A Sound Calculus for a Logic of Belief-Aware Cyber-Physical Systems

João G. Martins **André Platzer** **João Leite**

July 2019
CMU-CS-19-116

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Supported by the Alexander von Humboldt Foundation, NSF grant CNS-1446712, CMU | Portugal grant SFRH/BD/51886/2012, and PTDC/CCI-COM/30952/2017. Any opinions, findings, and conclusions or recommendations expressed in this publication are thoseof the author(s) and do not necessarily reflect the views of the National Science Foundation.

Keywords: differential dynamic logic, dynamic epistemic logic, sequent calculus, hybrid systems, cyber-physical systems

Abstract

Cyber-physical systems (CPS), such as airplanes, operate based on sensor and communication data, i.e. on potentially noisy or erroneous beliefs about the world. Realistic CPS models must therefore incorporate the notion of beliefs if they are to provide safety guarantees in practice as well as in theory. To fundamentally address this challenge, this paper introduces a first-principles framework for reasoning about CPS models where control decisions are explicitly driven by controller beliefs arrived at through observation and reasoning. We extend the differential dynamic logic $\mathsf{d}\mathcal{L}$ for CPS dynamics with belief modalities, and a learning operator for belief change. This new dynamic doxastic differential dynamic logic $\mathsf{d}^4\mathcal{L}$ does due justice to the challenges of CPS verification by having 1) real arithmetic for describing the world and beliefs about the world; 2) continuous and discrete world change; 3) discrete belief change by means of the learning operator. We develop a sound sequent calculus for $\mathsf{d}^4\mathcal{L}$, which enables us to illustrate the applicability of $\mathsf{d}^4\mathcal{L}$ by proving the safety of a simplified belief-triggered controller for an airplane.

1 Introduction

Cyber-physical systems (CPS) mix discrete cyber change and continuous physical change. Examples of CPS include self-driving cars, airplane autopilots, and industrial machines. With widespread espousal of automation in transportation, it is imperative that we develop methods capable of verifying the safety of the algorithms driving the CPSs on which human lives will increasingly depend.

However, because CPSs rely on sensors and partial human operation, both of which are imperfect, they face a possible discrepancy between reality, and the perception, understanding and beliefs thereof. Critical system components are engineered to be exceptionally reliable, so safety incidents often originate from just such a discrepancy between what is believed to be true versus what is actually true. This can be highlighted by three (of many) tragedies, some now known to be preventable, e.g., through neutral control inputs [5, 1, 12]. However, non-critical sensor failures led to erroneous pilot beliefs. These beliefs resulted in the pilots' inability to perform informed, safe control decisions, leading to 574 fatalities in these three incidents alone.

Verification efforts for practical system designs must therefore augment initial analyses which assume perfect information with an awareness of factors such as sensor errors, actuator disturbances, and, crucially, incomplete or incorrect perceptions of the world. Ideally, such factors ought to become an explicit part of the model so that CPS design and verification engineers can confront this challenge of uncertainty head on at design time, before safety violations occur.

We argue that the notion of beliefs (*doxastics*) about the state of the world, which has been extensively studied, can succinctly capture such phenomena. We develop a first-principles language and verification method for reasoning about *changing beliefs in a changing world*. Using this language, CPS designers may create more realistic controllers whose decisions are explicitly driven by their beliefs. The consequences of such decisions are borne out in the continuous-time and continuous-space evolution of these *belief-aware CPS*.

In this new paradigm, control decisions are grounded *only* in what can be observed and reasoned. By providing the tools to develop such *belief-triggered controllers*, we help bridge the gap between the theoretical safety of *CPS models*, and the practical safety of the *CPS vehicles* that will soon be driving and flying us to our destinations.

2 Technical Approach

Our approach is to integrate a framework for specifying and verifying real-world CPS with a suitable notion of dynamic beliefs. The result should be a single cohesive framework capable of complex reasoning about changing beliefs in a changing world, as required by belief-aware CPSs.

Work on control-theoretic *robust* solutions for CPS models seem promising, since they entail asymptotical steering towards a desired target domain despite perturbations in the system [11]: sensor and actuator noise could be modeled as perturbations rather than beliefs. However, perturbation analysis does not capture the complex causal relationship from observation, to reasoning, to actuation in an explicit way that can lead to e.g. malfunction checklists or pilot best practices. Accurate analyses for safety incidents such as [5, 1, 12] require the power to 1) model agents with reasoning capabilities, and 2) leverage complex logical arguments about perception versus fact in the pursuit of safety guarantees.

The differential dynamic logic $\mathsf{d}\mathcal{L}$ [16, 17, 19] is a successful tool for designing and verifying belief-*unaware* CPS, i.e. a "changing world" in a real-valued domain. Dynamic epistemic logics (DELs), on the other hand, deal with changing knowledge (which is tightly connected to beliefs[1]) in a propositional static world that never changes [3, 4, 10, 7], again through the lens of modal logic. Some previous work exists at the intersection of these two. However, belief-aware CPS requires unobservable world change under the real numbers, which is in conflict with the public propositional world-change in [6]; and a more comprehensive and less restrictive treatment of belief that goes beyond using the underlying dynamic modalities of world-change to emulate noise as in [14].

Since both $\mathsf{d}\mathcal{L}$ and DELs are dynamic modal logics, they are prime candidates for inspiration in the pursuit of a unified dynamic modal logic that can reason about changing beliefs in a changing world. We develop the *dynamic doxastic differential dynamic logic* $\mathsf{d}^4\mathcal{L}$, as an extension of $\mathsf{d}\mathcal{L}$ with 1) belief modalities, and 2) a learning operator for describing belief-change, inspired by DELs.

This new framework requires a fundamental conceptual shift in the design of CPS. Let `ctrl` be a program describing control decisions (e.g. a pilot pressing a button), and `plant` be a program for continuous evolution (e.g. an airplane flying). In the current, belief-unaware $\mathsf{d}\mathcal{L}$ paradigm, the primary mode of establishing the safety of CPS is by the validity of a formula $pre \rightarrow [(\mathtt{ctrl;\ plant})^*]\, safe$. It states that, starting from precondition *pre*, every possible execution of the program $(\mathtt{ctrl;\ plant})^*$ ends with the safety property *safe* being true, with the star * operator repeating `ctrl` followed by `plant` any number of times.

Example 1. *As a running example, suppose an airplane is controlled by directly setting its vertical velocity to 1 or -1 in thousands of feet per second. The safety goal of the controller is to keep the airplane above ground:*

1. $pre \equiv safe \equiv (alt > 0)$*, i.e., the airplane is above ground.*

2. $\mathtt{ctrl} \equiv (?alt > 1; yv := -1) \cup yv := 1$*, in which two things may happen, on either side of* $\cup$*. If the airplane is above 1000ft (*$?alt > 1$*), it may descend by setting vertical velocity yv to -1000 feet per second. Alternatively, it can climb with* $yv := 1$*, which may always happen since this action has no ? test.*

3. $\mathtt{plant} \equiv t := 0; t' = 1, alt' = yv \ \&\ t \leq 1$ *describes, using differential equations, that altitude changes with vertical velocity (*$alt' = yv$*) for a maximum of 1 unit of time using time counter* $t' = 1$*. The* evolution domain constraint $t \leq 1$ *bounds how much time may pass before the pilot reassesses this choice.*

Intuitively, this CPS is safe because the controller can only decide to descend if it is high enough above ground such that descending for 1 second at a velocity of -1000 feet per second, traveling a total of 1000 feet, keeps it above ground. This condition is based on ontic *(real world, or factual) truth and does not capture the reality that altitude is read from a noisy altimeter, and that* pilot beliefs *trigger actions, not ontics.*

[1]Beliefs may be erroneous, knowledge may not.

In contrast, in *belief-aware* CPS, control decisions are triggered by some belief $B_a(\phi)$, not ontic truth ϕ. This minor syntactic change belies the complexity of the underlying paradigm shift. The CPS model must now explicitly describe how an agent learns about the world and acquires such beliefs $B_a(\phi)$. In $\mathsf{d}^4\mathcal{L}$, this process of observation and reasoning is specified by means of a *learning operator*.

A $\mathsf{d}\mathcal{L}$ program α, describing ontic change, does not alter beliefs. In contrast, a learning operator program $L_a(\alpha)$ changes *only* agent a's beliefs, with the change described by α becoming doxastic rather than ontic. The pattern $\alpha; L_a(\alpha)$ describes *observed* ontic change, which also affects beliefs. This learning operator may be used in a program `obs` to describe the agent's learning processes of observation and reasoning. This leads to the addition of the belief-changing `obs` to the safety formula *pre* $\rightarrow [(\texttt{obs; ctrl; plant})^*]$ *safe* used for belief-aware CPS.

Example 2. *Consider a belief-triggered controller for the airplane of Example 1. The model now incorporates the fact that observation is imperfect, and that the altimeter, while operating properly, has some noise bounded by* $\varepsilon > 0$*.*

1. $\texttt{obs} \equiv L_a(?alt - alt_a < \varepsilon)$. *The pilot* a *learns, by observing the altimeter with known error bounds* ϵ*, that the* perceived *altitude* alt_a *can be lower than the* true *altitude* alt *by at most* ε*. Thus, the belief* $B_a(alt - alt_a < \varepsilon)$ *comes to be.*

2. $\texttt{ctrl} \equiv (?B_a(alt_a - \varepsilon > 1); yv := -1) \cup yv := 1)$. *Climbing, being safe, remains an always acceptable choice. However, the trigger for descending is that the pilot* believes *that the* perceived *altitude with worst-case noise is still high enough for the airplane to descend for one second, i.e.* $B_a(alt_a - \varepsilon > 1)$*.*

We must add $\varepsilon > 0$ *to pre, but* `plant` *does not change since beliefs do not directly affect the behavior of the real world: they do so only through agent actions.*

More generally, $\mathsf{d}^4\mathcal{L}$ allows for arbitrary combinations of ontic $\mathsf{d}\mathcal{L}$ actions and the learning operator, representing any interleaving of physical and doxastic change, the former potentially unobservable, and the latter potentially imperfect, e.g. through noisy sensors.

3 Syntax of $\mathsf{d}^4\mathcal{L}$

In this section, we will describe $\mathsf{d}^4\mathcal{L}$ terms, formulas and programs. As in $\mathsf{d}\mathcal{L}$, real arithmetic is used to accurately model CPSs. Thus, terms are real-valued.

The safety of well-functioning belief-aware CPS is often predicated on beliefs being grounded in reality so that informed decisions can be made, cf. formula $B_a(alt - alt_a < \varepsilon)$ of Example 2, where perceived altitude can underestimate factual altitude by at most ϵ. This relation between belief and truth is at the core of many safety arguments, and should be describable within the logic. We must therefore be able to refer to both ontic (factual) and doxastic (belief) states in the same context, as in $B_a(alt - alt_a < \varepsilon)$.

3.1 $\mathsf{d}^4\mathcal{L}$ Terms and Formulas

State variables describe ontic truth, e.g. *alt* is the airplane's real altitude. Doxastic variable alt_a is agent a's perception of *alt*. Basic arithmetic is also in the language, e.g. $x - y$. Constants $c \in \mathbb{Q}$ allow for digitally representable numbers in the syntax, e.g. 2.5 but not π, though the semantics can give variables any value in $\mathbb{R}$. Logical variables X are introduced by quantifiers over $\mathbb{R}$ to e.g. discharge reasoning about continuous time, or to find witnesses for existential modalities.

Let $\mathbb{A}$ be a finite set of agents, Σ be a countable set of logical variables, $\mathbb{V}$ be a countable set of state variables, and $\mathbb{V}_a = \{x_a : x \in \mathbb{V}\}$ the set of doxastic variables for agent $a \in \mathbb{A}$. The following definition distinguishes between terms with and without doxastic variables. The distinction is crucial when assigning to state or doxastic variables, as we will see in Definition 3.

Definition 1. *The doxastic terms θ and non-doxastic terms ζ of $\mathsf{d}^4\mathcal{L}$, with $\otimes \in \{+, -, \times, \div\}$, $X \in \Sigma$, $x \in \mathbb{V}, x_a \in \mathbb{V}_a$, $a \in \mathbb{A}$, $c \in \mathbb{Q}$, are given by the grammar:*

$$\begin{array}{lcl} \theta & ::= & \theta \otimes \theta \mid X \mid c \mid x \mid x_a \\ \zeta & ::= & \zeta \otimes \zeta \mid X \mid c \mid x \end{array}$$

The formulas of $\mathsf{d}^4\mathcal{L}$ are a superset of $\mathsf{d}\mathcal{L}$'s [17], which are a superset of those of first-order logic for real arithmetic. Alongside logical connectives, we may write propositions such as $\theta_1 \leq \theta_2$ and logical quantifiers $\forall X\ \phi$. To this, $\mathsf{d}^4\mathcal{L}$ adds the belief modality $B_a(\phi)$, meaning agent a believes ϕ. The dynamic modality formula $[\alpha]\,\phi$ (after all executions of program α, ϕ is true), and its dual $\langle\alpha\rangle\,\phi$ (after some execution of α, ϕ is true) capture belief-aware CPS behavior. The language of the programs α will be specified later in Definition 3.

Since $\mathsf{d}^4\mathcal{L}$ beliefs are *only* about the state of the world, it is useful to distinguish between formulas ξ which may appear inside belief modalities, and those ϕ which may not. We still allow doxastic terms θ in ϕ, since safety proofs may generate such formulas.

Definition 2. *The formulas ϕ, ξ of $\mathsf{d}^4\mathcal{L}$ are given by the grammar:*

$$\begin{array}{lcl} \phi & ::= & \phi \vee \phi \mid \neg\phi \mid \theta \leq \theta \mid \forall X\ \phi(X) \mid [\alpha]\,\phi \mid B_a(\xi) \\ \xi & ::= & \xi \vee \xi \mid \neg\xi \mid \theta \leq \theta \end{array}$$

The remaining logical connectives, $\wedge, \rightarrow$ and duals $\langle\alpha\rangle\,\phi$, $\exists X\ \phi(X)$, $P_a(\xi)$ are defined as usual, e.g. $\langle\alpha\rangle\,\phi \equiv \neg\,[\alpha]\,\neg\phi$, and $P_a(\xi) \equiv \neg B_a(\neg\xi)$ when a considers ξ possible. We may now generalize the noisy but accurate sensors of Example 2.

Example 3 (Noisy sensors)**.** *Sensors often come with known error bounds ε. A pilot reading from the altimeter should thus come to believe the indicated value to be within ε of the real alt, as captured by $B_a((alt_a - alt)^2 \leq \varepsilon^2)$, with integer exponentiation being definable from multiplication.*

Belief modalities with both state and doxastic variables are *meta-properties* of belief, e.g., how far doxastic truth is from ontic truth. Thus, their truth value indeed changes as either the world or beliefs change. Section 6 will show such formulas are part of the core argument for some belief-aware CPS safety proofs. When formulas such as $B_a((alt_a - alt)^2 \leq \varepsilon^2)$ are not true, it can become impossible for a to make informed decisions. Safety may then instead rely on very conservative actions, e.g. bringing a car to a stop, or flying straight and level.

3.2 Doxastic Hybrid Programs

The hybrid programs (HPs) of $\mathsf{d}\mathcal{L}$ [17] are able to describe both discrete and continuous ontic change. They are the starting point for the *doxastic hybrid programs* (DHPs) of $\mathsf{d}^4\mathcal{L}$. We introduce a learning operator $L_a(\gamma)$ for doxastic change, where γ encodes an agent observing the world, reading from a sensor, or suspecting some change to have happened. In this paper, the language of the learned program γ is nearly identical to that of hybrid programs, and to the epistemic actions of the epistemic action logic EAL [7].

3.2.1 Changing Physical State

Assignment $x := \zeta$ performs instantaneous ontic change, e.g. pushing the autopilot button, $\mathit{autopilot} := 1$, or resetting a time counter with $t := 0$, as in Examples 1 and 2. No doxastic variables are allowed in ζ, since ontic truth is not directly a function of belief!

Differential equations $x' = \zeta \,\&\, \chi$ describe continuous motion over a nondeterministic duration, so long as the evolution domain constraint formula χ is true throughout. For example, $\mathit{alt}' = \mathit{yv}, t' = 1 \,\&\, t \leq 10$ describes linear change of altitude for up to 10 seconds according to vertical velocity *yv*. Nondeterministic ontic assignment $x := *$ is definable as $x' = 1; x' = -1$, which assigns any value in $\mathbb{R}$ to x by increasing then decreasing it arbitrarily.

The test $?\phi$ transitions if and only if $\mathsf{d}^4\mathcal{L}$ formula ϕ is true. It was used in Example 1 as an ontic trigger $?(\mathit{alt} > 1)$ determining whether an airplane could descend, and similarly as a belief trigger $?B_a\,(\mathit{alt}_a - \varepsilon > 1)$ in Example 2, where a pilot can only descend if they believe the airplane is safely above 1000 feet while taking worst-case noise into account.

Sequential composition $\alpha; \beta$ is self-explanatory. The choice $\alpha \cup \beta$ nondeterministically executes either α or β. It may be used to encode multiple possible outcomes or actions, e.g. $(?\mathit{alt} > 1; \mathit{yv} := -1) \cup \mathit{yv} := 1$ from Example 2.

Nondeterministic repetition α^* lets α be iterated arbitrarily many times. It was used in the program $(\texttt{obs}; \texttt{ctrl}; \texttt{plant})^*$ to ensure the safety proof applies to a system that can run for a long time, not just to a one-time control decision.

3.2.2 Changing Belief State

Agent beliefs are updated by means of the *learning operator* $L_a(\gamma)$, where γ is a program describing belief change. Notably, to interleave ontic and belief change, the learning operator is a program itself rather than a modality as in [8, 6]. Under $\mathsf{d}^4\mathcal{L}$'s possible world semantics, each agent a considers multiple worlds possible. The intuitive behavior of $L_a(\gamma)$ is to execute program γ at each such world, and consider all outcomes of such executions as possible worlds.

The language of γ is a slightly modified subset of that of hybrid programs. Inside a learning operator, ontic assignment $x := \zeta$ becomes doxastic assignment $x_a := \theta$. Since doxastic change (unlike ontic change) may depend on previous beliefs, the assigned term θ allows doxastic variables. The language also includes test $?\phi$, choice $\gamma_1 \cup \gamma_2$ and sequential composition $\gamma_1; \gamma_2$.

This language of doxastic change captures the bulk of observation and reasoning phenomena found in belief-aware CPS, which tend to occur at distinct and discrete intervals, e.g. looking at a sensor periodically. The literature [20, 6] suggests that learned differential equations and repetition pose a very significant additional challenge, which is useful only in more specialized scenarios.

Learned programs may contain nondeterminism, as in $L_a(\gamma_1 \cup \gamma_2)$. Intuitively, this says that agent a is aware that either γ_1 or γ_2 happened, but cannot ascertain which: agent a must consider possible all outcomes of γ_1 and of γ_2. Thus, in $\mathsf{d}^4\mathcal{L}$, learned nondeterminism is unobservable, and leads to the *indistinguishability of outcomes*, as in action models and epistemic actions [3, 7]. This is in contrast to program $L_a(\gamma_1) \cup L_a(\gamma_2)$, in which agent a either learns γ_1, or learns γ_2, but in both case knows precisely which one happened.

Learned test $L_a(?\xi)$ eliminates those possible worlds for which $?\xi$ does not succeed, i.e. in which ξ is false. In this way, $[L_a(?\phi)]\,\psi$ is analogous to public announcements and the tests of epistemic actions [7].

So far, the set of possible worlds may contract through learned tests and finitely expand with learned choice. The nondeterministic doxastic assignment $x_a := *$ further enables uncountable expansion of possibilities by assigning any value in $\mathbb{R}$ to x_a. To let x_a take *any* value satisfying some property $\phi(x_a)$, the program $L_a(x_a := *; ?\phi(x_a))$ first "resets" the values x_a can take using nondeterministic assignment, and then contracts the set of possible worlds with $?\phi(x_a)$.

The grammar of programs divides programs into two categories. The first, denoted α, describes the language of ontic change, or the ontic fact $L_a(\gamma)$ that program γ was learned. The second, denoted γ, describes the language of doxastic change, and, as we have seen, is a subset of the first with minor modifications.

Definition 3. *Let $x \in \mathbb{V}$, $a \in \mathbb{A}$, $x_a \in \mathbb{V}_a$ ϕ, ξ be formulas per Def. 2, θ, ζ be terms per Def. 1. Doxastic hybrid programs (DHP) α and learnable programs γ are defined thus:*

$$\begin{array}{lllllllll} \alpha & ::= & x := \zeta & \mid x' = \zeta \& \chi & \mid ?\phi & \mid \alpha;\alpha & \mid \alpha \cup \alpha & \mid \alpha^* & \mid L_a(\gamma) \\ \gamma & ::= & x_a := \theta & \mid x_a := * & \mid ?\xi & \mid \gamma;\gamma & \mid \gamma \cup \gamma & & \end{array}$$

With a better understanding of $\mathsf{d}^4\mathcal{L}$ programs, we may now describe exactly how the belief of Example 3, $B_a\left((alt_a - alt)^2 \leq \varepsilon^2\right)$, is acquired.

Example 4 (Noisy sensors, cont'd)**.** *By observing a* trusted *altimeter, the pilot decides to forget previous beliefs about altitude and trust the current reading. Then, because the altimeter has a known error bound of ε, the pilot must now consider possible all altitude values at most ε away from the true value of alt.*

$$L_a\big(alt_a := *;\ ?(alt_a - alt)^2 \leq \varepsilon^2\big)$$

4 Semantics of $\mathsf{d}^4\mathcal{L}$

The $\mathsf{d}^4\mathcal{L}$ semantics are designed to allow agents to hold potentially erroneous beliefs (proper belief, not knowledge) about a world which may undergo unobserved change. We are inspired by the modal Kripke semantics, but diverge from it by completely decoupling the valuation describing ontic truth, denoted r in $\mathsf{d}^4\mathcal{L}$, from agent beliefs, since unobservable actions must change ontic truth *only*.

Because beliefs are exclusively about the world and not about other beliefs, different agents' worlds need not interact with one another. Therefore, each agent a has their own set of worlds W_a, which they consider possible. Each agent a's valuation $V_a(t)$ function holds the values of all doxastic variables at every world $t \in W_a$, e.g. agent a's perception of altitude at $t \in W_a$ is $V_a(t)(alt_a)$.

In these sets of possible worlds, every world $t_1 \in W_a$ is indistinguishable from any other world $t_2 \in W_a$. Under the usual Kripke semantics, this means that the accessibility relation $\sim_a$, determining indistinguishability between worlds, is an equivalence relation, i.e. an S5 system. Equivalence relations traditionally encode knowledge, and belief is usually obtained by waiving the reflexivity requirement. In such belief systems, a *distinguished world* $s \in W_a$ determines ontic truth, and yet may not be accessible through $\sim_a$.

In $\mathsf{d}^4\mathcal{L}$, we achieve belief by allowing discrepancies between the valuations of the possible worlds, including the distinguished one, and the separate ontic valuation r. Thus, a pilot could believe the airplane to be high with $V_a(t)(alt_a) > 1000$ for every $t \in W_a$, while it could be low in reality, with $r(alt) \leq 1000$.

This allows us to omit the accessibility relations entirely. It also simplifies learned program semantics since the learning operator can never inadvertently change ontic truth by altering the valuation of the distinguished world. We keep the distinguished world in Definition 4 as a means by which we may interpret every formula in every context, as we will see in Definitions 5 and 6.

This gives us the models of $\mathsf{d}^4\mathcal{L}$, called physical-doxastic models, or PD-models for short. For simplicity, we consider only one agent a from now on, and we omit the subscript where it can be easily inferred, e.g. V instead of V_a.

Definition 4 (Physical/doxastic model)**.** *A physical/doxastic model or PD-model $\omega = \langle r, W, V, s\rangle$ consists of 1) $r : \mathbb{V} \to \mathbb{R}$, the state of the physical world; 2) W, a set of worlds called the* possible worlds*; 3) $V : W \to (\mathbb{V}_a \to \mathbb{R})$, a valuation function in which $V(t)(x_a)$ returns agent a's perceived value of the doxastic variable x_a at world $t \in W$; and 4) $s \in W$, a distinguished world.*

PD-models are sufficient to give meaning to all terms, formulas and programs. We use ω, ν, μ to denote PD-models, and sub- and super-scripts are applied everywhere, e.g. $\omega' = \langle r', W', V', s'\rangle$. The shortcut $t \in \omega$ means $t \in W$; $\omega(t)(x_a)$ means $V(t)(x_a)$; and $\omega(x)$ means $r(x)$. The distinguished world of ω is $\textsc{dw}(\omega)$ and its distinguished valuation $\textsc{dv}(\omega) = \omega(\textsc{dw}(\omega)) = \omega(s) = V(s)$. The real world is $\textsc{r}(\omega) = r$. Finally, let $\langle r, W, V, s\rangle \oplus t = \langle r, W, V, t\rangle$ for any $t \in \omega$.

4.1 Interpretation of Terms, Formulas, and Programs

The interpretation of terms and formulas is standard, with logical variables X given meaning by a variable assignment $\eta : \Sigma \to \mathbb{R}$, state variables x by the physical state $\textsc{r}(\omega)$, and doxastic variables x_a by the distinguished valuation $\textsc{dv}(\omega)$. Terms and formulas such as alt_a and $alt_a > 1000$ may appear outside doxastic modalities during calculus proofs. The distinguished valuation (for the distinguished world) ensures that they have a well-defined meaning and can thus be used as part of the proof.

Definition 5 (Term interpretation)**.** *Let* $\omega = \langle r, W, V, s \rangle$ *be a PD-model, and* $\eta : \Sigma \rightarrow \mathbb{R}$ *be a logical variable assignment. Then, the interpretation of terms is defined inductively as follows:* $val_\eta(\omega, x) = r(x)$ *for state variable* x*;* $val_\eta(\omega, X) = \eta(X)$ *for logical variable* X*;* $val_\eta(\omega, x_a) = \text{DV}(\omega)(x_a)$ *for doxastic variable* x_a*;* $val_\eta(\omega, \theta_1 \otimes \theta_2) = val_\eta(\omega, \theta_1) \otimes val_\eta(\omega, \theta_2)$ *for* $\otimes \in \{+, -, \times, \div\}$.

Formula interpretation is derived directly from d$\mathcal{L}$, first-order logic for real arithmetic, and simplified Kripke semantics for beliefs. Definitions 6 and 7 are mutually recursive due to the box modality formula $[\alpha]\,\phi$ and test program $?\phi$.

Definition 6 (Interpretation of formulas)**.** *Let* $\omega = \langle r, W, V, s \rangle$ *be a PD-model,* η *be a variable assignment, and* $\langle r, W, V, s \rangle \oplus t = \langle r, W, V, t \rangle$*. Then, the valuation of a formula* ϕ *as 1 (true) or 0 (false) is defined inductively as follows.*

$$
\begin{array}{lll}
val_\eta(\omega, \theta_1 \leq \theta_2) = 1 & \textit{iff} & val_\eta(\omega, \theta_1) \leq val_\eta(\omega, \theta_2) \\
val_\eta(\omega, \phi_1 \vee \phi_2) = 1 & \textit{iff} & val_\eta(\omega, \phi_1) = 1 \textit{ or } val_\eta(\omega, \phi_2) = 1 \\
val_\eta(\omega, \neg\phi) = 1 & \textit{iff} & val_\eta(\omega, \phi) = 0 \\
val_\eta(\omega, \forall X\ \phi) = 1 & \textit{iff} & \textit{for all } v \in \mathbb{R}, val_{\eta[X \mapsto v]}(\omega, \phi) = 1 \\
val_\eta(\omega, B_a(\xi)) = 1 & \textit{iff} & \textit{for all } t \in \omega, val_\eta(\omega \oplus t, \xi) = 1 \\
val_\eta(\omega, [\alpha]\,\phi) = 1 & \textit{iff} & \textit{for all } (\omega, \omega') \in \rho_\eta(\alpha), val_\eta(\omega', \phi) = 1
\end{array}
$$

Under these semantics, $B_a(x = 0)$ is equivalent to $x = 0$ since state variable x is independent of the choice of distinguished world, unlike x_a. CPS designers have no reason to write such formulas, but when they do appear in calculus proofs, the doxastic modality is eliminated using the equivalence $B_a(x = 0) \leftrightarrow x = 0$.

4.2 Program Semantics

The program semantics is given as a reachability relation over PD-models, with $(\omega, \omega') \in \rho_\eta(\alpha)$ meaning that PD-model ω' is reachable from ω using program α. The semantics of DHPs starts with that of d$\mathcal{L}$'s hybrid programs. Most cases are intuitive. Differential equations use their solution y to evolve $\text{R}(\omega)$ for a nondeterministic duration, and ensure the evolution domain constraint χ is satisfied throughout. For a more in-depth treatment, see [17].

To this we add doxastic assignment, which affects the distinguished valuation $\text{DV}(\omega)$, and the learning operator, which represents the "execute γ at each possible world" semantics from DELs, as illustrated in Figure 1.

In Figure 1, let $(\omega, \omega') \in \rho_\eta(L_a(\gamma))$. Then, each world $\nu \in \omega'$ *after* learning has an "origin" world $t \in \omega$ from *before* learning, e.g. t_1 is the origin world for ν_1 and ν_2. Every PD-model ν that γ can reach from each origin world $t \in \omega$ (i.e. $(\omega \oplus t, \nu) \in \rho_\eta(\gamma)$) becomes a possible world $\nu \in \omega'$ after $L_a(\gamma)$. The valuation $\omega'(\nu)$ reflects the effects of γ, which can be found in the distinguished valuation of ν, and thus, we let $\omega'(\nu) = \text{DV}(\nu)$.

Finally, the distinguished world of ω' is chosen as any $t' \in \omega'$ whose origin world is $\text{DW}(\omega)$. This applies the principle of *learned nondeterminism as indistinguishability of outcomes to the distinguished world.*

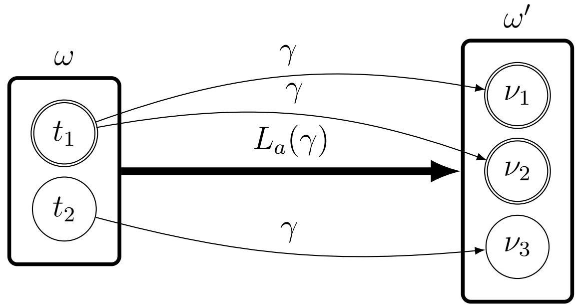

Figure 1: The double-circled $t_1 = \text{DW}(\omega)$ creates, through γ's nondeterminism, two post-learning worlds $\nu_1, \nu_2 \in \omega'$ worlds, either of which can be nondeterministically chosen as $\text{DW}(\omega')$. The world $t_2 \in \omega$ leads to $\nu_3 \in \omega'$, which cannot be chosen as $\text{DW}(\omega')$.

Definition 7 (Transition semantics)**.** *Let $\omega = \langle r, W, V, s\rangle$ be a PD-model, and η be a variable assignment. The transition relation for doxastic dynamic programs is inductively defined by:*

- $(\omega, \omega') \in \rho_\eta\,(x \coloneqq \zeta)$ *iff* $\omega' = \omega$ *except* $\text{R}(\omega')\,(x) = \mathit{val}_\eta\,(\omega, \zeta)$
- $(\omega, \omega') \in \rho_\eta\,(x_a \coloneqq \theta)$ *iff* $\omega' = \omega$ *except* $\text{DV}(\omega')\,(x_a) = \mathit{val}_\eta\,(\omega, \theta)$
- $(\omega, \omega') \in \rho_\eta\,(x_a \coloneqq *)$ *iff* $\omega' = \omega$ *except* $\text{DV}(\omega')\,(x_a) = v$ *for some* $v \in \mathbb{R}$
- $(\omega, \omega') \in \rho_\eta\,(x' = \zeta \,\&\, \chi)$ *iff* $\omega' = \langle r[x \mapsto y(\tau)], W, V, s\rangle$ *for the solution* $y : [0, \text{T}] \to \mathbb{R}$ *of the diff. eq., with* $\tau \in [0, \text{T}]$ *for some* $\text{T} \geq 0$*. Furthermore, for all* $t_i \in [0, \tau]$*, and* $\mathit{val}_\eta\,(\langle r[x \mapsto y(t_i)], W, V, s\rangle, \chi) = 1$.
- $(\omega, \omega) \in \rho_\eta\,(?\phi)$ *iff* $\mathit{val}_\eta\,(\omega, \phi) = 1$
- $\rho_\eta\,(\alpha; \beta) = \rho_\eta\,(\alpha) \circ \rho_\eta\,(\beta)$
  $= \{\omega_3 :$ *there is* ω_2 *s.t.* $(\omega_1, \omega_2) \in \rho_\eta\,(\alpha)$ *and* $(\omega_2, \omega_3) \in \rho_\eta\,(\beta)\}$
- $\rho_\eta\,(\alpha \cup \beta) = \rho_\eta\,(\alpha) \cup \rho_\eta\,(\beta)$
- $(\omega, \omega') \in \rho_\eta\,(\alpha^*)$ *iff there is* $n \in \mathbb{N}$ *such that* $(\omega, \omega') \in \rho_\eta\,(\alpha^n)$*, where* α^n *is* α *sequentially composed* n *times.*
- $(\omega, \omega') \in \rho_\eta\,(L\,(\gamma))$ *if:* $r' = r$*,* $W' = \{\nu :$ *there is* $t \in \omega$ *s.t.* $(\omega \oplus t, \nu) \in \rho_\eta\,(\gamma)\}$*,* $\omega'(\nu) = \text{DV}(\nu)$ *for all* $\nu \in \omega'$*, and* $\text{DW}(\text{DW}(\omega')) = \text{DW}(\omega)$.

Figure 1 and Definition 7 show that $\mathsf{d}^4\mathcal{L}$'s learning operator applies the DEL semantics to *any* language of change, so long as it has a transition semantics, as in $(\omega \oplus t, \nu) \in \rho_\eta\,(\gamma)$. It is possible to extend this operator to traditional multi-agent Kripke structures by letting two after-learning worlds be indistinguishable in ω' iff their origin worlds were indistinguishable in ω, as is standard in DELs.

5 Sound Sequent Calculus

Our main contribution towards the verification of belief-aware CPS is a sound proof calculus for $\mathsf{d}^4\mathcal{L}$. The meaning of a sequent $\Gamma \vdash \phi$ with a $\mathsf{d}^4\mathcal{L}$ formula ϕ and a set of $\mathsf{d}^4\mathcal{L}$ formulas Γ is captured with the following definition of validity.

Definition 8 (Validity). *A sequent* $\Gamma \vdash \phi$ *is* valid *iff for all* ω *and* η*,*

$$val_\eta\left(\omega, \bigwedge_{\psi\in\Gamma} \psi \to \phi\right) = 1$$

For simplicity's sake, we use a single definition of soundness for proof rules.

Definition 9 (Global Soundness). *A proof rule PR, as in* $_{PR}\,\dfrac{\Gamma_1 \vdash \phi_1}{\Gamma_2 \vdash \phi_2}$*, is* globally sound *when, if* $\Gamma_1 \vdash \phi_1$ *is valid then* $\Gamma_2 \vdash \phi_2$ *is valid.*

5.1 Overview of the Calculus

Figure 2 contains the fragment of the calculus that pertains to the learning operator. The $\mathsf{d}\mathcal{L}$ calculus [16] is omitted as it is easily adaptable to $\mathsf{d}^4\mathcal{L}$. Single-modality agent rationality axioms can be adopted for belief, i.e. $B_a(\phi_1 \to \phi_2) \to (B_a(\phi_1) \to B_a(\phi_2))$ and, if ϕ is valid, then $B_a(\phi)$ is too. The proof for the following theorem can be found Appendix B.

Theorem 1. *The proof rules in Figure 2 are globally sound.*

Sequent contexts Γ are partitioned into $\Gamma_R; \Gamma_B; \Gamma_P; \Gamma_O$. The set Γ_R is the set of formulas with only state and logical variables and no doxastic modalities, e.g. $alt > 0$. Γ_B and Γ_P are the sets of belief and possibility formulas respectively, e.g. $B_a((alt_a - alt)^2 \le \varepsilon^2)$ and $P_a((alt_a - alt)^2 \le \varepsilon^2)$. Γ_O is the set of formulas with doxastic variables but no modalities, e.g. $alt_a > 0$. The rules in Figure 2 are only applicable once this partitioning has been achieved. Finally, let $\Gamma\backslash_{x_a} = \{\phi \in \Gamma : x_a \text{ does not occur in } \phi\}$, and e.g. $\Gamma\backslash_{\Gamma_O} = \Gamma_R; \Gamma_B; \Gamma_P; \emptyset$.

Proof rules for learned programs that change doxastic state, like assignment or test, work by altering the contexts in suitable ways. Each learned program has two rules, for the $\Box$ and $\Diamond$ dynamic modalities, which deal with the nondeterminism in the choice of the distinguished world. The exception is $L_a(\alpha \cup \beta)$, where doxastic and dynamic modalities interact much more subtly.

The proof rules for assignment $L_a(x_a := \theta)$ capture the intuition that, since x_a now has the value of θ at each possible world, syntactically substituting all occurrences of x_a with θ ought to mean the same thing.

Since nondeterministic assignment $L_a(x_a := *)$ gives x_a any possible value, then anything previously possible about x_a remains possible. However, beliefs about x_a, which must hold for *all* worlds, do not survive the assignment (unless they are tautologies). The proof rules $[L{:=}*]$ and $\langle L{:=}*\rangle$ eliminate the formulas which may no longer hold after assignment from the context.

Formulas describing the distinguished world, i.e. in Γ_O, are retained or removed, respectively, depending on whether the dynamic modality allows us pick our distinguished world to suit our goals, as with $\Diamond$, or not, as with $\Box$.

$$[L{:=}]\quad \frac{\Gamma \vdash \phi(\theta)}{\Gamma \vdash [L_a(x_a := \theta)]\,\phi(x_a)}\,{}^1 \qquad \langle L{:=}\rangle \quad \frac{\Gamma \vdash \phi(\theta)}{\Gamma \vdash \langle L_a(x_a := \theta)\rangle\,\phi(x_a)}\,{}^1$$

$$[L{:=}*]\quad \frac{\Gamma_R; \Gamma_B\backslash_{x_a}; \Gamma_P; \Gamma_O\backslash_{x_a} \vdash \phi}{\Gamma \vdash [L_a(x_a := *)]\,\phi} \qquad \langle L{:=}*\rangle \quad \frac{\Gamma_R; \Gamma_B\backslash_{x_a}; \Gamma_P; \Gamma_O \vdash \phi}{\Gamma \vdash \langle L_a(x_a := *)\rangle\,\phi}$$

$$[L?]\quad \frac{\Gamma\backslash_{\Gamma_P} \vdash B_a\,(\xi) \to \psi}{\Gamma \vdash [L_a(?\xi)]\,\psi} \qquad \langle L?\rangle \quad \frac{\Gamma\backslash_{\Gamma_P} \vdash B_a\,(\xi) \land \psi}{\Gamma \vdash \langle L_a(?\xi)\rangle\,\psi}$$

$$[L;]\quad \frac{\Gamma \vdash [L_a(\gamma_1); L_a(\gamma_2)]\,\phi}{\Gamma \vdash [L_a(\gamma_1; \gamma_2)]\,\phi} \qquad \langle L;\rangle \quad \frac{\Gamma \vdash \langle L_a(\gamma_1); L_a(\gamma_2)\rangle\,\phi}{\Gamma \vdash \langle L_a(\gamma_1; \gamma_2)\rangle\,\phi}$$

$$[LB\cup]\quad \frac{\Gamma\backslash_{\Gamma_O} \vdash [L_a(\gamma_1)]\,B_a\,(\xi) \land [L_a(\gamma_2)]\,B_a\,(\xi)}{\Gamma \vdash [L_a(\gamma_1 \cup \gamma_2)]\,B_a\,(\xi)} \qquad \langle LB\cup\rangle \quad \frac{\Gamma \vdash \langle L_a(\gamma_1)\rangle\,B_a\,(\xi) \land \langle L_a(\gamma_2)\rangle\,B_a\,(\xi)}{\Gamma \vdash \langle L_a(\gamma_1 \cup \gamma_2)\rangle\,B_a\,(\xi)}$$

$$[LP\cup]\quad \frac{\Gamma\backslash_{\Gamma_O} \vdash [L_a(\gamma_1)]\,P_a\,(\xi) \land [L_a(\gamma_2)]\,P_a\,(\xi)}{\Gamma \vdash [L_a(\gamma_1 \cup \gamma_2)]\,P_a\,(\xi)} \qquad \langle LP\cup\rangle \quad \frac{\Gamma \vdash \langle L_a(\gamma_1)\rangle\,P_a\,(\xi) \lor \langle L_a(\gamma_2)\rangle\,P_a\,(\xi)}{\Gamma \vdash \langle L_a(\gamma_1 \cup \gamma_2)\rangle\,P_a\,(\xi)}$$

$$[L\cup]\quad \frac{\Gamma\backslash_{\Gamma_O} \vdash [L_a(\gamma_1)]\,\phi \land [L_a(\gamma_2)]\,\phi}{\Gamma \vdash [L_a(\gamma_1 \cup \gamma_2)]\,\phi}\,{}^2 \qquad \langle L\cup\rangle \quad \frac{\Gamma\backslash_{\Gamma_O} \vdash \langle L_a(\gamma_1)\rangle\,\phi \lor \langle L_a(\gamma_2)\rangle\,\phi}{\Gamma \vdash \langle L_a(\gamma_1 \cup \gamma_2)\rangle\,\phi}\,{}^2$$

[1] The substitution of x_a by θ must be admissible in ϕ, see **Doxastic Assignment**

[2] Formula ϕ does not contain doxastic modalities or variables, or learning operators

Figure 2: Dynamic doxastic fragment of the $\mathsf{d}^4\mathcal{L}$ calculus, with Γ being $\Gamma_R; \Gamma_B; \Gamma_P; \Gamma_O$

Learned test results in the belief about the test result, as in public announcements. The test contracts the set of possible worlds, so we must remove the set of possibility formulas from the context, as they may no longer hold. The underlying dynamic modality determines whether this belief is a precondition for ψ or a necessity ($\Diamond$ implies at least one transition, $\Box$ does not).

Learned sequential composition is merely reduced to regular sequential composition. Doxastic assignment and choice deserve further attention below.

5.1.1 Doxastic Assignment

The rule for doxastic assignments relies on its syntactic substitution being equivalent to the semantic substitution effected by learned assignment. This nontrival result can be captured succinctly by Lemma 1, whose full proof is found in Appendix C. This result only holds when the substitution is *admissible* with respect to a given formula ϕ, i.e. that syntactic conditions are in place ensuring the substitution will not change the meaning of the substituted variables, and therefore, of the formula.

Lemma 1 (Doxastic Substitution Lemma)**.** *Let ϕ be a formula. Let σ be an admissible substitution for ϕ which replaces only doxastic variable x_a. Then, for every η and $\omega = \langle r, W, V, s\rangle$, we have $val_\eta\,(\omega, \sigma\,(\phi)) = val_\eta\,(\sigma\,(\omega), \phi)$, where $\sigma\,(\phi)$ is syntactic substitution, and $\sigma\,(\omega)$ is semantic substitution, defined as $\sigma\,(\omega) = \langle r, W, \sigma\,(V), s\rangle$, with $\sigma\,(V)(t)(x_a) = val_\eta\,(\omega \oplus t, \sigma\,(x_a))$ and $\sigma\,(V)(t)(y_a) = V(t)(y_a) = \omega(t)(y_a)$ for $y_a \neq x_a$, for all $t \in \omega$.*

5.2 Nondeterministic Choice

Learned choice influences *doxastic* modalities, and the choice of distinguished world is influenced by *dynamic* modalities. This makes for some subtlety in the rules for learned choice. Consider the potential rule below, which assumes $L_a(\gamma_1 \cup \gamma_2)$ is equivalent to $L_a(\gamma_1) \cup L_a(\gamma_2)$.

$$\frac{P_a(\neg\xi)\,;\xi \vdash \langle L_a(?\xi)\rangle\, B_a(\xi) \vee \langle L_a(?\mathit{True})\rangle\, B_a(\xi)}{P_a(\neg\xi)\,;\xi \vdash \langle L_a(?\xi \cup ?\mathit{True})\rangle\, B_a(\xi)}$$

$$[LB\cup] \quad \frac{P_a(\neg\xi)\,;\xi \vdash \langle L_a(?\xi)\rangle\, B_a(\xi) \vee \langle L_a(?\mathit{True})\rangle\, B_a(\xi)}{P_a(\neg\xi)\,;\xi \vdash \langle L_a(?\xi \cup ?\mathit{True})\rangle\, B_a(\xi)}$$

The sequent contexts tell us that ξ holds in the distinguished world $\mathrm{DW}(\omega)$, but not in some other $t \in \omega$. The disjunction holds, since $\langle L_a(?\xi)\rangle\, B_a(\xi)$ is trivially true. The learning program $L_a(?\xi \;\cup\; ?\mathit{True})$ preserves all worlds, including t, because of $?\mathit{True}$. Since ξ is not true in t, agent a cannot therefore believe ξ. But if the top is valid and the bottom is not, this rule would be unsound.

This phenomenon occurs because the conclusion of the rule requires us to prove $B_a(\xi)$ for worlds originated through both $?\xi$ and $?\mathit{True}$. However, the premise of the rule implies we need only check those from either $?\xi$ *or* $?\mathit{True}$, as if the $\Diamond$ dynamic modality had control over learned nondeterminism. It does not: outcomes of learned nondeterminism are *always* considered indistinguishable.

Proof rules for $L_a(\gamma_1 \;\cup\; \gamma_2)$ must therefore be as conservative as the most conservative of their dynamic and doxastic modalities: the only proof rule that allows disjunction in the premise is $\langle LP\cup\rangle$ since both modalities $\Diamond$ and $P_a(\cdot)$ are existential. This realization informs the soundness proofs for learned choice.

Soundness sketch for $\langle LB\cup\rangle$. Let ω be an arbitrary PD-model.

We must show that $\mathrm{val}_\eta(\omega, \langle L_a(\gamma_1 \cup \gamma_2)\rangle\, B_a(\xi)) = 1$, i.e. that ξ is true at every world ν reachable by either $(t, \nu) \in \rho_\eta(\gamma_1)$ or $(t, \nu) \in \rho_\eta(\gamma_2)$ for $t \in \omega$.

Let $(t, \nu) \in \rho_\eta(\gamma_1)$. By hypothesis, $\mathrm{val}_\eta(\omega, \langle L_a(\gamma_1)\rangle\, B_a(\xi)) = 1$, i.e. ξ is true at every world reachable by γ_1, and ν in particular. The argument is symmetrical for $(t, \nu) \in \rho_\eta(\gamma_2)$, but only because the premise is a conjunction. Thus, for any world ν created by $L_a(\gamma_1 \cup \gamma_2)$, ξ is true at that world. Therefore, $B_a(\xi)$. $\square$

The proof rules for the $\square$ modality require us to abdicate of any facts about the distinguished world. The reason is that the $\square$ modality is vacuously true if there are no transitions. For this to happen, it is enough that the distinguished world does not transition with, e.g., $L_a(\gamma_1)$. However, other, not-distinguished worlds may still transition have transitions with γ_1, and thus contribute possible worlds in the $L_a(\gamma_1 \cup \gamma_2)$ transition. The soundness proof for the $\square$ rules in Appendix B.4 addresses this issue in detail, but we present a brief counter-example here. In the following rule, we neglect to remove facts about the distinguished world from the hypothesis.

$$\frac{P_a(x_a = 1)\,; x_a = 0 \vdash [L_a(x_a \coloneqq 0)]\, B_a(x_a \leq 0) \wedge [L_a(?x_a > 0)]\, B_a(x_a \leq 0)}{P_a(x_a = 1)\,; x_a = 0 \vdash [L_a(x_a \coloneqq 0 \;\cup\; ?x_a > 0)]\, B_a(x_a \leq 0)}$$

The premise of the proof rule is valid: the left conjunct is valid because the assignment ensures the post-condition is true; the right conjunct is valid because the distinguished world does not pass the test, and therefore there are no transitions, making the $\Box$ modality vacuously true.

The conclusion of the proof rule not valid. We know that $L_a(x_a \coloneqq 0 \cup ?x_a > 0)$ has a transition because $L_a(x_a \coloneqq 0)$ has a transition. But now, the pre-existing world where $x_a = 1$ survives the test $?x_a > 0$, and thus remains after $L_a(x_a \coloneqq 0 \cup ?x_a > 0)$. It can therefore not be the case that $B_a\,(x_a \leq 0)$, and the conclusion is false. If the premise is valid but the conclusion is not, the rule is unsound. This proof rule cannot rely on properties of the distinguished world for its soundness.

The same does not happen in the rules for the $\Diamond$ modality because $\Diamond$ requires a transition, meaning that, by hypothesis, the distinguished world *must* transition, eliminating the exact phenomenon that allowed the above rule to be unsound.

6 Validation and Application

We will now use $\mathsf{d}^4\mathcal{L}$ to illustrate how to prove the safety of a small belief-aware CPS. The scenario is similar to that of Example 2, and it is useful to have a reference for some of the most used $\mathsf{d}\mathcal{L}$ proof rules that $\mathsf{d}^4\mathcal{L}$ inherits [16].

$$[;]\,\frac{\Gamma \vdash [\alpha]\,[\beta]\,\phi}{\Gamma \vdash [\alpha;\beta]\,\phi} \qquad [?]\,\frac{\Gamma \vdash \phi \to \psi}{\Gamma \vdash [?\phi]\,\psi} \qquad {\to}R\,\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}$$

We let the pilot observe the altimeter with $\mathtt{O} \equiv L_a(\mathit{alt}_a \coloneqq *; ?\mathit{Noise})$, with $\mathit{Noise} \equiv (\mathit{alt}_a - \mathit{alt} < \varepsilon)$. The control program $\mathtt{C}$ climbs or descends by setting vertical velocity depending on whether descent is believed to be safe, $\mathtt{CB} \cup \mathtt{CP} \equiv (?B_a\,(\mathit{alt}_a - T - \varepsilon > 0)\,; \mathit{yv} \coloneqq -1) \cup (?P_a\,(\mathit{alt}_a - T - \varepsilon \leq 0)\,; \mathit{yv} \coloneqq 1)$. The two tests are mutually exclusive, leading to dual belief operators: descending requires the strong condition of belief, whereas the mere possibility of being too low triggers a climb. We use $\mathtt{F} \equiv t \coloneqq 0; t' = 1, \mathit{alt}' = \mathit{yv} \,\&\, t < T$ as very simplified flight dynamics, and an invariant $\mathit{inv} \equiv (\mathit{alt} > 0 \land T > 0)$ to handle repetition.

We will prove the validity of the formula $\mathit{alt} > 0, T > 0 \vdash [(\mathtt{O};\mathtt{C};\mathtt{F})^*]\,\mathit{alt} > 0$ by successively applying sound proof rules from $\mathsf{d}\mathcal{L}$ and Figure 2 to it. The leaves of the proof tree will be formulas that can be easily discharged using only $\mathsf{d}\mathcal{L}$ rules or real arithmetic. Once the proof tree is complete, we will know this safety formula is valid, and thus that the modeled system is safe.

$$\text{loop}\,\frac{\dfrac{*}{\mathit{alt} > 0, T > 0 \vdash \mathit{inv}} \qquad [;]\,[;]\,\dfrac{\mathit{inv} \vdash [\mathtt{O}]\,[\mathtt{C}]\,[\mathtt{F}]\,\mathit{inv}}{\mathit{inv} \vdash [\mathtt{O};\mathtt{C};\mathtt{F}]\,\mathit{inv}} \qquad \dfrac{*}{\mathit{inv} \vdash \mathit{alt} > 0}}{\mathit{alt} > 0, T > 0 \vdash [(\mathtt{O};\mathtt{C};\mathtt{F})^*]\,\mathit{alt} > 0}$$

The middle branch continues in:

$$[\mathrm{L;}]\,[;]\,\frac{[L{\coloneqq}*]\,\dfrac{[\mathrm{L?}]\,{\to}R\,\dfrac{[\cup]\,\dfrac{\mathit{inv}; B_a\,(\mathit{Noise}) \vdash [\mathtt{CB}]\,[\mathtt{F}]\,\mathit{inv} \qquad \mathit{inv}; B_a\,(\mathit{Noise}) \vdash [\mathtt{CP}]\,[\mathtt{F}]\,\mathit{inv}}{\mathit{inv}; B_a\,(\mathit{Noise}) \vdash [\mathtt{C}]\,[\mathtt{F}]\,\mathit{inv}}}{\mathit{inv} \vdash [L_a(?\mathit{Noise})]\,[\mathtt{C}]\,[\mathtt{F}]\,\mathit{inv}}}{\mathit{inv} \vdash [L_a(\mathit{alt}_a \coloneqq *)]\,[L_a(?\mathit{Noise})]\,[\mathtt{C}]\,[\mathtt{F}]\,\mathit{inv}}}{\mathit{inv} \vdash [L_a(\mathit{alt}_a \coloneqq *; ?\mathit{Noise})]\,[\mathtt{C}]\,[\mathtt{F}]\,\mathit{inv}}$$

The branch on the right closes using $\mathsf{d}\mathcal{L}$ proof rules and standard $\mathsf{d}\mathcal{L}$ reasoning independent of beliefs: if the airplane is above ground and climbs, it remains above ground. The left branch requires some doxastic reasoning.

$$
\dfrac{\dfrac{\dfrac{inv; B_a\,(Noise)\,, B_a\,(alt_a - T - \varepsilon > 0) \vdash alt > T \qquad inv; alt > T \vdash [\mathtt{F}(-1)]\,inv}{inv; B_a\,(Noise)\,, B_a\,(alt_a - T - \varepsilon > 0) \vdash [\mathtt{F}(-1)]\,inv}\,\text{cut}}{inv; B_a\,(Noise)\,, B_a\,(alt_a - T - \varepsilon > 0) \vdash [yv := -1]\,[\mathtt{F}(yv)]\,inv}\,[:=]}{inv; B_a\,(Noise) \vdash [?B_a\,(alt_a - T - \varepsilon > 0)\,; yv := -1]\,[\mathtt{F}(yv)]\,inv}\,[;]\,[?] \to R
$$

The left side of the cut rule must show that $alt > T$, and for that we will use the S5 rationality axioms that allow for reasoning about arithmetic. Thus, the agent may conclude (1) $B_a\,(alt > alt_a - \varepsilon)$ from $B_a\,(Noise)$, and (2) $B_a\,(alt_a > T + \varepsilon)$ from $B_a\,(alt_a - T - \varepsilon > 0)$. But (1) and (2) together lead to $B_a\,(alt > T)$, which no longer contains any doxastic variables. It is therefore equivalent to $alt > T$. We have thus used the belief meta-property (1), relating ontic and doxastic truth, to obtain an important fact about the world which we may now use in the right side of the proof.

This right side is a standard $\mathsf{d}\mathcal{L}$ proof without doxastics: the rules for differential equations show that, after evolving for at most T time at a speed of -1, the airplane cannot end up below ground, since it started above T altitude.

This completes the sequent proof. It leveraged a mix of ontic, doxastic and meta-doxastic statements in order to make the argument for the safety of this controller. When working with trusted sensors, we also see an intuitive partitioning of the proof: first, doxastic formulas such as $(B_a\,(alt_a - T - \varepsilon > 0))$ and meta-doxastic formulas $(B_a\,(Noise))$ are used to derive ontic formulas like $(alt > T)$. Second, such ontic statements form the basis for arguments made in $\mathsf{d}\mathcal{L}$-exclusive proof branches that ensure post-control actuation results in safe behavior. This clear separation of concerns allows CPS engineers to work more intuitively and compositionally during the design and verification stages of belief-aware CPS.

The ways in which agents learn and reason influence the ontic facts that can be deduced, but those facts must in turn be informed by safety requirements of the CPS's physical evolution. Doxastics and ontics clearly play off each and have, in the past, contributed to safety incidents. By making this explicit in the model, $\mathsf{d}^4\mathcal{L}$ ensures adequate attention is given to such dynamics so that hopefully, ontic/doxastic concerns can be identified before they lead to tragedy.

7 Related Work

The logic $\mathsf{d}^4\mathcal{L}$ takes heavy inspiration from two bodies of work: one for reasoning about a changing world, and one for reasoning about changing beliefs.

7.1 Changing world

The logic $\mathsf{d}\mathcal{L}$ for reasoning about the ontic dynamics of CPS [16, 17, 19] has shown itself to be capable of verifying interesting and relevant real world systems [18, 17]. However, it requires manual modeling discipline to express noise [14], rather than having noise or beliefs thereof as built-in primitives.

The example used in this paper is so simple that it can still be converted to $\mathsf{d}\mathcal{L}$ using modeling tricks [14]. The trick is to transform alt_a into a state variable and remove the learning operator from the observation program, i.e. $\mathit{alt}_a := *; ?\mathit{Noise}$ rather than $L_a(\mathit{alt}_a := *; ?\mathit{Noise})$. The agent's control would then be $(?\mathit{alt}_a - T - \varepsilon > 0; \mathit{yv} := -1) \cup (?\mathit{alt}_a - T - \varepsilon \leq 0; \mathit{yv} := 1)$.

However, this conversion relies fundamentally on the box dynamic modality $[\alpha]\, \phi$, which checks safety for *all* executions of $\mathit{alt}_a := *; ?\mathit{Noise}$. With liveness formulas using the diamond dynamic modality $\langle\alpha\rangle\, \phi$, safety need only be checked for *one* execution. Thus, in liveness formulas, this method would fail to capture the intended behavior of both the learning operator and the belief modality, which should still apply to *all* possible worlds, or, in $\mathsf{d}\mathcal{L}$ terms, all executions.

This conversion can also quickly become complex. A more detailed controller for a pilot trying to remain around or above cruising altitude A could be $(?B_a\, (\mathit{alt}_a - T - \varepsilon > A)\, ; \mathit{yv} := -1) \cup (?P_a\, (\mathit{alt}_a - T - \varepsilon > A)\, ; \mathit{yv} := -0.5) \cup (?B_a\, (\mathit{alt}_a - T - \varepsilon \leq 0)\, ; \mathit{yv} := 1)$. This is similar to previous controllers, but allows for a more gentle descent when the pilot considers the possibility of being close to A. The equivalent $\mathsf{d}\mathcal{L}$ controller is $(?\mathit{alt}_a - T - \varepsilon > A; \mathit{yv} := -1) \cup (?\mathit{alt}_a - T + \varepsilon > A; \mathit{yv} := -0.5) \cup (?\mathit{alt}_a - T - \varepsilon \leq 0; \mathit{yv} := 1)$. However, this elimination of doxastic modalities requires a change in the arithmetic itself, e.g. $(?P_a\, (\mathit{alt}_a - T - \varepsilon > A)$ turns into $(?\mathit{alt}_a - T + \varepsilon > A)$. Belief must consider worst case noise, whereas possibility can consider the best case. This can quickly become complex when going beyond simpler interval-based noise scenarios.

Both $\mathsf{d}\mathcal{L}$ and $\mathsf{d}^4\mathcal{L}$ controllers allow tests for deciding which action to take, but represent action triggers in first-order logic or doxastic logic, respectively, e.g. $\mathit{alt}_a - T + \varepsilon > A$ and $P_a\, (\mathit{alt}_a - T - \varepsilon > A)$. Decisions in real CPS are based on belief, and as the conversion from doxastic to non-doxastic action triggers quickly becomes non-trivial, it is best to avoid subtle modeling mistakes by working with belief during design and verification. With $\mathsf{d}^4\mathcal{L}$, safety engineers can rely on doxastic intuitions during verification, rather than having to infer them from formulas such as $\mathit{alt}_a - T + \varepsilon > A$, which does not clearly convey the concept of possibility that is so clear in $P_a\, (\mathit{alt}_a - T - \varepsilon > A)$.

The notion of robustness in hybrid systems control can capture complex notions of sensor and actuator noise [11], but is ultimately restrictive for the purpose of belief-aware CPS, as discussed at the beginning of Section 2. Adaptive control, where no *a priori* constraints are known, often depends on neural networks [15], and safety guarantees for systems relying on learning are known to add significant complexity to such efforts [9].

7.2 Changing belief

On the other side, we have dynamic epistemic logics (DELs) [6, 3, 4, 10, 7], of which a good overview can be found in the literature [8]. They provide several notions of learning for different languages, some similar to our programs [6]. *Public* propositional world-change [6] would make ontic change implicitly observable, which is in direct conflict with the unobservability requirements of belief-aware CPS. Furthermore, relevant DEL axiomatizations rely on creating a conjunction out of properties of each accessible possible world [4, 8], which is incompatible with the uncountably many worlds that CPS demand.

Belief revision through the AGM postulates [2] is an axiomatic, declarative approach to belief change. Because it is such a different approach, it presents many challenges in its integration with model-theoretic work such as $\mathsf{d}\mathcal{L}$.

In order to begin addressing safety concerns around ontic/doxastic interactions at design time, CPS engineers and agents must make complex logical arguments from both ontic facts and beliefs, as in Section 6. Despite their many successes, the works described in this section do not address this particular challenge directly in a principled way.

8 Conclusions

This paper considers interactions between belief and fact, which have significant safety implications. We proposed belief-aware CPSs as a first-principles paradigm under which safety concerns with such ontic/doxastic dynamics are expressly dealt with at design time, before safety violations occur. Our contribution is the logic $\mathsf{d}^4\mathcal{L}$ for modeling and verifying belief-aware CPSs, requiring simultaneous, complex belief- and world-change. Its formulas can describe ontic, doxastic and meta-doxastic statements, and its programs can model belief-aware CPS with belief-triggered controllers that make decisions based only on what they can observe and reason. We proposed a learning operator for belief-change, which is capable of transforming any transition-based semantics of change into a semantics of *belief*-change. We presented a sequent calculus for $\mathsf{d}^4\mathcal{L}$, which is proven to be sound, and used it to show the safety of a simple belief-aware CPS. This is, to the best of our knowledge, the first calculus for a dynamic logic of belief/knowledge change that can handle an uncountable domain, as in CPS.

Acknowledgment. We thank the anonymous reviewers for their helpful feedback.

References

[1] Aircraft Accident Investigation Bureau of Ethiopia: Report No. AI-01/19, Aircraft Accident Investigation Preliminary Report, Ethiopian Airlines Group, B737-8 (MAX) Registered ET-AVJ (2019)

[2] Alchourrón, C.E., Gärdenfors, P., Makinson, D.: On the logic of theory change: Partial meet contraction and revision functions. J. Symb. Log. **50**(2), 510–530 (1985)

[3] Baltag, A., Moss, L.S.: Logics for epistemic programs. Synthese **139**(2), 165–224 (2004)

[4] Baltag, A., Moss, L.S., Solecki, S.: The logic of public announcements, common knowledge, and private suspicions. In: TARK. pp. 43–56. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1998)

[5] Bureau d'Enquêtes et d'Analyses (BEA): Final report on the accident on 1st june 2009 to the airbus A330-203 registered F-GZCP operated by Air France flight AF 447 from Rio de Janeiro to Paris (2012)

[6] van Ditmarsch, H.P., van der Hoek, W., Kooi, B.P.: Dynamic epistemic logic with assignment. In: AAMAS. pp. 141–148. ACM, New York, NY, USA (2005)

[7] van Ditmarsch, H.P.: Descriptions of game actions. Journal of Logic, Language and Information **11**(3), 349–365 (2002)

[8] Ditmarsch, H.v., van der Hoek, W., Kooi, B.: Dynamic Epistemic Logic. Springer (2007)

[9] Fulton, N., Platzer, A.: Verifiably safe off-model reinforcement learning. In: Vojnar, T., Zhang, L. (eds.) TACAS. LNCS, vol. 11427, pp. 413–430. Springer (2019)

[10] Gerbrandy, J., Groeneveld, W.: Reasoning about information change. Journal of Logic, Language and Information **6**(2), 147–169 (1997)

[11] Goebel, R., Hespanha, J.P., Teel, A.R., Cai, C., Sanfelice, R.: Hybrid systems: Generalized solutions and robust stability. In: Proc. of the 6th IFAC Symp. on Nonlinear Contr. Systems (Sep 2004)

[12] Komite Nasional Keselamatan Transportasi: Preliminary Aircraft Accident Investigation Report, PT. Lion Mentari Airlines, Boeing 737-8 (MAX); PK-LQP (2018)

[13] Martins, J.G., Platzer, A., Leite, J.: A sound calculus for a logic of belief-aware cyber-physical systems. Tech. Rep. CMU-CS-19-116, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA (July 2019)

[14] Mitsch, S., Ghorbal, K., Vogelbacher, D., Platzer, A.: Formal verification of obstacle avoidance and navigation of ground robots. I. J. Robotics Res. **36**(12), 1312–1340 (2017)

[15] Nguyen, N.T., Krishnakumar, K.S., Kaneshige, J.T., Nespeca, P.P.: Flight dynamics and hybrid adaptive control of damaged aircraft. Journal of Guidance, Control, and Dynamics **31**(3), 751–764 (2008)

[16] Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. **41**(2), 143–189 (2008)

[17] Platzer, A.: Logics of dynamical systems. In: LICS. pp. 13–24. IEEE (2012)

[18] Platzer, A.: Logic & proofs for cyber-physical systems. In: Olivetti, N., Tiwari, A. (eds.) IJCAR. LNCS, vol. 9706, pp. 15–21. Springer (2016)

[19] Platzer, A.: Logical Foundations of Cyber-Physical Systems. Springer, Cham (2018)

[20] Platzer, A., Tan, Y.K.: Differential equation axiomatization: The impressive power of differential ghosts. In: Dawar, A., Grädel, E. (eds.) LICS. pp. 819–828. ACM, New York (2018)

A Semantic Equivalence of PD-models

Semantic subsumption and equivalence of PD-model is useful for soundness proofs, for instance in that the worlds from $L_a(\alpha)$ will be contained in $L_a(\alpha \cup \beta)$.

Definition 10 (Semantic subsumption)**.** *Let ω and ν be two PD-models. We say that ω semantically subsumes ν, or just subsumes ν, denoted $\nu \sqsubseteq \omega$, if $\mathrm{R}(\omega) = \mathrm{R}(\nu)$ and for all $t \in \nu$, there is $u \in \omega$ such that $\nu(t) = \omega(u)$.*

Definition 11 (Semantic equivalence)**.** *Let ω and ν. We say that ω and ν are semantically equivalent, denoted $\omega \sim \nu$, if $\nu \sqsubseteq \omega$ and $\omega \sqsubseteq \nu$.*

The reader more familiar with epistemic or doxastic logics may already have an intuition for the use of these notions, and be aware of the following results.

Proposition 1. *Let ω, ν be two PD-models such that $\nu \sqsubseteq \omega$. Then, $val_\eta(\nu, P_a(\xi))$ implies $val_\eta(\omega, P_a(\xi))$ and $val_\eta(\omega, B_a(\xi))$ implies $val_\eta(\nu, B_a(\xi))$.*

B Soundness of Sequent Calculus

The following sections address the soundness of the rules for different operators.

B.1 Nondeterministic doxastic assignment

The proof rule for nondeterministic assignment $[L{:=}*]$ is based on the insight that when a doxastic variable x_a is assigned any possible value, the doxastic universe expands. Therefore, any *beliefs* about that variable need no longer hold, and must be removed from the context. Possibilities, however, remain unaffected: any witnesses prior to nondeterministic doxastic assignment remain after the assignment.

Global soundness of $[L{:=}*]$. Let ω, ω' be PD-models such that $\mathrm{val}_\eta(\omega, \Gamma) = 1$, or $\mathrm{val}_\eta(\omega, \Gamma)$ for short, and $(\omega, \omega') \in \rho_\eta(L_a(x_a := *))$. We must show that $\mathrm{val}_\eta(\omega', \phi)$. Because we are using global soundness, it will suffice to show that $\mathrm{val}_\eta\left(\omega', \Gamma_R; \Gamma_B\backslash_{x_a}; \Gamma_P; \Gamma_O\backslash_{x_a}\right)$, at which point we may directly apply the rule's premise.

The semantics of learned nondeterministic doxastic assignment state that ω' differs from ω only about x_a. Thus, since x_a does not occur in Γ_R, $\Gamma_B\backslash_{x_a}$ and $\Gamma_O\backslash_{x_a}$, we may immediately claim $\mathrm{val}_\eta(\omega', \Gamma_R)$, $\mathrm{val}_\eta\left(\omega', \Gamma_B\backslash_{x_a}\right)$, and $\mathrm{val}_\eta\left(\omega', \Gamma_O\backslash_{x_a}\right)$ from the assumption that $\mathrm{val}_\eta(\omega, \Gamma_R)$, $\mathrm{val}_\eta\left(\omega, \Gamma_B\backslash_{x_a}\right)$, and $\mathrm{val}_\eta\left(\omega, \Gamma_O\backslash_{x_a}\right)$.

We now prove $\mathrm{val}_\eta(\omega', \Gamma_P)$. We know by assumption that $\mathrm{val}_\eta(\omega, \Gamma_P)$, and thus for each $P_a(\psi) \in \Gamma_P$, there is $t \in \omega$ such that $\mathrm{val}_\eta(\omega \oplus t, \psi)$. Let $v = \omega(t)(x_a)$ be the value that contributes to satisfying ψ. By the semantics of learned nondeterministic doxastic assignment, there will be $t' \in \omega'$, with $\mathrm{DW}(t') = t$, such that $\omega'(t')(x_a) = v'$ for all $v' \in \mathbb{R}$. In particular, there will be one world $u' \in \omega'$ where $v' = v$. Since only x_a has changed from ω to ω' and $\mathrm{val}_\eta(\omega \oplus t, \psi)$, then $\mathrm{val}_\eta(\omega' \oplus u, \psi)$. Thus, the world $u' \in \omega'$ serves as the witness for $\mathrm{val}_\eta(\omega', P_a(\psi))$.

Thus, $\mathrm{val}_\eta\left(\omega', \Gamma_R; \Gamma_B\backslash_{x_a}; \Gamma_P; \Gamma_O\backslash_{x_a}\right)$, and by the rule's premise, $\mathrm{val}_\eta(\omega', \phi)$. $\square$

It is interesting that in the soundness proof for $\langle L{:=}*\rangle$, we need not remove any formulas from Γ_O: the $\Diamond$ modality allows us to pick the distinguished world that satisfies the formulas in Γ_O, not unlike what we did for possibilities in $[L{:=}*]$.

B.2 Test rules

Global soundness of $[L?]$ *and* $\langle L?\rangle$. Let ω be a PD-model. Assume $\mathrm{val}_\eta(\omega, \Gamma_R; \Gamma_B; \Gamma_P; \Gamma_O)$.

We must show $\mathrm{val}_\eta(\omega, [L_a(?\xi)]\,\psi)$, which is true iff for all ω' such that $(\omega, \omega') \in \rho_\eta(L_a(?\xi))$, $\mathrm{val}_\eta(\omega', \psi)$.

If there are no transitions the formula is trivially true, so assume there is $(\omega, \omega') \in \rho_\eta(L_a(?\xi))$. By the semantics of the learning operator

$$
\begin{aligned}
&W(\omega') = \{t' : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, t') \in \rho_\eta(?\xi)\}\\
&\omega'(t') = \mathrm{DV}(t') \text{ for all } t' \in \omega'\\
&\mathrm{DW}(\mathrm{DW}(\omega')) = \mathrm{DW}(\omega)
\end{aligned}
$$

Thus, for each $t' \in \omega'$, there is some $t \in \omega$ such that $(\omega \oplus t, t') \in \rho_\eta(?\xi)$, $t' = (\omega \oplus t)$, and $\omega'(t') = \mathrm{DV}(t')$. We know that test does not alter valuations, and therefore, $\omega'(t') = \mathrm{DV}(t') = \mathrm{DV}(\omega \oplus t) = \omega \oplus t(t) = \omega(t)$.

The formula ξ, being inside a learning operator, cannot contain other learning operators or doxastic modalities. It follows from this and $\omega'(t') = \omega(t)$ that for all $t' \in \omega'$, $\mathrm{val}_\eta(\omega' \oplus t', \xi) = \mathrm{val}_\eta(\omega \oplus t, \xi) = 1$. We have thus established $\mathrm{val}_\eta(\omega', B_a(\xi))$.

We need only show that $\mathrm{val}_\eta(\omega', \Gamma_R; \Gamma_B; \emptyset; \Gamma_O)$ in order to apply the implication in the rule's premise. Since $\mathrm{val}_\eta(\omega, \Gamma_R)$ and $\mathrm{R}(\omega') = \mathrm{R}(\omega)$, $\mathrm{val}_\eta(\omega', \Gamma_R)$. Since $\omega \sqsubseteq \omega'$, by Proposition 1, $\mathrm{val}_\eta(\omega', \Gamma_B)$. Finally, since $\mathrm{DV}(\omega') = \mathrm{DV}(\omega)$, $\mathrm{val}_\eta(\omega', \Gamma_O)$. Thus, $\mathrm{val}_\eta(\omega', \Gamma_R; \Gamma_B; \emptyset; \Gamma_O)$.

The proof for $\langle L?\rangle$ differs only in that the hypothesis guarantees that $\mathrm{val}_\eta(\omega, B_a(\xi))$, and thus that there is a transition for $L_a(?\xi)$. The rest of the proof follows the same lines as $[L?]$. □

B.3 Sequential composition rules

To reduce subscripts and increase readability, let $\alpha = \gamma_1$ and $\beta = \gamma_2$.

Local soundness of $[L;]$. Let ω be a PD-model. Let ω'' be an arbitrary PD-model such that $(\omega, \omega'') \in \rho_\eta(L_a(\alpha;\beta))$. We must show $\mathrm{val}_\eta(\omega'', \phi)$. The first step is to examine the transitions for $L_a(\alpha;\beta)$ and $L_a(\alpha); L_a(\beta)$, as illustrated in Figure 3. We begin with $(\omega, \omega'') \in \rho_\eta(L(\alpha;\beta))$.

$$
\begin{aligned}
W(\omega'') &= \{\nu'' : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu'') \in \rho_\eta(\alpha;\beta)\}\\
&= \{\nu'' : \text{ there is } t \in \omega \text{ and } \mu \text{ s.t. } (\omega \oplus t, \mu) \in \rho_\eta(\alpha) \text{ and } (\mu, \nu'') \in \rho_\eta(\beta)\} \qquad (1)
\end{aligned}
$$

We draw attention to the PD-models μ, which we will call the intermediate PD-models of ω''. For every $\nu'' \in \omega''$, there is a $t \in \omega$ and an intermediate PD-model μ such that $(\omega \oplus t, \mu) \in \rho_\eta(\alpha)$ and $(\mu, \nu'') \in \rho_\eta(\beta)$.

Let us now look at $(\omega, \omega_2'') \in \rho_\eta\left(L\left(\alpha\right); L\left(\beta\right)\right)$. By the d$\mathcal{L}$ semantics of sequential composition, there exists ω_2' such that $(\omega, \omega_2') \in \rho_\eta\left(L_a(\alpha)\right)$ and $(\omega_2', \omega_2'') \in \rho_\eta\left(L_a(\beta)\right)$.

$$W(\omega_2') = \{\nu_2' : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_2') \in \rho_\eta\left(\alpha\right)\} \tag{2}$$

$$W(\omega_2'') = \{\nu_2'' : \text{ there is } \nu_2' \in \omega_2' \text{ s.t. } (\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta\left(\beta\right)\} \tag{3}$$

We will now establish a semantic correspondence between the intermediate worlds μ of $L_a(\alpha; \beta)$ and the worlds $\nu_2' \in \omega_2'$. This will allow us to prove that ω'' and ω_2'' are semantically equivalent, and therefore that $\mathrm{val}_\eta\left(\omega'', \phi\right) = \mathrm{val}_\eta\left(\omega_2'', \phi\right) = 1$ by the rule's hypothesis.

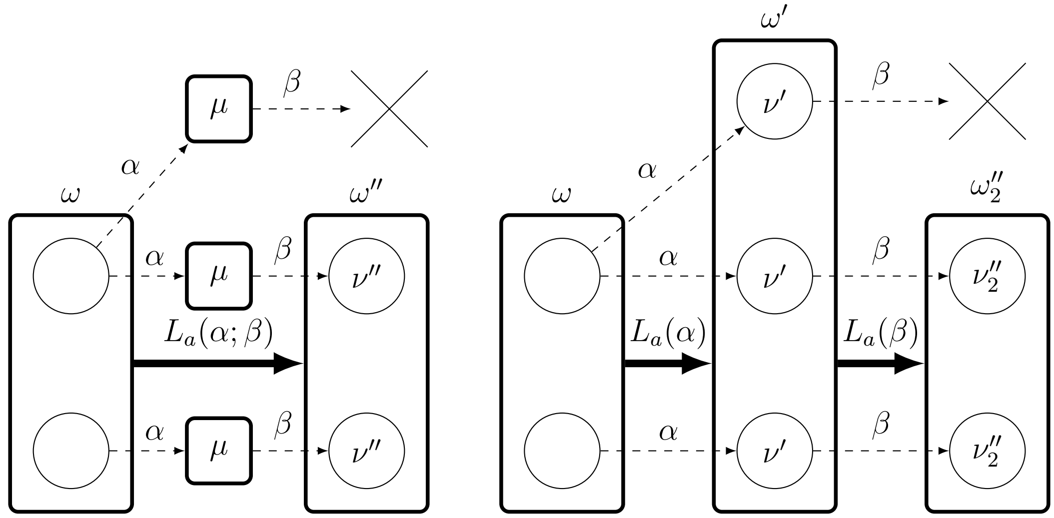

Figure 3: The transitions of $L_a(\alpha; \beta)$ and $L_a(\alpha); L_a(\beta)$

Claim 1: $\mathrm{R}(\omega'') = \mathrm{R}(\omega_2'')$. Trivial: learning operator does not change ontic state.

Claim 2: For every intermediate world μ of $\nu'' \in \omega''$, there is $\nu_2' \in \omega_2'$ such that $\omega_2'(\nu_2') = \mathrm{DV}(\mu)$.

Let $\nu'' \in \omega''$. We already know there is $t \in \omega$ and μ such that $(\omega \oplus t, \mu) \in \rho_\eta\left(\alpha\right)$. But these are exactly the conditions (2) of belonging to $W(\omega_2')$, and thus $\mu \in \omega_2'$. This is an equivalent statement to there being $\nu_2' \in \omega_2'$ such that $\mu = \nu_2'$. We will therefore use μ and ν_2' interchangeably from now on: $\omega_2'(\mu) = \omega_2'(\nu_2')$ and $\mathrm{DV}(\nu_2') = \mathrm{DV}(\mu)$.

Claim 3: ω_2'' subsumes ω'', or $\omega'' \sqsubseteq \omega_2''$.

For every $\nu'' \in \omega''$ we must show there is $\nu_2'' \in \omega_2''$ such that $\omega''(\nu'') = \omega_2''(\nu_2'')$. We already know there are transitions from ω using $t \in \omega$ and an intermediate PD-model μ.

But Claim 2 shows that there is $\nu_2' \in \omega_2'$ with exactly the same relevant valuations as μ: $\text{R}(\mu) = \text{R}(\nu_2') = \text{R}(\omega_2')$ and $\omega_2'(\nu_2') = \text{DV}(\nu_2') = \text{DV}(\mu)$. These are precisely those (and, since β is in a learning operator, *only* those) that β can use in the transitions of $(\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta(\beta)$.

Thus, for each transition $(\mu, \nu'') \in \rho_\eta(\beta)$, there is an equivalent transition $(\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta(\beta)$, as in (3), where $\mu = \nu_2'$, $\text{DV}(\mu) = \text{DV}(\nu_2')$ and, more importantly, $\text{DV}(\nu'') = \text{DV}(\nu_2'')$. By the semantics of the learning operator, $\omega''(\nu'') = \omega_2''(\nu_2'')$.

Claim 4: ω'' subsumes ω_2'', or $\omega_2'' \sqsubseteq \omega''$

Claim 2 already established a correspondence between each μ and some world $\nu_2' \in \omega_2'$. However, there may be some $\nu_2' \in \omega_2'$ that does not correspond to any μ, since the existence μ requires a successful transition $(\mu, \nu'') \in \rho_\eta(\beta)$, with $\nu'' \in \omega''$. In contrast, there is no such restriction on $\nu_2' \in \omega_2'$. There could be some transition $(\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta(\beta)$ for a world $\nu_2' \in \omega_2'$ that does not exist as an intermediate world μ, leading to a world $\nu_2'' \in \omega_2''$ without a corresponding $\nu'' \in \omega''$.

Let $\nu_2'' \in \omega_2''$. So, from (3) there exists some transition $(\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta(\beta)$ and furthermore, from (2), there is $t \in \omega$ such that $(\omega \oplus t, \nu_2') \in \rho_\eta(\alpha)$.

Let $\mu = \nu_2'$ so that, in particular, $\text{R}(\mu) = \text{R}(\nu_2')$ and $\text{DV}(\mu) = \text{DV}(\nu_2')$. Then, firstly, since there is a transition $(\omega \oplus t, \nu_2') \in \rho_\eta(\alpha)$ and $\mu = \nu_2'$, trivially there must be $(\omega \oplus t, \mu) \in \rho_\eta(\alpha)$. Secondly, because α and β are both learned programs, the statement $(\omega_2' \oplus \nu_2', \nu_2'') \in \rho_\eta(\beta)$ is equivalent to $(\mu, \nu'') \in \rho_\eta(\beta)$ where $\text{DV}(\nu'') = \text{DV}(\nu_2'')$ and $\text{R}(\nu'') = \text{R}(\nu_2'')$. This is because learned programs can read *only* from ontic state and the distinguished valuation, and both concur in $\omega_2' \oplus \nu_2'$ and μ.

But then, μ is in the conditions of (1), and thus $\nu'' \in \omega''$ and from the semantics of the learning operator, $\omega''(\nu'') = \omega_2''(\nu_2'')$.

Claims 3 and 4 together state $\omega'' \sim \omega_2''$. We may let $\text{DW}(\omega_2'') = \text{DW}(\omega'')$. From these two statements and the premise of the rule, we may then conclude $\text{val}_\eta(\omega'', \phi)$. $\square$

B.4 Nondeterministic choice rules

First, let us define three sets of worlds which are not necessarily connected to any transitions.

$$W_\alpha = \{\nu_\alpha : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_\alpha) \in \rho_\eta(\alpha)\}$$
$$W_\beta = \{\nu_\beta : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_\beta) \in \rho_\eta(\beta)\}$$
$$W_\cup = \{\nu_\cup : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_\cup) \in \rho_\eta(\alpha \cup \beta)\} = W_\alpha \cup W_\beta$$

We make a distinction between the sets W_α and $W(\omega_\alpha)$ from $(\omega, \omega_\alpha) \in \rho_\eta(L_a(\alpha))$ because the latter does not exist if $L_a(\alpha)$ has no transitions.

Global soundness $[LB\cup]$. Let ω be an arbitrary PD-model.

We must show that $\text{val}_\eta(\omega, [L_a(\alpha \cup \beta)]\, B_a(\xi))$. We will split the proof into multiple claims that cover all possible cases.

Claim 1: If there are no transitions $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$ or $(\omega, \nu_\beta) \in \rho_\eta(\beta)$, the rule is sound.

If there are no such transitions, then there can be no transition $(\omega, \omega_\cup) \in \rho_\eta(L_a(\alpha \cup \beta))$, and therefore the rule is trivially satisfied.

Claim 2: If there are transitions $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$ and $(\omega, \nu_\beta) \in \rho_\eta(\beta)$, the rule is sound.

If there is a transition $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$, then there must be $(\omega, \omega_\alpha) \in \rho_\eta(L_a(\alpha))$. Therefore, $W(\omega_\alpha) = W_\alpha$ and $W(\omega_\alpha) \subseteq W(\omega_\cup)$.

By the left conjunct of the hypothesis, $\text{val}_\eta(\omega_\alpha, B_a(\xi))$, and so for every $\nu_\alpha \in \omega_\alpha$, we have $\text{val}_\eta(\omega_\alpha \oplus \nu_\alpha, \xi)$. Using the same argument, $W(\omega_\beta) \subseteq W(\omega_\cup)$ and so for every $\nu_\beta \in \omega_\beta$, $\text{val}_\eta(\omega_\alpha \oplus \nu_\alpha, \xi)$.

However, $W(\omega_\cup) = W(\omega_\alpha) \cup W(\omega_\beta)$, and therefore for every $\nu_\cup \in \omega_\cup$, $\text{val}_\eta(\omega_\cup \oplus \nu_\cup, \xi)$. Thus, $\text{val}_\eta(\omega_\cup, B_a(\xi))$. This is exactly the statement for the conclusion of the proof rule.

The specific nondeterministic choice of the distinguished world for $\omega_\cup$ is irrelevant since $B_a(\xi)$ effectively overwrites it with every world of $\omega_\cup$.

Claim 3: If there is only one of the following two transitions, $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$ and $(\omega, \nu_\beta) \in \rho_\eta(\beta)$, the rule is sound.

Without loss of generality, let $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$ but not $(\omega, \nu_\beta) \in \rho_\eta(\beta)$.

If $W_\beta = \emptyset$, then β contributes no worlds to $W(\omega_\cup)$, thus $W_\cup = W_\alpha$. Because $(\omega, \nu_\alpha) \in \rho_\eta(\alpha)$, then there is a transition $(\omega, \omega_\alpha) \in \rho_\eta(L_a(\alpha))$, and $\omega_\cup = \omega_\alpha$. Thus, the program in the conclusion of the rule is reduced to the program in the left conjunct of the hypothesis, $[L_a(\alpha)]\, B_a(\xi)$, and the rule is sound.

However, it is possible that $W_\beta \neq \emptyset$. If there is no transition $(\omega, \omega_\beta) \in \rho_\eta(L_a(\beta))$, that only means the *distinguished world* failed to transition using β. There may be other worlds $t \in \omega$ such that $(\omega \oplus t, \nu_\beta) \in \rho_\eta(\beta)$, and thus $\nu_\beta \in \omega_\cup$. Thus, $W(\omega_\cup) = W(\omega_\alpha) \cup W_\beta$.

Claim 2 already shows that for all $\nu_\alpha \in \omega_\alpha$, $\text{val}_\eta(\omega_\cup \oplus \nu_\alpha, \xi)$. Unfortunately, we cannot use the hypothesis to show the same for $\nu_\beta \in \omega_\beta$, since $[L_a(\beta)]\, B_a(\xi)$ is trivially satisfied due to there being no transitions for $L_a(\beta)$.

Global soundness helps here. We will construct a PD-model that is semantically equivalent to ω, whose choice of distinguished world allows a transition, and thus the hypothesis to be applied. Because we are picking a new distinguished world, we must lose any information which we had from the previous choice, i.e. we must remove the formulas in Γ_O.

Since $W_\beta \neq \emptyset$, let $\mu \in W_\beta$ be one of those worlds which transitioned, and let $u = \textsc{dw}(\mu)$. Now consider the PD-model $\omega_\mu = \omega \oplus u$, which is equivalent to ω except we now know $(\omega \oplus u, \mu) \in \rho_\eta(\beta)$. Therefore, there is now $(\omega_\mu, \omega_\beta) \in \rho_\eta(L_a(\beta))$. To apply the hypothesis, we can no longer satisfy Γ_O because $u \neq \textsc{dw}(\omega)$, which is why it is no present in the antecedent of the premise's sequent. We may thus conclude that for all $\nu_\beta \in \omega_\beta$, $\text{val}_\eta(\omega_\cup \oplus \nu_\beta, \xi)$.

Thus, since for all $\nu_\alpha \in \omega_\alpha$, $\text{val}_\eta(\omega_\cup \oplus \nu_\alpha, \xi)$, $\nu_\beta \in \omega_\beta$, $\text{val}_\eta(\omega_\cup \oplus \nu_\beta, \xi)$, and $W(\omega_\cup) = W(\omega_\alpha) \cup W(\omega_\beta)$, then for all $\nu_\cup \in \omega_\cup$, $\text{val}_\eta(\omega_\cup \oplus \nu_\cup, \xi)$.

Therefore, $\mathrm{val}_\eta\left(\omega_\cup, B_a\left(\xi\right)\right)$. □

B.5 Doxastic assignment

The proof rules for doxastic assignment are sound, and are based on syntactic substitution. They follow directly from admissibility and the substitution lemmas proved in Appendix C below.

C Substitution Lemma

The substitution lemma means that the learned doxastic assignment proof rules are sound rather directly.

C.1 Admissibility

Definition 12 (Substitution)**.** *A substitution is a function σ from*

- *state variables into terms that do not contain doxastic variables, e.g. $\sigma\left(x\right) = \theta$, where θ does not contain doxastic variables, and*
- *doxastic variables to any term, $\sigma\left(x_a\right) = \theta$.*

Furthermore, substitutions can be lifted to formulas and PD-models:

- *$\sigma\left(\phi\right) = \psi$, where ψ concurs with ψ except every occurrence of substituted variable x has been replaced with $\sigma\left(x\right)$.*
- *$\sigma\left(\langle r, W, V, s\rangle\right) = \langle r, W, \sigma\left(V\right), s\rangle$, with $\sigma\left(V\right)(t)(x_a) = val_\eta\left(\omega \oplus t, \sigma\left(x_a\right)\right)$ for substituted variables x_a, and $\sigma\left(V\right)(t)(y_a) = \omega(t)(y_a)$ for unsubstituted variables y_a.*

Definition 13 (Admissibility)**.** *A substitution $\sigma\left(x\right) = \theta$ of state, logical or doxastic variable x is admissible for formula ϕ if no occurrence of x in ϕ appears within the scope of a binding quantifier or modality and no variable in the expression θ becomes bounded.*

Thus far, the definition does not differ from what we find in $\mathsf{d}\mathcal{L}$, though now we must address doxastic variables. Intuitively, the learning operator works on doxastic state, and therefore it will bind doxastic instead of physical variables.

Definition 14 (Bound variables)**.** *The following constructs bind variables.*

- *Quantifiers $\forall X$ and $\exists X$ bind logical variable X.*
- *$x := \theta$ and $x' = f(x)$ bind state variable x.*
- *$x_a := \theta$, inside or outside a learning operator, binds doxastic variable x_a.*
- *$?\phi$ inside a learning operator binds any doxastic variable that appears within ϕ.*

C.2 Proofs of substitution lemmas

Substitutions lemmas allow us to handle assignment as *syntactic substitution*, e.g. replacing $[x := \theta]\,\phi(x)$ with $\phi(\theta)$ during a sequent proof. In this, they serve to eliminate dynamic modalities and bring us closer to a pure first-order logic formula which can be addressed with quantifier-elimination procedures.

The first lemma is directly copied from $\mathsf{d}\mathcal{L}$.

Lemma 2 (Substitution Lemma)**.** *Let σ be an admissible substitution for the formula ϕ, and let σ replace only logical or state variables. Then, for each η and $\omega = \langle r, W, V, s\rangle$*

$$val_\eta\left(\omega, \sigma\left(\phi\right)\right) = val_{\sigma(\eta)}\left(\langle \sigma\left(r\right), W, V, s\rangle, \phi\right)$$

where $\sigma\left(\eta\right)$ concurs with η except $\sigma\left(\eta\right)(X) = val_\eta\left(\omega, \sigma\left(X\right)\right)$ for substituted variable logical X and $\sigma\left(r\right)$ concurs with r except $\sigma\left(r\right)(x) = val_\eta\left(\omega, \sigma\left(x\right)\right)$ for substituted state variable x.

The lemma of interest to us is, in some sense, an application of the above at each possible world $t \in \omega$.

Lemma 3 (Doxastic Substitution Lemma)**.** *Let ϕ be a formula. Let σ be an admissible substitution for ϕ which replaces only doxastic variable x_a. Then, for every η and $\omega = \langle r, W, V, s\rangle$,*

$$val_\eta\left(\omega, \sigma\left(\phi\right)\right) = val_\eta\left(\sigma\left(\omega\right), \phi\right)$$

where $\sigma\left(\omega\right) = \langle r, W, \sigma\left(V\right), s\rangle$, and for all $t \in \omega$

1. $\sigma\left(V\right)(t)(x_a) = val_\eta\left(\omega \oplus t, \sigma\left(x_a\right)\right)$
2. $\sigma\left(V\right)(t)(y_a) = V(t)(y_a) = \omega(t)(y_a)$

Thus, the substituted valuation $\sigma\left(V\right)$ only alters the interpretation of the substituted variable x_a, leaving every other interpretation unchanged. Using our shortcut notation, we may rewrite these two conditions more simply as, for all $t \in \omega$,

1. $\sigma\left(\omega\right)(t)(x_a) = \mathrm{val}_\eta\left(\omega \oplus t, \sigma\left(x_a\right)\right)$
2. $\sigma\left(\omega\right)(t)(y_a) = \omega(t)(y_a)$

This lemma will be proven by structural induction on ϕ, meaning that we will need the lemma for terms, formulas and programs.

Lemma 4. *Let θ be a term. Let σ be an admissible substitution for ϕ which replaces only one doxastic variable, x_a. Then, for every η, and $\omega = \langle r, W, V, s\rangle$,*

$$val_\eta\left(\omega, \sigma\left(\theta\right)\right) = val_\eta\left(\sigma\left(\omega\right), \theta\right)$$

Proof. By structural induction on θ.

- x: $\text{val}_\eta(\omega, \sigma(x)) = \text{val}_\eta(\omega, x) = \text{R}(\omega)(x) = \text{R}(\sigma(\omega))(x) = \text{val}_\eta(\sigma(\omega), x)$
- X: $\text{val}_\eta(\omega, \sigma(X)) = \text{val}_\eta(\omega, X) = \eta(X) = \text{val}_\eta(\sigma(\omega), X)$
- x_a: $\text{val}_\eta(\omega, \sigma(x_a)) = \text{val}_\eta(\omega \oplus s, \sigma(x_a))$, which, by Lemma 3's hypothesis 1) applied with $t = s$, means $\text{val}_\eta(\omega \oplus s, \sigma(x_a)) = \sigma(\omega)(s)(x_a) = \text{val}_\eta(\sigma(\omega), x_a)$
- $y_a \neq x_a$: $\text{val}_\eta(\omega, \sigma(y_a)) = \text{val}_\eta(\omega, y_a) = \omega(s)(y_a)$, which, by Lemma 3's hypothesis 2), $\omega(s)(y_a) = \sigma(\omega)(s)(y_a) = \text{val}_\eta(\sigma(\omega), y_a)$
- $\theta_1 \oplus \theta_2$: $\text{val}_\eta(\omega, \sigma(\theta_1 \oplus \theta_2)) = \text{val}_\eta(\omega, \sigma(\theta_1) \oplus \sigma(\theta_2)) = \text{val}_\eta(\omega, \sigma(\theta_1)) \oplus \text{val}_\eta(\omega, \sigma(\theta_2))$ which, by induction hypothesis, $\text{val}_\eta(\sigma(\omega), \theta_1) \oplus \text{val}_\eta(\sigma(\omega), \theta_2) = \text{val}_\eta(\sigma(\omega), \theta_1 \oplus \theta_2)$

□

Proposition 2. *Let Ω be the set of PD-models and σ be a substitution. Now let $\sigma(\Omega) = \{\sigma(\omega) : \omega \in \Omega\}$. Then, $\sigma(\Omega) \subseteq \Omega$.*

Lemma 5. *Let ϕ be a formula. Let σ be an admissible substitution for ϕ which replaces only doxastic variables. Then, for every η, and $\omega = \langle r, W, V, s\rangle$,*

$$val_\eta(\omega, \sigma(\phi)) = val_\eta(\sigma(\omega), \phi)$$

Proof. By structural induction on ϕ.

- $\theta_1 < \theta_2$. For propositions,

$$\begin{aligned} \text{val}_\eta(\omega, \sigma(\theta_1 < \theta_2)) &= \text{val}_\eta(\omega, \sigma(\theta_1) < \sigma(\theta_2)) \\ &= \text{val}_\eta(\omega, \sigma(\theta_1)) < \text{val}_\eta(\omega, \sigma(\theta_2)) \\ &\overset{lem.4}{=} \text{val}_\eta(\sigma(\omega), \theta_1) < \text{val}_\eta(\sigma(\omega), \theta_2) \\ &= \text{val}_\eta(\sigma(\omega), \theta_1 < \theta_2) \end{aligned}$$

- $\neg\phi$. For negation,

  $\text{val}_\eta(\omega, \sigma(\neg\phi)) = \text{val}_\eta(\omega, \neg\sigma(\phi)) = 1 - \text{val}_\eta(\omega, \sigma(\phi)) \overset{\text{IH}}{=}$
  $\overset{\text{IH}}{=} 1 - \text{val}_\eta(\sigma(\omega), \phi)) = \text{val}_\eta(\sigma(\omega), \neg\phi))$

- $\phi_1 \wedge \phi_2$. For conjunction,

  $\text{val}_\eta(\omega, \sigma(\phi_1 \wedge \phi_2)) = \text{val}_\eta(\omega, \sigma(\phi_1) \wedge \sigma(\phi_2)) = \min(\text{val}_\eta(\omega, \sigma(\phi_1)), \text{val}_\eta(\omega, \sigma(\phi_2))) \overset{\text{IH}}{=}$
  $\min(\text{val}_\eta(\sigma(\omega), \phi_1)), \text{val}_\eta(\sigma(\omega), \phi_2))) = \text{val}_\eta(\sigma(\omega), \phi_1 \wedge \phi_2))$

- $\forall X.\phi$. For logical quantifiers, $\text{val}_\eta(\omega, \sigma(\forall X.\phi)) = \text{val}_\eta(\omega, \forall X.\sigma(\phi))$.

  Now, $\text{val}_\eta(\omega, \forall X.\sigma(\phi))$ iff for all $v \in \mathbb{R}$, $\text{val}_{\eta[X\mapsto v]}(\omega, \sigma(\phi))$. We apply the induction hypothesis for each variable assignment $\eta[X \mapsto v]$. We may do this because the variable assignment is universally quantified in the statement of Lemma 5. Thus, for all $v \in \mathbb{R}$, $\text{val}_{\eta[X \mapsto v]} \left(\sigma_{\eta[X \mapsto v]}(\omega), \phi\right)$, where $\sigma_{\eta[X \mapsto v]}(\omega)(t)(x_a) = \text{val}_{\eta[X \mapsto v]} (\omega, \sigma (x_a))$.

Notice that the application of the induction hypothesis results in a different substitution $\sigma_{\eta[X \mapsto v]}(\omega)$ for each $v \in \mathbb{R}$, which means we cannot reintroduce the quantifier $\forall X$.

Crucially, however, because the substitution is admissible, X cannot occur in $\sigma (x_a)$, and its interpretation is independent of the variable assignment of X. Thus, for each $v \in \mathbb{R}$, $\text{val}_{\eta[X \mapsto v]} (\omega, \sigma (x_a)) = \text{val}_{\eta} (\omega, \sigma (x_a))$, and thus $\sigma_{\eta[X \mapsto v]}(\omega)(t)(x_a) = \sigma (\omega)(t)(x_a)$ for all $t \in \omega$. More generally and succinctly, $\sigma_{\eta[X \mapsto v]}(\omega) = \sigma (\omega)$. We find, then, that for all $v \in \mathbb{R}$, $\text{val}_{\eta[X \mapsto v]} \left(\sigma_{\eta[X \mapsto v]}(\omega), \phi\right)$ is equivalent to for all $v \in \mathbb{R}$, $\text{val}_{\eta[X \mapsto v]} (\sigma (\omega), \phi)$, from which we may directly conclude $\text{val}_{\eta} (\sigma (\omega), \forall X.\phi)$.

- $B (\phi)$. For the doxastic belief modality,
  $\text{val}_{\eta} (\omega, \sigma (B (\phi))) = \text{val}_{\eta} (\omega, B (\sigma (\phi)))$ iff
  for all $t \in \omega$, $\text{val}_{\eta} (\omega \oplus t, \sigma (\phi))$ iff, by induction hypothesis on each $\omega \oplus t$,
  for all $t \in \omega$, $\text{val}_{\eta} (\sigma (\omega \oplus t), \phi)$ iff
  for all $t \in \omega$, $\text{val}_{\eta} (\sigma (\omega) \oplus t, \phi)$ iff
  $\text{val}_{\eta} (\sigma (\omega), B (\phi))$.

- $[\alpha] \phi$. For the dynamic box modality, we must show $\text{val}_{\eta} (\omega, \sigma ([\alpha] \phi))$ iff $\text{val}_{\eta} (\sigma (\omega), [\alpha] \phi)$.

$\Rightarrow$ direction

We must prove $\text{val}_{\eta} (\sigma (\omega), [\alpha] \phi)$, for which it suffices to show that:

for all ν, if $(\sigma (\omega), \nu) \in \rho_{\eta} (\alpha)$, then $\text{val}_{\eta} (\nu, \phi)$

Thus, let ν be any PD-model such that $(\sigma (\omega), \nu) \in \rho_{\eta} (\alpha)$. We must show $\text{val}_{\eta} (\nu, \phi)$.

By Lemma 6.2, there is ω' such that $(\omega, \omega') \in \rho_{\eta} (\sigma (\alpha))$ and $\nu = \sigma (\omega')$. It thus suffices to show that $\text{val}_{\eta} (\sigma (\omega'), \phi)$ to conclude the proof.

By the hypothesis $\text{val}_{\eta} (\omega, \sigma ([\alpha] \phi))$, for all ω'', if $(\omega, \omega'') \in \rho_{\eta} (\sigma (\alpha))$, then $\text{val}_{\eta} (\omega'', \sigma (\phi))$. By taking $\omega'' = \omega'$, we obtain $\text{val}_{\eta} (\omega', \sigma (\phi))$.

By Lemma 5, we conclude $\text{val}_{\eta} (\sigma (\omega'), \phi)$.

$\Leftarrow$ direction

We must prove $\text{val}_{\eta} (\omega, [\sigma (\alpha)] \sigma (\phi))$, for which it suffices to show that:

for all ω', if $(\omega, \omega') \in \rho_{\eta} (\sigma (\alpha))$, then $\text{val}_{\eta} (\omega', \sigma (\phi))$

Thus, let $\omega' \in \Omega$ be an arbitrary PD-model such that $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$. We must show $\mathrm{val}_\eta(\omega', \sigma(\phi))$.

By Lemma 6.1, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$. By hypothesis, $\mathrm{val}_\eta(\sigma(\omega), [\alpha]\,\phi)$, and thus, for all ν, if $(\sigma(\omega), \nu) \in \rho_\eta(\alpha)$ then $\mathrm{val}_\eta(\nu, \phi)$. Choosing $\nu = \sigma(\omega')$, we get $\mathrm{val}_\eta(\sigma(\omega'), \phi)$, to which we may apply Lemma 5 to obtain $\mathrm{val}_\eta(\omega', \sigma(\phi))$.

□

Lemma 6. *Let γ be a program. Let σ be an admissible substitution for α which replaces only doxastic variable x_a. Then, for every η, ω,*

1. *If $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$ then $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$*
2. *If $(\sigma(\omega), \nu) \in \rho_\eta(\alpha)$ then there is ω' such that $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$ and $\nu = \sigma(\omega')$*

Proof. By structural induction on α.

- $y := \theta$.

$\Rightarrow$ direction.

Let $(\omega, \omega') \in \rho_\eta(y := \sigma(\theta))$. We will apply the substitution to ω and ω', and show that $\sigma(\omega)$ and $\sigma(\omega')$ conforms to the behavior of the program $y := \theta$, i.e. $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(y := \theta)$.

All unassigned physical variables are unchanged:
By the semantics of assignment, $\omega' = \omega$ except $\omega'(y) = \mathrm{val}_\eta(\omega, \sigma(\theta))$. Thus, for all $z \neq y$, $\omega'(z) = \omega(z)$. Because doxastic substitution does not affect physical variables,

$$\sigma(\omega')(z) = \sigma(\omega)(z)$$

The variable y changes according to assignment:
We must show $\mathrm{val}_\eta(\sigma(\omega'), y) = \mathrm{val}_\eta(\sigma(\omega), \theta)$.

The substitution σ does not affect physical variables, so $\mathrm{val}_\eta(\sigma(\omega'), y) = \mathrm{val}_\eta(\omega', y)$. By the definition of assignment, $\mathrm{val}_\eta(\omega', y) = \mathrm{val}_\eta(\omega, \sigma(\theta))$. Because doxastic variables cannot show up in regular assignment, and the substitution only affects doxastic variables, $\mathrm{val}_\eta(\omega, \sigma(\theta)) = \mathrm{val}_\eta(\omega, \theta) = \mathrm{val}_\eta(\sigma(\omega), \theta)$. Thus,

$$\mathrm{val}_\eta(\sigma(\omega'), y) = \mathrm{val}_\eta(\sigma(\omega), \theta)$$

All unsubstituted doxastic variables are unchanged:

By the semantics of assignment, for all doxastic variables z_a and all $t \in \omega$, $\omega'(t)(z_a) = \omega(t)(z_a)$. For all *unsubstituted* doxastic variables $z_a \neq x_a$, and $t \in \omega$,

$$\sigma(\omega')(t)(z_a) = \sigma(\omega)(t)(z_a)$$

The substituted variable is unchanged:

Assignment does not change the number of possible worlds, and therefore in the following, $t \in \omega$ and $t \in \omega'$ are interchangeable statements.

Because the substitution σ is admissible for the assignment, $\sigma(x_a)$ cannot contain occurrences of the bound variable y. This is the only change from ω to ω'. Therefore, for all $t \in \omega$, $\text{val}_\eta(\omega' \oplus t, \sigma(x_a)) = \text{val}_\eta(\omega \oplus t, \sigma(x_a))$.

But then, by the definition of substitution, $\sigma(\omega) = \omega$ and $\sigma(\omega') = \omega'$, except for all $t \in \omega$, $\sigma(\omega)(t)(x_a) = \text{val}_\eta(\omega \oplus t, \sigma(x_a))$, and $\sigma(\omega')(t)(x_a) = \text{val}_\eta(\omega' \oplus t, \sigma(x_a))$.

This, along with $\text{val}_\eta(\omega' \oplus t, \sigma(x_a)) = \text{val}_\eta(\omega \oplus t, \sigma(x_a))$, means that for all $t \in \omega$,

$$\sigma(\omega')(t)(x_a) = \sigma(\omega)(t)(x_a)$$

Conclusion

We have shown that $\sigma(\omega')$ and $\sigma(\omega)$ concur in everything except the differences explained precisely by the assignment $y := \theta$. As such, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$.

$\Leftarrow$ direction.

Since the program $y := \sigma(\theta)$ is deterministic, we can choose ω' as the unique PD-model such that $(\omega, \omega') \in \rho_\eta(y := \sigma(\theta))$. We are then in the exact same situation as the $\Rightarrow$ direction, for which we already have a proof.

- $?\phi$.

  $\Rightarrow$ direction.

  Assume $(\omega, \omega') \in \rho_\eta(?\sigma(\phi))$. By the semantics of test, this is equivalent to $(\omega, \omega) \in \rho_\eta(?\sigma(\phi))$, which is true iff $\text{val}_\eta(\omega, \sigma(\phi))$. By Lemma 5, it is true iff $\text{val}_\eta(\sigma(\omega), \phi)$, which, again by the semantics of test, is true iff $(\sigma(\omega), \sigma(\omega)) \in \rho_\eta(?\phi)$.

  $\Leftarrow$ direction.

  Same as previous case, by taking $\omega' = \omega$, and thus $\nu = \sigma(\omega)$.

- $\alpha \cup \beta$.

  $\Rightarrow$ direction.

  Assume $(\omega, \omega') \in \rho_\eta(\sigma(\alpha) \cup \sigma(\beta))$. Then, $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$ or $(\omega, \omega') \in \rho_\eta(\sigma(\beta))$. Without loss of generality, assume the former. By induction hypothesis, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$, and therefore, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha \cup \beta)$.

$\Leftarrow$ direction.

Assume $(\sigma(\omega), \nu) \in \rho_\eta(\alpha \cup \beta)$. Without loss of generality, assume $(\sigma(\omega), \nu) \in \rho_\eta(\alpha)$. By induction hypothesis, there is ω' such that $\nu = \sigma(\omega')$ and $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$. Therefore, $(\omega, \omega') \in \rho_\eta(\sigma(\alpha) \cup \sigma(\beta))$.

- $\alpha; \beta$.

$\Rightarrow$ direction.

Assume $(\omega, \omega'') \in \rho_\eta(\sigma(\alpha); \sigma(\beta))$. Then, there is ω' such that $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$ and $(\omega', \omega'') \in \rho_\eta(\sigma(\beta))$. By induction hypothesis, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$. Because the statement of this theorem quantifies over all PD-models, we can again use the induction hypothesis to obtain $(\sigma(\omega'), \sigma(\omega'')) \in \rho_\eta(\beta)$. Thus, $(\sigma(\omega), \sigma(\omega'')) \in \rho_\eta(\alpha; \beta)$.

$\Leftarrow$ direction.

Assume $(\sigma(\omega), \nu') \in \rho_\eta(\alpha; \beta)$. Then, there is ν such that $(\sigma(\omega), \nu) \in \rho_\eta(\alpha)$ and $(\nu, \nu') \in \rho_\eta(\beta)$. By induction hypothesis, there is ω' such that $\nu = \sigma(\omega')$ and $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$.

Since $\nu = \sigma(\omega')$, then $(\nu, \nu') \in \rho_\eta(\beta)$ is equivalent to $(\sigma(\omega'), \nu') \in \rho_\eta(\beta)$. We may therefore apply the induction hypothesis to ascertain that there is ω'' such that $\nu' = \sigma(\omega'')$ and $(\omega', \omega'') \in \rho_\eta(\sigma(\beta))$.

From $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$ and $(\omega', \omega'') \in \rho_\eta(\sigma(\beta))$ we conclude $(\omega, \omega'') \in \rho_\eta(\sigma(\alpha); \sigma(\beta))$.

- α^*

$\Rightarrow$ direction.

Assume $(\omega, \omega') \in \rho_\eta(\sigma(\alpha)^*)$. Then, there is $i \geq 0$, $(\omega, \omega') \in \rho_\eta\left(\sigma(\alpha)^i\right)$, with α^i being α sequentially composed i times, $\alpha; ...; \alpha$. We start with the base cases.

When $i = 0$. Then $\alpha^0 = ?\mathit{True}$. $(\omega, \omega') \in \rho_\eta(\sigma(?\mathit{True}))$ iff $(\omega, \omega) \in \rho_\eta(?\mathit{True})$ iff $(\sigma(\omega), \sigma(\omega)) \in \rho_\eta(?\mathit{True})$.

When $i = 1$. Then $\alpha^1 = \alpha$. Assume $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$. By structural induction hypothesis, $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\alpha)$.

When $i > 1$, let $\omega_0 = \omega$ and $\omega_i = \omega'$, and assume $(\omega_0, \omega_i) \in \rho_\eta\left(\sigma(\alpha)^i\right)$. Then, by the definition of sequential composition, there are ω_j with $0 \leq j < i$ such that $(\omega_j, \omega_{j+1}) \in \rho_\eta(\sigma(\alpha))$. Applying the induction hypothesis for all $0 \leq j < i$, then $(\sigma(\omega_j), \sigma(\omega_{j+1})) \in \rho_\eta(\alpha)$, and thus, $(\sigma(\omega_0), \sigma(\omega_i)) \in \rho_\eta(\alpha^i)$.

$\Leftarrow$ direction.

Assume $(\sigma(\omega), \nu) \in \rho_\eta(\alpha^*)$. Then, there is $i \geq 0$, $(\sigma(\omega), \nu) \in \rho_\eta(\alpha^i)$, with α^i being α sequentially composed i times, $\alpha; ...; \alpha$. We start with the base cases.

When $i = 0$. Then $\alpha^0 = ?\mathit{True}$. $(\sigma(\omega), \nu) \in \rho_\eta(?\mathit{True})$ iff $\nu = \sigma(\omega)$ and $(\sigma(\omega), \sigma(\omega)) \in \rho_\eta(?\mathit{True})$ iff $(\omega, \omega) \in \rho_\eta(?\mathit{True})$ iff $(\omega, \omega) \in \rho_\eta(\sigma(?\mathit{True}))$.

When $i = 1$. Then $\alpha^1 = \alpha$. Assume $(\sigma(\omega), \nu) \in \rho_\eta(\alpha)$. By structural induction hypothesis, there is ω' such that $\nu = \sigma(\omega')$ and $(\omega, \omega') \in \rho_\eta(\sigma(\alpha))$.

When $i > 1$, let $\omega_0 = \omega$ and $\nu_i = \nu$, and assume $(\sigma(\omega_0), \nu_i) \in \rho_\eta(\alpha^i)$. Then, there for all $1 \leq j < i$ there are ν_j such that $(\nu_j, \nu_{j+1}) \in \rho_\eta(\alpha^i)$, and also $(\sigma(\omega_0), \nu_1) \in \rho_\eta(\alpha)$.

Now, for $j = 0, 1, ..., i-1$, in this order, we make the following argument. We know $(\sigma(\omega_j), \nu_{j+1}) \in \rho_\eta(\alpha)$. By structural induction hypothesis, there is ω_{j+1} such that $\nu_{j+1} = \sigma(\omega_{j+1})$, and $(\omega_j, \omega_{j+1}) \in \rho_\eta(\sigma(\alpha))$. But since $\nu_{j+1} = \sigma(\omega_{j+1})$, then $(\sigma(\omega_j + 1), \nu_{j+2}) \in \rho_\eta(\alpha)$, so that we may apply this argument again. Finally, in the last step, $(\omega_{i-1}, \omega_i) \in \rho_\eta(\sigma(\alpha))$ with $\nu = \nu_i = \sigma(\omega_i)$. Then, there is indeed $\omega' = \omega_i$ such that $\nu = \sigma(\omega')$, and $(\omega, \omega') \in \rho_\eta\left(\sigma(\alpha)^i\right)$.

- $L_a(\gamma)$

  By Lemma 7.

$\square$

As a reminder, the semantics of learning are as follows. $(\omega, \omega') \in \rho_\eta(L(\gamma))$ iff all of the following:

1. $r' = r$
2. $W' = \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\gamma)\}$
3. $\omega'(\nu) = \mathrm{DV}(\nu)$ for all $\nu \in \omega'$
4. $\mathrm{DW}(\mathrm{DW}(\omega')) = \mathrm{DW}(\omega)$

Proposition 3. *If* $(\omega \oplus t, \nu) \in \rho_\eta(\gamma)$, *then* $\mathrm{DW}(\nu) = t$.

Lemma 7. *Let γ be a program. Let σ be an admissible substitution for $L_a(\gamma)$ which replaces only doxastic variable x_a. Then, for every η, ω,*

1. *If* $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma)))$ *then* $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma))$
2. *If* $(\sigma(\omega), \nu) \in \rho_\eta(L_a(\gamma))$ *then there is* ω' *such that* $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma)))$ *and* $\nu = \sigma(\omega')$

Proof. By structural induction on γ. Many of the following cases are proven by analyzing the effect of the substitution on the PD-models ω and ω' from the transition $(\omega, \omega') \in \rho_\eta(\sigma(\gamma))$, i.e. by analyzing $\sigma(\omega)$ and $\sigma(\omega')$. Then, the proof checks that those substituted PD-models satisfy the transition for γ, i.e. $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(\gamma)$.

- $y_a \coloneqq \theta$.

$$\Rightarrow \text{direction}$$
$$(\omega, \omega') \in \rho_\eta (L_a(y_a \coloneqq \sigma(\theta))) \text{ then } (\sigma(\omega), \sigma(\omega')) \in \rho_\eta (L_a(y_a \coloneqq \theta))$$

Let $(\omega, \omega') \in \rho_\eta (L_a(y_a \coloneqq \sigma(\theta)))$. We must show $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta (L_a(y_a \coloneqq \theta))$.

We begin by analyzing the component parts of ω' using the semantics of the learning operator.

  - $\textsc{r}(\omega') = \textsc{r}(\omega)$
  - $W(\omega') = \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta (y_a \coloneqq \sigma(\theta))\}$
  - $\textsc{dw}(\textsc{dw}(\omega')) = \textsc{dw}(\omega)$

We will look at $V(\omega')$ in terms of x_a, the substituted variable; y_a, the assigned variable; and of z_a, any other variable distinct from x_a and y_a. By the admissibility of substitution and because the assignment binds y_a, $x_a \neq y_a$.

By the semantics of learned assignment, for all $\nu \in \omega'$, let $t = \textsc{dw}(\nu)$, and

$$\omega'(\nu)(x_a) = \omega(t)(x_a) \tag{4}$$
$$\omega'(\nu)(y_a) = \text{val}_\eta (\omega \oplus t, \sigma(\theta)) \tag{5}$$
$$\omega'(\nu)(z_a) = \omega(t)(z_a) \tag{6}$$

We may now apply the substitution σ to ω and ω'. Since it only affects $V(\omega)$ and $V(\omega')$ respectively, this is our focus.

For all $t \in \omega$,

$$\sigma(\omega)(t)(x_a) = \text{val}_\eta (\omega \oplus t, \sigma(x_a)) \tag{7}$$
$$\sigma(\omega)(t)(y_a) = \omega(t)(y_a)$$
$$\sigma(\omega)(t)(z_a) = \omega(t)(z_a) \tag{8}$$

For all $\nu \in \omega'$,

$$\sigma(\omega')(\nu)(x_a) = \text{val}_\eta (\omega' \oplus \nu, \sigma(x_a))$$
$$\sigma(\omega')(\nu)(y_a) = \omega'(\nu)(y_a) \tag{9}$$
$$\sigma(\omega')(\nu)(z_a) = \omega'(\nu)(z_a) \tag{10}$$

We must now show that $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta (L_a(y_a \coloneqq \theta))$.

We note immediately that $\textsc{r}(\sigma(\omega')) = \textsc{r}(\omega') = \textsc{r}(\omega) = \textsc{r}(\sigma(\omega))$, and, with a similar argument, $W(\sigma(\omega')) = W(\sigma(\omega))$ and $\textsc{dw}(\sigma(\omega')) = \textsc{dw}(\sigma(\omega))$.

To satisfy the semantics of learned assignment, all that is left is to show that, for all $\nu \in \sigma(\omega')$, with $t = \textsc{dw}(\nu)$, i $\sigma(\omega')(\nu)(x_a) = \sigma(\omega)(t)(x_a)$

By the definition of substitution, $\sigma(\omega')(\nu)(x_a) = \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a))$. By the admissibility condition that one may not substitute in a bound variable, then y_a cannot occur in $\sigma(x_a)$. But, by (4)-(6), this is the only difference between ω' and ω.

Therefore, $\sigma(\omega')(\nu)(x_a) = \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) = \text{val}_\eta(\omega \oplus t, \sigma(x_a)) \overset{(7)}{=} \sigma(\omega)(t)(x_a)$.

ii $\sigma(\omega')(\nu)(y_a) = \text{val}_\eta(\sigma(\omega) \oplus t, \theta)$

As follows: $\sigma(\omega')(\nu)(y_a) \overset{(9)}{=} \omega'(\nu)(y_a) \overset{(5)}{=} \text{val}_\eta(\omega \oplus t, \sigma(\theta)) \overset{Lem.4}{=} \text{val}_\eta(\sigma(\omega \oplus t), \theta) = \text{val}_\eta(\sigma(\omega) \oplus t, \theta)$

iii $\sigma(\omega')(\nu)(z_a) = \sigma(\omega)(t)(z_a)$

As follows: $\sigma(\omega')(\nu)(z_a) \overset{(10)}{=} \omega'(\nu)(z_a) \overset{(6)}{=} \omega(t)(z_a) \overset{(8)}{=} \sigma(\omega')(\nu)(z_a)$

$\Leftarrow$ direction

If $(\sigma(\omega), \nu) \in \rho_\eta(L_a(y_a \coloneqq \theta))$ then there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(y_a \coloneqq \sigma(\theta)))$ and $\nu = \sigma(\omega')$

It is not hard to see from the definition of the learning operator and of doxastic assignment that the program $L_a(y_a \coloneqq \sigma(\theta))$ is deterministic. Therefore, we may choose ω' exactly as in the $\Rightarrow$ direction, and all of the equalities established for that directions apply here too, concluding the proof.

- $?\psi$.

$\Rightarrow$ direction

$(\omega, \omega') \in \rho_\eta(L_a(?\sigma(\psi)))$ then $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(?\psi))$

Let $(\omega, \omega') \in \rho_\eta(L_a(?\sigma(\psi)))$.

We begin by analyzing the component parts of ω' using the semantics of the learning operator.

- $\text{R}(\omega') = \text{R}(\omega)$
- $W(\omega') = \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(?\sigma(\psi))\}$
- $\text{DW}(\text{DW}(\omega')) = \text{DW}(\omega)$

Furthermore, according to the semantics of learned test, no variables change value. Thus, for all $\nu \in \omega'$ with $t = \text{DW}(\nu)$, and *any* doxastic variable y_a, including the substituted variable x_a,

$$\omega'(\nu)(y_a) = \omega(t)(y_a) \tag{11}$$

Let us now apply the substitution σ to ω and ω'. Since it only affects $V(\omega)$ and $V(\omega')$ respectively, this is our focus. As usual x_a is the substituted variable, and y_a is any unsubstituted variable, whether it shows up in ψ or not.

For all $t \in \omega$,

$$\begin{aligned} \sigma(\omega)(t)(x_a) &= \text{val}_\eta(\omega \oplus t, \sigma(x_a)) \\ \sigma(\omega)(t)(y_a) &= \omega(t)(y_a) \end{aligned} \tag{12}$$

For all $\nu \in \omega'$,

$$\begin{aligned} \sigma(\omega')(\nu)(x_a) &= \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) \\ \sigma(\omega')(\nu)(y_a) &= \omega'(\nu)(y_a) \end{aligned} \tag{13}$$

To show that $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(?\psi))$, by the semantics of learned test, it suffices to show that:

1. $W(\sigma(\omega')) = \{\nu :$ there is $t \in \sigma(\omega)$ s.t. $(\sigma(\omega) \oplus t, \nu) \in \rho_\eta(?\psi)\}$
   By the definition of substitution, we know

   $$\begin{aligned} W(\sigma(\omega')) &= W(\omega') \\ W(\sigma(\omega)) &= W(\omega) \end{aligned} \tag{14}$$

   Thus,

   $$\begin{aligned} W(\sigma(\omega')) &= W(\omega') \\ &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(?\sigma(\psi))\} \\ &\overset{(14)}{=} \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(?\sigma(\psi))\} \\ &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } \nu = \omega \oplus t \text{ and } \text{val}_\eta(\omega \oplus t, \sigma(\psi))\} \\ &\overset{Lem.5}{=} \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } \nu = \omega \oplus t \text{ and } \text{val}_\eta(\sigma(\omega) \oplus t, \psi)\} \\ &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(?\psi)\} \end{aligned}$$

2. For substituted variable x_a, and all $\nu \in \sigma(\omega')$ with $t = \text{DW}(\omega')$

   $$\sigma(\omega')(\nu)(x_a) = \sigma(\omega)(t)(x_a)$$

   By the definition of substitution,

   (a) $\sigma(\omega')(\nu)(x_a) = \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a))$
   (b) $\sigma(\omega)(t)(x_a) = \text{val}_\eta(\omega \oplus t, \sigma(x_a))$

   But, by (11), $\text{DV}(\omega' \oplus \nu) = \text{DV}(\omega \oplus t)$, and we know $\text{R}(\omega' \oplus \nu) = \text{R}(\omega \oplus t)$. It follows that

   $$\text{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) = \text{val}_\eta(\omega \oplus t, \sigma(x_a))$$

   and thus

   $$\sigma(\omega')(\nu)(x_a) = \sigma(\omega)(t)(x_a)$$

3. For any unsubstituted variable y_a, and all $\nu \in \sigma(\omega')$ with $t = \textsc{dw}(\omega')$,

$$\sigma(\omega')(\nu)(y_a) = \sigma(\omega)(t)(y_a)$$

By the following equalities: $\sigma(\omega')(\nu)(y_a) \overset{(13)}{=} \omega'(\nu)(y_a) \overset{(11)}{=} \omega(t)(y_a) \overset{(12)}{=} \sigma(\omega)(t)(y_a)$

$\Leftarrow$ direction

If $(\sigma(\omega), \nu) \in \rho_\eta(L_a(?\psi))$ then there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(?\sigma(\psi)))$ and $\nu = \sigma(\omega')$

Learned test is deterministic. Like the case for assignment, it is sufficient to let ν be defined as $\sigma(\omega')$, where ω' is the unique transition of $L_a(?\sigma(\psi))$.

However, it is possible that a learned test does not transition at all if the distinguished world does not pass the test, i.e. if $\text{val}_\eta(\omega, \sigma(\psi)) = 0$. Thus, while we may assume, by hypothesis, that $(\sigma(\omega), \nu) \in \rho_\eta(L_a(?\psi))$, we must ensure that $(\omega, \omega') \in \rho_\eta(L_a(?\sigma(\psi)))$.

Since $(\sigma(\omega), \nu) \in \rho_\eta(L_a(?\psi))$, then the distinguished world passes the test $?\psi$, that is, $\text{val}_\eta(\sigma(\omega), \psi)$. By Lemma 5, $\text{val}_\eta(\omega, \sigma(\psi))$. Thus, there is also some transition $(\omega, \omega') \in \rho_\eta(L_a(?\sigma(\psi)))$, which, learned test being deterministic, is exactly the same as for the $\Rightarrow$ direction.

- $\gamma_1 \cup \gamma_2$.

$\Rightarrow$ direction

If $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1) \cup \sigma(\gamma_2)))$ then $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$

Let $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1) \cup \sigma(\gamma_2)))$. By the semantics of the learning operator,

$$\begin{aligned}
W(\omega') &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1) \cup \sigma(\gamma_2))\} \\
&= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1)) \text{ or } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_2))\} \\
&= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1))\} \cup \\
&\quad\ \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_2))\} && (15) \\
\omega'(\nu) &= \textsc{dv}(\nu) \text{ for all } \nu \in \omega' && (16) \\
\textsc{dw}(\textsc{dw}(\omega')) &= \textsc{dw}(\omega) && (17)
\end{aligned}$$

By applying the substitution to ω',

$$\begin{aligned}
W(\sigma(\omega')) &= W(\omega') && (18) \\
\textsc{dw}(\textsc{dw}(\sigma(\omega'))) &= \textsc{dw}(\omega') \\
\sigma(\omega')(\nu)(x_a) &= \text{val}_\eta(\omega' \oplus \nu, \sigma(x)) \text{ for substituted variable } x_a && (19) \\
\sigma(\omega')(\nu)(y_a) &= \omega'(\nu)(y_a) \text{ for unsubstituted variable } y_a && (20)
\end{aligned}$$

We must show that $\sigma(\omega)$ and $\sigma(\omega')$ conform to the transition relation as expected, i.e. $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$. To do this, we will apply the induction hypothesis to transitions for $L_a(\gamma_1)$ and $L_a(\gamma_2)$. Some of these transitions may not exist due to the distinguished world not passing some test in γ_1 or γ_2. However, the programs may still contribute possible worlds in $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$. We dealt with this issue in the soundness proof in Appendix B.4, and use the same method here: we may pick a distinguished world that does not fail to transition with the subprograms γ_1 and γ_2 in order to obtain the desired properties for *all* possible worlds.

Let $(\omega, \omega_1') \in \rho_\eta(L_a(\sigma(\gamma_1)))$. Then,

$$\begin{aligned}
W(\omega_1') &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1))\} \qquad (21)\\
\omega_1'(\nu) &= \mathrm{DV}(\nu) \ \text{ for all } \nu \in \omega_1'\\
\mathrm{DW}(\mathrm{DW}(\omega_1')) &= \mathrm{DW}(\omega)
\end{aligned}$$

By applying the substitution σ to ω_1',

$$\begin{aligned}
W(\sigma(\omega_1')) &= W(\omega_1') && (22)\\
\sigma(\omega_1')(\nu)(x_a) &= \mathrm{val}_\eta(\omega_1' \oplus \nu, \sigma(x)) \ \text{ for substituted variable } x_a && (23)\\
\sigma(\omega_1')(\nu)(y_a) &= \omega_1'(\nu)(y_a) \text{ for unsubstituted variable } y_a
\end{aligned}$$

By induction hypothesis, $(\sigma(\omega), \sigma(\omega_1')) \in \rho_\eta(L_a(\gamma_1))$, with

$$\begin{aligned}
W(\sigma(\omega_1')) &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1)\} && (24)\\
\sigma(\omega_1')(\nu) &= \mathrm{DV}(\nu) && (25)
\end{aligned}$$

We may conclude the equivalent results for $(\sigma(\omega), \sigma(\omega_2')) \in \rho_\eta(L_a(\gamma_2))$.

To prove $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$, we must show all of the following:

1. $W(\sigma(\omega')) = \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1 \cup \gamma_2)\}$
   We use following reasoning:

$$\begin{aligned}
W(\sigma(\omega')) &\overset{(18)}{=} W(\omega')\\
&\overset{(15)}{=} \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1))\} \cup\\
&\qquad \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_2))\}\\
&\overset{(21)}{=} W(\omega_1') \cup W(\omega_2')\\
&\overset{(22)}{=} W(\sigma(\omega_1')) \cup W(\sigma(\omega_2'))\\
&\overset{(24)}{=} \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1)\} \cup\\
&\qquad \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_2)\}\\
&= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1 \cup \gamma_2)\}
\end{aligned}$$

2. $\sigma(\omega')(\nu) = \mathrm{DV}(\nu)$ for all $\nu \in \sigma(\omega')$
We will need to analyze the behavior of both the substituted variable x_a, and unsubstituted variables y_a. Let $\nu \in \sigma(\omega')$. Then, $\nu \in \sigma(\omega'_1)$ or $\nu \in \sigma(\omega'_2)$. Without loss of generality, let us assume $\nu \in \sigma(\omega'_1)$.
For the substituted variable x_a,

$$\begin{aligned}\sigma(\omega')(\nu)(x_a) &\overset{(19)}{=} \mathrm{val}_\eta(\omega' \oplus \nu, \sigma(x)) \\ &\overset{(*)}{=} \mathrm{val}_\eta(\omega'_1 \oplus \nu, \sigma(x)) \\ &\overset{(23)}{=} \sigma(\omega'_1)(\nu)(x_a) \\ &\overset{(25)}{=} \mathrm{DV}(\nu)(x_a)\end{aligned}$$

The (*) equality is valid because $\sigma(x_a)$ is a term, and terms are interpreted only over the distinguished valuation and the ontic state, which are the same in both PD-models: $\mathrm{DV}(\omega'_1 \oplus \nu) = \mathrm{DV}(\omega' \oplus \nu) = \mathrm{DV}(\nu)$, and $\mathrm{R}(\omega'_1 \oplus \nu) = \mathrm{R}(\omega' \oplus \nu)$ since learning can never affect ontic state.
For the unsubstituted variables y_a,

$$\begin{aligned}\sigma(\omega')(\nu)(y_a) &\overset{(20)}{=} \omega'(\nu)(y_a) \\ &\overset{(16)}{=} \mathrm{DV}(\nu)(y_a)\end{aligned}$$

3. $\mathrm{DW}(\mathrm{DW}(\sigma(\omega'))) = \mathrm{DW}(\sigma(\omega))$
This is trivial since distinguished worlds are not affected by substitution, and therefore $\mathrm{DW}(\mathrm{DW}(\sigma(\omega'))) = \mathrm{DW}(\mathrm{DW}(\omega')) \overset{(17)}{=} \mathrm{DW}(\omega) = \mathrm{DW}(\sigma(\omega))$.

$\Leftarrow$ direction

If $(\sigma(\omega), \nu) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$ then there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1) \cup \sigma(\gamma_2)))$ and $\nu = \sigma(\omega')$.

Let $(\sigma(\omega), \mu) \in \rho_\eta(L_a(\gamma_1 \cup \gamma_2))$.

The proof is going to follow similar steps to the $\Rightarrow$ direction.

$$\begin{aligned}W(\mu) &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1 \cup \gamma_2)\} \\ &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1)\} \cup \\ &\quad\ \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_2)\} \qquad (26) \\ \mu(\nu) &= \mathrm{DV}(\nu) \\ \mathrm{DW}(\mathrm{DW}(\mu)) &= \mathrm{DW}(\sigma(\omega)) \qquad (27)\end{aligned}$$

Now let $(\sigma(\omega), \mu_1) \in \rho_\eta(L_a(\gamma_1))$ (we may use the same trick of picking a helpful distinguished for $\sigma(\omega)$ to ensure there is a transition). Then,

$$\begin{aligned}
W(\mu_1) &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1)\} && (28)\\
\mu_1(\nu) &= \text{DV}(\nu)\\
\text{DW}(\text{DW}(\mu_1)) &= \text{DW}(\sigma(\omega)) && (29)
\end{aligned}$$

By induction hypothesis, there is ω_1' such that $(\omega, \omega_1') \in \rho_\eta(L_a(\sigma(\gamma_1)))$ and $\mu_1 = \sigma(\omega_1')$. Thus,

$$\begin{aligned}
W(\omega_1') &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1))\}\\
\omega_1'(\nu) &= \text{DV}(\nu) && (30)\\
\text{DW}(\text{DW}(\omega_1')) &= \text{DW}(\omega) && (31)
\end{aligned}$$

And, by applying the substitution,

$$\begin{aligned}
W(\mu_1) &= W(\sigma(\omega_1')) = W(\omega_1') && (32)\\
\mu_1(\nu)(x_a) &= \sigma(\omega_1')(\nu)(x_a) = \text{val}_\eta(\omega_1' \oplus \nu, \sigma(x_a)) && (33)\\
\mu_1(\nu)(y_a) &= \sigma(\omega_1')(\nu)(y_a) = \omega_1'(\nu)(y_a) && (34)\\
\text{DW}(\mu_1) &= \text{DW}(\sigma(\omega_1')) = \text{DW}(\omega_1') && (35)
\end{aligned}$$

Similar results can be obtained for $(\sigma(\omega), \mu_2) \in \rho_\eta(L_a(\gamma_2))$.

We must now show that there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1) \cup \sigma(\gamma_2)))$ and $\mu = \sigma(\omega')$.

Let ω' be as follows:

$$\begin{aligned}
W(\omega') &= W(\omega_1') \cup W(\omega_2') && (36)\\
\omega'(\nu) &= \text{DV}(\nu) && (37)\\
\text{DW}(\text{DW}(\omega')) &= \text{DW}(\omega) && (38)
\end{aligned}$$

and thus, by applying the substitution to ω',

$$\begin{aligned}
W(\sigma(\omega')) &= W(\omega')\\
\sigma(\omega')(\nu)(x_a) &= \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a))\\
\sigma(\omega')(\nu)(y_a) &= \omega'(\nu)(y_a) && (39)\\
\text{DW}(\sigma(\omega')) &= \text{DW}(\omega') && (40)
\end{aligned}$$

Since this choice of ω' is precisely the one which conforms to the transition $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1) \cup \sigma(\gamma_2)))$, we need only show $\mu = \sigma(\omega')$. To do so, we prove the following statements.

1. $W(\mu) = W(\sigma(\omega'))$

$$\begin{aligned} W(\mu) &\overset{(26)}{=} \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1)\} \cup \\ &\quad \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_2)\} \\ &\overset{(28)}{=} W(\mu_1) \cup W(\mu_2) \\ &\overset{(32)}{=} W(\omega'_1) \cup W(\omega'_2) \\ &\overset{(36)}{=} W(\omega') \\ &= W(\sigma(\omega')) \end{aligned}$$

The last step is borne out from the fact that substitution does not affect the possible worlds of a PD-model.

2. $\mu(\nu)(x_a) = \sigma(\omega')(\nu)(x_a)$ for all $\nu \in \mu$ and substituted variable x_a
Since $W(\mu) = W(\mu_1) \cup W(\mu_2)$, let $\nu \in W(\mu_1)$ without loss of generality.

$$\begin{aligned} \mu(\nu)(x_a) &= \mu_1(\nu)(x_a) \\ &\overset{(33)}{=} \sigma(\omega'_1)(\nu)(x_a) \\ &\overset{(33)}{=} \text{val}_\eta(\omega'_1 \oplus \nu, \sigma(x_a)) \\ &\overset{(*)}{=} \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) \\ &= \sigma(\omega')(\nu)(x_a) \end{aligned}$$

The (*) equality is valid because $\sigma(x_a)$ is a term, and terms are interpreted only over the distinguished valuation and the ontic state, which are the same in both PD-models: $\text{DV}(\omega'_1 \oplus \nu) = \text{DV}(\omega' \oplus \nu) = \text{DV}(\nu)$, and $\text{R}(\omega'_1 \oplus \nu) = \text{R}(\omega' \oplus \nu)$ since learning can never affect ontic state.

The last step is by the definition of substitution.

3. $\mu(\nu)(y_a) = \sigma(\omega')(\nu)(y_a)$ for all $\nu \in \mu$ and unsubstituted variable y_a
As for x_a, since $W(\mu) = W(\mu_1) \cup W(\mu_2)$, let $\nu \in W(\mu_1)$ without loss of generality.

$$\begin{aligned} \mu(\nu)(y_a) &= \mu_1(\nu)(y_a) \\ &\overset{(34)}{=} \sigma(\omega'_1)(\nu)(y_a) \\ &\overset{(34)}{=} \omega'_1(\nu)(y_a) \\ &\overset{(30)}{=} \text{DV}(\nu)(y_a) \\ &\overset{(37)}{=} \omega'(\nu)(y_a) \\ &\overset{(39)}{=} \sigma(\omega')(\nu)(y_a) \end{aligned}$$

4. $\textsc{dw}(\mu) = \textsc{dw}(\sigma(\omega'))$

   All we currently know about $\textsc{dw}(\mu)$ is that, by (27), $\textsc{dw}(\textsc{dw}(\mu)) = \textsc{dw}(\sigma(\omega))$. However, $W(\mu) = W(\mu_1) \cup W(\mu_2)$. Without loss of generality, let us assume $\textsc{dw}(\mu) \in W(\mu_1)$.

   Because $\textsc{dw}(\textsc{dw}(\mu_1)) \overset{(29)}{=} \textsc{dw}(\sigma(\omega)) = \textsc{dw}(\textsc{dw}(\mu))$, then we may make a choice of μ_1 such that $(\sigma(\omega), \mu_1) \in \rho_\eta(L_a(\gamma_1))$ and more importantly, $\textsc{dw}(\mu) = \textsc{dw}(\mu_1) \overset{(35)}{=} \textsc{dw}(\omega'_1)$.

   Because $W(\omega'_1) \subseteq W(\omega')$ (36), then $\textsc{dw}(\omega'_1) \in W(\omega')$. However, $\textsc{dw}(\textsc{dw}(\omega'_1)) \overset{(31)}{=} \textsc{dw}(\omega) \overset{(38)}{=} \textsc{dw}(\textsc{dw}(\omega'))$. In particular, because we choose ω' and the conditions for choosing its distinguished world are equivalent to those of ω'_1, we may pick $\textsc{dw}(\omega') = \textsc{dw}(\omega'_1)$.

   Because substitution does not affect the choice of distinguished world, $\textsc{dw}(\omega') \overset{(40)}{=} \textsc{dw}(\sigma(\omega'))$. Thus, $\textsc{dw}(\mu) = \textsc{dw}(\mu_1) \overset{(35)}{=} \textsc{dw}(\omega'_1) = \textsc{dw}(\omega') \overset{(40)}{=} \textsc{dw}(\sigma(\omega'))$.

- $\gamma_1; \gamma_2$.

$\Rightarrow$ direction

If $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1); \sigma(\gamma_2)))$, then $(\sigma(\omega), \sigma(\omega')) \in \rho_\eta(L_a(\gamma_1; \gamma_2))$

Let $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1); \sigma(\gamma_2)))$. Thus,

$$\begin{aligned} W(\omega') &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\sigma(\gamma_1); \sigma(\gamma_2))\} \\ &= \{\nu : \text{ there is } t \in \omega \text{ and } \nu_1 \text{ s.t. } (\omega \oplus t, \nu_1) \in \rho_\eta(\sigma(\gamma_1)) \\ &\qquad \text{and } (\nu_1, \nu) \in \rho_\eta(\sigma(\gamma_2))\} && (41) \\ \omega'(\nu) &= \textsc{dv}(\nu) \text{ for all } \nu \in \omega' && (42) \\ \textsc{dw}(\textsc{dw}(\omega')) &= \textsc{dw}(\omega) && (43) \end{aligned}$$

Applying substitution to ω and ω',

$$\begin{aligned} W(\sigma(\omega)) &= W(\omega) & W(\sigma(\omega')) &= W(\omega') && (44) \\ \sigma(\omega)(t)(x_a) &= \text{val}_\eta(\omega \oplus t, \sigma(x_a)) & \sigma(\omega')(\nu)(x_a) &= \text{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) && (45) \\ \sigma(\omega)(t)(y_a) &= \omega(t)(y_a) & \sigma(\omega')(\nu)(y_a) &= \omega'(\nu)(y_a) && (46) \\ \textsc{dw}(\sigma(\omega)) &= \textsc{dw}(\omega) & \textsc{dw}(\sigma(\omega')) &= \textsc{dw}(\omega') && (47) \end{aligned}$$

Let $(\omega, \omega_1) \in \rho_\eta(L_a(\sigma(\gamma_1)))$. Thus,

$$\begin{aligned} W(\omega_1) &= \{\nu_1 : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_1) \in \rho_\eta(\sigma(\gamma_1))\} && (48) \\ \omega_1(\nu_1) &= \textsc{dv}(\nu_1) && (49) \\ \textsc{dw}(\textsc{dw}(\omega_1)) &= \textsc{dw}(\omega) \end{aligned}$$

Let $(\omega_1, \omega_2) \in \rho_\eta\left(L_a(\sigma\left(\gamma_2\right))\right)$. Thus,

$$\begin{aligned}
W(\omega_2) &= \{\nu_2 : \text{ there is } \nu_1 \in \omega_1 \text{ s.t. } (\omega_1 \oplus \nu_1, \nu_2) \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)\} && (50)\\
\omega_2(\nu_2) &= \mathrm{DV}(\nu)\\
\mathrm{DW}(\mathrm{DW}(\omega_2)) &= \mathrm{DW}(\omega_1)
\end{aligned}$$

By applying the substitution to ω_1 and ω_2,

$$\begin{aligned}
W(\sigma\left(\omega_1\right)) &= W(\omega_1) & W(\sigma\left(\omega_2\right)) &= W(\omega_2) && (51)\\
\sigma\left(\omega_1\right)(\nu_1)(x_a) &= \mathrm{val}_\eta\left(\omega_1 \oplus \nu_1, \sigma\left(x_a\right)\right) & \sigma\left(\omega_2\right)(\nu_2)(x_a) &= \mathrm{val}_\eta\left(\omega_2 \oplus \nu_2, \sigma\left(x_a\right)\right) && (52)\\
\sigma\left(\omega_1\right)(\nu_1)(y_a) &= \omega_1(\nu_1)(y_a) & \sigma\left(\omega_2\right)(\nu_2)(y_a) &= \omega_2(\nu_2)(y_a)\\
\mathrm{DW}(\sigma\left(\omega_1\right)) &= \mathrm{DW}(\omega_1) & \mathrm{DW}(\sigma\left(\omega_2\right)) &= \mathrm{DW}(\omega_2)
\end{aligned}$$

But, by induction hypothesis, we have $(\sigma\left(\omega\right), \sigma\left(\omega_1\right)) \in \rho_\eta\left(L_a(\gamma_1)\right)$ and $(\sigma\left(\omega_1\right), \sigma\left(\omega_2\right)) \in \rho_\eta\left(L_a(\gamma_2)\right)$. By the semantics of the learning operator,

$$\begin{aligned}
W(\sigma\left(\omega_1\right)) &= \{\nu_1 : \text{ there is } t \in \sigma\left(\omega\right) \text{ s.t. } (\sigma\left(\omega\right) \oplus t, \nu_1) \in \rho_\eta\left(\gamma_1\right)\} && (53)\\
\sigma\left(\omega_1\right)(\nu_1) &= \mathrm{DV}(\nu_1)\\
\mathrm{DW}(\mathrm{DW}(\sigma\left(\omega_1\right))) &= \mathrm{DW}(\sigma\left(\omega\right))\\
W(\sigma\left(\omega_2\right)) &= \{\nu_2 : \text{ there is } \nu_1 \in \sigma\left(\omega_1\right) \text{ s.t. } (\sigma\left(\omega_1\right) \oplus \nu_1, \nu_2) \in \rho_\eta\left(\gamma_2\right)\} && (54)\\
\sigma\left(\omega_2\right)(\nu_2) &= \mathrm{DV}(\nu_2) && (55)\\
\mathrm{DW}(\mathrm{DW}(\sigma\left(\omega_2\right))) &= \mathrm{DW}(\sigma\left(\omega_1\right))
\end{aligned}$$

We must show $(\sigma\left(\omega\right), \sigma\left(\omega'\right)) \in \rho_\eta\left(L_a(\gamma_1; \gamma_2)\right)$, for which it suffices to show the following properties:

1. $W(\sigma\left(\omega'\right)) = \{\nu : \text{ there is } t \in \sigma\left(\omega\right) \text{ s.t. } (\sigma\left(\omega\right) \oplus t, \nu) \in \rho_\eta\left(\gamma_1; \gamma_2\right)\}$
   Let $\mu \in \sigma\left(\omega'\right)$. We must show that there is $t \in \sigma\left(\omega\right)$ such that $(\sigma\left(\omega\right) \oplus t, \mu) \in \rho_\eta\left(\gamma_1; \gamma_2\right)$.
   Since $\mu \in \sigma\left(\omega'\right)$, by (44), $\mu \in \omega'$. Thus, by (41), there exists $t \in \omega$ and ν_1 such that

$$(\omega \oplus t, \nu_1) \in \rho_\eta\left(\sigma\left(\gamma_1\right)\right) \tag{56}$$

$$(\nu_1, \mu) \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right) \tag{57}$$

   From (56) and (48), then $\nu_1 \in \omega_1$. We now wish to show that $\mu \in \omega_2$, but what we know from (57) differs from what we need, which, according to (50) is that there exists $\nu_1 \in \omega_1$ such that $(\omega_1 \oplus \nu_1, \mu) \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)$.
   However, $\sigma\left(\gamma_2\right)$ originally appeared inside a learning operator and, as such, it cannot contain other learning operators or doxastic modalities. Thus, in $(\omega_1 \oplus \nu_1, \mu) \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)$, program $\sigma\left(\gamma_2\right)$ only makes use of the ontic state $\mathrm{R}(\omega_1 \oplus \nu_1)$, and the distinguished valuation of $\mathrm{DV}(\omega_1 \oplus \nu_1)$.
   But,

– $\mathrm{R}(\omega_1 \oplus \nu_1) = \mathrm{R}(\omega) = \mathrm{R}(\nu_1)$ since neither learning operators nor learned programs alter ontic state.
– $\mathrm{DV}(\omega_1 \oplus \nu_1) = \omega_1(\nu_1) \overset{(49)}{=} \mathrm{DV}(\nu_1)$.

These are precisely the valuations that program $\sigma(\gamma_2)$ can use in (57). Thus, (57) is an equivalent statement to $(\omega_1 \oplus \nu_1, \mu) \in \rho_\eta(\sigma(\gamma_2))$, and by (50) we may finally claim

$$\mu \in \omega_2 \tag{58}$$

Since $\nu_1 \in \omega_1$ and $\mu \in \omega_2$, by (51), $\nu_1 \in \sigma(\omega_1)$ and $\mu \in \sigma(\omega_2)$, and thus, by (53) and (54),

$$(\sigma(\omega) \oplus t, \nu_1) \in \rho_\eta(\gamma_1) \tag{59}$$

$$(\sigma(\omega_1) \oplus \nu_1, \mu) \in \rho_\eta(\gamma_2) \tag{60}$$

Again using the argument that γ_2 can only use the ontic state and distinguished valuation of $\sigma(\omega_1) \oplus \nu_1$, (60) is equivalent to

$$(\nu_1, \mu) \in \rho_\eta(\gamma_2) \tag{61}$$

But, if (59) and (61), then there is a $t \in \sigma(\omega)$ such that $(\sigma(\omega) \oplus t, \mu) \in \rho_\eta(\gamma_1; \gamma_2)$, which is precisely the condition for inclusion in $W(\sigma(\omega'))$ that we wanted to show.

2. $\sigma(\omega')(\nu) = \mathrm{DV}(\nu)$ for all $\nu \in \omega'$

   We will handle the substituted variable x_a differently from the unsubstituted y_a.

   Let $\nu \in \sigma(\omega')$, equivalently, $\nu \in \omega'$. From (45) and (46) we know that $\sigma(\omega')(\nu)(x_a) = \mathrm{val}_\eta(\omega' \oplus \nu, \sigma(x_a))$ and $\sigma(\omega')(\nu)(y_a) = \omega'(\nu)(y_a)$.

   We already know $\nu \in \omega_2$ (58), equivalently $\nu \in \sigma(\omega_2)$. Therefore, $\mathrm{DV}(\nu)(x_a) \overset{(55)}{=} \sigma(\omega_2)(\nu)(x_a) \overset{(52)}{=} \mathrm{val}_\eta(\omega_2 \oplus \nu, \sigma(x_a))$. But, because $\sigma(x_a)$ is a term, then it can read only from the distinguished valuation and ontic state, and thus, $\mathrm{val}_\eta(\omega_2 \oplus \nu, \sigma(x_a)) = \mathrm{val}_\eta(\nu, \sigma(x_a))$. By the same argument, $\mathrm{val}_\eta(\nu, \sigma(x_a)) = \mathrm{val}_\eta(\omega' \oplus \nu, \sigma(x_a)) = \sigma(\omega')(\nu)(x_a)$. Thus, $\mathrm{DV}(\nu)(x_a) = \sigma(\omega')(\nu)(x_a)$.

   The case of y_a is much simpler: $\sigma(\omega')(\nu)(y_a) \overset{(46)}{=} \omega'(\nu)(y_a) \overset{(42)}{=} \mathrm{DV}(\nu)(y_a)$.

3. $\mathrm{DW}(\mathrm{DW}(\sigma(\omega'))) = \mathrm{DW}(\sigma(\omega))$

   We already know $\mathrm{DW}(\mathrm{DW}(\omega')) = \mathrm{DW}(\omega)$ from (43). We may directly obtain what we want by applying (47).

$\Leftarrow$ direction

If $(\sigma(\omega), \mu) \in \rho_\eta(L_a(\gamma_1; \gamma_2))$, then there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1); \sigma(\gamma_2)))$ and $\mu = \sigma(\omega')$.

Let $(\sigma(\omega), \mu) \in \rho_\eta(L_a(\gamma_1; \gamma_2))$.

We must show that there is ω' such that $(\omega, \omega') \in \rho_\eta(L_a(\sigma(\gamma_1); \sigma(\gamma_2)))$ and $\mu = \sigma(\omega')$.

By the semantics of the learning operator,

$$\begin{aligned} W(\mu) &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu) \in \rho_\eta(\gamma_1; \gamma_2)\} \\ &= \{\nu : \text{ there is } t \in \sigma(\omega) \text{ and } \nu_1 \text{ s.t. } (\sigma(\omega) \oplus t, \nu_1) \in \rho_\eta(\gamma_1) \\ &\qquad \text{and } (\nu_1, \nu) \in \rho_\eta(\gamma_2)\} \quad (62) \\ \mu(\nu) &= \mathrm{DV}(\nu) \text{ for all } \nu \in \mu \quad (63) \\ \mathrm{DW}(\mathrm{DW}(\mu)) &= \mathrm{DW}(\sigma(\omega)) \end{aligned}$$

Now let $(\sigma(\omega), \mu_1) \in \rho_\eta(L_a(\gamma_1))$. Then,

$$\begin{aligned} W(\mu_1) &= \{\nu_1 : \text{ there is } t \in \sigma(\omega) \text{ s.t. } (\sigma(\omega) \oplus t, \nu_1) \in \rho_\eta(\gamma_1)\} \quad (64) \\ \mu_1(\nu_1) &= \mathrm{DV}(\nu_1) \text{ for all } \nu_1 \in \mu_1 \quad (65) \\ \mathrm{DW}(\mathrm{DW}(\mu_1)) &= \mathrm{DW}(\sigma(\omega)) \end{aligned}$$

But, by induction hypothesis, there is ω_1 such that $(\omega, \omega_1) \in \rho_\eta(L_a(\sigma(\gamma_1)))$ and $\mu_1 = \sigma(\omega_1)$.

$$\begin{aligned} W(\omega_1) &= \{\nu_1 : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu_1) \in \rho_\eta(\sigma(\gamma_1))\} \quad (66) \\ \omega_1(\nu_1) &= \mathrm{DV}(\nu_1) \text{ for all } \nu_1 \in \omega_1 \quad (67) \\ \mathrm{DW}(\mathrm{DW}(\omega_1)) &= \mathrm{DW}(\omega) \quad (68) \end{aligned}$$

We may now let $(\sigma(\omega_1), \mu_2) \in \rho_\eta(L_a(\gamma_2))$.

$$\begin{aligned} W(\mu_2) &= \{\nu_2 : \text{ there is } \nu_1 \in \sigma(\omega_1) \text{ s.t. } (\sigma(\omega_1) \oplus \nu_1, \nu_2) \in \rho_\eta(\gamma_2)\} \quad (69) \\ \mu_2(\nu_2) &= \mathrm{DV}(\nu_2) \text{ for all } \nu_2 \in \mu_2 \\ \mathrm{DW}(\mathrm{DW}(\mu_2)) &= \mathrm{DW}(\sigma(\omega_1)) \end{aligned}$$

But, again by induction hypothesis, there is ω_2 such that $(\omega_1, \omega_2) \in \rho_\eta(L_a(\sigma(\gamma_2)))$ and

$$\mu_2 = \sigma(\omega_2) \quad (70)$$

By the definition of the learning operator,

$$\begin{aligned} W(\omega_2) &= \{\nu_2 : \text{ there is } \nu_1 \in \omega_1 \text{ s.t. } (\omega_1 \oplus \nu_1, \nu_2) \in \rho_\eta(\sigma(\gamma_2))\} \quad (71) \\ \omega_2(\nu_2) &= \mathrm{DV}(\nu_2) \text{ for all } \nu_2 \in \omega_2 \quad (72) \\ \mathrm{DW}(\mathrm{DW}(\omega_2)) &= \mathrm{DW}(\omega_1) \quad (73) \end{aligned}$$

We wish to show that there is ω' such that $(\omega, \omega') \in \rho_\eta\left(L_a(\sigma\left(\gamma_1\right); \sigma\left(\gamma_2\right))\right)$, meaning:

$$\begin{aligned}
W(\omega') &= \{\nu : \text{ there is } t \in \omega \text{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta\left(\sigma\left(\gamma_1\right); \sigma\left(\gamma_2\right)\right)\} && (74) \\
\omega'(\nu) &= \mathrm{DV}(\nu) \text{ for all } \nu \in \omega' && (75) \\
\mathrm{DW}(\mathrm{DW}(\omega')) &= \mathrm{DW}(\omega) && (76)
\end{aligned}$$

To show the existence of ω', we first note that μ_1, μ_2, ω_1 and ω_2 must all exist given our hypothesis that there exists a transition $(\sigma\left(\omega\right), \mu) \in \rho_\eta\left(L_a(\gamma_1; \gamma_2)\right)$. We will now show that $W(\omega') = W(\omega_2)$ thus ensuring the existence of ω'. We will then show that $\mu = \sigma\left(\omega'\right)$.

Let $\nu' \in \omega'$. Then by (74) there is $t \in \omega$ such that $(\omega \oplus t, \nu') \in \rho_\eta\left(\sigma\left(\gamma_1\right); \sigma\left(\gamma_2\right)\right)$. Therefore, there must be some ν_1 such that $(\omega \oplus t, \nu_1) \in \rho_\eta\left(\sigma\left(\gamma_1\right)\right)$ and $(\nu_1, \nu') \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)$. But, by (66), $\nu_1 \in \omega_1$ and by (67), $\omega_1(\nu_1) = \mathrm{DV}(\nu_1)$.

Because of this, and because $\sigma\left(\gamma_2\right)$ appears within a learning operator, $(\nu_1, \nu') \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)$ is equivalent to $(\omega_1 \oplus \nu_1, \nu') \in \rho_\eta\left(\sigma\left(\gamma_2\right)\right)$ and, by (71), $\nu' \in \omega_2$.

Similarly, we can show that if $\nu_2 \in \omega_2$, then $\nu_2 \in \omega'$. Thus,

$$W(\omega') = W(\omega_2) \tag{77}$$

This ensures that ω' exists. We may then let $\omega'(\nu) = \mathrm{DV}(\nu)$, as in (74), and choose some distinguished world such that $\mathrm{DW}(\mathrm{DW}(\omega')) = \mathrm{DW}(\omega)$, as per (76).

Now we need only prove that $\mu = \sigma\left(\omega'\right)$, for which it is sufficient to show the following properties, per the definition of substitution:

1. $W(\mu) = W(\sigma\left(\omega'\right))$
   Let $\nu \in \mu$. Then, by (62), there are $t \in \sigma\left(\omega\right)$ and ν_1 such that $(\sigma\left(\omega\right) \oplus t, \nu_1) \in \rho_\eta\left(\gamma_1\right)$ and $(\nu_1, \nu) \in \rho_\eta\left(\gamma_2\right)$.
   From $(\sigma\left(\omega\right) \oplus t, \nu_1) \in \rho_\eta\left(\gamma_1\right)$ and (64), $\nu_1 \in \mu_1$, and because of (65), $\mu_1(\nu_1) = \mathrm{DV}(\nu_1)$. Because of this, and because γ_1 appears inside a learning operator, then $(\nu_1, \nu) \in \rho_\eta\left(\gamma_2\right)$ is equivalent to $(\sigma\left(\omega_1\right) \oplus \nu_1, \nu) \in \rho_\eta\left(\gamma_2\right)$, and thus, by (69),

   $$\nu \in \mu_2 \tag{78}$$

   Again, an easy argument can be made that if $\nu \in \mu_2$, then $\nu \in \mu$, and therefore,

   $$\begin{aligned}
   W(\mu) &= W(\mu_2) \\
   &\overset{(70)}{=} W(\omega_2) \\
   &\overset{(77)}{=} W(\omega') \\
   &= W(\sigma\left(\omega'\right))
   \end{aligned}$$

2. $\mu(\nu)(x_a) = \sigma\left(\omega'\right)(\nu)(x_a)$ for all $\nu \in \mu$ and substituted variable x_a

By (63), $\mu(\nu)(x_a) = \textsc{dv}(\nu)\,(x_a)$. However, by (78) $\nu \in \mu_2$, and therefore,

$$\begin{aligned}
\mu(\nu)(x_a) &= \textsc{dv}(\nu)\,(x_a) \\
&\overset{(72)}{=} \mu_2(\nu)(x_a) \\
&\overset{(70)}{=} \sigma\,(\omega_2)(\nu)(x_a) \\
&= \mathrm{val}_\eta\,(\omega_2 \oplus \nu, \sigma\,(x_a)) \\
&\overset{(*)}{=} \mathrm{val}_\eta\,(\omega' \oplus \nu, \sigma\,(x_a)) \\
&= \sigma\,(\omega')(\nu)(x_a)
\end{aligned}$$

The step marked with (*) is possible because $\sigma\,(x_a)$ is a term, and therefore relies only on the distinguished valuation of $\omega_2 \oplus \nu$, which, given (77), is precisely the same as that of $\omega' \oplus \nu$, and on the ontic state, which is not affected by learning operators.

3. $\mu(\nu)(y_a) = \sigma\,(\omega')(\nu)(y_a)$ for all $\nu \in \mu$ and unsubstituted variable y_a

   By (63), $\mu(\nu)(y_a) = \textsc{dv}(\nu)\,(y_a)$. However, by (78) $\nu \in \mu_2$, and therefore,

$$\begin{aligned}
\mu(\nu)(y_a) &= \textsc{dv}(\nu)\,(y_a) \\
&\overset{(72)}{=} \mu_2(\nu)(y_a) \\
&\overset{(70)}{=} \sigma\,(\omega_2)(\nu)(y_a) \\
&= \omega_2(\nu)(y_a) \\
&\overset{(*)}{=} \omega'(\nu)(y_a) \\
&= \sigma\,(\omega')(\nu)(y_a)
\end{aligned}$$

   The step marked by (*) is possible because $W(\omega') = W(\omega_2)$, and both use $\omega_2(\nu) \overset{(72)}{=} \textsc{dv}(\nu) \overset{(76)}{=} \omega'(\nu)$.

4. $\textsc{dw}(\mu) = \textsc{dw}(\sigma\,(\omega'))$.

   Recall that by (76) we have a choice of the particular distinguished world we wish to use. We must show that the condition $\textsc{dw}(\textsc{dw}(\omega')) = \textsc{dw}(\omega)$ governing that choice is compatible with this $\textsc{dw}(\mu) = \textsc{dw}(\sigma\,(\omega'))$ requirement.

   Thus, let $\textsc{dw}(\mu) = \textsc{dw}(\sigma\,(\omega'))$. Since substitution does not affect distinguished worlds, $\textsc{dw}(\mu) = \textsc{dw}(\omega')$.

   Because $\textsc{dw}(\omega') \in \omega'$, then by (74) there must be some world $s \in \omega$ such that $(\omega \oplus s, \textsc{dw}(\omega')) \in \rho_\eta\,(\sigma\,(\gamma_1); \sigma\,(\gamma_2))\}$. In order to satisfy (76), we must show that $s = \textsc{dw}(\omega)$.

   Since $(\omega \oplus s, \textsc{dw}(\omega')) \in \rho_\eta\,(\sigma\,(\gamma_1); \sigma\,(\gamma_2))\}$, there must be some ν such that $(\omega \oplus s, \nu) \in \rho_\eta\,(\sigma\,(\gamma_1))$ and $(\nu, \textsc{dw}(\omega')) \in \rho_\eta\,(\sigma\,(\gamma_2))$.

   Since $(\omega \oplus s, \nu) \in \rho_\eta\,(\sigma\,(\gamma_1))$, then by (66) $\nu \in \omega_1$. By (72), $\omega_1(\nu) = \textsc{dv}(\nu)$.

   Because of this and the fact that $\sigma\,(\gamma_2)$ is inside a learning operator, then $(\nu, \textsc{dw}(\omega')) \in \rho_\eta\,(\sigma\,(\gamma_2))$ is equivalent to $(\omega_1 \oplus \nu, \textsc{dw}(\omega')) \in \rho_\eta\,(\sigma\,(\gamma_2))$.

But, by (73), it must then be the case that $\nu = \text{DW}(\omega_1)$. Thus, it follows from $(\omega \oplus s, \nu) \in \rho_\eta(\sigma(\gamma_1))$ that $(\omega \oplus s, \text{DW}(\omega_1)) \in \rho_\eta(\sigma(\gamma_1))$. We may now use (68) to conclude that $s = \text{DW}(\omega)$.

$\square$