Generic Weakest Precondition Semantics from Monads Enriched with Order

Ichiro Hasuo

Generic Weakest Precondition Semantics from Monads Enriched with Order

Ichiro Hasuo

University of Tokyo, Japan

Abstract. We devise a generic framework where a weakest precondition semantics, in the form of indexed posets, is derived from a monad whose Kleisli category is enriched by posets. It is inspired by Jacobs' recent identification of a categorical structure that is common in various predicate transformers, but adds generality in the following aspects: 1) different notions of modality (such as "may" vs. "must") are captured by Eilenberg-Moore algebras; 2) nested branching—like in games and in probabilistic systems with nondeterministic environments—is modularly modeled by a monad on the Eilenberg-Moore category of another.

1 Introduction

Among various styles of program semantics, the one by *predicate transformers* [5] is arguably the most intuitive. Its presentation is inherently logical, representing a program's behaviors by what properties (or *predicates*) hold before and after its execution. Predicate transformer semantics therefore form a basis of *program verification*, where specifications are given in the form of pre- and post-conditions [14]. It has also been used for *refinement* of specifications into programs (see e.g. [30]). Its success has driven extensions of the original nondeterministic framework, e.g. to the probabilistic one [18, 24] and to the setting with both nondeterministic and probabilistic branching [31].

A Categorical Picture More recently, Jacobs in his series of papers [16, 17] has pushed forward a categorical view on predicate transformers. It starts with a monad T that models a notion of branching. Then a program—henceforth called a *(branching) computation*—is a Kleisli arrow $X \to TY$; and the the weakest precondition semantics is given as a contravariant functor $\mathbb{P}^{\mathcal{K}\ell}\colon \mathcal{K}\ell(T)^{\mathrm{op}} \to \mathbb{A}$, from the Kleisli category to the category $\mathbb{A}$ of suitable ordered algebras.

For example, in the basic nondeterministic setting, T is the powerset monad $\mathcal{P}$ on **Sets** and $\mathbb{A}$ is the category $\mathbf{CL}_{\bigwedge}$ of complete lattices and $\bigwedge$-preserving maps. The weakest precondition functor $\mathbb{P}^{\mathcal{K}\ell}\colon \mathcal{K}\ell(T)^{\mathrm{op}} \to \mathbf{CL}_{\bigwedge}$ then carries a function $f\colon X \to \mathcal{P}Y$ to

$$\mathrm{wpre}(f) \ : \ \mathcal{P}Y \longrightarrow \mathcal{P}X \ , \qquad Q \longmapsto \{x \in X \mid f(x) \subseteq Q\} \ . \tag{1}$$

Moreover it can be seen that: 1) the functor $\mathbb{P}^{\mathcal{K}\ell}$ factors through the comparison functor $K\colon \mathcal{K}\ell(\mathcal{P}) \to \mathcal{EM}(\mathcal{P})$ to the Eilenberg-Moore category $\mathcal{EM}(\mathcal{P})$; and 2)

the extended functor $\mathbb{P}^{\mathcal{EM}}$ has a dual adjoint $\mathbb{S}$. The situation is as follows.

$$\begin{array}{ccc} \mathbf{CL}_{\bigwedge} & \overset{\mathbb{S}}{\underset{\mathbb{P}^{\mathcal{EM}}}{\rightleftarrows}} & (\mathbf{CL}_{\bigvee})^{\mathrm{op}} \cong \mathcal{EM}(\mathcal{P})^{\mathrm{op}} \\ {\scriptstyle \mathbb{P}^{\mathcal{KL}} = \mathbb{P}^{\mathcal{EM}} \circ K^{\mathrm{op}}} \nwarrow & \mathcal{KL}(\mathcal{P})^{\mathrm{op}} & \nearrow {\scriptstyle K^{\mathrm{op}}} \end{array} \tag{2}$$

Here the functor K carries $f\colon X \to TY$ to $f^{\dagger}\colon \mathcal{P}X \to \mathcal{P}Y, P \mapsto \bigcup_{x\in P} f(x)$ and is naturally thought of as a strongest postcondition semantics. Therefore the picture (2)—understood as the one below—identifies a categorical structure that underlies predicate transformer semantics. The adjunction here—it is in fact an isomorphism in the specific instance of (2)—indicates a "duality" between forward and backward predicate transformers.

$$\begin{array}{ccc} (\text{ backward predicate transformers }) & \overset{\mathbb{S}}{\underset{\mathbb{P}^{\mathcal{EM}}}{\rightleftarrows}} & (\text{ forward predicate transformers }) \\ \text{weakest precondition semantics} \nwarrow & \text{(computations)} & \nearrow \text{strongest postcondition semantics} \end{array} \tag{3}$$

Jacobs has identified other instances of (3) for: discrete probabilistic branching [16]; quantum logic [16]; and continuous probabilistic branching [17]. In all these instances the notion of *effect module*—originally from the study of quantum probability [6]—plays an essential role as algebras of "quantitative logics."

Towards Generic Weakest Precondition Semantics In [16, 17] the picture (3) is presented through examples and no categorical axiomatics—that induce the picture—have been explicitly introduced. Finding such is the current paper's aim. In doing so, moreover, we acquire additional generality in two aspects: *different modalities* and *nested branching*.

To motivate the first aspect, observe that the weakest precondition semantics in (1) is the *must* semantics. The *may* variant looks as interesting; it would carry a postcondition $Q \subseteq Y$ to $\{x \in X \mid f(x) \cap Q \neq \emptyset\}$. The difference between the two semantics is much like the one between the modal operators $\Box$ and $\Diamond$.

On the second aspect, situations are abound in computer science where a computation involves two layers of branching. Typically these layers correspond to two distinct *players* with conflicting interests. Examples are *games*, a two-player version of automata which are essential tools in various topics including model-checking; and *probabilistic systems* where it is common to include nondeterministic branching too for modeling the environment's choices. Further details will be discussed later in §3.

Predicates and Modalities from Monads In this paper we present two categorical setups that are inspired by [4, 23]—specifically by their use of $T1$ as a domain of *truth values* or *quantities*.

The first "one-player" setup is when we have only one layer of branching. Much like in [16, 17] we start from a monad T. Assuming that T is *order-enriched*—in the sense that its Kleisli category $\mathcal{KL}(T)$ is **Posets**-enriched—we observe that:

– a natural notion of *truth value* arises from an object $T\Omega$ (typically $\Omega = 1$);
– and a modality (like "may" and "must") corresponds to a choice of an Eilenberg-Moore algebra $\tau\colon T(T\Omega) \to T\Omega$.

The required data set (T, Ω, τ) shall be called a *predicate transformer situation*. We prove that it induces a *weakest precondition semantics* functor $\mathcal{K}\ell(T)^{\mathrm{op}} \to \mathbf{Posets}$, and that it factors through $K\colon \mathcal{K}\ell(T) \to \mathcal{EM}(T)$, much like in (2). The general setup addresses common instances like the original nondeterministic one [5] and the probabilistic predicate transformers in [18,24]. Moreover it allows us to systematically search for different modalities, leading e.g. to a probabilistic notion of partial correctness guarantee (which does not seem well-known).

The other setup is the "two-player" one. It is much like a one-player setup built on another, with two monads T and R and two "modalities" τ and ρ. A potential novelty here is that R is a monad on $\mathcal{EM}(T)$; this way we manage some known complications in nested branching, such as the difficulty of combining probability and nondeterminism. We prove that the data set $(T, \Omega, \tau, R, \rho)$ gives rise to a weakest precondition semantics, as before. Its examples include: a logic of *forced predicates* in games; and the probabilistic predicate transformers in [31].

In this paper we focus on one side of predicate transformers, namely weakest precondition semantics. Many components in the picture of [16,17] are therefore left out. They include the adjoint $\mathbb{S}$ in (3), and the role of effect modules. Indeed, on the top-left corner of (3) we always have **Posets** which is less rich a structure than complete lattices or effect modules. Incorporating these is future work.

Organization of the Paper In §2 we introduce our first "one-player" setup, and exhibit its examples. Our second "two-player" setup is first motivated in §3 through the examples of games and probabilistic systems, and is formally introduced in §4. Its examples are described in §5 in detail. In §6 we conclude.

Notations and Terminologies For a monad T, a *T-algebra* $TX \xrightarrow{a} X$ shall always mean an *Eilenberg-Moore algebra* for T, making the diagrams on the right commute. For categorical backgrounds see e.g. [1, 28].

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & TX \\ & \searrow^{\mathrm{id}} & \downarrow a \\ & & X \end{array} \qquad \begin{array}{ccc} T(TX) & \xrightarrow{Ta} & TX \\ {\scriptstyle \mu_X}\downarrow & & \downarrow{\scriptstyle a} \\ TX & \xrightarrow[a]{} & X \end{array} \tag{4}$$

Given a monad T on $\mathbb{C}$, an arrow in the Kleisli category $\mathcal{K}\ell(T)$ is denoted by $X \nrightarrow Y$; an identity arrow is by $\mathrm{id}_X^{\mathcal{K}\ell(T)}$; and composition of arrows is by $g \odot f$. These are to be distinguished from $X \to Y$, id_X and $g \circ f$ in the base category $\mathbb{C}$.

2 Generic Weakest Preconditions, One-Player Setting

2.1 Order-Enriched Monad

We use monads for representing various notions of "branching." These monads are assumed to have order-enrichment ($\sqsubseteq$ for, roughly speaking, "more options"); and this will be used for an entailment relation, an important element of logic.

The category **Posets** is that of posets and monotone functions.

Definition 2.1 An *order-enriched monad* T on a category $\mathbb{C}$ is a monad together with a **Posets**-enriched structure of the Kleisli category $\mathcal{K}\ell(T)$.

The latter means specifically: 1) each homset $\mathcal{K}\ell(T)(X,Y) = \mathbb{C}(X,TY)$ carries a prescribed poset structure; and 2) composition $\odot$ in $\mathcal{K}\ell(T)$ is monotone in each argument. Such order-enrichment typically arises from the poset structure of TY in the pointwise manner. In the specific setting of $\mathbb{C} = \mathbf{Sets}$ such enrichment can be characterized by *substitutivity* and *congruence* of orders on TX; see [21].

Below are some examples of order-enriched monads. Our intuition about an order-enriched monad T is that it represents one possible branching type, where $\eta_X \colon X \to TX$ represents the trivial branching with a unique option and $\mu_X \colon T(TX) \to TX$ represents flattening 'branching twice' into 'branching once' (see [13]). In fact each of the examples below has the Kleisli category $\mathcal{K}\ell(T)$ enriched by the category **Cppo** of pointed cpo's and continuous maps—not just by **Posets**—and hence is suited for generic *coalgebraic trace semantics* [13].

Example 2.2 1. The *lift monad* $\mathcal{L} = 1 + (\_)$—where the element of 1 is denoted by $\perp$—has a standard monad structure induced by coproducts. For example, the multiplication $\mu^{\mathcal{L}} \colon 1 + 1 + X \to 1 + X$ carries $x \in X$ to itself and both $\perp$'s to $\perp$. The set $\mathcal{L}X$ is a pointed dcpo with the flat order ($\perp \sqsubseteq x$ for each $x \in X$).
The lift monad $\mathcal{L}$ models the "branching type" of potential nontermination.
2. The *powerset monad* $\mathcal{P}$ models (possibilistic) nondeterminism. Its action on arrows takes direct images: $(\mathcal{P}f)U = \{f(x) \mid x \in U\}$. Its unit is given by singletons: $\eta^{\mathcal{P}}_X = \{\_\} \colon X \to \mathcal{P}X$, and its multiplication is by unions: $\mu^{\mathcal{P}}_X = \bigcup \colon \mathcal{P}(\mathcal{P}X) \to \mathcal{P}X$.
3. The *subdistribution monad* $\mathcal{D}$ models probabilistic branching. It carries a set X to the set of (probability) subdistributions over X:

$$\mathcal{D}X \;:=\; \left\{ d \colon X \to [0,1] \;\middle|\; \textstyle\sum_{x \in X} d(x) \leq 1 \right\} \;;$$

such d is called a *sub*distribution since the values need not add to 1. Given an arrow $f \colon X \to Y$ in **Sets**, $\mathcal{D}f \colon \mathcal{D}X \to \mathcal{D}Y$ is defined by $(\mathcal{D}f)(d)(y) := \sum_{x \in f^{-1}(\{y\})} d(x)$. Its unit is the *Dirac* (or *pointmass*) *distribution*: $\eta^{\mathcal{D}}_X(x) = [\, x \mapsto 1;\, x' \mapsto 0 \text{ (for } x' \neq x)]$; its multiplication is defined by $\mu^{\mathcal{D}}_X(\mathfrak{a}) = [x \mapsto \sum_{d \in \mathcal{D}X} \mathfrak{a}(d) \cdot d(x)]$ for $\mathfrak{a} \in \mathcal{D}(\mathcal{D}X)$.

Besides, the *quantum branching monad* $\mathcal{Q}$ is introduced in [12] for the purpose of modeling a quantum programming language that obeys the design principle of "quantum data, classical control." It comes with an order-enrichment, too, derived from the *Löwner partial order* between positive operators. Yet another example is the continuous variant of $\mathcal{D}$, namely the *Giry monad* on the category **Meas** of measurable spaces [7].

2.2 PT Situation and Generic Weakest Precondition Semantics

We introduce our first basic setup for our generic weakest precondition semantics. In our main examples we take $\mathbb{C} = \mathbf{Sets}$ and $\Omega = 1$ (a singleton).

Definition 2.3 (PT situation) A *predicate transformer situation* (a *PT situation* for short) over a category $\mathbb{C}$ is a triple (T, Ω, τ) of

- an order-enriched monad T on $\mathbb{C}$;
- an object $\Omega \in \mathbb{C}$; and
- an (Eilenberg-Moore) algebra $\tau\colon T(T\Omega) \to T\Omega$ that satisfies the following *monotonicity condition*: for each $X \in \mathbb{C}$, the correspondence

$$(\Phi_\tau)_X \;:\; \mathbb{C}(X, T\Omega) \longrightarrow \mathbb{C}(TX, T\Omega) \;\text{, i.e. } \mathcal{K}\ell(T)(X,\Omega) \longrightarrow \mathcal{K}\ell(T)(TX,\Omega) \;,$$
$$\text{given by} \quad \big(X \xrightarrow{p} T\Omega\big) \longmapsto \big(TX \xrightarrow{Tp} T(T\Omega) \xrightarrow{\tau} T\Omega\big)$$

  is monotone with respect to the order-enrichment of the Kleisli category $\mathcal{K}\ell(T)$ (Def. 2.1). Note here that $\Phi_\tau : \mathbb{C}(\_, T\Omega) \Rightarrow \mathbb{C}(T\_, T\Omega)$ is nothing but the natural transformation induced by the arrow τ via the Yoneda lemma.

The data τ is called a *modality*; see the introduction (§1) and also §2.3 below.

The following lemma gives a canonical (but not unique) modality for T.

Lemma 2.4 *If T is an order-enriched monad, (T, Ω, μ_Ω) is a PT situation.*

Proof. We have only to check the monotonicity condition of μ_Ω in Def. 2.3. It is easy to see that $(\Phi_{\mu_\Omega})_X = \mu_\Omega \circ T(\_)\colon \mathbb{C}(X, T\Omega) \to \mathbb{C}(TX, T\Omega)$ is equal to $(\_) \odot (\mathrm{id}_{TX})^\wedge\colon \mathcal{K}\ell(T)(X,\Omega) \to \mathcal{K}\ell(T)(TX,\Omega)$. Here $(\mathrm{id}_{TX})^\wedge\colon TX \nrightarrow X$ is the arrow that corresponds to the identity id_{TX} in $\mathbb{C}$. The claim follows from the monotonicity of $\odot$. □

We shall derive a weakest precondition semantics from a given PT situation (T, Ω, τ). The goal would consist of:

- a (po)set $\mathbb{P}^{\mathcal{K}\ell}(\tau)(X)$ of *predicates* for each object $X \in \mathbb{C}$, whose order $\sqsubseteq$ represents an *entailment relation* between predicates; and
- an assignment, to each *(branching) computation* $f\colon X \to TY$ in $\mathbb{C}$, a *predicate transformer*

$$\mathrm{wpre}(f) \;:\; \mathbb{P}^{\mathcal{K}\ell}(\tau)(Y) \longrightarrow \mathbb{P}^{\mathcal{K}\ell}(\tau)(X) \tag{5}$$

  that is a monotone function.

Since a computation is an arrow $f\colon X \nrightarrow Y$ in $\mathcal{K}\ell(T)$, we are aiming at a functor

$$\mathbb{P}^{\mathcal{K}\ell}(\tau) \;:\; \mathcal{K}\ell(T)^{\mathrm{op}} \longrightarrow \mathbf{Posets} \;. \tag{6}$$

Such a functor is known as an *indexed poset*, a special case of *indexed categories*. These "indexed" structures are known to correspond to "fibered" structures (*poset fibrations* and *(split) fibrations*, respectively), and all these have been used as basic constructs in categorical logic (see e.g. [15]). An indexed poset like (6) therefore puts us on a firm footing.

Proposition 2.5 (the indexed poset $\mathbb{P}^{\mathcal{K}\ell}(\tau)$) *Given a PT situation (T, Ω, τ), the following defines an indexed poset $\mathbb{P}^{\mathcal{K}\ell}(\tau)\colon \mathcal{K}\ell(T)^{\mathrm{op}} \to \mathbf{Posets}$.*[1]

- *On an object $X \in \mathcal{K}\ell(T)$, $\mathbb{P}^{\mathcal{K}\ell}(\tau)(X) := \mathcal{K}\ell(T)(X, \Omega) = \mathbb{C}(X, T\Omega)$.*
- *On an arrow $f\colon X \nrightarrow Y$, $\mathbb{P}^{\mathcal{K}\ell}(\tau)(f)\colon \mathbb{C}(Y, T\Omega) \to \mathbb{C}(X, T\Omega)$ is defined by*

$$\big(Y \xrightarrow{q} T\Omega\big) \longmapsto \big(X \xrightarrow{f} TY \xrightarrow{Tq} T(T\Omega) \xrightarrow{\tau} T\Omega\big) \ .$$

Proof. We need to check: the monotonicity of $\mathbb{P}^{\mathcal{K}\ell}(\tau)(f)$; and that the functor $\mathbb{P}^{\mathcal{K}\ell}(\tau)$ indeed preserves identities and composition of arrows. These will be proved later, altogether in the proof of Thm. 2.10. □

A consequence of the proposition—specifically the functoriality of $\mathbb{P}^{\mathcal{K}\ell}(\tau)$—is *compositionality* of the weakest precondition semantics: given two computations $f\colon X \to TY$, $g\colon Y \to TU$ and a postcondition $r\colon U \to T1$, we have

$$\mathbb{P}^{\mathcal{K}\ell}(\tau)(g \odot f)(r) \ = \ \mathbb{P}^{\mathcal{K}\ell}(\tau)(f)\big(\mathbb{P}^{\mathcal{K}\ell}(\tau)(g)(r)\big) \ .$$

That is, the semantics of a sequential composition $g \odot f$ can be computed step by step.

2.3 Examples of PT Situations

For each of $T = \mathcal{L}, \mathcal{P}, \mathcal{D}$ in Example 2.2, we take $\Omega = 1$ and the set $T1$ is naturally understood as a set of "truth values" (an observation in [4, 23]):

$$\mathcal{L}1 \ = \ \left[\begin{array}{c} (\mathtt{tt} := *) \\ \sqcup\!| \\ (\mathtt{ff} := \bot) \end{array}\right] , \qquad \mathcal{P}1 \ = \ \left[\begin{array}{c} (\mathtt{tt} := 1) \\ \sqcup\!| \\ (\mathtt{ff} := \emptyset) \end{array}\right] , \quad \text{and} \quad \mathcal{D}1 \ = \ \big([0,1], \leq\big) \ .$$

Here $*$ is the element of the argument 1 in $\mathcal{L}1$. Both $\mathcal{L}1$ and $\mathcal{P}1$ represent the Boolean truth values. In the $\mathcal{D}$ case a truth value is $r \in [0, 1]$; a predicate, being a function $X \to [0, 1]$, is hence a *random variable* that tells the certainty with which the predicate holds at each $x \in X$.

We shall introduce modalities for these monads T and $\Omega = 1$. The following observation (easy by diagram chasing) will be used.

Lemma 2.6 *The category $\mathcal{EM}(T)$ of Eilenberg-Moore algebra is iso-closed in the category of functor T-algebras. That is, given an Eilenberg-Moore algebra $a\colon TX \to X$, an arrow $b\colon TY \to Y$, and an isomorphism $f\colon X \xrightarrow{\cong} Y$ such that $f \circ a = b \circ Tf$, the arrow b is also an Eilenberg-Moore algebra.* □

[1] For brevity we favor the notation $\mathbb{P}^{\mathcal{K}\ell}(\tau)$ over more appropriate $\mathbb{P}^{\mathcal{K}\ell}(T, \Omega, \tau)$.

The Lift Monad $\mathcal{L}$: τ_{total} and τ_{partial} We have the following two modalities (and none other, as is easily seen).

$$\begin{array}{rl} \tau_{\text{total}}, \tau_{\text{partial}} : & \{\bot\} + \{\mathtt{tt}, \mathtt{ff}\} = \mathcal{L}(\mathcal{L}1) \quad \longrightarrow \quad \mathcal{L}1 = \{\mathtt{tt}, \mathtt{ff}\} \ , \\ \tau_{\text{total}} : & \bot \mapsto \mathtt{ff} \ , \quad \mathtt{tt} \mapsto \mathtt{tt} \ , \quad \mathtt{ff} \mapsto \mathtt{ff} \ , \\ \tau_{\text{partial}} : & \bot \mapsto \mathtt{tt} \ , \quad \mathtt{tt} \mapsto \mathtt{tt} \ , \quad \mathtt{ff} \mapsto \mathtt{ff} \ . \end{array}$$

The one we obtain from multiplication $\mu_1^{\mathcal{L}}$ is τ_{total}; the other τ_{partial} is nonetheless important in program verification. Given $q\colon Y \to \mathcal{L}1$ and $f\colon X \to \mathcal{L}Y$ where f is understood as a possibly diverging computation from X to Y, the predicate

$$\mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{partial}})(f)(q) = \tau_{\text{partial}} \circ \mathcal{L}q \circ f \quad : \quad X \longrightarrow \mathcal{L}1$$

carries $x \in X$ to $\mathtt{tt}$ in case $f(x) = \bot$, i.e., if the computation is diverging. This is therefore a *partial correctness* specification that is common in Floyd-Hoare logic (see e.g. [37]). In contrast, using τ_{total}, the logic is about *total correctness*.

The Powerset Monad $\mathcal{P}$: $\tau_\Diamond$ and $\tau_\Box$ The monad multiplication $\mu_1^{\mathcal{P}}$ yields a modality which shall be denoted by $\tau_\Diamond$. The other modality $\tau_\Box$ is given via the swapping $\sigma\colon \mathcal{P}1 \xrightarrow{\cong} \mathcal{P}1$:

$$\begin{array}{ccc} \mathcal{P}(\mathcal{P}1) & \xrightarrow[\cong]{\mathcal{P}\sigma} & \mathcal{P}(\mathcal{P}1) \\ {\scriptstyle \tau_\Box}\downarrow & \cong & \downarrow{\scriptstyle \tau_\Diamond} \\ \mathcal{P}1 & \xleftarrow[\sigma]{} & \mathcal{P}1 \ ; \end{array} \qquad \begin{array}{l} \text{explicitly,} \\ \tau_\Diamond\{\} = \mathtt{ff},\ \tau_\Diamond\{\mathtt{tt}\} = \mathtt{tt},\ \tau_\Diamond\{\mathtt{ff}\} = \mathtt{ff},\ \tau_\Diamond\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{tt}; \\ \tau_\Box\{\} = \mathtt{tt},\ \tau_\Box\{\mathtt{tt}\} = \mathtt{tt},\ \tau_\Box\{\mathtt{ff}\} = \mathtt{ff},\ \tau_\Box\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{ff}. \end{array} \tag{7}$$

In view of Lem. 2.6, we have only to check that the map $\tau_\Box$ satisfies the monotonicity condition in Def. 2.3. We first observe that, for $h\colon X \to \mathcal{P}1$ and $U \in \mathcal{P}X$,

$$(\tau_\Box \circ \mathcal{P}h)(U) = \mathtt{ff} \quad \Longleftrightarrow \quad \mathtt{ff} \in (\mathcal{P}h)(U) \quad \Longleftrightarrow \quad \exists x \in U.\, h(x) = \mathtt{ff} \ ,$$

where the first equivalence is by (7). Now assume that $f \sqsubseteq g\colon X \nrightarrow 1$ and $(\tau_\Box \circ \mathcal{P}g)(U) = \mathtt{ff}$. For showing $\tau_\Box \circ \mathcal{P}f \sqsubseteq \tau_\Box \circ \mathcal{P}g$ it suffices to show that $(\tau_\Box \circ \mathcal{P}f)(U) = \mathtt{ff}$; this follows from the above observation.

The modalities $\tau_\Diamond$ and $\tau_\Box$ capture the *may* and *must* weakest preconditions, respectively. Indeed, given a postcondition $q\colon Y \to \mathcal{P}1$ and $f\colon X \to \mathcal{P}Y$, we have $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Diamond)(f)(q)(x) = \mathtt{tt}$ if and only if there exists $y \in Y$ such that $y \in f(x)$ and $q(y) = \mathtt{tt}$; and $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Box)(f)(q)(x) = \mathtt{tt}$ if and only if $y \in f(x)$ implies $q(y) = \mathtt{tt}$.

Moreover, we can show that $\tau_\Diamond$ and $\tau_\Box$ are the only modalities (in the sense of Def. 2.3) for $T = \mathcal{P}$ and $\Omega = 1$. Since the unit law in (4) forces $\tau\{\mathtt{tt}\} = \mathtt{tt}$ and $\tau\{\mathtt{ff}\} = \mathtt{ff}$, the only possible variations are the following τ_1 and τ_2 (cf. (7)):

$$\tau_1\{\} = \mathtt{tt} \ , \ \tau_1\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{tt} \ ; \quad \tau_2\{\} = \mathtt{ff} \ , \ \tau_2\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{ff} \ .$$

Both of these, however, fail to satisfy the multiplication law in (4).

$$\begin{array}{ccc} \{\{\}, \{\mathtt{ff}\}\} & \xmapsto{\mathcal{P}\tau_1} & \{\mathtt{tt}, \mathtt{ff}\} \\ {\scriptstyle \cup_{\mathcal{P}1}}\downarrow & & \downarrow{\scriptstyle \tau_1} \\ \{\mathtt{ff}\} & \xmapsto[\tau_1]{} & \mathtt{ff} \end{array} \quad \neq \quad \mathtt{tt} \qquad \begin{array}{ccc} \{\{\}, \{\mathtt{tt}\}\} & \xmapsto{\mathcal{P}\tau_2} & \{\mathtt{tt}, \mathtt{ff}\} \\ {\scriptstyle \cup_{\mathcal{P}1}}\downarrow & & \downarrow{\scriptstyle \tau_2} \\ \{\mathtt{tt}\} & \xmapsto[\tau_2]{} & \mathtt{tt} \end{array} \quad \neq \quad \mathtt{ff}$$

The monotonicity condition in Def. 2.3, in the case of $T \in \{\mathcal{L}, \mathcal{P}\}$ (hence $T\Omega \cong 2$), coincides with monotonicity of a predicate lifting $2^{(\_)} \Rightarrow 2^{T(\_)}$. The latter is a condition commonly adopted in coalgebraic modal logic (see e.g. [25]).

The Subdistribution Monad $\mathcal{D}$: τ_{total} and τ_{partial} The modality $\tau_{\text{total}} \colon \mathcal{D}[0,1] \to [0,1]$ that arises from the multiplication $\mu_1^{\mathcal{D}}$ is such that: given $q \colon Y \to \mathcal{D}1$ and $f \colon X \to \mathcal{D}Y$, we have $\mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{total}})(f)(q)(x) = \sum_{y \in Y} q(y) \cdot f(x)(y)$. This is precisely the expected value of the random variable q under the distribution $f(x)$; thus τ_{total} yields the *probabilistic predicate transformer* of [18, 24].

In parallel to the powerset monad case, we have an isomorphism $\sigma \colon \mathcal{D}1 \xrightarrow{\cong} \mathcal{D}1, p \mapsto 1-p$. Another modality $\tau_{\text{partial}} \colon \mathcal{D}[0,1] \to [0,1]$ then arises by $\tau_{\text{partial}} := \sigma \circ \tau_{\text{total}} \circ \mathcal{D}\sigma$ like in (7), for which we have

$$\begin{aligned} \tau_{\text{partial}}(d) &= \big(1 - \textstyle\sum_{r \in [0,1]} d(r)\big) + \sum_{r \in [0,1]} r \cdot d(r) \quad \text{and} \\ \mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{partial}})(f)(q)(x) &= \big(1 - \textstyle\sum_{y \in Y} f(x)(y)\big) + \sum_{y \in Y} q(y) \cdot f(x)(y) \ . \end{aligned}$$

In the second line, the value $1 - \sum_{y \in Y} f(x)(y)$—the probability of f's divergence—is added to the τ_{total} case. Therefore the modalities τ_{partial} and τ_{total}, much like in the case of $T = \mathcal{L}$, carry the flavor of *partial* and *total* correctness guarantee.

To see that τ_{partial} is indeed a modality is easy: we use Lem. 2.6; and the monotonicity can be deduced from the following explicit presentation of $\tau_{\text{partial}} \circ \mathcal{D}p$ for $p \colon X \to \mathcal{D}1 = [0,1]$. For each $d \in \mathcal{D}X$,

$$\begin{aligned} (\tau_{\text{partial}} \circ \mathcal{D}p)(d) &= \tau_{\text{partial}}\Big[r \mapsto \textstyle\sum_{x \in p^{-1}(\{r\})} d(x)\Big]_{r \in [0,1]} \\ &= \big(1 - \textstyle\sum_{r \in [0,1]} \sum_{x \in p^{-1}(\{r\})} d(x)\big) + \sum_{r \in [0,1]} r \sum_{x \in p^{-1}(\{r\})} d(x) \\ &= \big(1 - \textstyle\sum_{x \in X} d(x)\big) + \sum_{x \in X} p(x) \cdot d(x) \ . \end{aligned}$$

We do not yet know if τ_{total} and τ_{partial} are the only modalities for $\mathcal{D}$ and $\Omega = 1$.

Remark 2.7 We note the difference between a subdistribution $d \in \mathcal{D}X$ and a predicate (i.e. a random variable) $p \colon X \to \mathcal{D}1$. An example of the latter is $p_\top$ that is everywhere 1—this is the *truth predicate*. In contrast, the former $d \in \mathcal{D}X$ is subject to the (sub)normalization condition $\sum_x d(x) \leq 1$. We understand it as one single "current state" whose whereabouts are known only probabilistically.

2.4 Factorization via the Eilenberg-Moore Category

The indexed poset $\mathbb{P}^{\mathcal{K}\ell}(\tau) \colon \mathcal{K}\ell(T)^{\text{op}} \to \mathbf{Posets}$ in Prop. 2.5 is shown here to factor through the comparison functor $K \colon \mathcal{K}\ell(T) \to \mathcal{EM}(T)$, much like in (2). In fact it is possible to see K as a *strongest postcondition semantics*; see Rem. 2.11.

We will be using the following result.

Lemma 2.8 *Let T be an order-enriched monad on $\mathbb{C}$, $X, Y, U \in \mathbb{C}$ and $f \colon X \to Y$ be an arrow in $\mathbb{C}$. Then $(\_) \circ f \colon \mathbb{C}(Y, TU) \to \mathbb{C}(X, TU)$ is monotone.*

Proof. Given $g\colon Y \to TU$ in $\mathbb{C}$,

$$g \circ f = \mu_U \circ \eta_{TU} \circ g \circ f = \mu_U \circ Tg \circ Tf \circ \eta_X = \mu_U \circ Tg \circ Tf \circ \mu_X \circ \eta_{TX} \circ \eta_X$$
$$= \mu_U \circ Tg \circ \mu_Y \circ T(Tf) \circ \eta_{TX} \circ \eta_X = \big(X \overset{J\eta_X}{\nrightarrow} TX \overset{Tf}{\nrightarrow} Y \overset{g}{\nrightarrow} U\big) \ ,$$

where $J : \mathbf{Sets} \to \mathcal{K}\ell(T)$ is the Kleisli inclusion that sends the arrow $\eta_X\colon X \to TX$ to $\eta_{TX} \circ \eta_X\colon X \nrightarrow TX$. In the calculation we used the monad laws as well as the naturality of η and μ. The correspondence $(\_) \odot (Tf \odot J\eta_X)$ is monotone by assumption (Def. 2.1); this proves the claim. □

Proposition 2.9 (the indexed poset $\mathbb{P}^{\mathcal{EM}}(\tau)$) *A PT situation (T, Ω, τ) induces an indexed poset $\mathbb{P}^{\mathcal{EM}}(\tau)\colon \mathcal{EM}(T)^{\mathrm{op}} \to \mathbf{Posets}$ in the following way.*

- *On objects,*
$$\mathbb{P}^{\mathcal{EM}}(\tau)\big(\begin{smallmatrix} TX \\ \downarrow a \\ X \end{smallmatrix}\big) := \mathcal{EM}(T)\big(\begin{smallmatrix} TX \\ \downarrow a \\ X \end{smallmatrix}, \begin{smallmatrix} T(T\Omega) \\ \downarrow \tau \\ T\Omega \end{smallmatrix}\big)$$
where the order $\sqsubseteq$ on the set $\mathcal{EM}(T)(a, \tau)$ is inherited from $\mathbb{C}(X, T\Omega)$ via the forgetful functor $U^T : \mathcal{EM}(T) \to \mathbb{C}$.
- *On an arrow $f\colon (TX \overset{a}{\to} X) \to (TY \overset{b}{\to} Y)$,*
$$\mathbb{P}^{\mathcal{EM}}(\tau)(f) : \mathcal{EM}(T)\big(\begin{smallmatrix} TY \\ \downarrow b \\ Y \end{smallmatrix}, \begin{smallmatrix} T(T\Omega) \\ \downarrow \tau \\ T\Omega \end{smallmatrix}\big) \longrightarrow \mathcal{EM}(T)\big(\begin{smallmatrix} TX \\ \downarrow a \\ X \end{smallmatrix}, \begin{smallmatrix} T(T\Omega) \\ \downarrow \tau \\ T\Omega \end{smallmatrix}\big) \ , \quad q \longmapsto q \circ f \ .$$

Proof. The monotonicity of $\mathbb{P}^{\mathcal{EM}}(\tau)(f)$ follows from the order-enrichment of T via Lem. 2.8. The functoriality of $\mathbb{P}^{\mathcal{EM}}(\tau)$ is obvious. □

Theorem 2.10 *For a PT situation (T, Ω, τ), the following diagram commutes up-to a natural isomorphism. Here K is the comparison functor.*

$$\begin{array}{ccc} \mathbf{Posets} & \xleftarrow{\ \mathbb{P}^{\mathcal{EM}}(\tau)\ } & \mathcal{EM}(T)^{\mathrm{op}} \\ & {\scriptstyle \mathbb{P}^{\mathcal{K}\ell}(\tau)} \nwarrow \quad \Psi \Uparrow \cong \quad \nearrow {\scriptstyle K^{\mathrm{op}}} & \\ & \mathcal{K}\ell(T)^{\mathrm{op}} & \end{array} \tag{8}$$

Proof. (Also of Prop. 2.5) The natural isomorphism Ψ in question is of the type

$$\Psi_X : \quad \mathbb{P}^{\mathcal{K}\ell}(\tau)(X) = \mathbb{C}(X, T\Omega) \xrightarrow{\cong} \mathcal{EM}(T)\big(\begin{smallmatrix} T(TX) \\ \downarrow \mu_X \\ TX \end{smallmatrix}, \begin{smallmatrix} T(T\Omega) \\ \downarrow \tau \\ T\Omega \end{smallmatrix}\big) = \mathbb{P}^{\mathcal{EM}}(\tau)(KX)$$

and it is defined by the adjunction $\mathbb{C}(X, U^T\tau) \cong \mathcal{EM}(T)(\mu_X, \tau)$ where U^T is the forgetful functor. Explicitly: $\Psi_X\big(X \overset{p}{\to} T\Omega\big) = \big(TX \overset{Tp}{\to} T(T\Omega) \overset{\tau}{\to} T\Omega\big)$; and its inverse is $\Psi_X^{-1}\big(TX \overset{f}{\to} T\Omega\big) = \big(X \overset{\eta_X}{\to} TX \overset{f}{\to} T\Omega\big)$. The function Ψ_X is monotonic by the monotonicity of τ, see Def. 2.3; so is its inverse Ψ_X^{-1} by Lem. 2.8.

Let us turn to naturality of Ψ. Given $f\colon X \nrightarrow Y$ in $\mathcal{K}\ell(T)$, it requires

$$\begin{array}{ccc} \mathbb{C}(Y, T\Omega) & \xrightarrow[\cong]{\Psi_Y} & \mathcal{EM}(T)(\mu_Y, \tau) \\ {\scriptstyle \mathbb{P}^{\mathcal{K}\ell}(\tau)(f) = \tau \circ T(\_) \circ f\downarrow} & & \downarrow{\scriptstyle \mathbb{P}^{\mathcal{EM}}(\tau)(Kf) = (\_) \circ \mu_Y \circ Tf} \\ \mathbb{C}(X, T\Omega) & \xrightarrow[\cong]{\Psi_X} & \mathcal{EM}(T)(\mu_X, \tau) \ . \end{array} \tag{9}$$

Indeed, given $q\colon Y \to T\Omega$,

$$\begin{aligned}\mathbb{P}^{\mathcal{EM}}(\tau)(Kf)(\Psi_Y q) &= \mathbb{P}^{\mathcal{EM}}(\tau)(Kf)(\tau \circ Tq) = \tau \circ Tq \circ \mu_Y \circ Tf \\ &= \tau \circ \mu_{T\Omega} \circ T(Tq) \circ Tf = \tau \circ T\tau \circ T(Tq) \circ Tf = \big(\Psi_X \circ \mathbb{P}^{\mathcal{Kl}}(\tau)(f)\big)q \ ,\end{aligned}$$

where the third equality is naturality of μ and the fourth is the multiplication law of τ (see (4)). By this naturality, in particular, we have that $\mathbb{P}^{\mathcal{Kl}}(\tau)(f)$ is monotone (since the other three arrows are monotone). This is one property needed in Prop. 2.5; the other—functoriality of $\mathbb{P}^{\mathcal{Kl}}(\tau)$—also follows from naturality of Ψ, via the functoriality of K and $\mathbb{P}^{\mathcal{EM}}(\tau)$. □

Remark 2.11 The comparison functor $K\colon \mathcal{Kl}(T) \to \mathcal{EM}(T)$ can be seen as a strongest postcondition semantics. Given a (branching) computation $f\colon X \to TY$, we obtain

$$\mathrm{spost}(f) := \mu_Y \circ Tf \ :\ TX \longrightarrow TY$$

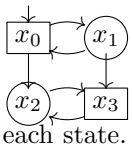
that is an algebra morphism Kf between free algebras. When $T = \mathcal{P}$ this indeed yields a natural notion: concretely it is given by $\mathrm{spost}^{\mathcal{P}}(f)(S) = \{y \mid \exists x \in S.\, y \in fx\}$; here we think of subsets as predicates. Some remarks are in order.

Firstly, note that the notion of predicate here diverges in general from the one in the weakest precondition semantics. This is manifest when $T = \mathcal{D}$: the former is a subdistribution $d \in \mathcal{D}X$ ("partial information on the current state's whereabouts", see Rem. 2.7), while the latter is a random variable $p\colon X \to [0, 1]$.

Secondly, there is no notion of modality involved here. This is unsatisfactory because, besides the above strongest postcondition semantics $\mathrm{spost}^{\mathcal{P}}(f)$ for $T = \mathcal{P}$ that carries the "may" flavor, the "must" variant $\mathrm{spost}^{\mathcal{P}}_{\mathrm{must}}(f)$ is also conceivable such that $\mathrm{spost}^{\mathcal{P}}_{\mathrm{must}}(f)(S) = \{y \mid \forall x \in S.\, y \in fx\}$. This does not arise from the comparison functor K.

3 The Two-Player Setting: Introduction

We extend the basic framework in the previous section by adding another layer of branching. This corresponds to adding another "player" in computations or systems. The additional player typically has an interest that conflicts with the original player's: the former shall be called *Opponent* and denoted by O, while the latter (the original player) is called *Player* P.[2]



The need for two players with conflicting interests is pervasive in computer science. One example is the (nowadays heavy) use of *games* in the automata-theoretic approach to model checking (see e.g. [8]). Games here can be understood as a two-player version of automata, where it is predetermined which player makes a move in each state. An example is above on the right, where P-states are x_0, x_3 and O-states are x_1, x_2. Typical questions asked here are about what Player P *can force*: can P force that x_3 be reached? (yes); can P force that x_0 be visited infinitely often?

[2] Note that (capitalized) *Player* and *Opponent* are altogether called *players*.

(no). In model checking, the dualities between $\wedge$ and $\vee$, ν and μ, etc. in the modal μ-calculus are conveniently expressed as the duality between P and O; and many algorithms and proofs rely on suitably formulated games and results on them (such as the algorithm in [19] that decides the winner of a parity game). Games have also been used in the coalgebraic study of fixed-point logics [26].

Another example of nested two-player branching is found in the process-theoretic study of *probabilistic systems*; see e.g. [3, 33]. There it is common to include nondeterministic branching too: while probabilistic branching models the behavior of a *system* (such as a stochastic algorithm) that flips an internal coin, nondeterministic branching models the *environment*'s behavior (such as requests from users) on which no statistical information is available. In this context, probabilistic branching is often called *angelic* while nondeterministic one is *demonic*; and a common verification goal would be to ensure a property—with a certain minimal likelihood—whatever demonic choices are to be made.

3.1 Leading Example: Nondeterministic P and Nondeterministic O

Let us first focus on the simple setting where: P moves first and O moves second, in each round; and both P and O make nondeterministic choices. This is a setting suited e.g. for bipartite games where P plays first. A computation with such branching is modeled by a function

$$f \,:\, X \longrightarrow \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y) \;, \tag{10}$$

where the occurrences of the powerset functor $\mathcal{P}$ are annotated to indicate which of the players it belongs to (hence $\mathcal{P}_{\mathsf{P}} = \mathcal{P}_{\mathsf{O}} = \mathcal{P}$). We are interested in what P can force; in this *logic of forced predicates*, the following notion of (pre)order seems suitable.

$$\mathfrak{a} \sqsubseteq \mathfrak{b} \quad \text{in } \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y) \quad \overset{\text{def.}}{\Longleftrightarrow} \quad \forall S \in \mathfrak{a}.\, \exists S' \in \mathfrak{b}.\, S' \subseteq_{\mathcal{P}_{\mathsf{O}}Y} S \tag{11}$$

That is: if $\mathfrak{a}$ can force Opponent to $S \subseteq Y$, then $\mathfrak{b}$—that has a greater power—can force Opponent to better (i.e. smaller) $S' \subseteq Y$.

In fact, we shall now introduce a modeling alternative to (10) which uses up-closed families of subsets, and argue for its superiority, mathematical and conceptual. It paves the way to our general setup in §4.

For a set Y, we define $\mathcal{UP}Y$ to be the collection of *up-closed* families of subsets of Y, that is,

$$\mathcal{UP}Y \;:=\; \big\{ \mathfrak{a} \subseteq \mathcal{P}Y \;\big|\; \forall S, S' \subseteq Y.\, (S \in \mathfrak{a} \wedge S \subseteq S' \Rightarrow S' \in \mathfrak{a}) \big\} \;. \tag{12}$$

On $\mathcal{UP}Y$ we define a relation $\sqsubseteq$ by: $\mathfrak{a} \sqsubseteq \mathfrak{b}$ if $\mathfrak{a} \subseteq \mathfrak{b}$. It is obviously a partial order.

Lemma 3.1 *1. For each set Y, the relation $\sqsubseteq$ in (11) on $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$ is a pre-order. It is not a partial order.*

2. *For* $\mathfrak{a} \in \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$, *let* $\uparrow\mathfrak{a} := \{S \mid \exists S' \in \mathfrak{a}.\, S' \subseteq S\}$ *be its* upward closure. *Then the following is an equivalence of (preorders considered to be) categories; here* ι *is the obvious inclusion map.*

$$\mathcal{UP}Y \underset{\iota}{\overset{\uparrow(\_)}{\underset{\simeq}{\rightleftarrows}}} \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$$

Proof. For 1., reflexivity and transitivity of $\sqsubseteq$ is obvious. To see it is not antisymmetric consider $\{\emptyset, Y\}$ and $\{\emptyset\}$.

For 2., ι is obviously monotone. If $\mathfrak{a} \sqsubseteq \mathfrak{b}$ in $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$, for any $S \in \uparrow\mathfrak{a}$ there exists $S' \in \mathfrak{b}$ such that $S' \subseteq S$, hence $S \in \uparrow\mathfrak{b}$. Therefore $\uparrow(\_)$ is monotone too. Obviously $\uparrow(\_) \circ \iota = \mathrm{id}$.

It must be checked that $\iota(\uparrow\mathfrak{a}) \simeq \mathfrak{a}$ for $\mathfrak{a} \in \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$, where $\simeq$ is the equivalence induced by $\sqsubseteq$. The $\sqsubseteq$ direction is immediate from the definition of $\uparrow\mathfrak{a}$; for the other direction, observe that in general $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\mathfrak{a} \sqsubseteq \mathfrak{b}$ in $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$. □

Proposition 3.2 *For each set* Y, $(\mathcal{UP}Y, \sqsubseteq)$ *is the poset induced by the preorder* $\big(\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y), \sqsubseteq\big)$. *Moreover* $(\mathcal{UP}Y, \sqsubseteq)$ *is a complete lattice.*

Proof. The first half is immediate from Lem. 3.1. For the latter, observe that supremums are given by unions. □

The constructions $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}\_)$ and $\mathcal{UP}\_$ have been studied from a coalgebraic perspective in the context of *neighborhood frames* [9, 10]. There a coalgebra for the former is a model of *non-normal* modal logic (meaning that axioms like $\Box p \wedge \Box q \to \Box(p \wedge q)$ and $\Box p \to \Box(p \vee q)$ can fail); one for the latter is a model of *monotone* modal logic (meaning that validity of $\Box p \to \Box(p \vee q)$ is retained). Prop. 3.2 shows that, as long as our interests are game-theoretic and are in the logical reasoning with respect to the preorder $\sqsubseteq$ in (11), we may just as well use $\mathcal{UP}\_$ which is mathematically better-behaved.

To argue further for the mathematical convenience of $\mathcal{UP}\_$, we look at its action on arrows. For $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}\_)$ there are two obvious choices ($\mathcal{PP}f$ and 2^{2^f}) of action on arrows, arising from the covariant and contravariant powerset functors, respectively. Given $f\colon X \to Y$ in **Sets**,

$$\mathcal{PP}f,\ 2^{2^f} \ :\ \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}X) \longrightarrow \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)\ ,$$
$$(\mathcal{PP}f)\mathfrak{a} := \{\amalg_f S \mid S \in \mathfrak{a}\}\ ,\quad 2^{2^f}\mathfrak{a} := \{T \subseteq Y \mid f^{-1}T \in \mathfrak{a}\}\ .$$

Here $\amalg_f S$ is the direct image of S by f.

These two choices are not equivalent with respect to $\sqsubseteq$ on $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y)$. In general we have $2^{2^f}\mathfrak{a} \sqsubseteq (\mathcal{PP}f)\mathfrak{a}$. To see that, assume $U \in 2^{2^f}\mathfrak{a}$, i.e. $f^{-1}U \in \mathfrak{a}$. Then $\amalg_f(f^{-1}U) \subseteq U$ (a general fact) and $\amalg_f(f^{-1}U) \in (\mathcal{PP}f)\mathfrak{a}$. However the converse $2^{2^f}\mathfrak{a} \sqsupseteq (\mathcal{PP}f)\mathfrak{a}$ can fail: consider $!\colon 2 \to 1$ (where $2 = \{0, 1\}$) and $\mathfrak{a} = \{\{0\}\}$; then $2^{2^f}\mathfrak{a} = \emptyset$ while $(\mathcal{PP}f)\mathfrak{a} = \{1\}$.

This discrepancy is absent with $\mathcal{UP}\_$. For a function $f\colon X \to Y$, the "covariant" action $\mathcal{UP}f$ and the "contravariant" action $\mathcal{UP}'f$ are defied as follows.

$$\begin{array}{ccc} \mathcal{UP}X & \xrightarrow{\mathcal{UP}f} & \mathcal{UP}Y \\ {\scriptstyle\iota}\downarrow & & \uparrow{\scriptstyle\uparrow(\_)} \\ \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}X) & \xrightarrow[\mathcal{PP}f]{} & \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y) \end{array} \qquad\qquad \begin{array}{ccc} \mathcal{UP}X & \overset{\mathcal{UP}'f}{- - \to} & \mathcal{UP}Y \\ \downarrow & & \downarrow \\ \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}X) & \xrightarrow[2^{2^f}]{} & \mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}Y) \end{array} \tag{13}$$

On the left, ι and $\uparrow(\_)$ are as in Lem. 3.1. On the right 2^{2^f} restricts to $\mathcal{UP}X \to \mathcal{UP}Y$ (easy by the fact that f^{-1} is monotone); on the left such is not the case (consider $f\colon 1 \to 2$, $0 \mapsto 0$ and $\mathfrak{a} = \{1\}$) and we need explicit use of $\uparrow(\_)$.

Lemma 3.3 *$\mathcal{UP}f = \mathcal{UP}'f$.*

Proof. Let $\mathfrak{a} \in \mathcal{UP}X$ (hence up-closed). In view of Lem. 3.1, it suffices to show that $2^{2^f}\mathfrak{a} \simeq (\mathcal{PP}f)\mathfrak{a}$; we have already proved the $\sqsubseteq$ direction. For the other direction, let $S \in \mathfrak{a}$; proving $\amalg_f S \in 2^{2^f}\mathfrak{a}$ will prove $(\mathcal{PP}f)\mathfrak{a} \subseteq 2^{2^f}\mathfrak{a}$, hence $(\mathcal{PP}f)\mathfrak{a} \sqsubseteq 2^{2^f}\mathfrak{a}$. That $S \subseteq f^{-1}(\amalg_f S)$ is standard; since $\mathfrak{a}$ is up-closed we have $f^{-1}(\amalg_f S) \in \mathfrak{a}$. Therefore $\amalg_f S \in (2^{2^f})\mathfrak{a}$. □

We therefore define $\mathcal{UP}\colon \mathbf{Sets} \to \mathbf{Sets}$ by (12) on objects and either of the actions in (13) on arrows. Its functoriality is obvious from (13) on the right.

3.2 Nondeterministic O, then Probabilistic P: Search for Modularity

We have argued for the convenience of the functor $\mathcal{UP}$, over $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}\_)$, for modeling two-layer branching in games. A disadvantage, however, is that *modularity* is lost. Unlike $\mathcal{P}_{\mathsf{P}}(\mathcal{P}_{\mathsf{O}}\_)$, the functor $\mathcal{UP}\colon \mathbf{Sets} \to \mathbf{Sets}$ is not an obvious composite of two functors, each of which modeling each player's choice.

The same issue arises also in the systems with both probabilistic and nondeterministic branching (briefly discussed before). It is known (an observation by Gordon Plotkin; see e.g. [35]) that there is no distributive law $\mathcal{DP} \Rightarrow \mathcal{PD}$ of the subdistribution monad $\mathcal{D}$ over the powerset monad $\mathcal{P}$. This means we cannot compose them to obtain a new monad $\mathcal{PD}$. Two principal fixes have been proposed: one is to refine $\mathcal{D}$ into the *indexed valuation monad* that distinguishes e.g. $[x \mapsto 1/2, x \mapsto 1/2]$ from $[x \mapsto 1]$ (see [35]). The other way (see e.g. [34]) replaces $\mathcal{P}$ by the *convex powerset construction* and uses

$$\mathcal{CD}X \;:=\; \{\mathfrak{a} \subseteq \mathcal{D}X \mid p_i \in [0,1], \textstyle\sum_i p_i = 1, d_i \in \mathfrak{a} \Rightarrow \sum_i p_i d_i \in \mathfrak{a}\}$$

in place of $\mathcal{PD}$, an alternative we favor due to our process-theoretic interests (see Rem. 5.8 later). However, much like with $\mathcal{UP}$, it is not immediate how to decompose $\mathcal{CD}$ into Player and Opponent parts.

We now introduce a categorical setup that addresses this issue of separating two players. It does so by identifying one layer of branching—like up-closed powerset and convex powerset—as a monad on an Eilenberg-Moore category.

4 Generic Two-Player Weakest Precondition Semantics

Definition 4.1 (2-player PT situation) A *2-player predicate transformer situation* over a category $\mathbb{C}$ is a quintuple $(T, \Omega, \tau, R, \rho)$ where:

- (T, Ω, τ) is a PT situation (Def. 2.3), where in particular $\tau\colon T(T\Omega) \to T\Omega$ is an Eilenberg-Moore algebra;
- R is a monad on the Eilenberg-Moore category $\mathcal{EM}(T)$; and
- $\rho\colon R\binom{T(T\Omega)}{T\Omega} \to \binom{T(T\Omega)}{T\Omega}$ is an Eilenberg-Moore R-algebra, that is also called a *modality*. It is further subject to the *monotonicity condition* that is much like in Def. 2.3: the map

$$\mathcal{EM}(T)\Big(\binom{TX}{X}, \binom{T(T\Omega)}{T\Omega}\Big) \longrightarrow \mathcal{EM}(T)\Big(R\binom{TX}{X}, \binom{T(T\Omega)}{T\Omega}\Big), \quad f \longmapsto \rho \circ Rf$$

  is monotone for each algebra a. Here the order of each homset is induced by the enrichment of $\mathcal{K}\ell(T)$ via $\mathcal{EM}(T)(b,\tau) \overset{U^T}{\to} \mathbb{C}(U^T b, T\Omega) = \mathcal{K}\ell(T)(U^T b, \Omega)$.

The situation is as in the following diagram.

$$\begin{array}{c} U^T U^R F^R F^T \\ = U^T R F^T \end{array} \quad \circlearrowleft \mathbb{C} \underset{F^T}{\overset{U^T}{\underset{\longleftarrow}{\overset{\longrightarrow}{\top}}}} \mathcal{EM}(T) \underset{F^R}{\overset{U^R}{\underset{\longleftarrow}{\overset{\longrightarrow}{\top}}}} \mathcal{EM}(R) \quad T \circlearrowleft \quad R \circlearrowleft \quad \uparrow K \quad \mathcal{K}\ell(U^T R F^T) \quad \top \tag{14}$$

The composite adjunction yields a new monad $U^T U^R F^R F^T = U^T R F^T$ on $\mathbb{C}$; then from the Kleisli category $\mathcal{K}\ell(U^T R F^T)$ for the new monad we obtain a comparison functor to $\mathcal{EM}(R)$. It is denoted by K.

We have a monad R on $\mathcal{EM}(T)$ and an algebra (modality) ρ for it. This is much like in the original notion of PT situation, where $\tau\colon T(T\Omega) \to T\Omega$ is a modality from which we derived a weakest precondition semantics. Indeed, the following construction is parallel to Prop. 2.9.

Proposition 4.2 (the indexed poset $\mathbb{P}^{\mathcal{EM}}(\tau,\rho)$) *A 2-player PT situation $(T, \Omega, \tau, R, \rho)$ induces an indexed poset $\mathbb{P}^{\mathcal{EM}}(\tau,\rho)\colon \mathcal{EM}(R)^{\mathrm{op}} \to$ **Posets** over $\mathcal{EM}(T)$ by:*

- *on an object $\alpha \in \mathcal{EM}(R)$,*

$$\mathbb{P}^{\mathcal{EM}}(\tau,\rho)\Big(\binom{R(TX \overset{a}{\to} X)}{(TX \overset{a}{\to} X)}\Big) := \mathcal{EM}(R)\Big(\binom{R(TX \overset{a}{\to} X)}{(TX \overset{a}{\to} X)}, \binom{R(T(T\Omega) \overset{\tau}{\to} T\Omega)}{(T(T\Omega) \overset{\tau}{\to} T\Omega)}\Big)$$

  where the order $\sqsubseteq$ on the set $\mathcal{EM}(R)(\alpha,\rho)$ is inherited from $\mathbb{C}(X, T\Omega)$ via the forgetful functors $\mathcal{EM}(R) \to \mathcal{EM}(T) \to \mathbb{C}$; and

– *on an arrow* $f\colon \binom{Ra}{a} \to \binom{Rb}{b}$,

$$\mathbb{P}^{\mathcal{EM}}(\tau,\rho)(f)\ :\ \mathcal{EM}(R)\Big(\begin{smallmatrix}Rb\\ \downarrow\beta\\ b\end{smallmatrix}\,,\ \begin{smallmatrix}R\tau\\ \downarrow\rho\\ R\tau\end{smallmatrix}\Big) \longrightarrow \mathcal{EM}(R)\Big(\begin{smallmatrix}Ra\\ \downarrow\alpha\\ a\end{smallmatrix}\,,\ \begin{smallmatrix}R\tau\\ \downarrow\rho\\ \tau\end{smallmatrix}\Big)\ ,\quad q \longmapsto q\circ f\ .$$

Proof. The same as the proof of Prop. 2.9, relying on Lem. 2.8. □

Much like in Thm. 2.10, composition of the indexed poset $\mathbb{P}^{\mathcal{EM}}(\tau,\rho)\colon \mathcal{EM}(R)^{\mathrm{op}} \to$ **Posets** and the comparison functor $K\colon \mathcal{K}\ell(U^TRF^T) \to \mathcal{EM}(R)$ will yield the weakest precondition calculus. The branching computations of our interest are therefore of the type $X \to U^TRF^TY$. We will later see, through examples, that this is indeed what models the scenarios in §3.

Note that in what follows we rely heavily on the adjunction $F^T \dashv U^T$.

Proposition 4.3 (the indexed poset $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)$) *A 2-player PT situation (T,Ω,τ,R,ρ) induces an indexed poset $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)\colon \mathcal{K}\ell(U^TRF^T)^{\mathrm{op}} \to$ **Posets** by:*

– *on an object $X \in \mathcal{K}\ell(U^TRF^T)$, $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(X) := \mathcal{K}\ell(T)(X,\Omega) = \mathbb{C}(X,T\Omega)$;*
– *given an arrow $f\colon X \nrightarrow Y$ in $\mathcal{K}\ell(U^TRF^T)$, it induces an arrow $f^\wedge\colon F^TX \to R(F^TY)$ in $\mathcal{EM}(T)$; this is used in*

$$\mathcal{EM}(T)(F^TY,\tau) \to \mathcal{EM}(T)(F^TX,\tau)\,,\quad q \longmapsto \big(F^TX \xrightarrow{f^\wedge} R(F^TY) \xrightarrow{Rq} R\tau \xrightarrow{\rho} \tau\big)\,.$$

The last map defines an arrow $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(f)\colon \mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(Y) \to \mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(X)$ since we have $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(U) = \mathbb{C}(U,T\Omega) \cong \mathcal{EM}(T)(F^TU,\tau)$.

We have the following natural isomorphism, where K is the comparison in (14).

$$\begin{array}{ccc} \mathbf{Posets} & \xleftarrow{\ \mathbb{P}^{\mathcal{EM}}(\tau,\rho)\ } & \mathcal{EM}(R)^{\mathrm{op}} \\ & {\scriptstyle \mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)}\ \nwarrow \quad \Xi\bullet\Psi \Uparrow\cong \quad \nearrow\ {\scriptstyle K^{\mathrm{op}}} & \\ & \mathcal{K}\ell(U^TRF^T)^{\mathrm{op}} & \end{array} \tag{15}$$

Proof. Note here that the comparison functor K is concretely described as follows: $KX = F^R(F^TX)$ on objects, and use the correspondence

$$\begin{aligned}\mathcal{K}\ell(U^TRF^T)(X,Y) = \mathbb{C}(X,U^TU^RF^RF^TY) &\cong \mathcal{EM}(T)(F^TX,U^RF^RF^TY)\\ &\cong \mathcal{EM}(R)(F^RF^TX,F^RF^TY) = \mathcal{EM}(R)(KX,KY)\end{aligned}$$

for its action on arrows. We claim that the desired natural isomorphism $\Xi \bullet \Psi$ is the (vertical) composite

$$\begin{aligned}\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(X) = \mathbb{C}(X,T\Omega) &\xrightarrow{\Psi_X} \mathcal{EM}(T)(F^TX,\tau)\\ &\xrightarrow{\Xi_X} \mathcal{EM}(R)(F^RF^TX,\rho) = \mathbb{P}^{\mathcal{EM}}(\tau,\rho)(KX)\end{aligned}$$

where Ψ and Ξ are isomorphisms induced by adjunctions.

We have to check that Ψ_X and Ξ_X are order isomorphisms. The map Ψ_X is monotone due to the monotonicity condition on τ (Def. 2.3); so is Ψ_X^{-1}

by Lem. 2.8. Similarly, Ξ_X is monotone by the monotonicity condition on ρ (Def. 4.1); so is Ξ_X^{-1} by Lem. 2.8.

We turn to the naturality: the following diagram must be shown to commute, for each $f\colon X \nrightarrow Y$ in $\mathcal{K}\ell(U^T R F^T)$.

$$\begin{array}{ccccc} \mathbb{C}(Y, T\Omega) & \xrightarrow[\cong]{\Psi_Y} & \mathcal{EM}(T)(F^T Y, \tau) & \xrightarrow[\cong]{\Xi_Y} & \mathcal{EM}(R)(F^R(F^T Y), \rho) \\ {\scriptstyle \mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(f)}\downarrow & & \downarrow{\scriptstyle \rho \circ R(\_) \circ f^\wedge} & & \downarrow{\scriptstyle \mathbb{P}^{\mathcal{EM}}(\tau,\rho)(Kf) = (\_)\circ Kf} \\ \mathbb{C}(X, T\Omega) & \xrightarrow[\cong]{\Psi_X} & \mathcal{EM}(T)(F^T X, \tau) & \xrightarrow[\cong]{\Xi_X} & \mathcal{EM}(R)(F^R(F^T Y), \rho) \ . \end{array} \tag{16}$$

The square on the left commutes by the definition of $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)(f)$ (Prop. 4.3); the one on the right is much like the one in (9) and its commutativity can be proved in the same way. Note here that $Kf = \mu^R_{F^T Y} \circ R(f^\wedge)$.

Since the diagram (16) commutes, and since Ψ and Ξ are order isomorphisms and $\mathbb{P}^{\mathcal{EM}}(\tau,\rho)(Kf)$ is monotone (Prop. 4.2), we have that $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)f$ is monotone. The functoriality of $\mathbb{P}^{\mathcal{K}\ell}(\tau,\rho)$ is easy, too. This concludes the proof. □

5 Examples of 2-Player PT Situations

5.1 Nondeterministic Player and then Nondeterministic Opponent

We continue §3 and locate the monad $\mathcal{UP}$—and the logic of forced predicates—in the general setup of §4. We identify a suitable 2-player PT situation $(\mathcal{P}, 1, \tau_\Box, \mathsf{R_G}, \rho_\mathsf{P})$, in which $T = \mathcal{P}$, $\Omega = 1$ and $\tau = \tau_\Box$ that is from §2.3. The choice of $\tau_\Box$ corresponds to the demonic nature of Opponent's choices: Player can force those properties that hold *whatever choices* Opponent makes.

To introduce the monad $\mathsf{R_G}$ on $\mathcal{EM}(\mathcal{P})$—corresponding to the up-closed powerset construction—we go via the following standard isomorphism.

Lemma 5.1 *Let $C\colon \mathcal{EM}(\mathcal{P}) \to \mathbf{CL}_\bigwedge$ be the functor such that $C\left(\begin{smallmatrix}\mathcal{P}X\\ \downarrow a \\ X\end{smallmatrix}\right) := (X, \sqsubseteq_a)$, where the order is defined by $x \sqsubseteq_a y$ if $x = a\{x, y\}$. Conversely, let $D\colon \mathbf{CL}_\bigwedge \to \mathcal{EM}(\mathcal{P})$ be such that $D(X, \sqsubseteq) := \left(\begin{smallmatrix}\mathcal{P}X\\ \downarrow \bigwedge \\ X\end{smallmatrix}\right)$. Both act on arrows as identities.*

Then C and D constitute an isomorphism $\mathcal{EM}(\mathcal{P}) \mathrel{\overset{\cong}{\rightrightarrows}} \mathbf{CL}_\bigwedge$. □

The monad $\mathsf{R_G}$ is then defined to be the composite $\mathsf{R_G} := D \circ \mathsf{Dw} \circ C$, using the *down-closed powerset monad* Dw on $\mathbf{CL}_\bigwedge$.

$$\mathsf{R_G} \circlearrowright \mathcal{EM}(\mathcal{P}) \underset{C}{\overset{D}{\underset{\longrightarrow}{\overset{\longleftarrow}{\cong}}}} \mathbf{CL}_\bigwedge \circlearrowright \mathsf{Dw} \tag{17}$$

The switch between *up-closed* subsets in $\mathcal{UP}$ and *down-closed* subsets Dw may seem confusing. Later in Prop. 5.3 it is shown that everything is in harmony; and after all it is a matter of presentation since there is an isomorphism $\mathbf{CL}_\bigwedge \mathrel{\overset{\cong}{\rightrightarrows}} \mathbf{CL}_\bigvee$ that reverses the order in each complete lattice. The switch here between up-

and down-closed is essentially because: the bigger the set of Opponent's options is, the smaller the power of Player (to force Opponent to somewhere) is.

Concretely, the monad $\mathsf{Dw}\colon \mathbf{CL}_\bigwedge \to \mathbf{CL}_\bigwedge$ carries a complete lattice $(X, \sqsubseteq)$ to the set $\mathsf{Dw}X := \{S \subseteq X \mid x \sqsubseteq x', x' \in S \Rightarrow x \in S\}$. We equip $\mathsf{Dw}X$ with the inclusion order; this makes $\mathsf{Dw}X$ a complete lattice, with sups and infs given by unions and intersections, respectively. An arrow $f\colon X \to Y$ is carried to $\mathsf{Dw}f\colon \mathsf{Dw}X \to \mathsf{Dw}Y$ defined by $S \mapsto {\downarrow}(\amalg_f S)$. Here ${\downarrow}(\_)$ denotes the downward closure and it is needed to ensure down-closedness (consider a $\bigwedge$-preserving map $f\colon 1 \to 2$, $0 \mapsto 1$ where $0 \sqsubseteq 1$ in 2). The monad structure of Dw is given by: $\eta^{\mathsf{Dw}}_X\colon X \to \mathsf{Dw}X, x \mapsto {\downarrow}\{x\}$; and $\mu^{\mathsf{Dw}}_X\colon \mathsf{Dw}(\mathsf{Dw}X) \to \mathsf{Dw}X, \mathfrak{a} \mapsto \bigcup \mathfrak{a}$. Note in particular that η^{Dw}_X is $\bigwedge$-preserving. As in (17) we define $\mathsf{R}_\mathsf{G} := D \circ \mathsf{Dw} \circ C$.

Finally, let us define the data $\rho_\mathsf{P}\colon \mathsf{R}_\mathsf{G}(\tau_\Box) \to \tau_\Box$ in the 2-player PT situation. Via the isomorphism (17) we shall think of it as an Dw-algebra, where the $\mathcal{P}$-algebra $\tau_\Box$ is identified with the 2-element complete lattice $[\mathtt{ff} \sqsubseteq \mathtt{tt}]$ (the order is because $\tau_\Box\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{ff}$). Therefore we are looking for a $\bigwedge$-preserving map

$$\mathsf{Dw}[\mathtt{ff} \sqsubseteq \mathtt{tt}] \;=\; \big[\, \emptyset \sqsubseteq \{\mathtt{ff}\} \sqsubseteq \{\mathtt{ff}, \mathtt{tt}\} \,\big] \;\xrightarrow{C\rho_\mathsf{P}}\; [\mathtt{ff} \sqsubseteq \mathtt{tt}]$$

subject to the conditions of an Eilenberg-Moore algebra in (4). In fact such $C(\rho_\mathsf{P})$ is uniquely determined: preservation of $\top$ forces $(C\rho_\mathsf{P})\{\mathtt{ff}, \mathtt{tt}\} = \mathtt{tt}$; the unit law forces $(C\rho_\mathsf{P})\{\mathtt{ff}\} = \mathtt{ff}$ and monotonicity of $C\rho_\mathsf{P}$ then forces $(C\rho_\mathsf{P})\emptyset = \mathtt{ff}$.

Lemma 5.2 *$(\mathcal{P}, 1, \tau_\Box, \mathsf{R}_\mathsf{G}, \rho_\mathsf{P})$ thus obtained is a 2-player PT situation.*

Proof. It remains to check the monotonicity condition (Def. 4.1) for ρ_P. We shall again think in terms of complete lattices and $\bigwedge$-preserving maps; then the requirement is that the map $\big(X \xrightarrow{f} [\mathtt{ff} \sqsubseteq \mathtt{tt}]\big) \mapsto \big(\mathsf{Dw}X \xrightarrow{\rho_\mathsf{P} \circ \mathsf{Dw}f} [\mathtt{ff} \sqsubseteq \mathtt{tt}]\big)$ is monotone. Assume $g \sqsubseteq f$, $S \in \mathsf{Dw}X$ and $(\rho_\mathsf{P} \circ \mathsf{Dw}f)(S) = \mathtt{ff}$. It suffices to show that $(\rho_\mathsf{P} \circ \mathsf{Dw}g)(S) = \mathtt{ff}$; this follows from the observation that, for $h = f$ or g,

$$(\rho_\mathsf{P} \circ \mathsf{Dw}h)(S) = \mathtt{ff} \iff (\mathsf{Dw}h)S \subseteq \{\mathtt{ff}\} \iff \forall x \in S.\, hx = \mathtt{ff}\ . \qquad \Box$$

Let us check that the logic $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Box, \rho_\mathsf{P})$ associated with this 2-player PT situation is indeed the logic of forced predicates in §3.1. For instance, we want "computations" $X \to U^\mathcal{P}\mathsf{R}_\mathsf{G}F^\mathcal{P}Y$ to coincide with "computations" $X \to \mathcal{U}\mathcal{P}Y$.

Proposition 5.3 *For any set X we have $U^\mathcal{P}\mathsf{R}_\mathsf{G}F^\mathcal{P} = \mathcal{U}\mathcal{P}X$. In fact they are isomorphic as complete lattices, that is, $\mathsf{Dw} \circ C \circ F^\mathcal{P} = \mathcal{U}\mathcal{P}\colon \mathbf{Sets} \to \mathbf{CL}_\bigwedge$ where the functor $\mathcal{U}\mathcal{P}$ is equipped with the inclusion order.*

Proof. Given $X \in \mathbf{Sets}$, the definition of C dictates that $C(F^\mathcal{P}X) = (\mathcal{P}X, \supseteq)$ and its order be given by the reverse inclusion order. Hence $\mathsf{Dw}(C(F^\mathcal{P}X))$ is the collection of families $\mathfrak{a} \subseteq \mathcal{P}X$ that are $\supseteq$-down-closed, i.e. $\subseteq$-up-closed. It is easily checked that the two functors coincide on arrows, too, using the characterization on the left in (13). $\Box$

Next we describe the logic $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Box, \rho_{\mathsf{P}})$ (Prop. 4.3) in concrete terms. We base ourselves again in $\mathbf{CL}_\bigwedge$ via the isomorphism $\mathcal{EM}(\mathcal{P}) \cong \mathbf{CL}_\bigwedge$ in (17). Consider a postcondition $q\colon Y \to \mathcal{P}1$ and a branching computation $f\colon X \to \mathcal{UP}Y$. These are in one-to-one correspondences with the following arrows in $\mathbf{CL}_\bigwedge$:

$$\begin{aligned} q^\wedge\colon\ & C(F^{\mathcal{P}}Y) = (\mathcal{P}Y, \supseteq) \longrightarrow [\mathtt{ff} \sqsubseteq \mathtt{tt}] = C(\tau_\Box)\ , \\ f^\wedge\colon\ & C(F^{\mathcal{P}}X) = (\mathcal{P}X, \supseteq) \longrightarrow \mathsf{Dw}(\mathcal{P}Y, \supseteq) = C(\mathsf{R}_{\mathsf{G}}(F^{\mathcal{P}}Y))\ , \end{aligned}$$

where we used Prop. 5.3. Since $q^\wedge$ are $f^\wedge$ are $\bigwedge$-preserving, we have

$$q^\wedge W = q^\wedge(\textstyle\bigcup_{y\in W}\{y\}) = q^\wedge(\bigwedge_{y\in W}\{y\}) = \bigwedge_{y\in W} q^\wedge\{y\} = \bigwedge_{y\in W} qy\ ;$$

and similarly $f^\wedge S = \bigcap_{x\in S} fx$. Recall that $\mathsf{Dw}(\mathcal{P}Y, \supseteq)$ has the inclusion order.

Now Prop. 4.3 states that the weakest precondition $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Box, \rho_{\mathsf{P}})(f)(q)$ is the arrow $X \to \mathcal{P}1$ that corresponds, via the adjunction $C \circ F^{\mathcal{P}} \dashv U^{\mathcal{P}} \circ D$, to

$$(\mathcal{P}X, \supseteq) \xrightarrow{f^\wedge} \mathsf{Dw}(\mathcal{P}Y, \supseteq) \xrightarrow{\mathsf{Dw}(q^\wedge)} \mathsf{Dw}[\mathtt{ff} \sqsubseteq \mathtt{tt}] \xrightarrow{\rho_{\mathsf{P}}} [\mathtt{ff} \sqsubseteq \mathtt{tt}] \quad \text{in } \mathbf{CL}_\bigwedge.$$

Unweaving definitions it is straightforward to see that, for $S \subseteq X$,

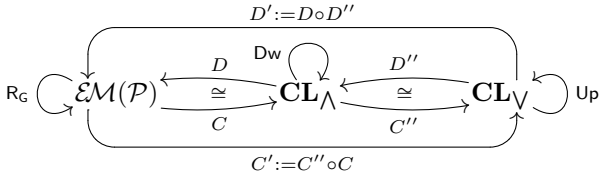
$$\begin{aligned} &\big(\rho_{\mathsf{P}} \circ \mathsf{Dw}(q^\wedge) \circ f^\wedge\big)S = \mathtt{tt} \iff \exists W \subseteq Y.\, \big(\forall x \in S.\, W \in fx \wedge \forall y \in W.\, qy = \mathtt{tt}\big)\ ; \\ &\text{therefore } \mathbb{P}^{\mathcal{K}\ell}(\tau_\Box, \rho_{\mathsf{P}})(f)(q)(x) = \mathtt{tt} \iff \exists W \subseteq Y.\, \big(W \in fx \wedge \forall y \in W.\, qy = \mathtt{tt}\big)\ . \end{aligned} \tag{18}$$

The last condition reads: among the set fx of possible moves of Player, there exists a move W, from which q holds no matter what Opponent's move y is. Therefore $\mathbb{P}^{\mathcal{K}\ell}(\tau_\Box, \rho_{\mathsf{P}})(f)(q)(x) = \mathtt{tt}$ if Player can *force* the predicate q from x after the (two-layer branching) computation f.

5.2 Nondeterministic Opponent and then Nondeterministic Player

We change the order of Player and Opponent: O moves first and then P moves. The general setup in §4 successfully models this situation too, with a choice of a 2-player PT situation $(\mathcal{P}, 1, \tau_\Diamond, \mathsf{R}_{\mathsf{G}}, \rho_{\mathsf{O}})$ that is dual to the previous one.

The modality $\tau_\Diamond$ is from §2.3. Although the monad R_{G} is the same as in §5.1, we now prefer to present it in terms of $\mathcal{EM}(\mathcal{P}) \cong \mathbf{CL}_\bigvee$ instead of $\mathbf{CL}_\bigwedge$. The reason is that this way the algebra $\tau_\Diamond$ gets identified with $[\mathtt{ff} \sqsubseteq \mathtt{tt}]$, which is intuitive. The situation is as follows.



(19)

The functors C'' and D'' carries a complete lattice $(X, \sqsubseteq)$ to $(X, \sqsupseteq)$, reversing the order. The monad Up is defined by $\mathsf{Up} := C'' \circ \mathsf{Dw} \circ D''$; concretely it carries

$(X, \sqsubseteq)$ to the set of its up-closed subsets, equipped with the *reverse* inclusion order $\supseteq$. That is,

$$\mathsf{Up}(X, \sqsubseteq) \;:=\; \big(\, \{S \subseteq X \mid S \ni x \sqsubseteq x' \Rightarrow x' \in S\}\,,\; \supseteq \big)\;.$$

We have $\mathsf{R_G} = D \circ \mathsf{Dw} \circ C = D' \circ \mathsf{Up} \circ C'$.

The modality $\rho_{\mathsf{O}} \colon \mathsf{R_G}(\tau_\Diamond) \to \tau_\Diamond$ is identified, via the isomorphism C' in (19), with an Up-algebra on $[\mathtt{ff} \sqsubseteq \mathtt{tt}]$. The latter is a $\bigvee$-preserving map

$$\mathsf{Up}[\mathtt{ff} \sqsubseteq \mathtt{tt}] = \big[\, \{\mathtt{ff}, \mathtt{tt}\} \sqsubseteq \{\mathtt{tt}\} \sqsubseteq \emptyset \,\big] \;\overset{C'\rho_{\mathsf{O}}}{\longrightarrow}\; [\mathtt{ff} \sqsubseteq \mathtt{tt}]\;;$$

note here that the order in $\mathsf{Up}(X, \sqsubseteq)$ is the reverse inclusion $\supseteq$. Such $C'\rho_{\mathsf{O}}$ is uniquely determined (as before): the unit law forces $(C'\rho_{\mathsf{O}})\{\mathtt{tt}\} = \mathtt{tt}$; preservation of $\bot$ forces $(C'\rho_{\mathsf{O}})\{\mathtt{tt}, \mathtt{ff}\} = \mathtt{ff}$; and then by monotonicity $(C'\rho_{\mathsf{O}})\emptyset = \mathtt{tt}$.

It is straightforward to see that $(\mathcal{P}, 1, \tau_\Diamond, \mathsf{R_G}, \rho_{\mathsf{O}})$ is indeed a 2-player PT situation; the proof is symmetric to the one in §5.1. Also symmetrically, the weakest precondition semantics $\mathbb{P}^{\mathcal{KL}}(\tau_\Diamond, \rho_{\mathsf{O}})$ is concretely described as follows: given a postcondition $q \colon Y \to \mathcal{P}1$ and a branching computation $f \colon X \to \mathcal{UP}Y$,

$$\mathbb{P}^{\mathcal{KL}}(\tau_\Diamond, \rho_{\mathsf{O}})(f)(q)(x) = \mathtt{tt} \iff \forall W \subseteq Y.\, \big(W \in fx \Rightarrow \exists y \in W.\, qy = \mathtt{tt}\big)\;.$$

This is dual to (18) and reads: whatever move W Opponent takes, there exists Player's move $y \in W$ so that q holds afterwards.

We note that the analogue of Prop. 5.3 becomes: $\mathsf{Up} \circ C' \circ F^{\mathcal{P}} = \mathcal{UP} \colon \mathbf{Sets} \to \mathbf{CL}_{\bigvee}$, where each $\mathcal{UP}X$ is equipped with the *reverse* inclusion order. This order ($\mathfrak{a} \sqsubseteq \mathfrak{b}$ in $\mathcal{UP}X$ if $\mathfrak{a} \supseteq \mathfrak{b}$) is intuitive if we think of $\sqsubseteq$ as the power of Player.

Remark 5.4 The constructions have been described in concrete terms; this is for intuition. An abstract view is possible too: the modality $\tau_\Diamond$ is the dual of $\tau_\Box$ via the swapping σ (see (7)); and the other modality ρ_{O} is also the dual of ρ_{P} by $\rho_{\mathsf{O}} = \big(\, \mathsf{R_G}(\tau_\Diamond) \overset{\mathsf{R_G}\sigma}{\to} \mathsf{R_G}(\tau_\Box) \overset{\rho_{\mathsf{P}}}{\to} \tau_\Box \overset{\sigma}{\to} \tau_\Diamond \,\big)$.

5.3 Nondeterministic Opponent and then Probabilistic Player

In our last example Opponent O moves nondeterministically first, and then Player P moves probabilistically. Such nested branching is in many process-theoretic models of probabilistic systems (see §3, in particular §3.2), most notably in Segala's *probabilistic automata* [27]. We identify a 2-player PT situation $(\mathcal{D}, 1, \tau_{\mathrm{total}}, \mathcal{C}v, \rho_{\mathrm{inf}})$ for this situation; then the associated logic $\mathbb{P}^{\mathcal{KL}}(\tau_{\mathrm{total}}, \rho_{\mathrm{inf}})$ is that of the probabilistic predicate transformers in [31]. The modality τ_{total} is from §2.3. The other components ($\mathcal{C}v$, ρ_{inf}) are to be described in terms of *convex cones* and their *convex subsets*.

In what follows a $\mathcal{D}$-algebra is referred to as a *convex cone*, adopting the notation $\sum_{i\in I} w_i x_i$ to denote $a\big([x_i \mapsto w_i]_{i\in I}\big) \in X$ in a convex cone $a \colon \mathcal{D}X \to X$. Here I is a countable index set,[3] $w_i \in [0,1]$, and $\sum_{i\in I} w_i \le 1$. Note that,

[3] The countability requirement is superfluous since, if $\sum_{i\in I} p_i = 1$, then only countably many p_i's are nonzero.

since $\mathcal{D}$ is the *sub*distribution monad, the zero distribution $\mathbf{0}$ is allowed in $\mathcal{D}X$ and therefore a convex cone $a\colon \mathcal{D}X \to X$ has its *apex* $a\mathbf{0} \in X$. Similarly, a morphism of $\mathcal{D}$-algebras is referred to as a *convex linear map*.

Definition 5.5 (convex subset) A subset $S \subseteq X$ of a convex cone $a\colon \mathcal{D}X \to X$ is said to be *convex* if, for any $p_i \in [0,1]$ such that $\sum_{i\in I} p_i = 1$ and any $x_i \in S$, the convex combination $\sum_{i\in I} p_i x_i$ belongs to S.

We emphasize that in the last definition $\sum_i p_i$ is required to be $= 1$. This is unlike $\sum_i w_i \leq 1$ in the definition of convex cone. Therefore a convex subset S need not include the apex $a\mathbf{0}$; one can think of the base of a 3-dimensional cone as an example. This variation in the definitions is also found in [34, §2.1.2]; one reason is technical: if we allow $\sum_i p_i \leq 1$ then it is hard to find the monad unit of $\mathcal{C}v$ (see below). Another process-theoretic reason is described later in Rem. 5.8.

Definition 5.6 (the monad $\mathcal{C}v$) The functor $\mathcal{C}v\colon \mathcal{EM}(\mathcal{D}) \to \mathcal{EM}(\mathcal{D})$ carries a convex cone $a\colon \mathcal{D}X \to X$ to $\mathcal{C}vX := \{S \subseteq X \mid S \text{ is convex}\}$; the latter is a convex cone by

$$\textstyle\sum_i w_i S_i \;:=\; \{\, \sum_i w_i x_i \mid x_i \in S_i \,\} \;.$$

It is easy to see that $\sum_i w_i S_i$ is indeed a convex subset of X. Given a convex linear map $f\colon X \to Y$, $\mathcal{C}vf\colon \mathcal{C}vX \to \mathcal{C}vY$ is defined by $(\mathcal{C}vf)S := \amalg_f S$, which is obviously convex in Y, too.

The monad structure of $\mathcal{C}v$ is as follows. Its unit is $\eta^{\mathcal{C}v}_X := \{\_\}\colon X \to \mathcal{C}vX$; note that a singleton $\{x\}$ is a convex subset of X (Def. 5.5). The monad multiplication is $\mu^{\mathcal{C}v}_X := \bigcup\colon \mathcal{C}v(\mathcal{C}vX) \to \mathcal{C}vX$. It is easy to see that $\eta^{\mathcal{C}v}_X$ and $\mu^{\mathcal{C}v}_X$ are convex linear maps, and that they satisfy the monad axioms.

We introduce the last component, namely the modality $\rho_{\inf}\colon \mathcal{C}v(\tau_{\text{total}}) \to \tau_{\text{total}}$. A convex subset S of the carrier $\mathcal{D}1 = [0,1]$ of τ_{total} is nothing but an interval (its endpoints may or may not be included); $\rho_{\inf}$ then carries such S to its infimum $\inf S \in [0,1]$. That $\rho_{\inf}$ is convex linear, and that it satisfies the Eilenberg-Moore axioms, are obvious.

Much like in Lem. 5.2, we obtain:

Lemma 5.7 $(\mathcal{D}, 1, \tau_{\text{total}}, \mathcal{C}v, \rho_{\inf})$ *thus obtained is a 2-player PT situation.* □

The resulting logic $\mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{total}}, \rho_{\inf})$ is as follows. Given a postcondition $q\colon Y \to \mathcal{D}1$ and a computation $f\colon X \to U^{\mathcal{D}}\mathcal{C}vF^{\mathcal{D}}Y$, the weakest precondition is

$$\mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{total}}, \rho_{\inf})(f)(q)(x) \;=\; \inf\big\{\, \textstyle\sum_{y\in Y} d(y)\cdot q(y) \,\big|\, d \in f(x) \,\big\} \;. \qquad (20)$$

Here d is a subdistribution chosen by Opponent; and the value $\sum_{y\in Y} d(y)\cdot q(y)$ is the expected value of the random variable q under the distribution d. Therefore the weakest precondition computed above is the least expected value of q when Opponent picks a distribution in harm's way. This is the same as in [31].

Remark 5.8 The use of the convex powerset construction, instead of (plain) powersets, was motivated in §3.2 through the technical difficulty in getting a monad. Convex powersets are commonly used in the process-theoretic study of probabilistic systems, also because they model a *probabilistic scheduler*: Opponent (called a *scheduler* in this context) can not only pick one distribution but also use randomization in doing so. See e.g. [2].

The definition of convex subset (Def. 5.5)—where we insist on $\sum_i p_i = 1$ instead of ≤ 1—is natural in view of the logic $\mathbb{P}^{\mathcal{K}\ell}(\tau_{\text{total}}, \rho_{\text{inf}})$ described above. Relaxing this definition entails that the zero distribution $\mathbf{0}$ is always included in a "convex subset," and hence always in Opponent's options. This way, however, the weakest precondition in (20) can always be forced to 0 and the logic gets trivial.

We can also model the situation where the roles of Player and Opponent are swapped: we can follow the same path as in Rem. 5.4 and obtain a 2-player PT situation $(\mathcal{D}, 1, \tau_{\text{partial}}, \mathcal{C}v, \rho_{\text{sup}})$; the resulting modality ρ_{sup} carries an interval to its supremum.

6 Conclusions and Future Work

Inspired by Jacobs' recent work [16, 17] we pursued a foundation of predicate transformers (more specifically weakest precondition semantics) based on an order-enriched monad. There different notions of modality (such as "may" vs. "must") are captured by Eilenberg-Moore algebras. Nested branching with two conflicting players can be modeled in a modular way, too, by a monad R on an Eilenberg-Moore category $\mathcal{EM}(T)$. Instances of this generic framework include probabilistic weakest preconditions, those augmented with nondeterminism, and the logic of forced predicates in games.

As future work we wish to address the components in the picture (2–3) that are missing in the current framework. A generic weakest precondition calculus presented in a *syntactic* form is another direction. Most probably relationships between monads and algebraic theories (see e.g. [32]) will be exploited there. So-called *healthiness conditions*—i.e. characterization of the image of $\mathbb{P}^{\mathcal{K}\ell}(\tau)$ in (8), to be precise its action on arrows—are yet another topic, generalizing [5, 31].

The current work is hopefully a step forward towards a coalgebraic theory of automata (on infinite trees), games and fixed-point logics. For example, we suspect that our categorical formulation of the logic of forced predicates be useful in putting *game (bi)simulation* (studied e.g. in [22, 36]) in coalgebraic terms. Possibly related, we plan to work on the relationship to the coalgebraic theory of traces and simulations formulated in a Kleisli category [11, 13] since all the monads in Example 2.2 fit in this trace framework.

In this paper we relied on an order-enrichment of a monad to obtain the entailment order. We are nevertheless interested in what our current framework brings for other monads, like the ones that model computational effects [29] (global state, I/O, continuation, etc.). Also interesting is a higher-order extension

of the current work, where the logic will probably take the form of dependent types. Related work in this direction is [20].

Acknowledgments Thanks are due to Kazuyuki Asada, Kenta Cho, Corina Cîrstea and Tetsuri Moriya for useful discussions. The author is supported by Grants-in-Aid for Young Scientists (A) No. 24680001, JSPS, and by Aihara Innovative Mathematical Modelling Project, FIRST Program, JSPS/CSTP.

References

1. Barr, M., Wells, C.: Toposes, Triples and Theories. Springer, Berlin (1985), available online.
2. Cattani, S., Segala, R.: Decision algorithms for probabilistic bisimulation. In: Brim, L., Jancar, P., Kretínský, M., Kucera, A. (eds.) CONCUR. Lecture Notes in Computer Science, vol. 2421, pp. 371–385. Springer (2002)
3. Cheung, L.: Reconciling Nondeterministic and Probabilistic Choices. Ph.D. thesis, Radboud Univ. Nijmegen (2006)
4. Cîrstea, C.: A coalgebraic approach to linear-time logics. In: FoSSaCS (2014), to appear
5. Dijkstra, E.W.: A Discipline of Programming. Prentice Hall (1976)
6. Foulis, D.J., Bennett, M.K.: Effect algebras and unsharp quantum logics. Found. Physics 24(10), 1331–1352 (1994)
7. Giry, M.: A categorical approach to probability theory. In: Proc. Categorical Aspects of Topology and Analysis. Lect. Notes Math., vol. 915, pp. 68–85 (1982)
8. Grädel, E., Thomas, W., Wilke, T. (eds.): Automata, Logics, and Infinite Games: A Guide to Current Research 2001], Lecture Notes in Computer Science, vol. 2500. Springer (2002)
9. Hansen, H.H., Kupke, C.: A coalgebraic perspective on monotone modal logic. Electr. Notes Theor. Comput. Sci. 106, 121–143 (2004)
10. Hansen, H.H., Kupke, C., Pacuit, E.: Neighbourhood structures: Bisimilarity and basic model theory. Logical Methods in Computer Science 5(2) (2009)
11. Hasuo, I.: Generic forward and backward simulations II: Probabilistic simulation. In: Gastin, P., Laroussinie, F. (eds.) CONCUR. Lect. Notes Comp. Sci., vol. 6269, pp. 447–461. Springer (2010)
12. Hasuo, I., Hoshino, N.: Semantics of higher-order quantum computation via geometry of interaction. In: LICS. pp. 237–246. IEEE Computer Society (2011)
13. Hasuo, I., Jacobs, B., Sokolova, A.: Generic trace semantics via coinduction. Logical Methods in Comp. Sci. 3(4:11) (2007)
14. Hoare, C.A.R.: An axiomatic basis for computer programming. Commun. ACM 12, 576–580, 583 (1969)
15. Jacobs, B.: Categorical Logic and Type Theory. North Holland, Amsterdam (1999)
16. Jacobs, B.: New directions in categorical logic, for classical, probabilistic and quantum logic. Logical Methods in Comp. Sci. (2013), to appear
17. Jacobs, B.: Measurable spaces and their effect logic. In: LICS. pp. 83–92. IEEE Computer Society (2013)
18. Jones, C.: Probabilistic Non-Determinism. Ph.D. thesis, Univ. Edinburgh (1990)
19. Jurdzinski, M.: Small progress measures for solving parity games. In: Reichel, H., Tison, S. (eds.) STACS. Lecture Notes in Computer Science, vol. 1770, pp. 290–301. Springer (2000)

20. Katsumata, S.: Relating computational effects by $\top\top$-lifting. Inf. Comput. 222, 228–246 (2013)
21. Katsumata, S., Sato, T.: Preorders on monads and coalgebraic simulations. In: Pfenning, F. (ed.) FoSSaCS. Lecture Notes in Computer Science, vol. 7794, pp. 145–160. Springer (2013)
22. Kissig, C., Venema, Y.: Complementation of coalgebra automata. In: Kurz, A., Lenisa, M., Tarlecki, A. (eds.) CALCO. Lect. Notes Comp. Sci., vol. 5728, pp. 81–96. Springer (2009)
23. Kock, A.: Monads and extensive quantities (2011), arXiv:1103.6009
24. Kozen, D.: Semantics of probabilistic programs. J. Comput. Syst. Sci. 22(3), 328–350 (1981)
25. Kupke, C., Pattinson, D.: Coalgebraic semantics of modal logics: An overview. Theor. Comput. Sci. 412(38), 5070–5094 (2011)
26. Kupke, C., Venema, Y.: Coalgebraic automata theory: Basic results. Logical Methods in Computer Science 4(4) (2008)
27. Lynch, N.A., Segala, R., Vaandrager, F.W.: Compositionality for probabilistic automata. In: Amadio, R.M., Lugiez, D. (eds.) CONCUR 2003. Lect. Notes Comp. Sci., vol. 2761, pp. 204–222. Springer (2003)
28. Mac Lane, S.: Categories for the Working Mathematician. Springer, Berlin, 2nd edn. (1998)
29. Moggi, E.: Notions of computation and monads. Inf. & Comp. 93(1), 55–92 (1991)
30. Morgan, C.: Programming from Specifications. Prentice-Hall (1990)
31. Morgan, C., McIver, A., Seidel, K.: Probabilistic predicate transformers. ACM Trans. Program. Lang. Syst. 18(3), 325–353 (1996)
32. Plotkin, G.D., Power, J.: Adequacy for algebraic effects. In: Honsell, F., Miculan, M. (eds.) FoSSaCS. Lecture Notes in Computer Science, vol. 2030, pp. 1–24. Springer (2001)
33. Sokolova, A.: Coalgebraic Analysis of Probabilistic Systems. Ph.D. thesis, Techn. Univ. Eindhoven (2005)
34. Tix, R., Keimel, K., Plotkin, G.D.: Semantic domains for combining probability and non-determinism. Elect. Notes in Theor. Comp. Sci. 129, 1–104 (2005)
35. Varacca, D., Winskel, G.: Distributing probabililty over nondeterminism. Math. Struct. in Comp. Sci. 16(1), 87–113 (2006)
36. Venema, Y., Kissig, C.: Game bisimulations between basic positions. Talk at Highlights of Logic, Games and Automata, Paris (2013)
37. Winskel, G.: The Formal Semantics of Programming Languages. MIT Press (1993)