquare A} [\mathsf{bx}]\varphi}$$

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 $x \in \Gamma[\![B \to A]\!]$ and assume that $x \in \wr[\mathsf{ev}(\phi)]\varphi\wr$. Let furthermore $y \in \Gamma[\![B]\!]$ such that $y \in \wr\psi\wr$. We have to show $\mathsf{ev} \circ \langle x, y\rangle \in \wr\varphi\wr$. By induction hypothesis we have $y \in \wr\psi \Rightarrow \phi\wr$, so that $y \in \wr\phi\wr$. But this implies $\mathsf{ev} \circ \langle x, y\rangle \in \wr\varphi\wr$ since $x \in \wr[\mathsf{ev}(\phi)]\varphi\wr$.

Case of

$$\overline{\vdash^{A_0+A_1} \left([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\right) \wedge \neg\left([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\right)}$$

Consider $x \in \Gamma[\![A_0 + A_1]\!] \simeq \Gamma[\![A_0]\!] + \Gamma[\![A_1]\!]$ (via Lem. C.2). Hence $x = \mathsf{in}_i(y)$ for some $y \in \Gamma[\![A_i]\!]$ and we have $x \in \wr[\mathsf{in}_i]\top\wr$. Moreover, since the injections in_0 and in_1 have disjoint images, we have $\wr[\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\wr = \emptyset$ so $x \in \wr\neg([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top)\wr$.

Case of

$$\overline{\vdash^{A_0+A_1} [\mathsf{in}_i]\top \;\Rightarrow\; (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)}$$

Let $x \in \Gamma[\![A_0 + A_1]\!] \simeq \Gamma[\![A_0]\!] + \Gamma[\![A_1]\!]$, and assume $x \in \wr[\mathsf{in}_i]\top\wr$, so that $x = \mathsf{in}_i(y)$ for some (unique) $y \in \Gamma[\![A_i]\!]$. We show

$$x \in \wr\neg[\mathsf{in}_i]\varphi \;\Rightarrow\; [\mathsf{in}_i]\neg\varphi\wr \qquad \text{and} \qquad x \in \wr[\mathsf{in}_i]\neg\varphi \;\Rightarrow\; \neg[\mathsf{in}_i]\varphi\wr$$

For the former, assume $x \notin \wr[\mathsf{in}_i]\varphi\wr$. Since y is unique such that $x = \mathsf{in}_i(y)$, we have $y \notin \wr\varphi\wr$. But this implies $y \in \wr\neg\varphi\wr$ and we are done.

For the latter, assume $x \in \wr[\mathsf{in}_i]\neg\varphi\wr$. Assume toward a contradiction that $x \in \wr[\mathsf{in}_i]\varphi\wr$. Since y is unique such that $x = \mathsf{in}_i(y)$, we have both $y \notin \wr\varphi\wr$ and $y \in \wr\varphi\wr$, a contradiction.

Cases of

$$\overline{\vdash^A \nu\alpha^0\varphi \;\Leftrightarrow\; \top} \qquad \overline{\vdash^A \nu\alpha^{\mathsf{t}+1}\varphi \;\Leftrightarrow\; \varphi[\nu\alpha^{\mathsf{t}}\varphi/\alpha]} \qquad \overline{\vdash^A \mu\alpha^0\varphi \;\Leftrightarrow\; \bot} \qquad \overline{\vdash^A \mu\alpha^{\mathsf{t}+1}\varphi \;\Leftrightarrow\; \varphi[\mu\alpha^{\mathsf{t}}\varphi/\alpha]}$$

By definition of $\wr\theta\alpha^{\mathsf{t}}\varphi\wr$.

Cases of

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

These cases follows from Lem. E.3 (in $\theta\alpha^{\mathsf{t}}\varphi$ we assume that α is positive in φ) and the definition of $\wr\theta\alpha^{\mathsf{t}}\varphi\wr$.

Cases of

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

By Lem. E.3 and Knaster-Tarski Theorem. □

E.1.2 Proof of Lem. C.13.(2) (Lem. 7.3.(2))

Lemma E.4. *If* $\vdash^A \varphi$ *then* $[\![\varphi]\!] = [\![A]\!]$.

Corollary C.17 gives almost everything we need for the semantic correctness of the modal theory. We begin with the axioms of Table 1.

Lemma E.5. *If* $\varphi : A$ *is an axiom of Table 1, then* $[\![\varphi]\!]^A = [\![A]\!]$.

Proof. Most of the axioms follow from Cor. C.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 $[\pi_i]$, [fd] and [bx] follows from the fact that $[\![[\pi_i]]\!]$, $[\![[\mathsf{fd}]]\!]$ and $[\![[\mathsf{bx}]]\!]$ are maps of Heyting algebras.

As for $[\mathsf{in}_i]$, it follows from the fact that $[\![[\mathsf{in}_i]]\!]$ preserves $\bot$ (Cor. C.17).

Case of ($\mathrm{C}_\vee$). By Cor. C.17.

Case of ($\mathrm{C}_\Rightarrow$). Since $[\![[\pi_i]]\!]$, $[\![[\mathsf{fd}]]\!]$ and $[\![[\mathsf{bx}]]\!]$ are maps of Heyting algebras. □

In order to handle fixpoints, we have the usual monotonicity property w.r.t. subobject posets.

Lemma E.6. *Consider, for a formula $\alpha_1 : A_1, \dots, \alpha_k : A_k \vdash \varphi$, the map*

$$[\![\varphi]\!] \quad : \quad \mathrm{Sub}([\![A_1]\!]) \times \cdots \times \mathrm{Sub}([\![A_k]\!]) \quad \longrightarrow \quad \mathrm{Sub}([\![A]\!]), \quad v \longmapsto [\![\varphi]\!]_v$$

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 E.4.

Proof of Lemma E.4. By induction on $\vdash^A \varphi$. The rules of Fig. 11 follow from the fact that in a topos, the subobjects of a given object form a Heyting algebra.

Case of

$$(\mathrm{RM})\ \frac{\vdash \psi \Rightarrow \varphi}{\vdash [\triangle]\psi \Rightarrow [\triangle]\varphi}$$

The result holds for $[\pi_i]$, [fd] and [bx] since $[\![[\pi_i]]\!]$, $[\![[\mathsf{fd}]]\!]$ and $[\![[\mathsf{bx}]]\!]$ are maps of Heyting algebras.
As for $[\mathsf{in}_i]$, [next] and [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

$$\frac{\vdash_{\mathrm{c}}^A \varphi}{\vdash^{\blacksquare A} [\mathsf{bx}]\varphi}$$

By Cor. C.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. C.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 $u \Vdash_\ell^B \psi$. We have to show $\mathsf{ev} \circ \langle t{\uparrow}\ell, u\rangle \Vdash_\ell^A \varphi$. By induction hypothesis we have $u \Vdash_\ell^B \psi \Rightarrow \phi$, so that $u \Vdash_\ell^B \phi$. But this implies $\mathsf{ev} \circ \langle t{\uparrow}\ell, u\rangle \Vdash_\ell^A \varphi$ since $t{\uparrow}k \Vdash_k [\mathsf{ev}(\phi)]\varphi$.

Case of

$$\overline{\vdash^{A_0+A_1} \big([\mathsf{in}_0]\top \vee [\mathsf{in}_1]\top\big) \ \wedge\ \neg\big([\mathsf{in}_0]\top \wedge [\mathsf{in}_1]\top\big)}$$

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

$$\overline{\vdash^{A_0+A_1} [\mathsf{in}_i]\top \ \Rightarrow\ (\neg[\mathsf{in}_i]\varphi \Leftrightarrow [\mathsf{in}_i]\neg\varphi)}$$

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

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

By definition of $[\![\theta\alpha^{\mathsf{t}}\varphi]\!]$.

Cases of

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

These cases follows from Lem. E.6 (in $\theta\alpha^{\mathsf{t}}\varphi$ we assume that α is positive in φ) and the definition of $[\![\theta\alpha^{\mathsf{t}}\varphi]\!]$.

Cases of

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

By Lem. E.6 and Knaster-Tarski Theorem, since subobject lattices of $\mathcal{S}$ are complete ([36, Prop. I.8.5]). □

E.2 The Safe Fragment

Lemma E.7 (Lem. 7.5). *The greatest fixpoint of a Scott cocontinuous function $f : L \longrightarrow L$ is given by*

$$\nu(f) \quad := \quad \bigwedge_{n\in\mathbb{N}} f^n(\top)$$

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

$$b \quad := \quad \bigvee \{a \in L \mid a \leq f(a)\}$$

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 E.8 (Lem. 7.6). *Consider a safe formula $\alpha_1 : P_1^+, \ldots, \alpha_k : P_k^+ \vdash \varphi : P^+$. The following two functions are Scott-cocontinuous:*

$$\begin{array}{rcccc} [\![\varphi]\!] & : & \mathrm{Sub}([\![P_1^+]\!]) \times \cdots \times \mathrm{Sub}([\![P_k^+]\!]) & \longrightarrow & \mathrm{Sub}([\![P^+]\!]), \quad v \longmapsto [\![\varphi]\!]_v \\ \wr\varphi\int & : & \mathcal{P}(\Gamma[\![P_1^+]\!]) \times \cdots \times \mathcal{P}(\Gamma[\![P_k^+]\!]) & \longrightarrow & \mathcal{P}(\Gamma[\![P^+]\!]), \quad v \longmapsto \wr\varphi\int_v \end{array}$$

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 $\wr\varphi\int$. We reason by induction on φ.

Cases of α, $\top$, $\bot$.
Trivial.

Case of $\varphi \wedge \psi$.
Let $D_1 \subseteq \mathcal{P}(\Gamma[\![P_1^+]\!]), \ldots, D_k \subseteq \mathcal{P}(\Gamma[\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$\wr\varphi\wedge\psi\int(\bigcap D_1, \ldots, \bigcap D_k) \quad = \quad \bigcap \wr\varphi\int(D_1, \ldots, D_k) \cap \bigcap \wr\psi\int(D_1, \ldots, D_k)$$

and the result is trivial.

Case of $\varphi \vee \psi$.
This is the interesting case. Let $D_1 \subseteq \mathcal{P}(\Gamma[\![P_1^+]\!]), \ldots, D_k \subseteq \mathcal{P}(\Gamma[\![P_k^+]\!])$ be codirected. By induction hypothesis we obtain

$$\wr\varphi\wedge\psi\int(\bigcap D_1, \ldots, \bigcap D_k) \quad = \quad \bigcap \wr\varphi\int(D_1, \ldots, D_k) \cup \bigcap \wr\psi\int(D_1, \ldots, D_k)$$

We then trivially get

$$\bigcap \wr\varphi\int(D_1, \ldots, D_k) \cup \bigcap \wr\psi\int(D_1, \ldots, D_k) \quad \subseteq \quad \bigcap \wr\varphi\vee\psi\int(D_1, \ldots, D_k)$$

It remains to show the converse direction

$$\bigcap \wr\varphi\vee\psi\int(D_1, \ldots, D_k) \quad \subseteq \quad \bigcap \wr\varphi\int(D_1, \ldots, D_k) \cup \bigcap \wr\psi\int(D_1, \ldots, D_k)$$

So let $x \in \Gamma[\![P^+]\!]$ such that $x \in \wr\varphi\vee\psi\int(S_1, \ldots, S_k)$ for every $S_1 \in D_1, \ldots, S_k \in D_k$. Assume toward a contradiction that there are $S_1 \in D_1, \ldots, S_k \in D_k$ such that $x \notin \wr\varphi\int(S_1, \ldots, S_k)$ and that there are $S_1' \in D_1, \ldots, S_k' \in D_k$ such that $x \notin \wr\psi\int(S_1', \ldots, S_k')$. Since the D_i's are codirected for inclusion, there are $S_1'' \in D_1, \ldots, S_k'' \in D_k$ such that $S_i'' \subseteq S_i \cap S_i'$ for $i = 1, \ldots, k$. By monoticity w.r.t. inclusion, we have $x \notin \wr\varphi\int(S_1'', \ldots, S_k'')$ and $x \notin \wr\psi\int(S_1'', \ldots, S_k'')$. But this implies $x \notin \wr\varphi\vee\psi\int(S_1'', \ldots, S_k'')$, a contradiction.

Case of $[\pi_i]\varphi$.
Let $D_1 \subseteq \mathcal{P}(\Gamma[\![P_1^+]\!]), \ldots, D_k \subseteq \mathcal{P}(\Gamma[\![P_k^+]\!])$ be codirected. Let $x \in \Gamma[\![P^+]\!]$ and write $P^+ = Q_0^+ \times Q_1^+$. Then we are done since by induction hypothesis

$$\begin{array}{lll} x \in \wr[\pi_i]\varphi\int(\bigcap D_1, \ldots, \bigcap D_k) & \text{iff} & \pi_i \circ x \in \wr\varphi\int(\bigcap D_1, \ldots, \bigcap D_k) \\ & \text{iff} & \pi_i \circ x \in \bigcap \wr\varphi\int(D_1, \ldots, D_k) \\ & \text{iff} & \forall S_1 \in D_1, \ldots, S_k \in D_k,\ \pi_i \circ x \in \wr\varphi\int(D_1, \ldots, D_k) \\ & \text{iff} & \forall S_1 \in D_1, \ldots, S_k \in D_k,\ x \in \wr[\pi_i]\varphi\int(D_1, \ldots, D_k) \\ & \text{iff} & x \in \bigcap \wr[\pi_i]\varphi\int(D_1, \ldots, D_k) \end{array}$$

Case of $[\mathsf{in}_i]\varphi$**.**
Let $D_1 \subseteq \mathcal{P}(\mathbf{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\mathbf{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \mathbf{\Gamma}[\![P^+]\!]$ and write $P^+ = Q_0^+ + Q_1^+$. By Lem. C.2, we have $x = \mathsf{in}_j \circ y$ for some unique $j \in \{0,1\}$ and $y \in \mathbf{\Gamma}[\![Q_j^+]\!]$. Then we are done since by induction hypothesis we have $x \in \wr[\mathsf{in}_i]\varphi\wr(\bigcap D_1, \dots, \bigcap D_k)$

$$\begin{array}{ll}
\text{iff } j = i \text{ and} & y \in \wr\varphi\wr(\bigcap D_1, \dots, \bigcap D_k) \\
\text{iff } j = i \text{ and} & y \in \bigcap \wr\varphi\wr(D_1, \dots, D_k) \\
\text{iff } j = i \text{ and} & \forall S_1 \in D_1, \dots, S_k \in D_k,\ y \in \wr\varphi\wr(D_1, \dots, D_k) \\
\text{iff} & \forall S_1 \in D_1, \dots, S_k \in D_k,\ x \in \wr[\mathsf{in}_i]\varphi\wr(D_1, \dots, D_k) \\
\text{iff} & x \in \bigcap \wr[\mathsf{in}_i]\varphi\wr(D_1, \dots, D_k)
\end{array}$$

Case of $[\mathsf{next}]\varphi$**.**
Let $D_1 \subseteq \mathcal{P}(\mathbf{\Gamma}[\![P_1^+]\!]), \dots, D_k \subseteq \mathcal{P}(\mathbf{\Gamma}[\![P_k^+]\!])$ be codirected. Let $x \in \mathbf{\Gamma}[\![P^+]\!]$ and write $P^+ = \blacktriangleright Q^+$. By Lem. C.2, we have $x = \mathsf{next} \circ y$ for some unique $y \in \mathbf{\Gamma}[\![Q^+]\!]$. Then we are done since by induction hypothesis we have

$$\begin{array}{lll}
x \in \wr[\mathsf{next}]\varphi\wr(\bigcap D_1, \dots, \bigcap D_k) & \text{iff} & y \in \wr\varphi\wr(\bigcap D_1, \dots, \bigcap D_k) \\
& \text{iff} & y \in \bigcap \wr\varphi\wr(D_1, \dots, D_k) \\
& \text{iff} & \forall S_1 \in D_1, \dots, S_k \in D_k,\ y \in \wr\varphi\wr(D_1, \dots, D_k) \\
& \text{iff} & \forall S_1 \in D_1, \dots, S_k \in D_k,\ x \in \wr[\mathsf{next}]\varphi\wr(D_1, \dots, D_k) \\
& \text{iff} & x \in \bigcap \wr[\mathsf{next}]\varphi\wr(D_1, \dots, D_k)
\end{array}$$

Case of $[\mathsf{fd}]\varphi$**.**
This case is dealt-with similarly as that of $[\pi_i]$.
Case of $[\mathsf{bx}]\varphi$**.**
Trivial since φ is required to be closed.
Case of $[\mathsf{ev}(\psi)]\varphi$**.**
Trivial since ψ and φ are required to be closed.
Cases of $\theta\alpha^{\mathsf{t}}\varphi$ **and** $\theta\alpha^{\omega}\varphi$**.**
Trivial since φ is required to have at most α as free variable.

We now turn to the case of $[\![\varphi]\!]$. Most of cases are similar to those for $\wr\varphi\wr$. Also, note that

$$[\![\varphi]\!] \ : \ \mathrm{Sub}([\![P_1^+]\!]) \times \cdots \times \mathrm{Sub}([\![P_k^+]\!]) \longrightarrow \mathrm{Sub}([\![P^+]\!])$$

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

$$[\![\varphi]\!]\Big(\bigwedge D_1, \dots, \bigwedge D_k\Big) \quad = \quad \bigwedge [\![\varphi]\!](D_1, \dots, D_k)$$

But since meets in subobject lattices of $\mathcal{S}$ are pointwise, the above is equivalent to have, for all $n > 0$ that

$$[\![\varphi]\!]\Big(\bigwedge D_1, \dots, \bigwedge D_k\Big)(n) \quad = \quad \bigcap [\![\varphi]\!](D_1, \dots, D_k)(n)$$

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

$$[\![\varphi \wedge \psi]\!]\Big(\bigwedge D_1, \dots, \bigwedge D_k\Big) \quad = \quad \bigwedge [\![\varphi]\!](D_1, \dots, D_k) \ \wedge \ \bigwedge [\![\psi]\!](D_1, \dots, D_k)$$

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

$$[\![\varphi \wedge \psi]\!]\Big(\bigwedge D_1, \dots, \bigwedge D_k\Big) \quad = \quad \bigwedge [\![\varphi]\!](D_1, \dots, D_k) \ \vee \ \bigwedge [\![\psi]\!](D_1, \dots, D_k)$$

By monotonicity w.r.t. subobject lattice orders, we trivially get

$$\bigwedge [\![\varphi]\!](D_1, \dots, D_k) \ \vee \ \bigwedge [\![\psi]\!](D_1, \dots, D_k) \quad \subseteq \quad \bigwedge [\![\varphi \vee \psi]\!](D_1, \dots, D_k)$$

It remains to show the converse direction

$$\bigwedge [\![\varphi \vee \psi]\!](D_1, \dots, D_k) \quad \subseteq \quad \bigwedge [\![\varphi]\!](D_1, \dots, D_k) \ \vee \ \bigwedge [\![\psi]\!](D_1, \dots, D_k)$$

Since meets and joins are computed pointwise in subobject lattices, we are done if for each $n > 0$ we show

$$\bigcap [\![\varphi \vee \psi]\!](D_1, \ldots, D_k)(n) \quad \subseteq \quad \bigcap [\![\varphi]\!](D_1, \ldots, D_k)(n) \cup \bigcap [\![\psi]\!](D_1, \ldots, D_k)(n)$$

We can then conclude as in the case of $\wr - \wr$. Fix $n > 0$ and let $t \in [\![P^+]\!]$ such that $t \in [\![\varphi \vee \psi]\!](A_1, \ldots, A_k)(n)$ for every $A_1 \in D_1, \ldots, A_k \in D_k$. Assume toward a contradiction that there are $A_1 \in D_1, \ldots, A_k \in D_k$ such that $t \notin [\![\varphi]\!](A_1, \ldots, A_k)(n)$ and that there are $A'_1 \in D_1, \ldots, A'_k \in D_k$ such that $t \notin [\![\psi]\!](A'_1, \ldots, A'_k)(n)$. Since the D_i's are codirected for inclusion, there are $A''_1 \in D_1, \ldots, A''_k \in D_k$ such that $A''_i \leq A_i \wedge A'_1$ for $i = 1, \ldots, k$. By monoticity w.r.t. subobject lattice orders, we have $t \notin [\![\varphi]\!](A''_1, \ldots, A''_k)(n)$ and $t \notin [\![\psi]\!](A''_1, \ldots, A''_k)(n)$. But this implies $t \notin [\![\varphi \vee \psi]\!](A''_1, \ldots, A''_k)(n)$, a contradiction.

Case of $[\pi_i]\varphi$.

Let $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \ldots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. We show that for all $n > 0$ we have

$$[\![[\pi_i]\varphi]\!](\bigwedge D_1, \ldots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\pi_i]\varphi]\!](D_1, \ldots, D_k)(n)$$

and this goes similarly as for $\wr - \wr$.

Case of $[\mathsf{in}_i]\varphi$.

Let $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \ldots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. We show that for all $n > 0$ we have

$$[\![[\mathsf{in}_i]\varphi]\!](\bigwedge D_1, \ldots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\mathsf{in}_i]\varphi]\!](D_1, \ldots, D_k)(n)$$

and this goes similarly as for $\wr - \wr$ 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 $D_1 \subseteq \mathrm{Sub}([\![P^+_1]\!]), \ldots, D_k \subseteq \mathrm{Sub}([\![P^+_k]\!])$ be codirected. Write $P^+ = \blacktriangleright Q^+$. We show that for all $n > 0$ we have

$$[\![[\mathsf{next}]\varphi]\!](\bigwedge D_1, \ldots, \bigwedge D_k)(n) \quad = \quad \bigcap [\![[\mathsf{next}]\varphi]\!](D_1, \ldots, D_k)(n)$$

The result is trivial if $n = 1$. For $n > 1$, it reduces to

$$[\![\varphi]\!](\bigwedge D_1, \ldots, \bigwedge D_k)(n-1) \quad = \quad \bigcap [\![\varphi]\!](D_1, \ldots, D_k)(n-1)$$

which follows from the induction hypothesis.

Case of $[\mathsf{fd}]\varphi$.

This case is handled similarly as that of $[\pi_i]$.

Case of $[\mathsf{bx}]\varphi$.

Trivial since φ is required to be closed.

Case of $[\mathsf{ev}(\psi)]\varphi$.

Trivial since ψ and φ are required to be closed.

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

Trivial since φ is required to have at most α as free variable. □

Proposition E.9 (Prop. 7.7)**.** *Let $\alpha_1 : P^+_1, \ldots, \alpha_k : P^+_k \vdash \varphi : P^+$ be a safe formula. Given $S_1 \in \mathrm{Sub}([\![P^+_1]\!]), \ldots, S_k \in \mathrm{Sub}([\![P^+_k]\!])$, we have*

$$\wr \varphi \wr(\Gamma(S_1), \ldots, \Gamma(S_k)) \quad = \quad \Gamma\big([\![\varphi]\!](S_1, \ldots, S_k)\big)$$

Proof. We reason by induction on the derivation of $\alpha_1 : P^+_1, \ldots, \alpha_k : P^+_k \vdash \varphi : P^+$. In all cases but $\nu\alpha^{\omega}\varphi$, the parameters are irrelevant and we omit them.

Cases of α, $\top$ and $\bot$.

Trivial.

Case of $\varphi \wedge \psi$.

Let $x \in \Gamma[\![P^+]\!]$. Then we are done since by induction hypothesis we have

$$\begin{array}{lll} x \in \wr \varphi \wedge \psi \wr & \text{iff} & x \in \wr \varphi \wr \text{ and } x \in \wr \psi \wr \\ & \text{iff} & (\forall n > 0,\ x_n(\bullet) \in [\![\varphi]\!](n)) \text{ and } (\forall n > 0,\ x_n(\bullet) \in [\![\psi]\!](n)) \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in [\![\varphi]\!](n) \text{ and } x_n(\bullet) \in [\![\psi]\!](n) \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in [\![\varphi \wedge \psi]\!](n) \end{array}$$

Case of $\varphi \vee \psi$.

Let $x \in \Gamma[\![P^+]\!]$. Assume first that $x \in \wr \varphi \vee \psi \wr$. If (say) $x \in \wr \varphi \wr$, then by induction hypothesis we get $x_n(\bullet) \in [\![\varphi]\!](n)$ for all $n > 0$, which implies $x_n(\bullet) \in [\![\varphi \vee \psi]\!](n)$ for all $n > 0$.

Conversely, assume that $x_n(\bullet) \in [\![\varphi \vee \psi]\!](n)$ for all $n > 0$. Assume toward a contradiction that there are $k, \ell > 0$ with (say) $k \leq \ell$ such that $x_k(\bullet) \notin [\![\varphi]\!](n)$ and $x_\ell(\bullet) \notin [\![\psi]\!](n)$. Since $k \leq \ell$, by Lem. C.16 we have $x_k(\bullet) \notin [\![\psi]\!](n)$, but this

contradicts $x_k(\bullet) \in [\![\varphi \vee \psi]\!](n)$. Hence, we have either $x_n(\bullet) \in [\![\varphi]\!](n)$ for all $n > 0$ or $x_n(\bullet) \in [\![\psi]\!](n)$ 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 $x \in \Gamma[\![P^+]\!]$ 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

$$\begin{array}{rll} x \in \wr[\pi_i]\varphi\wr & \text{iff} & \pi_i \circ x \in \wr\varphi\wr \\ & \text{iff} & \forall n > 0,\ (\pi_i \circ x)_n(\bullet) \in [\![\varphi]\!](n) \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in [\![[\pi_i]\varphi]\!](n) \end{array}$$

Case of $[\mathsf{in}_i]\varphi$.

Let $x \in \Gamma[\![P^+]\!]$ and write $P^+ = Q_0^+ + Q_1^+$. By Lem. C.2, we have $x = \mathsf{in}_j \circ y$ for some unique $j \in \{0,1\}$ and $y \in \Gamma[\![Q_j^+]\!]$. 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

$$\begin{array}{rlll} x \in \wr[\mathsf{in}_i]\varphi\wr & \text{iff } j = i \text{ and} & y \in \wr\varphi\wr \\ & \text{iff } j = i \text{ and} & \forall n > 0,\ y_n(\bullet) \in [\![\varphi]\!](n) \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in [\![[\mathsf{in}_i]\varphi]\!](n) \end{array}$$

Case of $[\mathsf{next}]\varphi$.

Let $x \in \Gamma[\![P^+]\!]$ and write $P^+ = \blacktriangleright Q^+$. By Lem. C.2, we have $x = \mathsf{next} \circ y$ for some unique $y \in \Gamma[\![Q^+]\!]$. Assume first $x \in \wr[\mathsf{next}]\varphi\wr$. Hence we have $y \in \wr\varphi\wr$, 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 $y \in \wr\varphi\wr$ so that $x \in \wr[\mathsf{next}]\varphi\wr$.

Case of $[\mathsf{fd}]\varphi$.

This case is handled similarly as that of $[\pi_i]$.

Case of $[\mathsf{bx}]\varphi$.

Recall that φ is required to be closed. Also, by definition we have

$$\begin{array}{rcl} [\![[\mathsf{bx}]\varphi]\!]^{\blacksquare A}(n) & := & \left\{ t \in [\![\blacksquare A]\!](n) = \Gamma[\![A]\!] \;\middle|\; t \in \wr\varphi\wr^A \right\} \\ \wr[\mathsf{bx}]\varphi\wr^{\blacksquare A} & := & \left\{ x \in \Gamma[\![\blacksquare A]\!] \;\middle|\; x_1(\bullet) \in \wr\varphi\wr^A \right\} \end{array}$$

It follows that given $x \in \Gamma[\![\blacksquare A]\!]$, we have

$$\begin{array}{rll} x \in \wr[\mathsf{bx}]\varphi\wr^{\blacksquare A} & \text{iff} & x_1(\bullet) \in \wr\varphi\wr^A \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in \wr\varphi\wr^A \\ & \text{iff} & \forall n > 0,\ x_n(\bullet) \in [\![[\mathsf{bx}]\varphi]\!]^{\blacksquare A}(n) \end{array}$$

Case of $[\mathsf{ev}(\psi)]\varphi$.

This case cannot occur since P^+ is assumed to be positive.

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

Assume $\alpha : P^+ \vdash \varphi(\alpha) : P^+$. We show by induction on $m \in \mathbb{N}$ that

$$\wr\varphi^m(\top)\wr = \Gamma[\![\varphi^m(\top)]\!] \qquad \text{and} \qquad \wr\varphi^m(\bot)\wr = \Gamma[\![\varphi^m(\bot)]\!]$$

The base case $m = 0$ is trivial. As for the inductive case we have

$$\begin{array}{rclcrcl} \wr\varphi^{m+1}(\top)\wr & = & \wr\varphi(\varphi^m(\top))\wr & \text{and} & [\![\varphi^{m+1}(\top)]\!] & = & [\![\varphi(\varphi^m(\top))]\!] \\ \wr\varphi^{m+1}(\bot)\wr & = & \wr\varphi(\varphi^m(\bot))\wr & \text{and} & [\![\varphi^{m+1}(\bot)]\!] & = & [\![\varphi(\varphi^m(\bot))]\!] \end{array}$$

By induction hypothesis on m we have

$$\wr\varphi^m(\top)\wr = \Gamma[\![\varphi^m(\top)]\!] \qquad \text{and} \qquad \wr\varphi^m(\bot)\wr = \Gamma[\![\varphi^m(\bot)]\!]$$

and we conclude by induction hypothesis on φ.

Case of $\nu\alpha^{\omega}\varphi$.

Assume $\alpha : P^+ \vdash \varphi : P^+$. Reasoning as above, for all $m \in \mathbb{N}$ we have

$$\wr\varphi^m(\top)\wr = \Gamma[\![\varphi^m(\top)]\!]$$

It then directly follows that for all $x \in \mathbf{\Gamma}[\![P^+]\!]$, we have

$$x \in \bigcap_{m\in\mathbb{N}} \wr \varphi^m(\top) \wr \qquad \text{iff} \qquad \forall n > 0,\ x_n(\bullet) \in \bigcap_{m\in\mathbb{N}} [\![\varphi^m(\top)]\!](n)$$

and we conclude by Lem. E.8 and Lem. E.7. □

E.3 Flat Fixpoints

Lemma E.10 (Lem. 7.8). *Consider, for a flat formula $\alpha : B \vdash \varphi : A$, the function*

$$\wr \varphi \wr \ : \ \mathcal{P}(\mathbf{\Gamma}[\![B]\!]) \longrightarrow \mathcal{P}(\mathbf{\Gamma}[\![A]\!]), \quad S \longmapsto \wr \varphi \wr_{[S/\alpha]}$$

- *If α is positive in φ (i.e. α Pos φ), then $\wr \varphi \wr$ is Scott-continuous as well as Scott-cocontinuous.*
- *If α is negative in φ (i.e. α Neg φ) , then $\wr \varphi \wr$ is (antimonotone and) takes joins of directed sets to meets of codirected sets and takes meets of codirected sets to joins of directed sets.*

Proof. The proof is by induction on formation of formulae $\alpha : B \vdash \varphi : A$. Monotonicity and antimonotonicity follow from Lem. E.3. Note that formulae of the form $\theta\alpha^{\mathsf{t}}\varphi$, $\theta\alpha^{\omega}\varphi$ as well as $[\mathrm{bx}]\varphi$ and $[\mathrm{ev}(\psi)]\varphi$ are necessarily closed, nothing has to be proved for these. Some cases are already handled by Lem. 7.6 (Lem. E.8), and we do not repeat them.

Cases of $\alpha, \top, \bot$.
Trivial.

Case of $\varphi \wedge \psi$ (monotone).
Preservation of codirected meets is trivial (see Lem. 7.6 (Lem. E.8)). As for the preservation of directed joins, assume $\alpha : B \vdash \varphi \wedge \psi : A$, and let $D \subseteq \mathcal{P}(\mathbf{\Gamma}[\![B]\!])$ be directed. Then by induction hypothesis we have

$$\wr \varphi \wedge \psi \wr(\bigcup D) \quad = \quad \bigcup \wr \varphi \wr(D) \cap \bigcup \wr \psi \wr(D) \quad \supseteq \quad \bigcup \wr \varphi \wedge \psi \wr(D)$$

For the converse inclusion, consider some x both in $\bigcup \wr \varphi \wr(D)$ and $\bigcup \wr \psi \wr(D)$. Hence there are $S, S' \in D$ such that $x \in \wr \varphi \wr(S)$ and $x \in \wr \psi \wr(S')$. Now since D is directed and by monotonicity, there is some $S'' \in D$ such that $x \in \wr \varphi \wr(S'') \cap \wr \psi \wr(S'')$.

Case of $\varphi \wedge \psi$ (antimonotone).
Assume $\alpha : B \vdash \varphi \wedge \psi : A$. That $\wr \varphi \wedge \psi \wr$ turns directed joins into codirected meets is trivial (as codirected meets commute over binary meets) and omitted. Let us show that $\wr \varphi \wedge \psi \wr$ turns codirected meets into directed joins. So let $D \subseteq \mathcal{P}(\mathbf{\Gamma}[\![B]\!])$ be codirected. Then by induction hypothesis we have

$$\wr \varphi \wedge \psi \wr(\bigcap D) \quad = \quad \bigcup \wr \varphi \wr(D) \cap \bigcup \wr \psi \wr(D) \quad \supseteq \quad \bigcup \wr \varphi \wedge \psi \wr(D)$$

We then conclude as for preservation of directed joins in the monotone case. Given x both in $\bigcup \wr \varphi \wr(D)$ and $\bigcup \wr \psi \wr(D)$, there are $S, S' \in D$ such that $x \in \wr \varphi \wr(S)$ and $x \in \wr \psi \wr(S')$. Now since D is codirected there is some $S'' \in D$ such that $S'' \subseteq S \cap S'$, and by antimonotonicity we have $x \in \wr \varphi \wr(S'') \cap \wr \psi \wr(S'')$.

Case of $\varphi \vee \psi$ (monotone).
Preservation of codirected meets is handled in Lem. 7.6 (Lem. E.8) while preservation of directed join is trivial.

Case of $\varphi \vee \psi$ (antimonotone).
Assume $\alpha : B \vdash \varphi \wedge \psi : A$. That $\wr \varphi \vee \psi \wr$ turns codirected meets into directed joins is trivial (as directed joins commute over binary joins) and omitted. Let us show that $\wr \varphi \vee \psi \wr$ turns directed joins into codirected meets. So let $D \subseteq \mathcal{P}(\mathbf{\Gamma}[\![B]\!])$ be directed. By induction hypothesis we have

$$\wr \varphi \vee \psi \wr(\bigcup D) \quad = \quad \bigcap \wr \varphi \wr(D) \cup \bigcap \wr \psi \wr(D) \quad \subseteq \quad \bigcap \wr \varphi \vee \psi \wr(D)$$

We can then conclude similarly as in Lem. 7.6 (Lem. E.8). Let $x \in \bigcap \wr \varphi \vee \psi \wr(D)$ and assume toward a contradiction that there are $S, S' \in D$ such that $x \notin \wr \varphi \wr(S)$ and $x \notin \wr \psi \wr(S')$. Then since D is directed, there is some $S'' \in D$ such that $S \cup S' \subseteq S''$, and by antimonotonicty we get $x \notin \wr \varphi \vee \psi \wr(S'')$, a contradiction.

Case of $\psi \Rightarrow \varphi$.
With the classical semantics, the interpretation of $\Rightarrow$ can be decomposed into $\vee$ and $\neg$, where $\wr \neg\varphi \wr$ is the complement of $\wr \varphi \wr$ (at the appropriate type). Let α be positive in φ and negative in ψ, with $\alpha : B \vdash \varphi, \psi : A$, and let furthermore by D

and D' (of the appropriate type) be resp. directed and codirected. We then trivially have

$$\begin{array}{rcl} \wr\neg\varphi\S(\bigcup D) & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\varphi\S(\bigcup D) \\ & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \bigcup \wr\varphi\S(D) \\ & = & \bigcap (\mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\varphi\S(D)) \end{array} \qquad \begin{array}{rcl} \wr\neg\varphi\S(\bigcap D') & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\varphi\S(\bigcap D') \\ & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \bigcap \wr\varphi\S(D') \\ & = & \bigcup (\mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\varphi\S(D')) \end{array}$$

$$\begin{array}{rcl} \wr\neg\psi\S(\bigcup D) & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\psi\S(\bigcup D) \\ & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \bigcap \wr\psi\S(D) \\ & = & \bigcup (\mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\psi\S(D)) \end{array} \qquad \begin{array}{rcl} \wr\neg\psi\S(\bigcap D') & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\psi\S(\bigcap D') \\ & = & \mathcal{P}(\Gamma[\![A]\!]) \setminus \bigcup \wr\psi\S(D') \\ & = & \bigcap (\mathcal{P}(\Gamma[\![A]\!]) \setminus \wr\psi\S(D')) \end{array}$$

Cases of $[\pi_i]\varphi$, $[\mathsf{in}_i]\varphi$, $[\mathsf{next}]\varphi$ and $[\mathsf{fd}]\varphi$.
These modalities are handled similarly as in Lem. 7.6 (Lem. E.8).

□

E.4 Realizability

Lemma E.11 (Monotonicity of Realizability (Lem. C.22)). *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 refined 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 $y \in \Gamma[\![|T_i|]\!]$ 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 $y \in \Gamma[\![|U|]\!]$ 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 $y \in \Gamma[\![T]\!]$ 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 $\mathsf{ufd} \circ x \Vdash_n A[\mathsf{Fix}(X).A/X]$, so that $\mathsf{ufd} \circ x \Vdash_k A[\mathsf{Fix}(X).A/X]$ by induction hypothesis and thus $x \Vdash_k \mathsf{Fix}(X).A$.

Case of $\blacksquare T$.
Trivial. □

Lemma E.12 (Lem. C.23). *For a pure type A and $x \in \Gamma[\![A]\!]$, we have $x \Vdash_n A$ for all $n > 0$.*

Proof. The proof is by induction on pairs (n, A), using implicitly Lem. C.2 whenever required.

Case of 1.
Trivial.

Case of $A_0 + A_1$.
Given $x \in \Gamma[\![A_0 + A_1]\!] \simeq \Gamma[\![A_0]\!] + \Gamma[\![A_1]\!]$, we have $x = \mathsf{in}_i \circ y$ for some $y \in \Gamma[\![A_i]\!]$. Then we are done since $y \Vdash_n A_i$ by induction hypothesis.

Case of $A_0 \times A_1$.
Given $x \in \Gamma[\![A_0 \times A_1]\!] \simeq \Gamma[\![A_0]\!] \times \Gamma[\![A_1]\!]$, 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 $x \in \Gamma[\![B \to A]\!]$. Given $y \in \Gamma[\![B]\!]$ 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 $x \in \mathbf{\Gamma}[\![\blacktriangleright A]\!]$, we have $x = \mathrm{next} \circ y$ for some $y \in \mathbf{\Gamma}[\![A]\!]$. But then $y \Vdash_{n-1} A$ by induction hypothesis, so that $x \Vdash_n \blacktriangleright A$.
Case of $\mathsf{Fix}(X).A$**.**
Let $x \in \mathbf{\Gamma}[\![\mathsf{Fix}(X).A]\!]$. It follows by induction on A from the induction hypothesis on n and the guardedness of X in A that $\mathrm{ufd} \circ x \Vdash_n A[\mathsf{Fix}(X).A/X]$, and we are done.
Case of $\blacksquare T$**.**
Let $x \in \mathbf{\Gamma}[\![\blacksquare T]\!]$. Given $n > 0$, we have $x_n(\bullet) \in \mathbf{\Gamma}[\![T]\!]$, so that $x_n(\bullet) \Vdash_m T$ for all $m > 0$ by induction hypothesis. But this implies $x \Vdash_n \blacksquare T$. □

Lemma E.13 (Correctness of Subtyping (Lem. C.25))**.** *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 $x : \mathbf{1} \to_{\mathcal{S}} \mathbf{\Delta\Gamma}[\![U]\!]$ 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. C.23.
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. E.4 (Lem. C.13.(2)).
Case of

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

Let $x \in \mathbf{\Gamma}[\![B \to A]\!]$ and $n > 0$. Assume $x \Vdash_n \{B \to A \mid [\mathrm{ev}(\psi)]\varphi\}$, that is $x_n(\bullet) \in [\![[\mathrm{ev}(\psi)]\varphi]\!](n)$. Let further $y \in \mathbf{\Gamma}[\![B]\!]$ and $k \leq n$ such that $y \Vdash_k \{B \mid \psi\}$, that is $y_k(\bullet) \in [\![\psi]\!](k)$. Then by monotonictiy of $[\![-]\!]$ (Lem. C.16) we have $x_k(\bullet) \in [\![[\mathrm{ev}(\psi)]\varphi]\!](k)$, from which it follows that $(x_k(\bullet))(y_k(\bullet)) \in [\![\varphi]\!](k)$. But this means $\mathrm{ev} \circ \langle x, y\rangle \Vdash_k \{A \mid \varphi\}$ and we are done.
Case of

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

Let $x \in \mathbf{\Gamma}[\![B]\!] \to A$ 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. C.24 ([13, Cor. 3.8]) there is some $y \in \mathbf{\Gamma}[\![B]\!]$ such that $y_k(\bullet) = u$. We thus have $y \Vdash_k \{B \mid \psi\}$, and it follows that $\mathrm{ev} \circ \langle x, y\rangle \Vdash_k \{A \mid \varphi\}$, that is $x_k(\bullet)(y_k(\bullet)) \in [\![\varphi]\!](k)$, and we are done.

Case of

$$\frac{}{\blacktriangleright\{A \mid \varphi\} \equiv \{\blacktriangleright A \mid [\mathsf{next}]\varphi\}}$$

Let $x \in \mathbf{\Gamma}[\![\blacktriangleright A]\!]$. 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. C.2 we have $x = \mathsf{next} \circ y$ for some $y \in \mathbf{\Gamma}[\![A]\!]$. Since $x_n(\bullet) = y_{n-1}(\bullet)$, we have

$$\begin{array}{lll} x \Vdash_n \blacktriangleright\{A \mid \varphi\} & \text{iff} & y \Vdash_{n-1} \{A \mid \varphi\} \\ & \text{iff} & y_{n-1}(\bullet) \in [\![\varphi]\!]^A(n-1) \\ & \text{iff} & x_n(\bullet) = y_{n-1}(\bullet) \in [\![[\mathsf{next}]\varphi]\!]^{\blacktriangleright A}(n) \\ & \text{iff} & x \Vdash_n \{\blacktriangleright A \mid [\mathsf{next}]\varphi\}\,. \end{array}$$

Case of

$$\frac{}{\forall k \cdot \blacktriangleright T \equiv \blacktriangleright \forall k \cdot T}$$

Let $x \in \mathbf{\Gamma}[\![\blacktriangleright |T|]\!]$.
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. C.2, there some unique $y \in \mathbf{\Gamma}[\![|T|]\!]$ 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. C.2 let $y \in \mathbf{\Gamma}[\![|T|]\!]$ 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

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

Let $x : \mathbf{1} \to_{\mathcal{S}} \mathbf{\Delta\Gamma}[\![A]\!]$. Since φ is safe we have $\wr\varphi\wr^A = [\![\varphi]\!]^A]$ by Prop. E.9 (Prop. 7.7). Then we are done since:

$$\begin{array}{lll} x \Vdash_n \blacksquare\{A \mid \varphi\} & \text{iff} & x_n(\bullet) \Vdash_m \{A \mid \varphi\} \text{ for all } m > 0 \\ & \text{iff} & (x_n(\bullet))_m(\bullet) \in [\![\varphi]\!]^A(m) \text{ for all } m > 0 \\ & \text{iff} & x_n(\bullet) \in \wr\varphi\wr^A \\ & \text{iff} & x_n(\bullet) \in [\![[\mathsf{bx}]\varphi]\!]^{\blacksquare A}(n) \\ & \text{iff} & x \Vdash_n \{\blacksquare A \mid [\mathsf{bx}]\varphi\} \end{array}$$

Case of

$$\frac{\vdash_{\mathsf{c}}^A \varphi \Rightarrow \psi}{\{\blacksquare A \mid [\mathsf{bx}]\varphi\} \leq \{\blacksquare A \mid [\mathsf{bx}]\psi\}}$$

By Lem. E.1 (Lem. C.13.(1)). □

Theorem E.14 (Adequacy (Thm. C.26))**.** *Let Γ, T have free iteration variables among $\overline{\ell}$, and let $\overline{m} \in \mathbb{N}$. If $\Gamma \vdash M : T$ and $\rho \models \Gamma$, then*

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

Proof. The proof is by induction on typing derivations. We implicitely use Lem. C.2 whenever required. We omit iteration variables when possible.

Case of

$$\frac{\Gamma, x : \blacktriangleright T \vdash M : T}{\Gamma \vdash \mathsf{fix}(x).M : T}$$

Let $\rho \models \Gamma$ and write $y := [\![\mathsf{fix}(x).M]\!]_\rho \in \mathbf{\Gamma}[\![T]\!]$. Note that

$$y \;=\; [\![M[\mathsf{next}(\mathsf{fix}(x).M)/x]]\!]_\rho \;=\; [\![M]\!]_{\rho[\mathsf{next}\circ y/x]}$$

We show by induction on $n > 0$ that $\rho \Vdash_n \Gamma$ implies $y \Vdash_n T$. In the base case $n = 1$, since $\mathsf{next} \circ y \Vdash_1 \blacktriangleright T$, we have $\rho[\mathsf{next} \circ y/x] \Vdash_1 \Gamma, x : \blacktriangleright T$, 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 $\rho \Vdash_{n+1} \Gamma$. By Monotonicity of Realizability (Lem. E.11), we have $\rho \Vdash_n \Gamma$, 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 $\rho[\mathsf{next} \circ y/x] \Vdash_{n+1} \Gamma, x : \blacktriangleright T$ and the induction hypothesis on typing derivations gives $y = [\![M]\!]_{\rho[\mathsf{next}\circ y/x]} \Vdash_{n+1} T$.

Case of

$$\frac{\Gamma \vdash M : T}{\Gamma \vdash \mathsf{next}(M) : \blacktriangleright T}$$

Let $\rho \models \Gamma$ and write $x := [\![\mathsf{next}(M)]\!]_\rho \in \mathbf{\Gamma}[\![\blacktriangleright T]\!]$. 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. E.11), we have $\rho \Vdash_{n-1} \Gamma$, so that the induction hypothesis on typing derivations gives $y \Vdash_{n-1} T$ and we are done.

Case of

$$\frac{x_1 : T_1, \ldots, x_k : T_k \vdash M : T \qquad \Gamma \vdash M_1 : T_1 \quad \ldots \quad \Gamma \vdash M_k : T_k}{\Gamma \vdash \mathsf{bx}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : \blacksquare T} \ (T_1, \ldots, T_k \text{ constant})$$

Let $\rho \models \Gamma$ and write $x := [\![\mathsf{bx}_\sigma(M)]\!]_\rho$ where $\sigma = [x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$. Let $n > 0$ such that $\rho \Vdash_n \Gamma$. 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

$$x_m(\bullet) \quad : \quad \ell \quad \longmapsto \quad [\![M]\!]_\ell\Big([\![M_1]\!]_m(\rho_m(\bullet)), \ \ldots \ , \ [\![M_k]\!]_m(\rho_m(\bullet))\Big)\Big)$$

For $i = 1, \ldots, k$, since the type T_i is constant, we have by Lem C.21 that $[\![M_i]\!]_m(\rho_m(\bullet)) = [\![M_i]\!]_\ell(\rho_\ell(\bullet))$ for all $\ell > 0$, so that

$$x_m(\bullet) \quad = \quad \ell \longmapsto [\![M]\!]_\ell\Big([\![M_1]\!]_\ell(\rho_\ell(\bullet)), \ \ldots \ , \ [\![M_k]\!]_\ell(\rho_\ell(\bullet))\Big)\Big)$$

Now, by induction hypothesis, since $\rho \Vdash_n \Gamma$ 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 C.21 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

$$\begin{aligned} x_m(\bullet) \quad &= \quad \ell \longmapsto [\![M]\!]_\ell\Big([\![M_1]\!]_\ell(\rho_\ell(\bullet)), \ \ldots \ , \ [\![M_k]\!]_\ell(\rho_\ell(\bullet))\Big)\Big) \\ &= \quad [\![M]\!] \circ \langle [\![M_1]\!]_\rho, \ldots, [\![M_k]\!]_\rho \rangle \end{aligned}$$

Case of

$$\frac{\Gamma \vdash M : \blacksquare T}{\Gamma \vdash \mathsf{ubx}(M) : T}$$

Let $\rho \models \Gamma$ and write $x := [\![\mathsf{ubx}(M)]\!]_\rho$. Let $n > 0$ such that $\rho \Vdash_n \Gamma$. 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

$$\frac{x_1 : T_1, \ldots, x_k : T_k \vdash M : \blacktriangleright T \qquad \Gamma \vdash M_1 : T_1 \quad \ldots \quad \Gamma \vdash M_k : T_k}{\Gamma \vdash \mathsf{prev}_{[x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]}(M) : T} \ (T_1, \ldots, T_k \text{ constant})$$

Let $\rho \models \Gamma$ and write $x := [\![\mathsf{bx}_\sigma(M)]\!]_\rho$ where $\sigma = [x_1 \mapsto M_1, \ldots, x_k \mapsto M_k]$. Let $n > 0$ such that $\rho \Vdash_n \Gamma$. 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

$$x_m(\bullet) \quad = \quad [\![M]\!]_{m+1}\Big([\![M_1]\!]_m(\rho_m(\bullet)), \ \ldots \ , \ [\![M_k]\!]_m(\rho_m(\bullet))\Big)\Big)$$

For $i = 1, \ldots, k$, since the type T_i is constant, we have by Lem C.21 that $[\![M_i]\!]_m(\rho_m(\bullet)) = [\![M_i]\!]_{m+1}(\rho_{m+1}(\bullet))$, so that

$$x_m(\bullet) \quad = \quad [\![M]\!]_{m+1}\Big([\![M_1]\!]_{m+1}(\rho_{m+1}(\bullet)), \ \ldots \ , \ [\![M_k]\!]_{m+1}(\rho_{m+1}(\bullet))\Big)\Big)$$

and it follows that

$$x \quad = \quad \mathsf{next} \circ [\![M]\!] \circ \langle [\![M_1]\!]_\rho, \ldots, [\![M_k]\!]_\rho \rangle$$

Now, by induction hypothesis, since $\rho \Vdash_n \Gamma$ 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 C.21 this implies $[\![M_i]\!]_\rho \Vdash_{n-1} T_i$. By induction hypothesis again, this in turn gives $[\![M]\!] \circ \langle [\![M_1]\!]_\rho, \ldots, [\![M_k]\!]_\rho \rangle \Vdash_{n-1} T$ and we are done.

Case of

$$\frac{\Gamma \vdash M : T \qquad T \leq U}{\Gamma \vdash M : U}$$

By Lem. C.25 (Lem. E.13).

Case of

$$\frac{\Gamma \vdash M : \{A \mid \psi \Rightarrow \varphi\} \qquad \Gamma \vdash M : \{A \mid \psi\}}{\Gamma \vdash M : \{A \mid \varphi\}}$$

Let $\rho \models \Gamma$ and write $x := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A]\!]$. Let $n > 0$ such that $\rho \Vdash_n \Gamma$. 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

$$\frac{\Gamma \vdash M : \{A \mid \varphi_0 \vee \varphi_1\} \qquad \begin{array}{l}\text{for } i \in \{0,1\},\\ \Gamma, x : \{A \mid \varphi_i\} \vdash N : U\end{array}}{\Gamma \vdash N[M/x] : U}$$

Let $\rho \models \Gamma$ and write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A]\!]$ and $z := [\![N]\!]_{\rho[y/x]} \in \mathbf{\Gamma}[\![|U|]\!]$. Let $n > 0$ and assume $\rho \Vdash\!\!\vdash_n \Gamma$. By induction hypothesis we have $y \in [\![\varphi_i]\!]$ for some $i \in \{0,1\}$. It follows that $\rho[y/x] \Vdash\!\!\vdash_n \Gamma, x : \{A \mid \varphi_i\}$, from which we get $z \Vdash\!\!\vdash_n B$ by induction hypothesis.

Case of

$$\frac{\Gamma \vdash M : \{A \mid \bot\} \qquad \Gamma \vdash N : |U|}{\Gamma \vdash N : U}$$

Let $\rho \models \Gamma$ and write $x := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A]\!]$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. By induction hypothesis, the left premise gives $x_n(\bullet) \in [\![\bot]\!](n) = \emptyset$, a contradiction. Hence $\rho \not\Vdash\!\!\vdash_n \Gamma$, and the result follows.

Case of

$$\frac{\Gamma \vdash M_i : \{A_i \mid \varphi\} \qquad \Gamma \vdash M_{1-i} : A_{1-i}}{\Gamma \vdash \langle M_0, M_1\rangle : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}$$

Let $\rho \models \Gamma$. Write $y_0 := [\![M_0]\!]_\rho \in \mathbf{\Gamma}[\![A_0]\!]$, $y_1 := [\![M_1]\!]_\rho \in \mathbf{\Gamma}[\![A_1]\!]$, and $x := [\![\langle M_0, M_1\rangle]\!]_\rho = \langle y_0, y_1\rangle$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. 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

$$\frac{\Gamma \vdash M : \{A_0 \times A_1 \mid [\pi_i]\varphi\}}{\Gamma \vdash \pi_i(M) : \{A_i \mid \varphi\}}$$

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A_0 \times A_1]\!]$ and $x := [\![\pi_i(M)]\!]_\rho = \pi_i \circ y$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. 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

$$\frac{\Gamma \vdash M : \{A_i \mid \varphi\}}{\Gamma \vdash \mathsf{in}_i(M) : \{A_0 + A_1 \mid [\mathsf{in}_i]\varphi\}}$$

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A_i]\!]$, and $x := [\![\mathsf{in}_i(M)]\!]_\rho = \mathsf{in}_i \circ y$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. 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

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

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A_0 + A_1]\!] \simeq \mathbf{\Gamma}[\![A_0]\!] + \mathbf{\Gamma}[\![A_1]\!]$. Hence $y = \mathsf{in}_j \circ z$ for some (unique) $j \in \{0,1\}$ and $z \in \mathbf{\Gamma}[\![A_j]\!]$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. 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 $z \Vdash\!\!\vdash_n \{A_i \mid \varphi\}$. It follows that $\rho[z/x] \Vdash\!\!\vdash_n \Gamma, x : \{A_i \mid \varphi\}$, and the induction hypothesis on typing derivations gives $[\![N_i]\!]_{\rho[z/x]} \Vdash\!\!\vdash_n U$. But then we are done since

$$[\![\mathsf{case}\, M \text{ of } (x.N_0 | x.N_1)]\!]_\rho \;=\; [\![N_i]\!]_{\rho[z/x]}$$

Case of

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

Let $\rho \models \Gamma$. Write $y := [\![\lambda x.M]\!]_\rho \in \mathbf{\Gamma}[\![B \to A]\!]$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. We show $y_n(\bullet) \in [\![[\mathsf{ev}(\psi)]\varphi]\!](n)$. So let $k \leq n$ and $u \in \mathbf{\Gamma}[\![B]\!](k)$ such that $u \in [\![\psi]\!](k)$. By [13, Cor. 3.8] there is some $z \in \mathbf{\Gamma}[\![B]\!]$ such that $z_k(\bullet) = t$. By Monotonicity of Realizability (Lem. E.11), we have $\rho \Vdash\!\!\vdash_k \Gamma$, so that $\rho[z/x] \Vdash\!\!\vdash_k \Gamma, x : \{B \mid \psi\}$. 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

$$\frac{\Gamma \vdash M : \{B \to A \mid [\mathsf{ev}(\psi)]\varphi\} \qquad \Gamma \vdash N : \{B \mid \psi\}}{\Gamma \vdash MN : \{A \mid \varphi\}}$$

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![B \to A]\!]$, $z := [\![N]\!]_\rho \in \mathbf{\Gamma}[\![B]\!]$ and $x := [\![MN]\!]_\rho = \mathsf{ev} \circ \langle y, z\rangle$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. 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

$$\frac{\Gamma \vdash M : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}{\Gamma \vdash \mathsf{fd}(M) : \{\mathsf{Fix}(X).A \mid [\mathsf{fd}]\varphi\}}$$

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![A[\mathsf{Fix}(X).A/X]]\!]$ and $x := [\![\mathsf{fd}(M)]\!]_\rho = \mathsf{fd} \circ y$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. By induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![\varphi]\!]$. But then we are done since $\mathsf{ufd}_n(x_n(\bullet)) = y_n(\bullet)$.

Case of

$$\frac{\Gamma \vdash M : \{\mathsf{Fix}(X).A \mid [\mathsf{fd}]\varphi\}}{\Gamma \vdash \mathsf{ufd}(M) : \{A[\mathsf{Fix}(X).A/X] \mid \varphi\}}$$

Let $\rho \models \Gamma$. Write $y := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![\mathsf{Fix}(X).A]\!]$ and $x := [\![\mathsf{ufd}(M)]\!]_\rho = \mathsf{ufd} \circ y$. Let $n > 0$ such that $\rho \Vdash\!\!\vdash_n \Gamma$. By induction hypothesis on typing derivations we have $y_n(\bullet) \in [\![[\mathsf{fd}]\varphi]\!]$. Hence $\mathsf{ufd}_n(y_n(\bullet)) \in [\![\varphi]\!]$ and we are done since $x_n(\bullet) = \mathsf{ufd}_n(y_n(\bullet))$.

Cases of

$$\frac{\Gamma \vdash M : T[\mathtt{0}/\ell] \qquad \Gamma \vdash M : T[\ell{+}\mathtt{1}/\ell]}{\Gamma \vdash M : \forall \ell \cdot T}\ (\ell \text{ not free in } \Gamma) \qquad \frac{\Gamma \vdash M : T}{\Gamma \vdash M : \forall \ell \cdot T}\ (\ell \text{ not free in } \Gamma)$$

Let $\rho \models \Gamma$ and write $x := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![|T|]\!]$. Let $n > 0$ and assume $\rho \Vdash\!\!\vdash_n \Gamma$. Let $m \in \mathbb{N}$. We have to show $M \Vdash\!\!\vdash_n T[\mathtt{m}/\ell]$. Since ℓ does not occur free in Γ, we have $\rho \Vdash\!\!\vdash_n \Gamma[\mathtt{m}'/\ell]$ for all $m' \in \mathbb{N}$. For both rules we can conclude from the induction hypothesis.

Case of

$$\frac{\Gamma \vdash M : \forall \ell \cdot T}{\Gamma \vdash M : T[\mathtt{t}/\ell]}$$

Let $\rho \models \Gamma$ and write $x := [\![M]\!]_\rho \in \mathbf{\Gamma}[\![|T|]\!]$. Let $n > 0$ and assume $\rho \Vdash\!\!\vdash_n \Gamma$. By induction hypothesis we have $x \Vdash\!\!\vdash_n T[\mathtt{m}/\ell]$ for $m = [\![\mathtt{t}]\!]$ and the result follows.

Cases of

$$\frac{\Gamma \vdash M : \left\{\blacksquare A \;\middle|\; [\mathsf{bx}]\gamma[\nu\alpha^{\ell}\varphi/\beta]\right\} \qquad \beta \text{ Pos } \gamma}{\Gamma \vdash M : \{\blacksquare A \mid [\mathsf{bx}]\gamma[\nu\alpha^{\omega}\varphi/\beta]\}}\ (\ell \text{ not free in } \Gamma, \gamma) \qquad \frac{\Gamma \vdash M : \{\blacksquare A \mid [\mathsf{bx}]\gamma[\nu\alpha^{\omega}\varphi/\beta]\} \qquad \beta \text{ Pos } \gamma}{\Gamma \vdash M : \{\blacksquare A \mid [\mathsf{bx}]\gamma[\nu\alpha^{\mathsf{t}}\varphi/\beta]\}}$$

First, by Cor. 7.9 we have

$$\wr \nu\alpha^{\omega}\varphi(\alpha) \wr \;=\; \bigcap_{m\in\mathbb{N}} \wr \varphi^m(\top) \wr$$

Moreover, since β is positive in γ, it follows from Lem. E.10 (Lem. 7.8) that $\wr \gamma \wr$ is cocontinuous. We thus get

$$\wr \gamma[\nu\alpha^{\omega}\varphi(\alpha)/\beta] \wr \;=\; \bigcap_{m\in\mathbb{N}} \wr \gamma[\varphi^m(\top)/\beta] \wr$$

For both rules, the result then follows from the induction hypothesis.

Cases of

$$\frac{\Gamma \vdash M : \left\{\blacksquare A \;\middle|\; [\mathsf{bx}]\gamma[\mu\alpha^{\mathsf{t}}\varphi/\beta]\right\} \qquad \beta \text{ Pos } \gamma}{\Gamma \vdash M : \{\blacksquare A \mid [\mathsf{bx}]\gamma[\mu\alpha^{\omega}\varphi/\beta]\}}$$

$$\frac{\Gamma \vdash M : \{\blacksquare A \mid [\mathsf{bx}]\gamma[\mu\alpha^{\omega}\varphi/\beta]\} \qquad \Gamma, x : \left\{\blacksquare A \;\middle|\; [\mathsf{bx}]\gamma[\mu\alpha^{\ell}\varphi/\beta]\right\} \vdash N : U \qquad \beta \text{ Pos } \gamma}{\Gamma \vdash N[M/x] : U}\ (\ell \text{ not free in } \Gamma, U, \gamma)$$

Similar. □

Contents