dL_ι: Definite Descriptions in Differential Dynamic Logic

Brandon Bohrer, Manuel Fernandez, and André Platzer

Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213, USA {bbohrer,manuelf,aplatzer}@andrew.cmu.edu
http://www.ls.cs.cmu.edu

Abstract. We introduce dL_ι, which extends differential dynamic logic (dL) for hybrid systems with definite descriptions and tuples, thus enabling its theoretical foundations to catch up with the implementation of dL practiced in the theorem prover KeYmaera X. Definite descriptions enable partial, nondifferentiable, and discontinuous terms, which have many examples in applications, such as divisions, nth roots, and absolute values. Tuples enable systems of multiple differential equations, arising in almost every application. Together, definite description and tuples combine to support long-desired features such as vector arithmetic. We overcome the unique challenges posed by extending dL with these features: Definite descriptions expose the subtleties of reasoning about differential equations which may not be locally Lipschitz continuous, and thus whose solutions may not be unique. Likewise, tuples are simple when considered in isolation, but in the context of hybrid systems will demand that differentials are treated in full generality. The addition of definite descriptions also makes dL_ι a free logic; we investigate the interaction of free logic and the differential equations (ODEs) of dL, showing that this combination is sound, and characterize its expressivity. We give a new example system that can be defined and verified using these extensions.

Keywords: Dynamic logic, definite description, hybrid systems, theorem proving, uniform substitution

1 Introduction

Cyber-physical systems (CPSs) such as self-driving cars, trains, and airplanes combine discrete control and continuous physical dynamics and are often safety-critical because they operate around humans. Thus it is essential to achieve the highest possible confidence in their correctness, e.g., using formal methods with strong theoretical foundations. Differential dynamic logic (dL) [14,18,19] is a logic for formal verification of *hybrid systems* [8], widely-used models of CPSs that incorporate both their discrete and continuous behaviors. Among formal methods for CPSs, dL is notable both for its case studies [13,10,12] using the KeYmaera X [7] theorem prover, and for its strong foundations, as evidenced by its completeness results [14,18] and a formal proof of soundness in both Isabelle/HOL and Coq [3].

However, there is a tension between the goals of practical applicability and rigorous foundations. In practice, theorem prover implementations often demand new features which were not anticipated in theory. Formalizations of KeYmaera X [4], Coq [2], and NuPRL [1] all omit or simplify whichever practical features are most theoretically challenging for their specific logic: discontinuous and partial terms in KeYmaera X, termination-checking in Coq, or context management in NuPRL. When formalizations of theorem provers *do* succeed in reflecting the implementation [11], they owe a credit to the generality of the underlying theory: it is much more feasible to formalize a general base theory than to formalize ad-hoc extensions as they arise.

In this paper, we introduce dL_ι: a new, generalized foundation for dL using definite descriptions $\iota x\ \phi$ that denote the unique x for which ϕ holds and pairs (θ_1, θ_2). Definite descriptions and pairs let us define all extensions used by KeYmaera X in practice, e.g., divisions θ_1/θ_2, roots $\sqrt[n]{\theta}$, functions $\min(\theta_1, \theta_2)$, $\max(\theta_1, \theta_2)$, and $|\theta|$, and ODE *systems*. Useful new features like trigonometric functions and vectors are also definable, and existing features like differentials $(\theta)'$ achieve simpler axiomatizations in dL_ι.

While definite description and tuples are certainly widespread, we solve novel challenges in integrating them with differential equations (ODEs), the distinguishing feature of hybrid systems: Definite descriptions allow partiality, discontinuity, and nondifferentiability, all of which interact subtly with sound ODE reasoning, while the multidimensional systems enabled by tuples push the generality of differentials and expose the subtle dependency structure of advanced ODE reasoning principles.

An example demonstrates a fundamental increase in power: definite description allows us to express non-polynomial ODEs, including those with non-unique solutions, in contrast to the polynomial ODEs of dL and their unique solutions. The foundational changes are equally deep: supporting partiality makes dL_ι a free logic, for which we adopt a 3-valued Łukasiewicz semantics. We show this profound change in foundations needs only small changes to the proof calculus. We develop the theory of dL_ι, showing that the proof calculus is sound and comparing the expressive power of dL_ι with dL.

2 Syntax

We present the core syntax of dL_ι, which extends dL with definite descriptions and tuples. We describe the constructs informally here, giving formal semantics in Sec. 3. As a free logic, dL_ι contains terms that do not denote and formulas whose truth values are unknown (truth is indicated $\oplus$, falsehood by $\ominus$, and unknown by $\circledplus$); handling these cases is a major point in the development of the semantics and proof calculus. Our calculus, as with modern implementations [7] and machine-checked correctness proofs [3] for dL, is based on uniform substitution [5, §35,§40]: symbols ranging over predicates, programs, etc. are explicitly represented in the syntax. This improves the ease with which dL_ι can be implemented and its soundness proof checked mechanically in future work. The syntax of dL_ι

is divided into terms, programs, and formulas, whose definitions are mutually recursive. The terms θ of dL_ι extend the terms of dL with definite descriptions, pairs, and reductions:

$$\theta \ ::= \ q \mid x \mid f(\theta) \mid \theta + \theta \mid \theta \cdot \theta \mid (\theta)' \mid \iota\mathbf{x}\ \phi \mid (\theta, \theta) \mid \mathsf{red}(\theta, \mathbf{s}\ \theta, \mathbf{lr}\ \theta)$$

for literal $q \in \mathbb{Q}$ and variable $x \in \mathcal{V}$, where $\mathcal{V}$ is the set of all variable names, f is a function symbol, and ϕ is a formula. The first six cases: polynomials, differentials, and function symbols, are as in dL. Variables are *flexible*: they are modified by quantifiers and programs. Variables x always denote some value and thus assignments to variables follow strict semantics: Assigning a non-denoting expression like $1/0$ to a variable x aborts execution even if x is never read again. In contrast, $f(\theta)$ is an *uninterpreted function* f applied to term θ, but both θ and $f(\theta)$ are allowed to be non-denoting. Functions f are used to state axioms in their full generality, thus we are able to write axioms that reason even about non-denoting terms. The definite description $\iota x\ \phi$ denotes the *unique* value of x that makes formula ϕ true, if exactly one such value exists, else it does not denote. The pair (θ_1, θ_2) denotes the pair of the denotations of θ_1 and θ_2. The elimination form for pairs, $\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$, recursively reduces the value denoted by θ_1 : base case θ_2 handles scalars and θ_3 combines the results of reducing the left and right of each pair.

The programs α, β of dL_ι are *hybrid programs*, a program syntax for *hybrid systems* combining discrete and continuous dynamics. Hybrid programs of dL_ι are identical to those of dL with the exception that any formula or term contained therein is again any formula or term of dL_ι, not necessarily just dL.

$$\alpha, \beta \ ::= \ x := \theta \mid x' = \theta \,\&\, \phi \mid ?\phi \mid \alpha \cup \beta \mid \alpha;\ \beta \mid \alpha^* \mid a$$

Assignments $x := \theta$ assign the value of θ to variable x, if θ denotes a value. Tests $?\phi$ abort execution if formula ϕ is not true. Nondeterministic choices $\alpha \cup \beta$ behave as either α or β, nondeterministically. Sequential composition $\alpha;\ \beta$ performs β in any state resulting from α. Loops α^* repeat α sequentially any number of times, nondeterministically. The defining construct of hybrid programs are the *differential equations* (ODEs) $x' = \theta \,\&\, \phi$, which continuously evolve x according to the differential equation $x' = \theta$ for any duration such that formula ϕ is true throughout. Note the core syntax of dL_ι need only contain systems with a single variable x: in Sec. 4 we will derive systems with multiple variables from systems of one variable. Uninterpreted program constants a range over programs. We parenthesize programs α as $\{\alpha\}$ with braces for disambiguation and readability.

$$\phi, \psi \ ::= \ \phi \wedge \psi \mid \neg\phi \mid \forall x\ \phi \mid \theta_1 \geq \theta_2 \mid [\alpha]\phi \mid p(\theta) \mid C(\phi)$$

Conjunctions $\phi \wedge \psi$, negations $\neg\phi$, and quantifiers $\forall x\ \phi$ are as is standard in first-order Łukasiewicz logic. The quantifier $\exists x\ \phi$ is also as in first-order Łukasiewicz logic and can be derived $\exists x\ \phi \equiv \neg\forall x\ \neg\phi$. In comparing $\theta_1 \geq \theta_2$, if terms θ_1 and θ_2 both denote reals, those reals are compared, if they both denote tuples they are compared elementwise, in all other cases the result is unknown ($\oplus$). The defining

construct of dynamic logics is $[\alpha]\phi$, which says ϕ holds in all states reachable by running α. Its dual, $\langle\alpha\rangle\phi$, says there exists a state reachable by running α where ϕ holds, and can be derived by the equivalence $\langle\alpha\rangle\phi \equiv \neg[\alpha]\neg\phi$. Uninterpreted predicate symbols p expect terms θ as arguments. The uninterpreted quantifier symbol C (applied to formula ϕ) is a second-order predicate symbol that binds all variables of ϕ and thus its truth value may depend upon the truth value of ϕ in multiple states. They are not strictly necessary, but enable efficient, convenient contextual reasoning. We write P, Q for definable nullary quantifier symbols, definable as $P \equiv C(0 \geq 0)$.

Example 1 (Robot Water Cooler). The textbook examples of non-Lipschitz ODEs (and non-unique solutions) are those of form $h' = k \cdot \sqrt{h}$ for constant k. We show that in contrast to dL, dL_ι can directly represent a hybrid system featuring such ODEs, which we base on Hubbard's leaky bucket [9, §4.2].

Consider a water cooler of height h and an opening of surface area a in its bottom of surface area A, where g is acceleration due to gravity. Suppose an enterprising student has equipped the cooler's valve with robotic control. We could then model the cooler as:

$$\alpha_B \equiv \left\{\{?h > 0;\ a := 1\} \ \cup\ a := 0\}; h' = -\sqrt{2gh}\frac{a}{A} \,\&\, h \geq 0\right\}^*$$

This says that so long as there is water in the cooler ($?h > 0$) we can choose to open the valve ($a := 1$), but we can always close the valve ($a := 0$). Then the water drains out the cooler at a rate proportional to the square root of the current volume by Torricelli's Law [6], or rate 0 if the valve is closed. This control process repeats arbitrarily often.

This system contains two constructs which are not part of dL: the root $\sqrt{2gh}$ and division $\frac{a}{A}$. We can rewrite α_B using definite descriptions:

$$\left\{\{?h > 0;\ a := 1\} \cup a := 0\}; h' = -(\iota y\ y^2 = 2gh \wedge y \geq 0)(\iota z\ zA = a) \,\&\, h \geq 0\right\}^*$$

As mentioned above, this example is significant because the ODE is non-Lipschitz: the solution is unique at $h = 0$ *only* within the constraint $h \geq 0$. The terms $\sqrt{2gh}$ and $\frac{a}{A}$ are also both *partial*: defined only assuming $gh \geq 0$ and $A \neq 0$, respectively. The interactions between partiality, uniqueness, and the constraint combine to make the proof subtle, even if short.

Common dL (and likewise, dL_ι) theorems include *safety assertions* of the form $\phi \to [\alpha]\psi$ which say that if ϕ holds initially, then ψ will necessarily hold after α. For example, we might wish to prove α_B is actually *leaky*, i.e., its final water height never exceeds the initial height:

Proposition 1 (Leakiness). *This is valid (definitely true $\oplus$ in all states):*

$$g > 0 \wedge h = h_0 \wedge h_0 > 0 \wedge A > 0 \to [\alpha_B](h \leq h_0)$$

We will revisit Prop. 1 after we have introduced a proof calculus for dL_ι in Sec. 5.

3 Denotational Semantics

We now formally define the semantics of dL_ι terms, formulas, and programs. Due to the presence of definite descriptions $\iota x\ \phi(x)$, not every dL_ι term denotes in every state, i.e., dL_ι is a *free logic*. We write $\perp$ for the interpretation of a term that does not denote any value. When a term does denote, it denotes either reals or pairs of reals, which may be nested to any finite depth. Because the nesting is arbitrarily deep, a term can denote an arbitrary *finite, binary* tree of reals with values at the leaves. We call the set of such values $\mathbf{Tree}(\mathbb{R})$, where for any S, $\mathbf{Tree}(S)$ is the smallest set such that: i) $\mathrm{S} \subseteq \mathbf{Tree}(S)$, and ii) for any l and $r \in \mathbf{Tree}(S)$, $(l, r) \in \mathbf{Tree}(S)$. We treat typing extrinsically, i.e., we do not make typing distinctions between $\mathbb{R}$ and $\mathbf{Tree}(\mathbb{R})$ in the semantics; any typing constraints will be expressed explicitly as predicates. To account for terms with no denotation, formulas can take on three truth values: $\oplus$ (definitely true), $\oplus\!\!\!\!-$ (unknown), and $\ominus$ (definitely false). Thus dL_ι is also a *3-valued* logic, and first-order connectives take on their Łukasiewicz interpretation.

The interpretation functions are parameterized by a state $\omega : \mathcal{V} \to \mathbf{Tree}(\mathbb{R})$, which maps variables to values and by an interpretation I which maps rigid symbols to interpretation, including the possibility of not denoting a value. Writing $\mathcal{S}$ for the set of all states, we have $I(a) : \wp(\mathcal{S} \times \mathcal{S}), I(p) : (\mathbf{Tree}(\mathbb{R}) \cup \perp) \to \{\oplus, \oplus\!\!\!\!-, \ominus\}, I(f) : (\mathbf{Tree}(\mathbb{R}) \cup \perp) \to (\mathbf{Tree}(\mathbb{R}) \cup \perp)$, and $I(C) : (\mathcal{S} \to \{\oplus, \oplus\!\!\!\!-, \ominus\}) \to (\mathcal{S} \to \{\oplus, \oplus\!\!\!\!-, \ominus\})$ where $\wp(U)$ is the power set of a set U.

Definition 1 (Term semantics). *The denotation of a term is either a tree or undefined, i.e.* $I\omega[\![\theta]\!] : \mathbf{Tree}(\mathbb{R}) \cup \{\perp\}$*, and is inductively defined as:*

$$
\begin{aligned}
I\omega[\![q]\!] &= q \quad I\omega[\![x]\!] = \omega(x) \quad I\omega[\![f(\theta)]\!] = I(f)(I\omega[\![\theta]\!]) \\
I\omega[\![\theta_1 + \theta_2]\!] &= I\omega[\![\theta_1]\!] + I\omega[\![\theta_2]\!] \text{ if } I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!] \in \mathbb{R} \\
I\omega[\![\theta_1 \cdot \theta_2]\!] &= I\omega[\![\theta_1]\!] \cdot I\omega[\![\theta_2]\!] \text{ if } I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!] \in \mathbb{R} \\
I\omega[\![\iota x\ \phi]\!] &= \begin{cases} t & \text{if there is a unique } t \in \mathbf{Tree}(\mathbb{R}) \text{ where } I\omega^t_x[\![\phi]\!] = \oplus \\ \perp & \text{otherwise} \end{cases} \\
I\omega[\![(\theta_1, \theta_2)]\!] &= (I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!]) \text{ if } I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!] \neq \perp \\
I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!] &= \mathsf{Fold}(I\omega[\![\theta_1]\!], s\ \theta_2, lr\ \theta_3, I\omega) \\
I\omega[\![(\theta)']\!] &= \sum_{x \in \mathcal{V}} \omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x} \text{ if } I[\![\theta]\!] \text{ totally differentiable at } \omega \\
I\omega[\![\theta]\!] &= \perp \textbf{ in all other cases}
\end{aligned}
$$

where $\omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x}$ is admittedly an abuse of notation when $\omega(x)$ is a tuple: the partial is taken with respect to each *real* appearing in x and scaled by the corresponding component of x'; our precise treatment of partial and total differentials is technically subtle, and so is given in App. D. In previous formalisms for dL [19] the semantics of $(\theta)'$ do not explicitly require that θ is totally differentiable because all pure dL terms are smooth, thus totally differentiable. In contrast, not

all dL_ι terms are smooth, thus we require total differentiability explicitly, as it required for soundness of standard dL axioms (specifically $\mathrm{DI}_{\geq}$, Sec. 5). If differentiability conditions are not met, the denotation of $I\omega[\![(\theta)']\!]$ is $\bot$.

The reduction $\mathsf{Fold}(t, s\ \theta_R, lr\ \theta_T, I\omega)$ is defined as:

$$\begin{aligned}\mathsf{Fold}(val, s\ \theta_2, lr\ \theta_3, I\omega) &\equiv I\omega_s^{val}[\![\theta_2]\!] \text{ when } val \in \mathbb{R}\\ \mathsf{Fold}((L,R), s\ \theta_2, lr\ \theta_3, I\omega) &\equiv I\omega_{l,r}^{K,S}[\![\theta_3]\!] \text{ where}\\ K = \mathsf{Fold}(L, s\ \theta_2, lr\ \theta_3, I\omega), &S = \mathsf{Fold}(R, s\ \theta_2, lr\ \theta_3, I\omega)\end{aligned}$$

Definition 2 (Formula semantics). *The formula semantics are 3-valued: definitely-true ($\oplus$), maybe-true ($\oplusminus$), or definitely-false ($\ominus$):*

$$\begin{aligned} I\omega[\![\phi \wedge \psi]\!] &= I\omega[\![\phi]\!] \sqcap I\omega[\![\psi]\!] & I\omega[\![\neg\phi]\!] &= \overline{I\omega[\![\phi]\!]}\\ I\omega[\![\forall x \phi]\!] &= \sqcap_{t\in\mathbf{Tree}(\mathbb{R})} I\omega_x^t[\![\phi]\!] & I\omega[\![[\alpha]\phi]\!] &= \sqcap_{(\omega,\nu)\in I[\![\alpha]\!]} I\nu[\![\phi]\!]\\ I\omega[\![p(\theta)]\!] &= I(p)(I\omega[\![\theta]\!]) & I\omega[\![C(\phi)]\!] &= I(C)(I[\![\phi]\!])(\omega)\\ I\omega[\![\theta_1 \geq \theta_2]\!] &= \mathsf{Geq}(I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!]) \end{aligned}$$

$$\begin{aligned}\mathsf{Geq}(r_1, r_2) &\equiv r_1 \geq r_2 \text{ if } r_1, r_2 \in \mathbb{R}\\ \mathsf{Geq}((l_1, r_1), (l_2, r_2)) &\equiv \mathsf{Geq}(l_1, l_2) \sqcap \mathsf{Geq}(r_1, r_2)\\ \mathsf{Geq}(v_1, v_2) &\equiv \oplusminus \text{ otherwise}\end{aligned}$$

$tv \leftrightarrow tv$	$\oplus$	$\oplusminus$	$\ominus$
$\oplus$	$\oplus$	$\oplusminus$	$\ominus$
$\oplusminus$	$\oplusminus$	$\oplus$	$\oplusminus$
$\ominus$	$\ominus$	$\oplusminus$	$\oplus$

$tv \rightarrow tv$	$\oplus$	$\oplusminus$	$\ominus$
$\oplus$	$\oplus$	$\oplusminus$	$\ominus$
$\oplusminus$	$\oplus$	$\oplus$	$\oplus$
$\ominus$	$\oplus$	$\oplus$	$\oplus$

$\overline{tv}$	
$\oplus$	$\ominus$
$\oplusminus$	$\oplusminus$
$\ominus$	$\oplus$

$tv \sqcap tv$	$\oplus$	$\oplusminus$	$\ominus$
$\oplus$	$\oplus$	$\oplusminus$	$\ominus$
$\oplusminus$	$\oplusminus$	$\oplusminus$	$\ominus$
$\ominus$	$\ominus$	$\ominus$	$\ominus$

We say a formula ϕ is *valid* if $I\omega[\![\phi]\!] = \oplus$ for all ω and I. Connectives $\phi \rightarrow \psi$ and $\phi \leftrightarrow \psi$ are defined; their truth tables are given for clarity. Comparisons $\theta_1 \geq \theta_2$ are taken elementwise and are unknown ($\oplusminus$) for differing shapes. Predicates p and quantifier symbols C are interpreted by the interpretation I, where the partial application $I[\![\phi]\!] : \mathcal{S} \rightarrow \{\oplus, \oplusminus, \ominus\}$ is shorthand for the function mapping each ω to $I\omega[\![\phi]\!]$. The meaning of quantifiers $\forall x\ \phi$ and $[\alpha]\phi$ are taken as conjunctions $\sqcap_S$ over potentially-uncountable sets S. The truth value of such conjunctions is the least (most false) truth value taken on any $x \in S$, which always exists because there are finitely many (3) truth values.

Definition 3 (Program semantics).

Program semantics generalize those of dL as conservatively as possible so that verification finds as many bugs as possible: e.g. assignments of non-denoting terms and tests of unknown formulas abort. The denotation of a program α is

relation $I[\![\alpha]\!]$ where $(\omega,\nu) \in I[\![\alpha]\!]$ whenever final state ν is reachable from initial state ω by running α.

$$I[\![x := \theta]\!] = \{(\omega, \omega_x^{I\omega[\![\theta]\!]}) \mid I\omega[\![\theta]\!] \neq \bot\} \qquad I[\![?\phi]\!] = \{(\omega,\omega) \mid I\omega[\![\phi]\!] = \oplus\}$$
$$I[\![\alpha \cup \beta]\!] = I[\![\alpha]\!] \cup I[\![\beta]\!] \qquad I[\![\alpha;\beta]\!] = I[\![\alpha]\!] \circ I[\![\beta]\!]$$
$$I[\![\alpha^*]\!] = I[\![\alpha]\!]^* = \bigcup_{n\in\mathbb{N}} I[\![\alpha^n]\!]$$

$$I[\![x' = \theta \,\&\, \psi]\!] = \{(\omega, \varphi(r)) \mid \text{exists } \varphi : [0,r] \to \mathcal{S} \text{ for } r \geq 0 \text{ where for all } s \in [0,r]$$
$$\text{have } I\varphi(s)[\![x' = \theta \wedge \psi]\!] = \oplus \text{ and } \frac{\partial \varphi(t)(x)}{\partial t}(s) = I\varphi(s)(x') \text{ and } \omega = \varphi(0)$$
$$\text{on } \{x'\}^C \text{ and } \varphi(s) = \varphi(0) \text{ on } \{x, x'\}^C\}$$

Assignments $x := \theta$ are eager: they store the value of θ in variable x, or abort if θ does not denote a value. Note the following axiom does not suffice for assignment as the left side may abort even when the right hand side holds:

$$[x := f]p(x) \leftrightarrow p(f)$$

Tests $?\phi$ succeed if ϕ is definitely true ($\oplus$); if ϕ is unknown ($\circledplus$) because it depends on an undefined term, execution aborts. Likewise, the domain constraint ψ of a differential equation $x' = \theta \,\&\, \psi$ must be definitely-true ($\oplus$) throughout the entire evolution and the term θ (implicitly) must denote values throughout the evolution, since $\frac{\partial \varphi(t)(x)}{\partial t}(s) \neq \bot$ whenever φ is the solution of an ODE.

4 Derived Constructs

A key benefit of dL_ι is extensibility: Many practical constructs can be defined with definite descriptions $\iota x\ \phi$ and tuples whose definition in plain dL requires complex, impractical reductions. In this section we reap the benefits of extensibility by defining such new term constructs.

Arithmetic operations. In practice, we often wish to use arithmetic operations beyond the core dL operations. Fig. 1 demonstrates basic arithmetic operations definable in dL_ι but not dL: Of these, $\max, \min$, and $|\cdot|$ preserve Lipschitz-continuity but not differentiability. Roots $\sqrt{\theta}$ can violate even Lipschitz-continuity and both roots and divisions are non-total. In practice (as in Ex. 1), these operators are used in ODE models, making their continuity properties essential.

Tuples. We make tuples first-class in dL_ι to simultaneously simplify the treatment of ODEs compared to prior work [14] and provide support for data structures such as vectors, widely used in physical computations. In contrast to the indexed variables of $\mathsf{Qd}\mathcal{L}$ [16], they are equipped with an induction operator, making it easier to write sophisticated computations. These structures are likely

$$
\begin{aligned}
(\mathsf{if}(\phi)\{\theta_1\}\mathsf{else}\{\theta_2\}) &= \iota x\ (\phi \wedge x{=}\theta_1) \vee (\neg\phi \wedge x{=}\theta_2) \\
\max(\theta_1,\theta_2) &= \iota x\ (\theta_1 \geq \theta_2 \wedge x = \theta_1) \vee (\theta_2 \geq \theta_1 \wedge x = \theta_2) \\
\min(\theta_1,\theta_2) &= \iota x\ (\theta_1 \geq \theta_2 \wedge x = \theta_2) \vee (\theta_2 \geq \theta_1 \wedge x = \theta_1) \\
|\theta| &= \max(\theta,-\theta) \quad \sqrt{\theta} = \iota x\ (x^2{=}\theta \wedge x \geq 0) \quad \theta_1/\theta_2 = \iota x\ (x \cdot \theta_2{=}\theta_1) \\
(\sin\theta,\cos\theta) &= \iota z\ [t := 0; s := 0; c := 1; s'{=}c, c'{=}{-}s, t'{=}1; ?t{=}\theta]z{=}(s,c)
\end{aligned}
$$

Fig. 1. Derived arithmetic operations

useful for systems with non-scalar inputs, for example a robot which must avoid many obstacles at once.

While pairs (θ_1,θ_2) are core dL_ι constructs, the left and right projections $\pi_1\theta$ and $\pi_2\theta$ are derivable, as are convenience predicates $\mathsf{in}\mathbb{R}(\theta)$ and $\mathsf{isT}(\theta)$ which hold only of reals or tuples respectively:

$$
\begin{aligned}
\pi_1\theta &\equiv \iota x\ \exists r(\theta = (x,r)) & \qquad \pi_2\theta &\equiv \iota x\ \exists l(\theta = (l,x)) \\
\mathsf{in}\mathbb{R}(\theta) &\equiv (\mathsf{red}(\theta, s\ 1, lr\ 0) = 1) & \qquad \mathsf{isT}(\theta) &\equiv (\mathsf{red}(\theta, s\ 1, lr\ 0) = 0)
\end{aligned}
$$

When combined with the reduce operation on trees, these operations can be used to implement a variety of data structures. Fig. 2 shows an example library of operations on lists and matrices. As is common (e.g. in Lisp), lists are represented as nested pairs. As shown in App. A, matrices likewise are represented as nested lists. We name the argument L when it should be a list rather than an arbitrary tree. Lists are trees where each left projection is real-valued.

$$
\begin{aligned}
\mathsf{map}(T, x\ f(x)) &= \mathsf{red}(T, s\ f(s), lr\ (l,r)) \qquad \mathsf{snoc}(L,x) = \mathsf{red}(L, s\ (s,x), lr\ (\pi_1 l, r)) \\
\mathsf{rev}(L) &= \mathsf{red}(L, s\ s, lr\ \mathsf{snoc}(r,l)) \\
\mathsf{zip}(L_1,L_2) &= \mathsf{red}(\mathsf{rev}(L_1), s\ ((s,\pi_1 L_2),\pi_2 R_2), lr\ ((\pi_1\pi_1 l, \pi_1\pi_2 r), \pi_2\pi_2 r)) \\
(L_1{+}L_2) &= \mathsf{map}(\mathsf{zip}(L_1,L_2), x\ \pi_1 x + \pi_2 x) \\
L_1{\cdot}L_2 &= \mathsf{red}(\mathsf{zip}(L_1,L_2), s\ \pi_1 s \cdot \pi_2 s, lr\ l + r) \quad \|L\| = \sqrt{L{\cdot}L}
\end{aligned}
$$

Fig. 2. Example vector functions

Systems of ODEs. Tuples reduce ODE systems to individual ODEs, e.g.:

$$\{x_1' = \theta_1, x_2' = \theta_2\} \ \equiv\ (z := (x_1,x_2);\ \{z' = (\theta_1,\theta_2)\};\ x_1 := \pi_1 z;\ x_2 := \pi_2 z)$$

While this encoding is simple, it will enable us in Sec. 5 to support systems of arbitrary dimension in axiom DG, which implementation experience [7] has proven challenging due to the variable dependencies involved.

Types and Definedness. Many of the operations in dL_ι are specific, for example, to reals or to terms that denote values. For simplicity, we make these type distinctions extrinsically: core dL terms are untyped, and proposition $\mathsf{in}\mathbb{R}(\theta)$ says θ belongs to type $\mathbb{R}$. For convenience, we can then use the definable typed quantifiers, e.g., $\forall x{:}\mathbb{R}\ \phi \equiv \forall x\ (\mathsf{in}\mathbb{R}(x) \rightarrow \phi)$.Whether terms denote at all is also treated extrinsically. Formula $\mathsf{E}(\theta) \equiv \mathsf{D}(\theta = \theta)$ only holds for terms that denote, where $\mathsf{D}(\phi)$ says ϕ *is definitely true*, which has truth value $\oplus$ when ϕ has truth value $\oplus$ and has value $\ominus$ otherwise. We give its truth table and a definition:

$$\frac{\mathsf{D}(tv)\ \mathsf{D}(\oplus)\ \mathsf{D}(\boxplus)\ \mathsf{D}(\ominus)}{\oplus \quad \ominus \quad \ominus} \qquad \mathsf{D}(\phi) \equiv \langle\phi\rangle\mathrm{true}$$

These constructs will be used freely in the axioms of Sec. 5.

In the same spirit, we sometimes need to know a function $f(x)$ is continuous, a notion that can be derived. We write $\mathsf{Con}(f(x))$ to say that $f(x)$ is continuous as x varies around its current value:

$$\mathsf{Con}(f(x)) \equiv \mathsf{D}(\forall\varepsilon\,\exists\delta\,\forall y\,(0 < \|y - x\| < \delta \rightarrow \|f(y) - f(x)\| < \epsilon))$$

Note that when $\mathsf{Con}(f(x))$ holds, the shape of $f(x)$ is constant in a neighborhood of x, since the Euclidean norm $\|f(y) - f(x)\|$ does not exist when $f(y)$ and $f(x)$ differ in shape. Likewise, $\mathsf{Con}(f(x))$ requires only continuity on y whose shape agrees with that of x, since the Euclidean norm $\|y - x\|$ does not exist otherwise.

5 dL Axioms

Our proof system is given in the Hilbert style, with a minimum number of proof rules and larger number of axioms, each of which is an individual concrete formula. The core proof rule is uniform substitution [19][5, §35,§40]: from the validity of ϕ we can conclude validity of $\sigma(\phi)$ where substitution σ specifies concrete replacements for some or all predicates, functions, program constants, and quantifier symbols in a formula ϕ:

$$\text{(US)}\ \ \frac{\phi}{\sigma(\phi)}$$

The soundness side-conditions on substitutions σ are non-trivial, and make up much of the soundness proof in Sec. 6. The payoff is that uniform substitution enables a modular design where such subtle arguments need only be done once in the proof of the substitution rule, and every axiom, which is now an individual concrete formula, is significantly simpler to prove valid and to implement.

Fig. 3 gives axioms and rules for the discrete programming constructs, which are generalizations of corresponding axioms [19] for dL to account for non-denoting terms and formulas. The idea is to augment axioms with definedness conditions whenever multiple occurrences of terms or formulas differ in their tolerance for partiality.

Recall the operator $\mathsf{D}(\phi)$ says ϕ is *definitely* true. For example, axiom [?] says that a test $?Q$ succeeds when Q is definitely true. The induction axiom I

$$([\cdot])\ \langle a\rangle P \leftrightarrow \neg[a]\neg P$$

$$([:=])\ ([x := f]p(x) \leftrightarrow p(f)) \leftarrow \mathsf{E}(f)$$

$$([?])\ [?Q]P \leftrightarrow (\mathsf{D}(Q) \to P)$$

$$([\cup])\ [a \cup b]P \leftrightarrow [a]P \wedge [b]P$$

$$([;])\ [a;b]P \leftrightarrow [a][b]P$$

$$([*])\ [a^*]P \leftrightarrow P \wedge [a][a^*]P$$

$$(\forall I)\ (\forall x p(x)) \to (\mathsf{E}(f) \to p(f))$$

$$(\forall \to)\ \forall x\,(p(x) \to q(x)) \to (\forall x\, p(x) \to \forall x\, q(x))$$

$$(V_\forall)\ p \to \forall x\, p$$

$$(\mathrm{K})\ [a]\,(P \to Q) \to ([a]P \to [a]Q)$$

$$(\mathrm{I})\ [a^*]\,(\mathsf{D}(P \to [a]P)) \to (\mathsf{D}(P \to [a^*]P))$$

$$(\mathrm{V})\ p \to [a]p$$

$$(\mathrm{G})\ \frac{P}{[a]P}$$

$$(\forall)\ \frac{p(x)}{\forall x\, p(x)}$$

$$(\mathrm{MP})\ \frac{p \to q \quad p}{q}$$

$$(\mathrm{CQ})\ \frac{f(x) = g(x) \quad \mathsf{E}(\mathrm{h}(f(x))) \wedge \mathsf{E}(\mathrm{h}(g(x)))}{\mathrm{h}(f(x)) = \mathrm{h}(g(x))}$$

$$(\mathrm{CE})\ \frac{P \leftrightarrow Q}{C(P) \leftrightarrow C(Q)}$$

Fig. 3. Discrete dL Axioms

requires the inductive step proved definitely true, and concludes definite truth. The other axioms for program constructs ([·],[∪],[;][∗]) carry over from dL without modification, since partiality primarily demands changes when mediating between formulas and programs or between terms and program variables.

As is standard in free logics, axiom $\forall I$ says that since quantifiers range over values, they must be instantiated only to terms that denote values. Likewise, [:=] says assignments require that the term being assigned denotes a value, since program variables x range over values. The contextual reasoning rules CE and CQ allow rewriting a term or formula in context. Rule CQ additionally requires as its second premise that terms $f(x)$ and $g(x)$ still denote in the context h, since equalities in dL_ι can only hold between terms that denote, whereas equivalences may hold when both sides are unknown. Fig. 4 gives the dL_ι generalizations of dL's axioms for reasoning about differential equations: DC is generalized to require definite truth and DG is generalized to require continuity, otherwise the axioms carry over unchanged. DW says the constraint of an ODE always holds as a postcondition. DC says any postcondition which is proven (definitely) true may be added to the constraint. DE says the ODE holds as an equation in the postcondition. $\mathrm{DI}_\geq$ is the *differential induction* [15] axiom for proving nonstrict inequalities $f(x) \geq g(x)$ follow from their *differential formula* $(f(x))' \geq (g(x))'$. The strict case $f(x) > g(x)$ is analogous; axioms for equality, inequality, conjunction, and disjunction can be derived from these. Note the assumptions in $\mathrm{DI}_\geq$ hold only when $f(x)$ and $g(x)$ are *totally* differentiable within the constraint, as required for soundness. DG allows extending a system with an additional ghost dimension, and is used when reasoning, for example, about exponentially-decaying systems. The new dimension is required to be Lipschitz so that solutions exist and is required to be linear in the existing variables so that the solutions

$$((\theta)') \quad (f(x))' = x' \cdot \iota M\ \forall \xi{>}0\ \exists \delta\ \forall y\ \mathsf{D}(0{<}\|y{-}x\|{<}\delta \rightarrow (f(y){-}f(x)){-}M\cdot(y{-}x){<}\xi\cdot\|y{-}x\|) \leftarrow \mathsf{E}((f(x))')$$

$$(\mathrm{DW}) \quad [x' = f(x)\&q(x)]q(x)$$

$$(\mathrm{DC}) \quad ([x' = f(x)\&q(x)]p(x) \leftrightarrow [x' = f(x)\&q(x) \wedge r(x)]p(x)) \leftarrow \mathsf{D}([x' = f(x)\&q(x)]r(x))$$

$$(\mathrm{DE}) \quad [x' = f(x)\&q(x)][x' := f(x)]p(x,x') \leftrightarrow [x' = f(x)\&q(x)]p(x,x')$$

$$(\mathrm{DI}_{\geq}) \quad \big([x' = h(x)\&q(x)]f(x) \geq g(x) \leftrightarrow [?q(x)]f(x) \geq g(x)\big) \leftarrow [x' = h(x)\&q(x)](f(x))' \geq (g(x))'$$

$$(\mathrm{DG}) \quad \forall x\,(q(x) \rightarrow \mathsf{Con}(a(x)) \wedge \mathsf{Con}(b(x))) \rightarrow ([x' = f(x)\&q(x)]p(x) \leftrightarrow \exists y : \mathbb{R}\ [x'{=}f(x),\ y' = a(x)y + b(x)\&q(x)]p(x))$$

$$(\mathrm{DS}) \quad (\forall t : \mathbb{R}\ ((\forall 0{\leq}s{\leq}t\ q(x+fs)) \rightarrow [x := x+ft]p(x))) \rightarrow [x' = f\,\&\,q(x)]p(x)$$

Fig. 4. Differential axioms

of the extended system exist as long as those of the initial system. DS says the solution of a constant ODE system is linear. It generalizes to f that stand for tuple (multidimensional systems) by making $x + fs$ and $x + ft$ pairwise vector sums per Fig. 2. Axiom $(\theta)'$ expands a differential $(f(x))'$ according to the definition of total differential. It assumes $\mathsf{E}((f(x))')$ because equalities are not allowed to hold between nondenoting terms; in practice existence assumptions can be proved automatically by recursion on the term syntax. Since axiom $(\theta)'$ is long-winded for practical proving, we will use it to implement simpler special-case axioms in Ex. 2. The definition of $(\theta)'$ above considers only the case where x and $f(x)$ are real-valued, implicitly, because scalar differences $f(y) - f(x)$ and $y - x$ only denote a value when $x, y, f(x)$, and $f(y)$ are reals. In App. A we discuss its generalization to tree-valued functions of tree-valued arguments.

$$(\iota)\ p(\iota z\ p(z)) \leftrightarrow \exists x\ (p(x) \wedge (\forall y(p(y) \rightarrow y = x))) \quad (=\mathrm{T})\ l_1{=}l_2 \wedge r_1{=}r_2 \leftrightarrow (l_1,r_1){=}(l_2,r_2)$$

$$(\mathrm{QE}) \quad \frac{*}{\Big(\bigwedge_{x\in \mathrm{V}(\phi)} \mathsf{in}\mathbb{R}(x)\Big) \rightarrow \phi} \qquad \text{(where } \phi \text{ is a valid formula of first-order arithmetic)}$$

$$(\mathrm{redT}) \quad \mathsf{red}((L,R), s\ f(s), lr\ g(l,r)) = g(\mathsf{red}(L, s\ f(s), lr\ g(l,r)), \mathsf{red}(R, s\ f(s), lr\ g(l,r)))$$

$$(\mathrm{redR}) \quad \mathsf{in}\mathbb{R}(r) \rightarrow \mathsf{red}(r, s\ f(s), lr\ g(l,r)) = f(r)$$

$$(\mathrm{TI}) \quad \mathsf{D}(p(\iota x\ \mathrm{false}) \wedge \forall s(\mathsf{in}\mathbb{R}(s) \rightarrow p(s)) \wedge \forall lr\ \ (p(l) \wedge p(r) \rightarrow p((l,r)))) \rightarrow \mathsf{D}(p(t))$$

Fig. 5. New dL_ι Axioms

Fig. 5 gives axioms for differentiation, definite descriptions, and tuples. Axiom ι fully characterizes definite descriptions, and it is used to derive axioms for

defined term constructs like those in Ex. 2. Axiom =T enables comparisons on tuples. Quantifier elimination rule QE says first-order arithmetic, a fragment, is decidable [21]. Since variables of dL_ι may range over tuples, which are not part of first-order arithmetic, it must first check that all variables of the formula (denoted $\mathrm{V}(\phi)$) are indeed real-valued. Axioms redT and redR evaluate reductions when their shape is known, and TI allows proving a property of an arbitrary value by induction on its shape, including a second base case $p(\iota x \text{ false})$ where the argument to p does not denote.

Example 2 (Derived axioms). The following are examples of derived axiom schemata that have been proved (App. C) from those above.

$$\pi_1(l,r) = l \quad \pi_2(l,r) = r \quad \mathsf{E}(f) \to \mathsf{in}\mathbb{R}(f) \vee \mathsf{is}\mathsf{T}(f) \quad (x)' = x'$$

$$\mathsf{E}((f(x))') \wedge \mathsf{E}((g(x))') \to (f(x)+g(x))' = (f(x))' + (g(x))' \quad \mathsf{E}(f) \to (f)' = 0$$

$$\mathsf{E}((f(x))') \wedge \mathsf{E}((g(x))') \to (f(x)\cdot g(x))' = (f(x))'\cdot g(x) + (g(x))'\cdot f(x)$$

It is significant that the differential axioms of Ex. 2 are *derived*: when new term constructs are added in the future, we expect to derive their differential axioms as well, so that these extensions lie entirely *outside* the core dL_ι calculus. Note that while axioms for simplifying differentials require proving existence of the subterm differentials, they also implicit prove that the combined differential denotes (because it is equal to something), thus the assumptions are easily satisfied in practice.

Example 3 (Proof of Leakiness). Prop. 1 of Sec. 2 is provable in dL.

Proof (Sketch). By axiom I with loop invariant $P \equiv (g > 0 \wedge A > 0 \wedge 0 \leq h \leq h_0)$. The first two conditions are trivially invariant by axiom V because g and A are constant throughout α_B. Proceed by cases with axiom [$\cup$]. In each case, show $h \leq h_0$ to be an invariant of the ODE by $\mathrm{DI}_{\geq}$. Because $h \leq h_0$ holds initially and the ODE is locally Lipschitz-continuous under the constraint $h \geq 0$, then it suffices to show $(h)' \leq (h_0)' = 0$ throughout the ODE. By algebra:

$$\begin{aligned}
(h)' \leq 0 &\iff -\sqrt{2gh}\frac{a}{A} \leq 0 && \text{[DE]}\\
&\iff \sqrt{h} \geq 0 && \text{[Signs of } a, A, g\text{]}\\
&\iff \text{true} && \text{[Domain constraint } h \geq 0\text{, DW]}
\end{aligned}$$

Then in each case, $h \leq h_0$.

6 Theory

A central theoretical result says the dL_ι proof calculus is sound:

Theorem 1 (Soundness of dL_ι). *If ϕ is provable in dL_ι, then ϕ is valid.*

The proof of soundness proceeds by induction on the structure of derivations. That is, we prove each axiom (which is an individual formula) to be *valid* and prove every proof rule to be *sound* (producing sound conclusions from sound premisses). Because dL_ι supports the same formula and program connectives as dL, many of the axioms are extensions of corresponding dL axioms. The axiom validity proofs also have a similar flavor to those of dL: each axiom is proven valid by direct proof, showing truth of the axiom according to denotational semantics in an arbitrary state. The full proofs for each axiom and rule are given in App. C; Lem. 1 gives an example.

Lemma 1 (Assignment axiom is valid). *The following formula is valid:* $([x := f]p(x) \leftrightarrow p(f)) \leftarrow \mathsf{E}(f)$

Proof. Assume (1) $I\omega[\![\mathsf{E}(f)]\!] = \oplus$ for some state ω and interpretation I, then observe $I\omega[\![[x := f]p(x)]\!] = I\omega[\![p(f)]\!]$ by the chain of equalities $I\omega[\![[x := f]p(x)]\!] = \sqcap_{\nu \mid (\omega,\nu)\in\{(\omega,\omega_x^{I\omega[\![f]\!]})\},I\omega[\![f]\!]\neq\perp} I\nu[\![p(x)]\!] = I\omega_x^{I\omega[\![f]\!]}[\![p(x)]\!] = I(p)I(f) = I\omega[\![p(f)]\!]$ □

6.1 Uniform Substitution

The US rule in dL_ι is analogous to that in dL:

$$(\text{US})\ \frac{\phi}{\sigma(\phi)}$$

In dL, the US rule is sound when the substitution σ does not introduce free references to bound variables. Such substitutions are called *admissible*, a condition which can be checked syntactically.

We show that the same holds of dL_ι when adding terms $\iota x\ \phi, (\theta_1, \theta_2)$ and $\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$ and generalizing dL to a three-valued semantics. As in dL, we formulate admissibility in terms of U-admissibility (Def. 4) checks.

Definition 4 (Admissible Uniform Substitution). *A substitution σ is U-admissible for ϕ (or θ or α) with respect to a set $U \subseteq \mathcal{V}\cup\mathcal{V}'$ iff $FV(\sigma|_{\Sigma(\phi)})\cap U = \emptyset$ where $\sigma|_{\Sigma(\phi)}$ is the restriction of σ that only replaces symbols that occur in ϕ and $FV(\sigma) = \bigcup_{f\in\sigma} FV(\sigma f(\cdot)) \cup \bigcup_{p\in\sigma} FV(\sigma p(\cdot))$ are the free variables that σ introduces, and where $\mathcal{V}' = \{x' \mid x \in \mathcal{V}\}$. The substitution σ is admissible for ϕ (or θ or α) if all such checks during its applications hold, per Fig. 6.*

We give the new cases of $\mathrm{FV}(\cdot)$ here and the full static semantics in App. C.10:

$$\mathrm{FV}((\theta_1,\theta_2)) = \mathrm{FV}(\theta_1)\cup\mathrm{FV}(\theta_2) \qquad \mathrm{FV}(\iota x\ \phi) = \mathrm{FV}(\phi)\backslash\{x\}$$
$$\mathrm{FV}(\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_1)) = \mathrm{FV}(\theta_1)\cup(\mathrm{FV}(\theta_2)\backslash\{s\})\cup(\mathrm{FV}(\theta_3)\backslash\{l,r\})$$

Admissibility checks employ static semantics consisting of free-variable ($\mathrm{FV}(\cdot)$), bound-variable ($\mathrm{BV}(\cdot)$), and must-bound-variable ($\mathrm{MBV}(\cdot)$) functions that are bound on every execution path. Generally speaking, the free variables of a compound expression θ are the free variables of its immediate subexpressions, minus any variables that it binds. Formally, $\mathrm{FV}(\theta)$ (or ϕ, α) must contain all variables that influence meaning:

Case	Replacement	Admissible when
$\sigma((\theta_1,\theta_2))$	$= (\sigma(\theta_1),\sigma(\theta_2))$	
$\sigma(\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3))$	$= \mathsf{red}(\sigma(\theta_1), s\ \sigma(\theta_2), lr\ \sigma(\theta_3))$	σ is $\{s\}$-admissible for θ_2
		σ is $\{l,r\}$-admissible for θ_3
$\sigma(\iota x\ \phi)$	$= \iota x\ \sigma(\phi)$	σ is $\{x\}$-admissible for ϕ
$\sigma(\forall x \phi)$	$= \forall x \sigma(\phi)$	σ is $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi)$	$= [\sigma(\alpha)]\sigma(\phi)$	σ is BV(α)-admissible for (ϕ)
$\sigma(f(\theta))$	$= f(\sigma(\theta))$, if $f \notin \sigma$, else $\sigma f(\sigma(\theta))$	

Fig. 6. Uniform substitution algorithm (selected cases)

Lemma 2 (Coincidence). *The interpretation of an expression depends only on the values of its free variables and constants, e.g. for any term θ, any interpretations I and J that agree on the signature (rigid symbols) $\Sigma(\theta)$ of θ, and any states ω and $\tilde{\omega}$ that agree on $FV(\theta)$, we have $I\omega[\![\theta]\!] = J\tilde{\omega}[\![\theta]\!]$*

The substitution result for a compound expression is found by substituting in each immediate subexpression, and is defined so long as all admissibility checks hold recursively. In general, the admissibility check for each constructor says that the substitution result must not contain any new occurences of the variables bound at that constructor.

Lemma 3 (Substitution lemma). *Rule US is sound.*

Soundness of the proof system then follows from validity of the axioms and soundness of US and the other rules.

6.2 Expressive Power

After showing soundness of dL_ι, we explore its expressive power: can dL_ι express formulas that are inexpressible in dL, or is its advantage the ease with which certain formulas are expressed? Conversely, are all dL formulas expressible in dL_ι? Because dL_ι is an extension of dL, it is unsurprising that it can express all dL formulas. However, a valid dL formula ϕ is not always valid in dL_ι.

Remark 1 (Conservativity Counterexample). There exist valid formulas of dL that are not valid formulas of dL_ι.

Proof. The formula $\phi \equiv (x \cdot x \geq 0)$ is a counterexample. It is true for all real values of x, but fails when x is assigned a tuple such as $\{x \mapsto (0,0)\}$, which is outside the domain of the multiplication operator.

This problem is easily resolved by expressing real-valued quantifiers in dL_ι:

Theorem 2 (Converse reducibility). *There exists a linear-time transformation T such that for all ϕ in dL, $T(\phi)$ is valid in dL_ι iff ϕ is valid in dL.*

The greater challenge is to show that dL also suffices to express all dL$_\iota$ formulas and thus dL and dL$_\iota$ are equi-expressive:

Theorem 3 (Reducibility). *There exists a computable transformation T such that for all formulas ϕ, interpretations I, and states ω in* dL$_\iota$*, $I\omega[\![\phi]\!] = \oplus$ in* dL$_\iota$ *iff $\omega[\![T(\phi)]\!] = \oplus^1$ in* dL*.*

This equi-expressiveness result is of theoretical interest because it allows us to inherit results from dL [14]:

Theorem 4 (Completeness and Decidability). dL$_\iota$ *is reducible to* dL*, and therefore semidecidable relative to properties of differential equations.*

While the reduction gives a semi-decision procedure for dL$_\iota$ in principle, it is infeasible for implementation, especially since deciding even core dL is infeasible in practice. Moreover, this would defeat our purpose: easing implementation of practical term language extensions in dL, where interactive proof is standard.

7 Future Work and Conclusion

In this paper we developed dL$_\iota$, an extension to differential dynamic logic (dL) for formal verification of hybrid systems models of safety-critical cyber-physical systems. The key feature of dL$_\iota$ is definite description $\iota x\ \phi$, which provides a foundation for defining new term language constructs from their characteristic formulas. We develop the theory of dL$_\iota$, including semantics, a proof calculus, and soundness and expressiveness proofs. We apply dL$_\iota$ to verify a classic example of a non-Lipschitz ODE, which could not be directly verified in dL.

In particular, we give a novel axiomatization that accounts for the interactions between partial and non-differentiable operators with systems of differential equations, an interaction which does not occur for dL's simpler language where all terms are continuous. More generally, example applications abound: almost every serious case study of dL employs these constructs in practice; we give a fully rigorous foundation to these case studies for the first time. In future work, implementing dL$_\iota$ in KeYmaera X would enable case studies to soundly employ the constructs given herein and to define their own. We expect few core changes would be needed, thanks to our use of uniform substitution, rather the challenge is to efficiently prove and track the new assumptions on existence and continuity.

References

1. Anand, A., Rahli, V.: Towards a formally verified proof assistant. In: Klein, G., Gamboa, R. (eds.) ITP. LNCS, vol. 8558, pp. 27–44. Springer (2014). DOI: 10.1007/978-3-319-08970-6_3

[1] we omit the interpretation here to indicate the result of the reduction contains no rigid symbols

2. Barras, B.: Sets in Coq, Coq in sets. J. Formalized Reasoning **3**(1), 29–48 (2010). DOI: 10.6092/issn.1972-5787/1695
3. Bohrer, B., Rahli, V., Vukotic, I., Völp, M., Platzer, A.: Formally verified differential dynamic logic. In: Bertot, Y., Vafeiadis, V. (eds.) CPP. pp. 208–221. ACM (2017). DOI: 10.1145/3018610.3018616
4. Bohrer, B., Tan, Y.K., Mitsch, S., Myreen, M.O., Platzer, A.: VeriPhy: Verified controller executables from verified cyber-physical system models. In: Grossman, D. (ed.) PLDI. pp. 617–630. ACM (2018). DOI: 10.1145/3192366.3192406
5. Church, A.: Introduction to Mathematical Logic. Princeton University Press (1956)
6. Driver, R.: Torricelli's law: An ideal example of an elementary ODE. The American Mathematical Monthly **105**(5), 453–455 (1998)
7. Fulton, N., Mitsch, S., Quesel, J.D., Völp, M., Platzer, A.: KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In: Felty, A.P., Middeldorp, A. (eds.) CADE. LNCS, vol. 9195, pp. 527–538. Springer (2015). DOI: 10.1007/978-3-319-21401-6_36
8. Henzinger, T.A.: The theory of hybrid automata. In: LICS. IEEE (1996), https://doi.org/10.1109/LICS.1996.561342
9. Hubbard, J.H., West, B.H.: Differential Equations: A Dynamical Systems Approach, Texts in Applied Mathematics, vol. 18. Springer. DOI: 10.1007/978-1-4612-4192-8
10. Jeannin, J., Ghorbal, K., Kouskoulas, Y., Schmidt, A., Gardner, R., Mitsch, S., Platzer, A.: A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system. STTT **19**(6), 717–741 (2017). DOI: 10.1007/s10009-016-0434-1
11. Kumar, R., Arthan, R., Myreen, M.O., Owens, S.: Self-formalisation of higher-order logic: Semantics, soundness, and a verified implementation. J. Autom. Reasoning **56**(3), 221–259 (2016). DOI: 10.1007/s10817-015-9357-x
12. Mitsch, S., Gario, M., Budnik, C.J., Golm, M., Platzer, A.: Formal verification of train control with air pressure brakes. In: Fantechi, A., Lecomte, T., Romanovsky, A. (eds.) RSSRail. LNCS, vol. 10598, pp. 173–191. Springer (2017). DOI: 10.1007/978-3-319-68499-4_12
13. 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). DOI: 10.1177/0278364917733549
14. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. **41**(2), 143–189 (2008). DOI: 10.1007/s10817-008-9103-8
15. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. **20**(1), 309–352 (2010). DOI: 10.1093/logcom/exn070, advance Access published on November 18, 2008
16. Platzer, A.: A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems. Logical Methods in Computer Science **8**(4), 1–44 (2012). DOI: 10.2168/LMCS-8(4:17)2012, special issue for selected papers from CSL'10
17. Platzer, A.: The complete proof theory of hybrid systems. In: LICS. pp. 541–550. IEEE (2012). DOI: 10.1109/LICS.2012.64
18. Platzer, A.: Logics of dynamical systems. In: LICS. pp. 13–24. IEEE (2012). DOI: 10.1109/LICS.2012.13
19. Platzer, A.: A complete uniform substitution calculus for differential dynamic logic. J. Autom. Reas. **59**(2), 219–265 (2017). DOI: 10.1007/s10817-016-9385-1
20. Platzer, A.: Differential hybrid games. ACM Trans. Comput. Log. **18**(3), 19:1–19:44 (2017). DOI: 10.1145/3091123

21. Tarski, A.: A decision method for elementary algebra and geometry. In: Quantifier elimination and cylindrical algebraic decomposition, pp. 24–84. Springer (1998)

A Defined Constructs

We collect the definable term and formula constructs from the paper here for the sake of reference. We also extend the proposed vector library from the paper with additional practical functions including operations on matrices.

Formula connective $\mathsf{D}(\phi)$ is definable: $\mathsf{D}(\phi) \equiv \langle\phi\rangle\text{true}$
As is continuity:

$$\mathsf{Con}(f(x)) \equiv \mathsf{D}(\forall\varepsilon\,\exists\delta\,\forall y\,(0 < \|y-x\| < \delta \to \|f(y)-f(x)\| < \epsilon))$$

Typed assignments and typed quantifiers are definable:

$$\begin{aligned} x{:}\mathbf{Tree}(\mathbb{R}) := \theta &\equiv x := \theta;\ ?\mathsf{isT}(x) \\ \forall x{:}\mathbf{Tree}(\mathbb{R})\phi &\equiv \forall x \mathsf{isT}(x) \to \phi \\ \exists x{:}\mathbf{Tree}(\mathbb{R})\phi &\equiv \exists x \mathsf{isT}(x) \wedge \phi \end{aligned}$$

Scalar arithmetic operations:

$$\begin{aligned} (\mathsf{if}(\phi)\{\theta_1\}\mathsf{else}\{\theta_2\}) &= \iota x\ (\phi \wedge x{=}\theta_1) \vee (\neg\phi \wedge x{=}\theta_2) \\ \max(\theta_1,\theta_2) &= \iota x\ (\theta_1 \geq \theta_2 \wedge x = \theta_1) \vee (\theta_2 \geq \theta_1 \wedge x = \theta_2) \\ \min(\theta_1,\theta_2) &= \iota x\ (\theta_1 \geq \theta_2 \wedge x = \theta_2) \vee (\theta_2 \geq \theta_1 \wedge x = \theta_1) \\ |(\theta)| &= \max(\theta,-\theta) \quad \sqrt{\theta} = \iota x\ (x^2{=}\theta \wedge x \geq 0) \quad \theta_1/\theta_2 = \iota x\ (x\cdot\theta_2{=}\theta_1 \wedge \theta_2 \neq 0) \\ (\sin\theta,\cos\theta) &= \iota z\ [t := 0; s := 0; c := 1; s'{=}c, c'{=}-s, t'{=}1; ?t{=}\theta] z{=}(s,c) \end{aligned}$$

Tuple operations:

$$\begin{aligned} \pi_1\theta &\equiv \iota x\ \exists r(\theta = (x,r)) & \pi_2\theta &\equiv \iota x\ \exists l(\theta = (l,x)) \\ \mathsf{in}\mathbb{R}(\theta) &\equiv (\mathsf{red}(\theta, s\ 1, lr\ 0) = 1) & \mathsf{isT}(\theta) &\equiv (\mathsf{red}(\theta, s\ 1, lr\ 0) = 0) \end{aligned}$$

Systems of differential equations:

$$\{x_1' = \theta_1, x_2' = \theta_2\}\ \equiv\ (z := (x_1,x_2);\ \{z' = (\theta_1,\theta_2)\};\ x_1 := \pi_1 z;\ x_2 := \pi_2 z)$$

The extended library for vectors and matrices is as follows:

$$\begin{aligned} \mathsf{map}(T, x\ f(x)) &= \mathsf{red}(T, s\ f(s), lr\ (l,r)) \\ \mathsf{size}(T) &= \mathsf{red}(T, s\ 1, lr\ l+r) \\ \mathsf{depth}(T) &= \mathsf{red}(T, s\ 1, lr\ \max(l,r)+1) \\ \mathsf{shape}(T) &= \mathsf{red}(T, s\ 0, lr\ (l,r)) \\ \mathsf{islist}(T) &= (\mathsf{depth}(T) = \mathsf{size}(T)) \wedge (\mathsf{isT}(T) \to \mathsf{in}\mathbb{R}(\pi_1 T)) \\ \mathsf{mmap}(M, f(x)\ ) &= \mathsf{if}\ (\mathsf{islist}(M))\ \{\mathsf{map}(M, x\ f)\}\mathsf{else}\ \{f(M)\} \\ \mathsf{snoc}(L, x) &= \mathsf{red}(L, s\ (s,x), lr\ (\pi_1 l, r)) \\ \mathsf{rev}(L) &= \mathsf{red}(L, s\ s, lr\ \mathsf{snoc}(r,l)) \\ \mathsf{transpose}(M) &= \mathsf{if}(\mathsf{islist}(M))\ \{M\}\ \{ \end{aligned}$$

$$\begin{aligned}
&\mathsf{red}(\pi_1 M, s\ (\mathsf{map}(M, x\ \pi_1 x), \mathsf{map}(M, x\ \pi_2 x)), lr\\
&(\mathsf{zip}(\mathsf{map}(\pi_1 x, x\ \pi_2 r), \pi_1 r), \mathsf{map}(\pi_2 x, x\ \pi_2 r)))\}\\
(M \times N) &= \mathsf{mmap}(N, v\ \mathsf{mmap}(\mathsf{transpose}(N), u\ u{\cdot}v))\\
\mathsf{zip}(L_1, L_2) &= \mathsf{red}(\mathsf{rev}(L_1), s\ ((s, \pi_1 L_2), \pi_2 R_2), lr\ ((\pi_1\pi_1 l, \pi_1\pi_2 r), \pi_2\pi_2 r))\\
(L_1{+}L_2) &= \mathsf{map}(\mathsf{zip}(L_1, L_2), x\ \pi_1 x + \pi_2 x)\\
(L_1{-}L_2) &= \mathsf{map}(\mathsf{zip}(L_1, L_2), x\ \pi_1 x - \pi_2 x)\\
L_1{\cdot}L_2 &= \mathsf{red}(\mathsf{zip}(L_1, L_2), s\ \pi_1 s \cdot \pi_2 s, lr\ l + r)\\
\|L\| &= \sqrt{L{\cdot}L}
\end{aligned}$$

$\mathsf{map}(T, x\ f(x))$ applies the operation $f(x)$ at every leaf of T. $\mathsf{islist}(T)$ checks that T is either a left or right-facing list ($\mathsf{depth}(T) = \mathsf{size}(T)$) then specifically that it's a right-facing list ($\mathsf{isT}(T) \to \mathsf{in}\mathbb{R}(\pi_1 T)$). $\mathsf{mmap}(M, f(x)\ )$ applies $f(x)$ to each list in matrix M. $\mathsf{snoc}(L, x)$ cons'es x onto the *rear* of L. $(L_1{+}L_2)$ and $(L_1{-}L_2)$ are pairwise vector addition and subtraction.

B Uniform Substitution Algorithm

We give the complete presentation of the uniform substitution algorithm, i.e.

- The $\mathrm{FV}(e)$ function computing flexible symbols which can influence expression e
- The $\mathrm{BV}(\alpha)$ function computing flexibles which can change during program α (unchanged from prior work)
- The $\mathrm{MBV}(\alpha)$ function computing flexibles which are necessarily bound on *all* execution paths of α
- The signature $\Sigma(e)$ of rigid symbols in expression e.
- The substitution algorithm $\sigma(e)$ proper.

Equations (1-11) are as in previous work [19]. In Equation 11, $\mathrm{MBV}(\alpha)$ is the set of variables that are bound on *all* executions of α. It may be surprising that the free program variables of ϕ and θ make no appearance.

$$\begin{aligned}
\mathrm{BV}(?\phi) &= \emptyset\\
\mathrm{BV}(x := \theta) &= \{x\}\\
\mathrm{BV}(x' = \theta \,\&\, \psi) &= \{x, x'\}\\
\mathrm{BV}(\alpha \cup \beta) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta)\\
\mathrm{BV}(\alpha; \beta) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta)\\
\mathrm{BV}(\alpha^*) &= \mathrm{BV}(\alpha)\\
\mathrm{BV}(a) &= \mathcal{V} \cup \mathcal{V}
\end{aligned}$$

$$\begin{aligned}
\mathrm{MBV}(\alpha \cup \beta) &= \mathrm{MBV}(\alpha) \cap \mathrm{MBV}(\beta)\\
\mathrm{MBV}(\alpha; \beta) &= \mathrm{MBV}(\alpha) \cup \mathrm{MBV}(\beta)\\
\mathrm{MBV}(a) = \mathrm{MBV}(\alpha^*) &= \emptyset\\
\mathrm{MBV}(\alpha) &= \mathrm{BV}(\alpha) \text{ in all other cases}
\end{aligned}$$

$$\mathrm{FV}(c) = \emptyset \tag{1}$$
$$\mathrm{FV}(x) = \{x\} \tag{2}$$
$$\mathrm{FV}(\theta_1 + \theta_2) = \mathrm{FV}(\theta_1) \cup \mathrm{FV}(\theta_2) \tag{3}$$
$$\mathrm{FV}(\theta_1 \cdot \theta_2) = \mathrm{FV}(\theta_1) \cup \mathrm{FV}(\theta_2) \tag{4}$$
$$\mathrm{FV}(\exists x \phi) = \mathrm{FV}(\phi) \setminus \{x\} \tag{5}$$
$$\mathrm{FV}(f(\theta)) = \mathrm{FV}(\theta) \tag{6}$$
$$\mathrm{FV}(\phi \wedge \psi) = \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi) \tag{7}$$
$$\mathrm{FV}(\neg \phi) = \mathrm{FV}(\phi) \tag{8}$$
$$\mathrm{FV}(\iota x\ \phi) = \mathrm{FV}(\phi) \setminus \{x\} \tag{9}$$
$$\mathrm{FV}(\theta_1 \geq \theta_2) = \mathrm{FV}(\theta_1) \cup \mathrm{FV}(\theta_2) \tag{10}$$
$$\mathrm{FV}(\langle \alpha \rangle \phi) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha)) \tag{11}$$

$$\mathrm{FV}(p(\theta)) = \mathrm{FV}(\theta) \tag{12}$$
$$\mathrm{FV}(?\phi) = \mathrm{FV}(\phi) \tag{13}$$
$$\mathrm{FV}(x := \theta) = \mathrm{FV}(\theta) \tag{14}$$
$$\mathrm{FV}(x' = \theta \,\&\, \psi) = \mathrm{FV}(\theta) \cup \mathrm{FV}(\psi) \tag{15}$$
$$\mathrm{FV}(\alpha \cup \beta) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) \tag{16}$$
$$\mathrm{FV}(\alpha; \beta) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) \tag{17}$$
$$\mathrm{FV}(\alpha^*) = \mathrm{FV}(\alpha) \tag{18}$$
$$\mathrm{FV}(a) = \mathcal{V} \cup \mathcal{V}' \tag{19}$$

Fig. 7. Free variable computation

Analogously to FV(e), the signature $\Sigma(e)$ indicates all *rigid* symbols which influence the meaning of e.

$$\Sigma(sym \in f, a, p, P) = \{sym\}$$
$$\Sigma(\otimes(e_1, \ldots, e_n)) = \Sigma(e_1) \cup \cdots \cup \Sigma(e_n)$$

Fig. 8. Signature computation (sym is an arbitrary rigid)

Admissibility conditions are checked recursively during the substitution algorithm proper (Figure 9). These checks use an auxilliary notion called $U-$admissiblity:

Definition 5 (U-admissibility). *We say a substitution σ is U-admissible for an expression e with a flexible symbol set U iff* $\bigcup_{sym \in \sigma|_{\Sigma(e)}} FV(\sigma sym) \cap U = \emptyset$ *where $\sigma|_{\Sigma(e)}$ is the restriction of σ that replaces only symbols occurring in e.*

This makes the admissibility conditions as expressed in the main paper precise. Note also in Figure 9 that the symbol $\cdot$ is a reserved function (or nominal) symbol standing for the argument.

C Proofs

We begin by proving soundness (Thm. 1). Soundness follows by induction on the structure of proofs: we prove each core axiom, which is a concrete axiom, valid. Then we prove each proof rule sound, of which the main proof effort is for uniform substitution.

C.1 Discrete Axioms Sound

We begin with validity proofs of axioms that deal solely with the discrete fragment of dL_ι. Recall that in these axioms, uppercase letters P, Q stand for nullary quantifier symbols, which can be defined $P \equiv C(\text{true})$ for fresh quantifier symbol C, i.e., as unary quantifier symbols with constant arguments. In the semantics, we write $I(P)$ for the interpretation $I(C)(I[\![\text{true}]\!])$.

As is commonplace with Łukasiewicz logics, it is sometimes convenient to consider arithmetic operations on truth values, where $\oplus$ is interpreted as 1, $\oplus\!\!\!\!-$ as 0.5, and $\ominus$ as 0. For example, we write $\text{tv}_1 > \text{tv}_2$ if the truth value tv_1 is strictly more true than tv_2.

[$\cdot$] Formula $\langle a \rangle P \leftrightarrow \neg[a]\neg P$ is valid in dL_ι.

Case	Replacement	Admissible when:	
	$\sigma(c) = c$		(20)
	$\sigma(x) = x$		(21)
	$\sigma(\theta_1 + \theta_2) = \sigma(\theta_1) + \sigma(\theta_2)$		(22)
	$\sigma(\theta_1 \cdot \theta_2) = \sigma(\theta_1) \cdot \sigma(\theta_2)$		(23)
	$\sigma(f(\theta)) = \{\cdot \mapsto \sigma(\theta)\}(\sigma f), f \in \sigma$, else $f(\sigma(\theta))$		(24)
	$\sigma(\iota x\ \phi) = \iota x\ \sigma(\phi)$	σ $\{x\}$-adm. in ϕ	(25)
	$\sigma(a) = \sigma a, a \in \sigma$, else a		(26)
	$\sigma(?(\phi)) = ?(\sigma(\phi))$		(27)
	$\sigma(\{x' = \theta \,\&\, \psi\}) = \{x' = \sigma(\theta) \,\&\, \sigma(\psi)\}$	σ $\{x, x'\}$-adm. in θ, ψ	(28)
	$\sigma(p(w)) = \{\cdot \mapsto \sigma(w)\}(\sigma p), p \in \sigma$,else $p(\sigma(w))$		(29)
	$\sigma(\alpha; \beta) = \sigma(\alpha); \sigma(\beta)$	σ BV$(\sigma(\alpha))$-adm. in β	(30)
	$\sigma(\alpha \cup \beta) = \sigma(\alpha) \cup \sigma(\beta)$		(31)
	$\sigma(\alpha^*) = \sigma(\alpha)^*$	σ BV$(\sigma(\alpha))$-adm. in α	(32)
	$\sigma(\theta_1 \geq \theta_2) = \sigma(\theta_1) \geq \sigma(\theta_2)$		(33)
	$\sigma(p(\theta)) = \{\cdot \mapsto \sigma(\theta)\}(\sigma p), p \in \sigma$,else $p(\sigma(\theta))$		(34)
	$\sigma(P) = (\sigma P), P \in \sigma$, else P		(35)
	$\sigma(\neg\phi) = \neg\sigma(\phi)$		(36)
	$\sigma(\phi \wedge \psi) = \sigma(\phi) \wedge \sigma(\psi)$		(37)
	$\sigma(\exists x \phi) = \exists x \sigma(\phi)$	σ $\{x\}$-adm. in ϕ	(38)
	$\sigma(\langle\alpha\rangle\phi) = \langle\sigma(\alpha)\rangle\sigma(\phi)$	σ BV$(\sigma(\alpha))$-adm. in ϕ	(39)
			(40)

Fig. 9. Uniform Substitution Algorithm

Proof. By cases, in each case the LHS and RHS have the same truth value.
Case 1: $\oplus$

$$\begin{aligned}
& I\omega[\![\langle a\rangle P]\!] = \oplus \\
\equiv\ & \text{exists } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I(P)(\nu)=\oplus \\
\equiv\ & \text{exists } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I\nu[\![\neg P]\!] = \ominus \\
\equiv\ & I\omega[\![[a]\neg P]\!] = \ominus \\
\equiv\ & I\omega[\![\neg[a]\neg P]\!] = \oplus
\end{aligned}$$

Case 2: $\ominus$ Symmetric.
Case 3:

$$\begin{aligned}
& I\omega[\![\langle a\rangle P]\!] = \oplus\!\!\!\!\ominus \\
\equiv\ & \text{exists no } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I(P)(\nu)=\oplus \\
& \text{and exists } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I(P)(\nu)=\oplus\!\!\!\!\ominus \\
\equiv\ & \text{exists no } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I\nu[\![\neg P]\!] = \ominus \\
& \text{and exists } \nu \text{ s.t. } (\omega,\nu)\in I(a) \text{ and } I\nu[\![\neg P]\!] = \oplus\!\!\!\!\ominus \\
\equiv\ & I\omega[\![[a]\neg P]\!] = \oplus\!\!\!\!\ominus \\
\equiv\ & I\omega[\![\neg[a]\neg P]\!] = \oplus\!\!\!\!\ominus
\end{aligned}$$

[:=] Formula $([x:=f]p(x)\leftrightarrow p(f))\leftarrow \mathsf{E}(f)$ is valid in dL_ι.

Proof. Assume (1) $I\omega[\![\mathsf{E}(f)]\!] = \oplus$ for some state ω and interpretation I, since the case $I\omega[\![\mathit{denote} f]\!] = \ominus$ makes the implication vacuously true, and $I\omega[\![\mathsf{E}(\theta)]\!]$ never assumes value $\oplus\!\!\!\!\ominus$. Then observe $I\omega[\![[x:=f]p(x)]\!] = I\omega[\![p(f)]\!]$ by the chain of equalities

$$\begin{aligned}
& I\omega[\![[x:=f]p(x)]\!] \\
=& \sqcap_{\nu \mid (\omega,\nu)\in\{(\omega,\omega_x^{I\omega[\![f]\!]})\},I\omega[\![f]\!]\neq\bot} I\omega[\![p(x)]\!] \\
=& I\omega_x^{I\omega[\![f]\!]}[\![p(x)]\!] && \text{[By (1)]} \\
=& I(p)I(f) \\
=& I\omega[\![p(f)]\!]
\end{aligned}$$

[?] $[?Q]P\leftrightarrow(\mathsf{D}(Q)\to P)$
Case 1: $\oplus$

$$\begin{aligned}
& I\omega[\![[?Q]P]\!] = \oplus \\
\equiv\ & I\omega[\![Q]\!] = \oplus \text{ and } I\omega[\![P]\!] = \oplus \text{ or} \\
& I\omega[\![Q]\!] \in \{\oplus\!\!\!\!\ominus, \ominus\} \\
\equiv\ & I\omega[\![\mathsf{D}(Q)]\!] = \oplus \text{ and } I\omega[\![P]\!] = \oplus \text{ or} \\
& I\omega[\![\mathsf{D}(Q)]\!] = \ominus \\
\equiv\ & I\omega[\![\mathsf{D}(Q)\to P]\!] = \oplus
\end{aligned}$$

Case 2: $\ominus$

$$\begin{aligned}
& I\omega[\![[?Q]P]\!] = \ominus \\
\equiv\ & I\omega[\![Q]\!] = \oplus \text{ and } I\omega[\![P]\!] = \ominus \\
\equiv\ & I\omega[\![\mathsf{D}(Q)]\!] = \oplus \text{ and } I\omega[\![P]\!] = \ominus \\
\equiv\ & I\omega[\![\mathsf{D}(Q) \to P]\!] = \ominus
\end{aligned}$$

Case 3: $\oplus\!\!\!\!\ominus$

$$\begin{aligned}
& I\omega[\![[?Q]P]\!] = \ominus \\
\equiv\ & I\omega[\![Q]\!] = \oplus \text{ and } I\omega[\![P]\!] = \oplus\!\!\!\!\ominus \\
\equiv\ & I\omega[\![\mathsf{D}(Q)]\!] = \oplus \text{ and } I\omega[\![P]\!] = \oplus\!\!\!\!\ominus \\
\equiv\ & I\omega[\![\mathsf{D}(Q) \to P]\!] = \oplus\!\!\!\!\ominus
\end{aligned}$$

$[\cup]$ $[a \cup b]P \leftrightarrow [a]P \wedge [b]P$

$$\begin{aligned}
& I\omega[\![[a \cup b]P]\!] \\
\equiv\ & \sqcap_{\nu \mid (\omega,\nu)\in I[\![a \cup b]\!]} I\nu[\![P]\!] \\
\equiv\ & \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!] \text{ or } I[\![b]\!]} I\nu[\![P]\!] \\
\equiv\ & \left(\sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![P]\!]\right) \sqcap \left(\sqcap_{\nu \mid (\omega,\nu)\in I[\![b]\!]} I\nu[\![P]\!]\right) \\
\equiv\ & I\omega[\![[a]P]\!] \sqcap I\omega[\![[b]P]\!] \\
\equiv\ & I\omega[\![[a]P \wedge [b]P]\!]
\end{aligned}$$

$[;]$ $[a;b]P \leftrightarrow [a][b]P$

$$\begin{aligned}
& I\omega[\![[a;b]P]\!] \\
\equiv\ & \sqcap_{\nu \mid (\omega,\nu)\in I[\![a;b]\!]} I\nu[\![P]\!] \\
\equiv\ & \sqcap_{\nu,\mu \mid (\omega,\mu)\in I[\![a]\!],(\mu,\nu)\in I[\![b]\!]} I\nu[\![P]\!] \\
\equiv\ & \sqcap_{\mu \mid (\omega,\mu)\in I[\![a]\!]} \sqcap_{\nu \mid \in I[\![b]\!]} I\nu[\![P]\!] \\
\equiv\ & \sqcap_{\mu \mid (\omega,\mu)\in I[\![a]\!]} I\mu[\![[b]P]\!] \\
\equiv\ & I\omega[\![[a][b]P]\!]
\end{aligned}$$

$[*]$ $[a^*]P \leftrightarrow P \wedge [a][a^*]P$

$$\begin{aligned}
& I\omega[\![[a^*]P]\!] \\
\equiv\ & \sqcap_{\nu \mid (\omega,\nu)\in I[\![a^*]\!]} I\nu[\![P]\!] \\
\equiv\ & \sqcap_{\nu \mid \omega=\nu \text{ or } (\omega,\nu)\in I[\![a]\!]\circ I[\![a^*]\!]} I\nu[\![P]\!] \\
\equiv\ & I\omega[\![P]\!] \sqcap \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]\circ I[\![a^*]\!]} I\nu[\![P]\!] \\
\equiv\ & I\omega[\![P]\!] \sqcap I\omega[\![[\alpha][a^*]P]\!] \\
\equiv\ & I\omega[\![P \wedge [\alpha][a^*]P]\!]
\end{aligned}$$

K $[a]\,(P \to Q) \to ([a]P \to [a]Q)$ Cases on $I\omega[\![[a]\,(P \to Q)]\!]$.
Case $\oplus$: Let $k = \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![P]\!]$. Consider any ν s.t. $(\omega,\nu) \in I[\![a]\!]$,

and let $j = I\nu[\![P]\!]$. By definition of $\sqcap$ have $k \leq j$. Let $n =$. By case, have $j \leq I\nu[\![Q]\!] = n$, so by transitivity $k \leq n$ for all such ν and corresponding n. Then let $m = \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![P]\!]$. Since this held for all possible ν then also have $k \leq m$ yielding $I\omega[\![([a]P \to [a]Q)]\!] = \oplus$ so the axiom has value $\oplus$ in this case.

Case $\oplus\!\!\!\!-$: Let $k = \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![P]\!]$. Consider any ν s.t. $(\omega,\nu) \in I[\![a]\!]$, and let $j = I\nu[\![P]\!]$. By definition of $\sqcap$ have $k \leq j$. Let $n = I\nu[\![Q]\!]$. By case, have $j = I\nu[\![P]\!] \leq \oplus\!\!\!\!- + I\nu[\![Q]\!] = 0.5 + n$ so by transitivity $k \leq 0.5 + n$ for all such ν and corresponding n. Then let $m = \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![P]\!]$. Since this held for all possible ν then also have $k \leq 0.5 + m$ yielding $I\omega[\![([a]P \to [a]Q)]\!] \geq \oplus\!\!\!\!-$. Since $I\omega[\![A \to B]\!] = \oplus$ when $I\omega[\![A]\!] = I\omega[\![B]\!] = \oplus\!\!\!\!-$, the truth value of the axiom is $\oplus$ in this case.

Case $\ominus$: Implication holds vacuously when $I\omega[\![[a](P \to Q)]\!]$.

I $[a^*](\mathsf{D}(P \to [a]P)) \to (\mathsf{D}(P \to [a^*]P))$ Assume (1) $I\omega[\![[a^*](\mathsf{D}(P \to [a]P))]\!] = \oplus$ and (2) $I\omega[\![P]\!] = \oplus$, since the other cases are vacuous. Show $I\omega[\![[a^*]P]\!] = \oplus$, i.e., $\nu[\![P]\!] = \oplus$ for all ν such that $(\omega,\nu) \in I[\![a]\!]^* = I[\![a^n]\!]$ for some $n \in \mathbb{N}$. By induction on the natural number n with induction predicate $P(n)$ defined by "if $(\omega,\nu) \in I[\![a]\!]^* = I[\![a^n]\!]$ then $\nu[\![P]\!] = \oplus$.

Base case: When $n = 0$ then $\nu = \omega$ so $I\nu[\![P]\!] = \oplus$ by assumption (2).

Inductive case: The inductive hypothesis states for $k \in \mathbb{N}$ and state μ such that $(\omega,\mu) \in I[\![a^k]\!]$ and $I\mu[\![P]\!] = \oplus$. Now consider any $\nu \in I[\![a^{k+1}]\!]$: By definition of composition, we have such a μ and additionally (3)$(\mu,\nu) \in I[\![a]\!]$. Then (4) $I\mu[\![P \to [a]P]\!] = \oplus$ from (1) and because $(\omega,\mu) \in I[\![a^*]\!]$. Then from (4) and and (3) and the IH, have $I\nu[\![P]\!] = \oplus$ as desired.

V $p \to [a]p$ Let $t = I\omega[\![p]\!] = I(p) = I\nu[\![p]\!]$ (since p is a nullary predicate, ergo constant) for all ν including ν for which $(\omega,\nu) \in I[\![a]\!]$ so $I\omega[\![[a]p]\!] = \sqcap_{\nu \mid (\omega,\nu)\in I[\![a]\!]} I\nu[\![p]\!] = t$ when there exists ν such that $(\omega,\nu) \in I[\![a]\!]$ or $\oplus$ when no such ν exists. In either case the axiom is true since $t \leq \oplus$ for all truth values t.

$\forall I$ $(\forall x\, p(x)) \wedge \mathsf{E}(f) \to p(f)$ Note we can ignore the $\oplus\!\!\!\!-$ case because $\mathsf{E}(f)$ never takes on value $\oplus\!\!\!\!-$, and case $\ominus$ is vacuous. Assume $I\omega[\![\forall x\, p(x)]\!] = \oplus$ and $I\omega[\![\mathsf{E}(f)]\!] = \oplus$ for all ω, so $I\omega^T_x[\![p(x)]\!] = \oplus$ for all $T \in \mathbb{R} \cup \mathbf{Tree}(\mathbb{R})$ and $I\omega[\![f]\!] \in \mathbb{R} \cup \mathbf{Tree}(\mathbb{R})$ so letting $T = I(f)$ have $\omega^{I(f)}_x[\![p(x)]\!] = \oplus$ i.e., $I\omega[\![p(f)]\!] = \oplus$ so the implication holds and the axiom is valid.

$\forall \to$ $\forall x\ (p(x) \to q(x)) \to (\forall x\, p(x) \to \forall x\, q(x))$

Cases on $I\omega[\![\forall x\ (p(x) \to q(x))]\!]$.

Case $\oplus$: Let $k = \sqcap_{T \in \mathbb{R}\cup\mathbf{Tree}(\mathbb{R})} I\omega^T_x[\![p(x)]\!]$. Consider any $T \in \mathbb{R} \cup \mathbf{Tree}(\mathbb{R})$ and let $j = I\omega^T_x[\![p(x)]\!]$. By definition of $\sqcap$ have $k \leq j$. Let $n = I\omega^T_x[\![q(x)]\!]$. By case, have $I\omega^T_x[\![p(x)]\!] \leq I\omega^T_x[\![q(x)]\!]$ (i.e., $j \leq n$) so by transitivity $k \leq n$ for all such ν, n. Then let $m = \sqcap_{T \in \mathbb{R}\cup\mathbf{Tree}(\mathbb{R})} I\omega^T_x[\![p(x)]\!]$. Since this held for all possible T then also have $k \leq m$ yielding $I\omega[\![\forall x\, p(x) \to \forall x\, q(x)]\!] = \oplus$ so the axiom holds in this case.

Case $\oplus\!\!\!\!-$: Let $k = \sqcap_{T \in \mathbb{R}\cup\mathbf{Tree}(\mathbb{R})} I\omega^T_x[\![p(x)]\!]$. Let $T \in \mathbb{R} \cup \mathbf{Tree}(\mathbb{R})$, and $j = I\omega^T_x[\![p(x)]\!]$. By definition of $\sqcap$ have $k \leq j$. Let $n = I\omega^T_x[\![q(x)]\!]$. By case, have $I\omega^T_x[\![p(x)]\!] \leq \oplus\!\!\!\!- + I\omega^T_x[\![q(x)]\!]$ (i.e., $j \leq 0.5 + n$) so by transitivity $k \leq 0.5 + n$ for all such T, n. Then let $m = \sqcap_{T \in \mathbb{R}\cup\mathbf{Tree}(\mathbb{R})} I\omega^T_x[\![p(x)]\!]$. Since this held for all

possible T then also have $k \leq 0.5+m$ yielding $I\omega[\![(\forall x\, p(x) \to \forall x\, q(x))]\!] \geq \bigoplus$. Since $I\omega[\![A \to B]\!] = \oplus$ when $I\omega[\![A]\!] = I\omega[\![B]\!] = \bigoplus$, the truth value of the axiom is $\oplus$ in this case.

Case $\ominus$: Implication holds vacuously.

$V_\forall$ $p \to \forall x\, p$ Let $k = I\omega[\![p]\!]$. Then since p is constant, $k = I(p) = I\nu[\![p]\!]$ for all ν. Then $\sqcap_{T \in \mathbb{R} \cup \mathbf{Tree}(\mathbb{R})} I\omega_x^T[\![p]\!] = k$ by plugging in each ω_x^T for ν in turn. Then $I\omega[\![\forall x p]\!] = k$ implying $I\omega[\![\forall x\, p \to p]\!] = \oplus$, i.e., the axiom holds in every ω, and so is valid.

ι $p(\iota z\, p(z)) \leftrightarrow \exists x p(x) \wedge (\forall y\ \ p(y) \to y = x)$ Start by observing $I\omega[\![p(\iota z\, p(z))]\!] = I(p)(t)$ where t is the unique $\mathbf{Tree}(\mathbb{R})$ such that $I\omega_z^t[\![p(z)]\!] = \oplus$ This exists iff there exists t such that $I\omega_z^t[\![p(z)]\!] = \oplus$ and such that (0) for all $s \in \mathbf{Tree}(\mathbb{R})$, $I\omega_z^s[\![p(z)]\!] = \oplus$ implies $s = t$. Because (0) is quantified over $t, s \in \mathbf{Tree}(\mathbb{R})$ by the semantics of quantifiers which specifically do not include $s, t = \bot$, then (0) holds exactly when $I\omega[\![\exists x p(x) \wedge \forall y (p(y) \to y = x)]\!] = \oplus$ holds.

=T $(l_1, r_1) = (l_2, r_2) = l_1 = l_2 \wedge r_1 = r_2$ because

$$\begin{aligned}
& I\omega[\![(l_1, r_1) = (l_2, r_2)]\!] \\
= {} & I\omega[\![(l_1, r_1) \leq (l_2, r_2) \wedge (l_2, r_2) \leq (l_1, r_1)]\!] \\
= {} & I\omega[\![(l_1, r_1) \leq (l_2, r_2)]\!] \sqcap I\omega[\![(l_2, r_2) \leq (l_1, r_1)]\!] \\
= {} & \mathsf{Geq}((l_1, l_2), (r_1, r_2)) \sqcap \mathsf{Geq}((r_1, r_2), (l_1, l_2)) \\
= {} & \mathsf{Geq}(l_1, r_1) \sqcap \mathsf{Geq}(l_2, r_2) \sqcap \mathsf{Geq}(r_1, l_1) \sqcap \mathsf{Geq}(r_2, l_2) \\
= {} & I\omega[\![l_1 = r_1 \wedge l_2 = r_2]\!]
\end{aligned}$$

redR $\mathsf{in}\mathbb{R}(r) \to \mathsf{red}(r, s\ f(s), lr\ g(l, r)) = f(r)$ Assume $I\omega[\![\mathsf{in}\mathbb{R}(r)]\!] = \oplus$ so $I(r) \in \mathbb{R}$, else the implication holds vacuously. Then $I\omega[\![\mathsf{red}(r, s\ f(s), lr\ g(l, r))]\!] = \mathsf{Fold}(I(r), s\ f(s), lr\ g(l, r), I\omega) = I\omega_s^{I(r)}[\![f(s)]\!] = I(f)(I(r)) = I\omega[\![f(r)]\!]$.

redT Assume $I\omega[\![\mathsf{isT}(T)]\!] = \oplus$ so exists $L, R \in \mathbf{Tree}(\mathbb{R})$ where $I(T) = (L, R)$. So m

$$\begin{aligned}
& I\omega[\![\mathsf{red}(T, s\ f(s), lr\ g(l, r))]\!] \\
= {} & \mathsf{Fold}((L, R), s\ f(s), lr\ g(l, r), I\omega) \\
= {} & I\omega_{l,r}^{L', R'}[\![g(l, r)]\!]
\end{aligned}$$

where $L', R' = \mathsf{Fold}(L, R, s\ f(s), lr\ g(l, r), I\omega)$ so

$$\begin{aligned}
& I\omega_{l,r}^{L', R'}[\![g(l, r)]\!] \\
= {} & I(g)(\mathsf{Fold}(T, s\ f(s), lr\ g(l, r), I\omega)) \\
= {} & I\omega[\![g(\mathsf{red}(\pi_1 T, s\ f(s), lr\ g(l, r))), \mathsf{red}(\pi_2 T, s\ f(s), lr\ g(l, r))]\!]
\end{aligned}$$

since $I\omega[\![\mathsf{red}(\pi_1 T, s\ f(s), lr\ g(l, r))]\!] = L'$ likewise for R'.

TI $\mathsf{D}(p(\mathsf{Err}) \wedge \forall s(\mathsf{in}\mathbb{R}(s) \to p(s)) \wedge \forall lr(p(l) \wedge p(r) \to p((l, r)))) \to \mathsf{D}(p(t))$. Note the assumption and conclusion are both definite for the same reason that the assumptions and conclusions of axiom I are: The inductive step assumption will typically need to be applied multiple times. Assume (0) $I\omega[\![p(\mathsf{Err}) \wedge$

$\forall s(\mathsf{in}\mathbb{R}(s) \to p(s)) \land \forall lr(p(l) \land p(r) \to p((l,r)))\rrbracket = \oplus$, else the implication holds vacuously. By inversion on (0), have (1a) $I\omega[\![\iota x \text{ false}]\!] = \oplus$ and (2a) $I\omega[\![\forall s(\mathsf{in}\mathbb{R}(s) \to p(s))]\!] = \oplus$ and (3a) $I\omega[\![\forall lr(p(l) \land p(r) \to p((l,r)))]\!] = \oplus$ which simplify respectively to (1b) $I(p)(\bot) = \oplus$ (since there is no value of x that satisfies falsehood in ιx false) and (2b) for all $s \in \mathbb{R}, I(p)(s) = \oplus$ and (3b) for all and $l, r \in \mathbf{Tree}(\mathbb{R})$ have $I(p)(l) = \oplus$ and $I(p)(r) = \oplus$ implies $I(p)((l,r)) = \oplus$. Let $v = I\omega[\![t]\!] = I(v)$ and proceed by induction on the tree structure of v to show $I(p)(v) = \oplus$. The induction is well founded because the set $\mathbf{Tree}(\mathbb{R})$ is defined inductively, ergo v has finite width and depth.
Base case 1, $v = \bot$**:** Using assumption (1b), have $I(p)(v) = I(p)(\bot) = \oplus$ as desired.
Base case 2, $v \in \mathbb{R}$**:** Using assumption (2b), have $I(p)(v) = \oplus$ since $v \in \mathbb{R}$.
Inductive case, $v = (l,r)$ **for some** $l, r \in \mathbf{Tree}(\mathbb{R})$**:** By inductive hypothesis have (4) $I(p)(l) = \oplus$ and (5) $I(p)(r) = \oplus$. By (4) and (5) and because $l, r \in \mathbf{Tree}(\mathbb{R})$ can apply (3b) yielding $I(p)(v) = I(p)((l,r)) = \oplus$. This completes the induction on v yielding $I(p)(v) = \oplus$, so that by definition of v have $\oplus = I(p)(I(t)) = I\omega[\![p(t)]\!]$ as desired.

C.2 Continuous Axioms

$(\theta)'$

$$\begin{aligned}((f(x))' = x' \cdot \big(\iota L \;\; \forall \xi > 0 \; \exists \delta \; \forall y \; (\mathsf{D}(0 < \| (y-x) \| < \delta) \\ \to ((f(y) - f(x)) - L \cdot (y-x)) < \xi \| (y-x) \| \big)))\\ \leftarrow \mathsf{E}((f(x))')\end{aligned}$$

We assume without loss of generality that x and $f(x)$ are both flat, i.e., they may be lists of reals but not arbitrary trees. This loses no generality because we could apply a preprocessing step to reduce across x and $f(x)$ flattening them into lists. In this case, L is a matrix, and is equal to the Jacobian of $f(x)$ at x. Herein we overload norm notation $\|\cdot\|$ to represent also the distances between values $t \in \mathbf{Tree}(\mathbb{R})$ where $\|v_1 - v_2\|$ is the Euclidean distance between v_1 and v_2, or precisely $\|v_1 - v_2\| = \sqrt{f(v_1, v_2)}$ for f defined inductively by $f((l_1, r_1), (l_2, r_2)) = f(l_1, l_2) + f(r_1, r_2)$ or $f(v_1, v_2) = (v_1 - v_2)^2$ for $v_1, v_2 \in \mathbb{R}$ or $f(t_1, t_2) = \bot$ in all other cases. In summary, $\|v_1 - v_2\|$ expects v_1 and v_2 to have the same shape, in which case the distance is equivalent to the Euclidean distance between their vectorial flattenings, else the distance is undefined if the shapes differ. To be formal, for any value v_1 we have that the set $\{v_2 \mid \|v_1 - v_2\| \text{ exists}\}$ forms a real-normed vector space under the Euclidean norm, and thus forms a suitable space for differentiation. We use the notation $\theta_1 \cdot \theta_2$ to denote the matrix product of θ_1 with θ_2, and to minimize confusion we write scalar multiplication as juxtaposition $\theta_1\theta_2$.
We assume (0) $I\omega[\![\mathsf{E}((f(x))')]\!] = \oplus$, else the implication holds trivially. Assumption (0) is essential because equalities in dL_ι only hold over terms that denote. Next we show each side of axiom $(\theta)'$ equals $\frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x')$, then

the axiom follows from transitivity and (0). Starting from the left hand side, we have: $I\omega[\![(f(x))']\!] = \sum_{y\in\mathcal{V}} \frac{\partial I\omega[\![f(y)]\!]}{\partial y} \cdot \omega(y') = \frac{\partial I\omega[\![f(x)]\!]}{\partial x} \cdot \omega(x') = \frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x')$ since $\mathrm{FV}(f(x)) = \{x\}$ and the partial derivative with respect to all $y \neq x$ is zero. Note that in this notation the partial $\frac{\partial I\omega[\![\theta]\!]}{\partial x}$ is the derivative of the function $I\omega^X_x[\![\theta]\!]$ of X at $\omega(x)$.
To prove that the right hand side equals $\frac{\partial I(f)(\omega(x))}{\partial x}\cdot\omega(x')$, the key observation is to understand ω' (i.e. the state containing all $\omega x'$) as a direction vector and recall that the Jacobian multiplied by ω' agrees with the directional derivative $\frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x')$ in direction ω'. that is, $\frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x') = \omega(x') \cdot L$ where $L \in \mathbf{Tree}(\mathbb{R})$ is the Jacobian at x. To complete the proof, we note that L in axiom $(\theta)'$ indeed denotes the Jacobian derivative, because L denotes the unique value such that for all $\xi > 0$ exists δ such that for all $t \in \mathbf{Tree}(\mathbb{R})$ such that $0 < \|t - \omega(x)\| < \delta$ have $I(f)(t) - I(f)(\omega(x)) - (t - \omega(x)) \cdot L < \xi\|t - \omega(x)\|$, which agrees with standard definitions of the Jacobian. We know a unique such value exists by assumption (0).
Because both sides of the equation denote a value and denote the *same* value, the axiom holds.

DW Fix I, ω and show that $I\omega[\![[x' = f(x)\,\&\,q(x)]q(x)]\!] = \oplus$. Suffices to show $\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![q(x)]\!] = \oplus$ and likewise suffices to show for all such ν that $I\nu[\![q(x)]\!] = \oplus$. If no ODE solution should exist then the conjuction $\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]}$ is empty and trivially $\oplus$. Else there exists a solution φ s.t. $\varphi(t) = \nu$ for some $t \in \mathbb{R}^+$ where for all $0 \leq s \leq t$ have $I\varphi(s)[\![q(x)]\!] = \oplus$, so letting $s = t$ have $I\nu[\![q(x)]\!] = \oplus$. Since this was generic in ν we have shown $I\omega[\![[x' = f(x)\,\&\,q(x)]q(x)]\!] = \oplus$. Remark: DW is typically not used directly in an interactive proof, rather it is used to first derive a more friendly, but equivalent, axiom.

DC Fix I, ω and assume (1) $I\omega[\![[x' = f(x)\,\&\,q(x)]r(x)]\!] = \oplus$, since by the semantics of $\mathsf{D}(\cdot)$ and $\to$ there is nothing to show otherwise. Consider any (need not be unique)solution φ of $x' = f(x)\,\&\,q(x)$ with $\omega = \varphi(0)$ on $\{x'\}^C$. Define set $T = \{\varphi(t) \mid \varphi(t)\text{exists and for all } s \in [0,t], I\varphi(s)[\![q(x)]\!] = \oplus\}$, i.e., the set of trajectories of φ. Then decompose assumption (1):

$$\begin{aligned} & I\omega[\![[x' = f(x)\,\&\,q(x)]r(x)]\!] = \oplus \\ \equiv\ & \sqcap_T I\varphi(t)[\![r(x)]\!] = \oplus \\ \equiv\ & I\varphi(t)[\![r(x)]\!] = \oplus \text{ for all } t, \varphi \end{aligned} \tag{41}$$

then show $I\omega[\![[x' = f(x)\,\&\,q(x)]p(x)]\!] = I\omega[\![[x' = f(x)\,\&\,q(x) \wedge r(x)]p(x)]\!]$ First note:

$$\begin{aligned} & I\omega[\![[x' = f(x)\,\&\,q(x)]p(x)]\!] \\ =\ & \sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![p(x)]\!] \\ =\ & \sqcap_T I\nu[\![p(x)]\!] \end{aligned}$$

Recal φ is a solution of the ODE on $t \geq 0$ where for all $0 \leq s \leq t$ have $I\varphi(s)[\![q(x)]\!] = \oplus$. Then by (41) note for each φ and t have $I\varphi(t)[\![q(x) \wedge$

$r(x)]\!] = I\varphi(t)[\![q(x)]\!]$ since $I\varphi(t)[\![r(x)]\!] = \oplus$, then repacking we get

$$\begin{aligned}&\dots\\ =&\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)\wedge r(x)]\!]} I\nu[\![p(x)]\!]\\ =&I\omega[\![[x'=f(x)\,\&\,q(x)\wedge r(x)]p(x)]\!]\end{aligned}$$

DE Fix I, ω and show that

$$\begin{aligned}&I\omega[\![[x'=f(x)\,\&\,q(x)]p(x,x')]\!]\\ =&I\omega[\![[x'=f(x)\,\&\,q(x)][x':=f(x)]p(x,x')]\!]\end{aligned}$$

$$\begin{aligned}&I\omega[\![[x'=f(x)\,\&\,q(x)]p(x,x')]\!]\\ =&\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![p(x,x')]\!]\end{aligned}$$

By def. each such ν is $\varphi(t)$ for $t \in \mathbb{R}^+$, and because φ is a solution of $x' = f(x)\,\&\,q(x)$ at t satisfies $\varphi(t)(x') = I\varphi(t)[\![f(x)]\!]$ and thus $I\nu[\![p(x,x')]\!] = I\nu^{I\nu[\![f(x)]\!]}_{x'}[\![p(x,x')]\!]$ so we continue the equality chain

$$\begin{aligned}&\dots\\ =&\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu^{\nu[\![f(x)]\!]}_{x'}[\![p(x,x')]\!]\\ =&\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![[x':=f(x)]p(x,x')]\!]\\ =&I\omega[\![[x'=f(x)\,\&\,q(x)][x':=f(x)]p(x,x')]\!]\end{aligned}$$

as desired.

$\mathrm{DI}_{\geq}$ We give the main argument here to elucidate the impact of 3-valued dL_ι by showing the case for $\geq$. The remaining cases generalize in the same fashion from their dL proofs [19]. In this proof, the term $\mathsf{shape}(\cdot)$ is given per its definition in App. A. Fix I and ω, assume (1)$I\omega[\![[?q(x)][x'=f(x)\&q(x)]g(x)' \geq h(x)']\!] = \oplus$ show $I\omega[\![[x'=f(x)\&q(x)]g(x) \geq h(x) \leftrightarrow [?q(x)]g(x) \geq h(x)]\!] = \oplus$. By (1), for every solution $\varphi : [0,t] \to \mathbf{Tree}(\mathbb{R})$ (for any $t \geq 0$) have (2) $I\varphi(s)[\![(g(x))' \geq (h(x))']\!] = \oplus$ holds for all $0 \leq s \leq t$. Note this implies (3) $I\varphi(s)[\![g(x)]\!], I\varphi(s)[\![h(x)]\!] \neq \bot$ because the terms $g(x)$ and $h(x)$ denote a value whenever their differentials $(g(x))'$ and $(h(x))'$ do, and (4a) $I\varphi(s)[\![g(x)]\!]$ and $I\varphi(s)[\![h(x)]\!]$ are continuous on $0 \leq s \leq t$ because their differentials exist (4b) forall $t_1, t_2 \in [0,t], I\varphi(t_1)[\![\mathsf{shape}(g(x))]\!] = I\varphi(t_2)[\![\mathsf{shape}(g(x))]\!]$ and $I\varphi(t_1)[\![\mathsf{shape}(h(x))]\!] = I\varphi(t_2)[\![\mathsf{shape}(h(x))]\!]$ as a consequence of existence of the differentials: recall the differentials $(g(x))'$ and $(h(x))'$ exist only when shape is constant in some neighborhood: by taking the uncountable union of such neighborhoods at all $s \in [0,t]$ we get constancy of shape acroos $[0,t]$. We focus first on the case that $I\varphi(s)[\![g(x)]\!], I\varphi(s)[\![h(x)]\!] \in \mathbb{R}$ for all $s \in [0,t]$. From (4b) we conclude $I\varphi(s)[\![g(x) \geq h(x)]\!] \in \{\oplus, \ominus\}$ We show $[x'=f(x)\&q(x)]\, g(x) \geq h(x)$ and $[?q(x)]\, g(x) \geq h(x)$ imply each other.

Case 1: Assume (5) $I\omega[\![[x'=f(x)\&q(x)]g(x) \geq h(x)]\!] = \oplus$ in order to show $I\omega[\![[?q(x)]g(x) \geq h(x)]\!]$. From (5) have for all ν s.t. $(\omega,\nu) \in I[\![x' =$

$f(x)\&q(x)]\!]$ that $I\nu[\![g(x) \geq h(x)]\!]$. Assume (6) $I\omega[\![q(x)]\!] = \oplus$ as there is nothing to show otherwise, and let $\nu = \omega_{x'}^{I\omega[\![f(x)]\!]}$ then $(\omega,\nu) \in I[\![x' = f(x)\&q(x)]\!]$ so by (5) have (6) $I\nu[\![g(x) \geq h(x)]\!] = \oplus$. Then we can apply Lem. 2 because $\omega = \nu$ on $\{x'\}^C \subseteq \mathrm{FV}(g(x) \geq h(x))$, yielding $I\omega[\![g(x) \geq h(x)]\!] = \oplus$ as desired.

Case 2 Assume (5) $I\omega[\![[?q(x)]g(x) \geq h(x)]\!]$ to show $I\omega[\![[x' = f(x)\&q(x)]g(x) \geq h(x)]\!] = \oplus$. If $I\omega[\![q(x)]\!] \neq \oplus$ then trivially $I\omega[\![[x' = f(x)\&q(x)]g(x) \geq h(x)]\!] = \oplus$ because $\{\nu \mid (\omega,\nu) \in I[\![x' = f(x)\&q(x)]\!]\} = \emptyset$. So consider the case where (6) $I\omega[\![q(x)]\!] = \oplus$ and from (5) have (7) $I\omega[\![g(x) \geq h(x)]\!] = \oplus$. Next, case on all the transitions of the ODE. Of these consider first the case that $t = 0$ and let $\nu = \omega_{x'}^{I\omega[\![f(x)]\!]}$. By (6) and coincidence have $I\nu[\![q(x)]\!] = \oplus$ yielding $(\omega,\nu) \in I[\![x' = f(x)\&q(x)]\!]$ which with (7) (again by coincidence) shows the case.

Else assume $t > 0$. We proceed from (1) and (7) to apply the mean value theorem to a function $\mathrm{rel}(s) = I\varphi(s)[\![g(x)]\!] - I\varphi(s)[\![h(x)]\!]$ with domain $[0,t]$. To show $I\varphi(t)[\![g(x) \geq h(x)]\!] = \oplus$ assume for the sake of contradiction that $I\varphi(t)[\![g(x) \geq h(x)]\!] = \ominus$. Then $\mathrm{rel}(t) < 0$ but $\mathrm{rel}(0) \geq 0$ (i.e $\mathrm{rel}(t) < \mathrm{rel}(0)$) then since $t > 0$ by mean value theorem have $\mathrm{rel}'(\zeta) < 0$ at some $\zeta \in [0,t]$. But this contradicts (1) which directly implies $\mathrm{rel}'(s) \geq 0$ for all $s \in [0,t]$.

This generalizes to comparisons of tuples by repeating the mean-value theorem argument for each component.

DG Fix I and ω. Assume (1) $I\omega[\![\mathsf{LLC}(q(x)(x))]\!] = I\omega[\![\mathsf{LLC}(q(x)(x))]\!] = \oplus$ since by the semantics of $\mathsf{D}(\cdot)$ continuity predicates $\mathsf{LLC}(q(x)(x))$ never take on value $\oplus\!\!\!\!-$. Then $I(a)$ and $I(b)$ are Lipschitz continuous at all values $\xi \in \mathbf{Tree}(\mathbb{R})$ such that $I(q)(\xi) = \oplus$. Now consider $I\omega[\![[x' = f(x)\,\&\,q(x)]p(x)]\!] = \sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![p(x)]\!]$. We wish to show that this is equal to $I\omega[\![\exists y{:}\mathbb{R}[z := (x,y)][z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\,\&\,q(\pi_1 z);\ (x,y) := z]p(x)]\!] \equiv \sqcap_{\nu \mid (\omega_y^t,\nu)\in I[\![z:=(x,y);z'=(f(\pi_1 z),a(\pi_1 z)\pi_2 z+b(\pi_1 z))\,\&\,q(\pi_1 z)]\!],\ \text{some } t\in\mathbb{R}} I\omega[\![p(x)]\!]$. The variable z can be understood here as being fresh, since it is not a dependency of any function, predicate, etc. in the original system being ghosted. To prove the equivalence, it suffices to let the sets

$$
\begin{aligned}
L &\equiv \{\nu \mid (\omega,\nu) \in I[\![x' = f(x)\&q(x)\,\&\,p(x)]\!]\}\\
R &\equiv \{\nu \mid (\omega_y^t,\nu) \in I[\![z := (x,y);\\
&\quad z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\&q(\pi_1 z); (x,y) := z]\!],\ \text{some } t \in \mathbb{R}\}
\end{aligned}
$$

And show $L = R$ by two inclusions: $R \subseteq L$ and $L \subseteq R$.

Case $R \subseteq L$: Let $(\omega_y^r,\nu) \in I[\![z := (x,y); z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\&q(\pi_1 z)]\!]$ for some $r \in \mathbb{R}$. Let $\mu = \omega_{y,z}^{r,(\omega(x),r)}$ for short. Now consider any solution φ to $x' = f(x)\&q(x)$ where $\mu = \varphi(0)$ on $\{x'\}^C$. We will augment φ to a solution $\tilde{\varphi}$ of $z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))$ of the same duration. We construct $\tilde{\varphi}$ as follows: let $y : \mathsf{EI} \to \mathbb{R}$, where EI is the existence interval of ODE $x' = f(x)$, be the unique solution of the initial-value

problem:

$$y(0) = r$$
$$y'(t) = F(t, y(t)) = y(t)(I\varphi(t)[\![a(x)]\!]) + I\varphi(t)[\![b(x)]\!]$$

By Picard-Lindelöf this exists: by inversion on assumption (1) and because the definition of $\mathsf{LLC}(\phi(x))$ coincides with local Lipschitz-continuity of θ with respect to x within ϕ, then interpretations of $a(x)$ and $b(x)$ are locally Lipschitz-continuous in x. Because φ is a solution of an ODE φ is differentiable and thus locally Lipschitz-continuous. Then F is a composition of continuous functions under operators so the solution $y(t)$ exists uniquely, because also F satisfies the Lipschitz condition:

$$\|F(t,y) - F(t,z)\| = \|(y-z)I\varphi(t)[\![a(x)]\!]\| \leq \|y-z\| \max_{s\in[0,t]} I\varphi(t)[\![a(x)]\!]$$

where the maximum exists because $[0,t]$ is compact and by assumption (1) $a(x)$ is continuous on $\{\nu \mid I\nu[\![q(x)]\!] = \oplus\} \supseteq [0,t]$. We can now define the modification $\tilde{\varphi}$ as such: It agrees with μ on $\{z,z'\}^C$, agrees with φ in the sense that $\varphi(t)(x) = \pi_1\tilde{\varphi}(t)(z)$, then the new component $\pi_2 z$ is defined by $\pi_2\tilde{\varphi}(0)(z) = r$ and $\pi_2\tilde{\varphi}(t)(z') = F(t,y(t))$ for the solution $y(t)$. In particular the right component of $\tilde{\varphi}(t)(z')$ agrees with the time-derivative $y'(t)$ of the value $\pi_2\tilde{\varphi}(t)(z) = y(t)$ of y along $\tilde{\varphi}$. By construction $\pi_2\tilde{\varphi}(y) = r$ and $I, \tilde{\varphi} \models z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z)) \wedge q(x)$ because $\pi_2(z') = a(\pi_1 z)\pi_2 z + b(\pi_1 z)$ holds by construction of y and $\pi_1(z)$ agrees with $\varphi(t)(x)$ so that $I\varphi(s)[\![f(x)]\!] = I\tilde{\varphi}(s)^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}_x[\![f(x)]\!]$ by coincidence, then $I\tilde{\varphi}(s)^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}_x[\![f(x)]\!] = I\tilde{\varphi}(s)[\![f(\pi_1 z)]\!]$ and likewise $I\tilde{\varphi}(s)[\![q(\pi_1 z)]\!] = I\tilde{\varphi}(s)^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}_x[\![q(x)]\!] = I\varphi(s)[\![q(x)]\!]$ by coincidence again

$$\begin{aligned}&\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![p(x)]\!]\\ =&\sqcap_{\nu \mid (\omega_y^t,\nu) I[\![z:=(x,y);z'=(f(\pi_1 z),a(\pi_1 z)\pi_2 z+b(\pi_1 z))\&q(\pi_1 z)]\!], \text{ some } t\in\mathbb{R}} I\nu[\![p(x)]\!]\end{aligned}$$

so the inclusion $R \subseteq L$ holds.

Case $L \subseteq R$: We show a more general result in this direction: this direction of DG holds even if the term $a(\pi_1 z)\pi_2 z + b(\pi_1 z)$ for the ghost dimension is replaced with any term η, value r assigned to $\pi_2 z$. This is the case, for example, even if η, is not Lipschitz-continuous, not real-valued, or even partial, since these conditions can only restrict the duration of a trajectory. Show $\nu \in \{\nu \mid (\omega_y^r, \nu) \in I[\![z := (x,y); z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\&q(\pi_1 z); (x,y) :=]\!], r \in \mathbb{R}\}$ Consider any term η, any $r \in \mathbf{Tree}(\mathbb{R})$ and any φ of some duration t where $I, \varphi \models z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z)) \wedge q(\pi_1 z)$ with $\varphi(0) = \mu$ on $\{z'\}^C$. Consider the restriction $\varphi_{|L}$ where $\varphi_{|L}(x) = \pi_1\varphi(z)$ and $\varphi_{|L}(w) = \omega(w)$ for all other base variables w. By coincidence lemma $I, \varphi_{|L} \models x' = f(x) \wedge q(x)$ because $\varphi_{|L}(x)$ is defined to match $\varphi(z)$ and $\mathrm{FV}(f(x)) = \{x\}$. This ends the case. Then because the sets L and R are identical on all variables except $\{y, y', z, z'\}$ then by formula coincidence $I\nu[\![p(x)]\!]$ agrees between them, completing the proof.

DS Fix I and ω. Assume without loss of generality (1) $I(f) \neq \bot$, otherwise $I[\![x' = f \,\&\, q(x)]\!]$ is empty as $I[\![f]\!] = \bot$ throughout, implication is vacuous. Then show $I\omega[\![[x' = f \,\&\, q(x)]p(x)]\!] = I\omega[\![\forall t : \mathbb{R}\ ((\forall 0 \leq s \leq t\ q(x{+}fs)) \rightarrow [x := x + ft]p(x))]\!]$ The key of the proof is to observe first that (2) φ as defined by $\varphi(s)(x) = I\omega^s_t[\![x + ft]\!]$ solves $x' = f$ on $[0, \infty)$ and that because f is trivially Lipschitz, this solution is unique. In the following, let the domain D be defined by $D = \{t \mid \text{for all } s \in [0, t], \varphi(s)[\![q(x)]\!] = \oplus\}$. This is interchangeable with $\{t \mid \text{for all } s \in [0, t], \varphi(s)[\![q(x + fs)]\!] = \oplus\}$ by construction of φ. Then

$$
\begin{aligned}
& I\omega[\![[x' = f \,\&\, q(x)]p(x)]\!] \\
= \ & \sqcap_{\nu \mid (\omega,\nu) \in I[\![x' = f \,\&\, q(x)]\!]}\, I\nu[\![p(x)]\!] \\
= \ & \sqcap_D\, I\varphi(t)[\![p(x)]\!] \\
= \ & \sqcap_D\, I(p)(\varphi(t)(x)) \\
= \ & \sqcap_D\, I(p)(I\omega^{\varphi(t)(x)}_x[\![x + ft]\!]) \\
= \ & \sqcap_D\, I(p)(I\omega^{\varphi(t)(x)}_x[\![x + ft]\!]) \\
= \ & \sqcap_D\, (I\omega^{I\omega[\![x+ft]\!]}_x[\![p(x + ft)]\!]) \\
= \ & \sqcap_D\, (I\omega[\![[x := x + ft]p(x + ft)]\!]) \\
= \ & \sqcap_D\, (I\omega[\![[x := x + ft]p(x + ft)]\!]) \\
= \ & \sqcap_{r:\mathbb{R} \mid I\omega^r_t[\![(\forall 0 \leq s \leq t\ q(x+fs))]\!]}\, I\omega^r_t[\![[x := x + ft]p(x + ft)]\!] \\
= \ & I\omega[\![\forall t : \mathbb{R}\ (\forall 0 \leq s \leq t\ q(x + fs)) \rightarrow [x := x + ft]p(x + ft)]\!]
\end{aligned}
$$

C.3 Derived Axioms Sound

We derive the axiom schemata of Ex. 2 from the core axioms. In proving the axiom schemata for differential terms, we will exploit the following proposition:

Proposition 2 (Uniqueness of differentials). *Define the abbreviation:*

$$
\begin{aligned}
P(\theta) \equiv\ \forall \varepsilon > 0\ \exists \delta\, \forall y\ \big(0 < |y - x| < \delta \rightarrow \\
(f(y) - f(x)) - \theta \cdot (y - x) < \epsilon \cdot |y - x|\big)
\end{aligned}
$$

Then the formula $P(M) \rightarrow M = \iota M\ P(M)$ is provable.

Proof. Apply ι. The first premise holds by assumption. The second premise is the uniqueness of derivatives, whose truth is common knowledge since derivatives can be defined as limits. Since it is true and is a formula of first-order arithmetic, it is provable by QE.

Note also in general that the differential term axiom schemata $(+)'$ and $(\cdot)'$ expect univariate functions: this is no restriction in practice because because the one argument is not restricted to reals. These axioms are needed only when simplifying the right-hand side of an ODE, and all multidimensional ODE's are already implemented as single ODEs over a tuple. Implicitly, the functions in

$(+)'$ and $(\cdot)'$ do *return* a single real as the builtin operators $+$ and $\cdot$ are defined only on reals. If we wished, we could generalize these axioms to vectorial sums and products, since the core $(\theta)'$ axiom holds even for tree-valued differentials of tree-valued arguments. These generalizations are unlikely to be needed in practice, however: condition provable with them is provable also without them.

- (π_1) $\mathsf{E}((l,r)) \to \pi_1(l,r) = l$ By ι with $p(x) \equiv x = l$. Then $(l,r) = (l,r)$ by $=$T and reflexivity. Forall branch proves by transitivity.
- (π_2) $\pi_2(l,r) = r$ By ι with $p(x) \equiv x = r$. Then $(l,r) = (l,r)$ by $=$T and reflexivity. Forall branch proves by transitivity.
- (tC) $\mathsf{E}(f) \to \mathsf{in}\mathbb{R}(f) \vee \mathsf{isT}(f)$ Apply TI with invariant $J(\theta) \equiv \neg\mathsf{E}(\theta) \vee \mathsf{in}\mathbb{R}(\theta) \vee \mathsf{isT}(f)$ By propositional rewriting is equivalent to tC, suffices to prove J. By TI reduces to three cases:
  - $J(\mathsf{Err})$, STS $\neg\mathsf{E}(\iota x\ \bot)$. By ι and since the RHS is false everywhere, it doesn't denote and is not equal to itself..
  - By disjunction introduction.
  - By redT.
- $((f)')$ $\mathsf{E}(f) \to (f)' = 0$ By Prop. 2 differentials are unique and by axiom $(\theta)'$ the constant 0 is a differential if

$$\forall \xi > 0\ \exists\ \delta \forall y\ \ (0 < \|y - x\| < \delta \to (f - f) - (y - x) \cdot 0 < \xi \|y - x\|) \quad (42)$$

  so it suffices to prove validity Eq. 42. By QE and CQ, reduces to $\xi > 0 \wedge 0 < \|y - x\| < \delta \to 0 < \xi\|y - x\|$ which proves by QE. CQ applies by the assumption that $\mathsf{E}(f)$. Then applying $(\theta)'$, have $\mathsf{E}(f) \to (f)' = x' \cdot 0$, and by QE and CQ again, $\mathsf{E}(f) \to (f)' = 0$.
- $((x)')$ $(x)' = x'$: By Prop. 2, suffices to prove the validity of the formula $\forall \xi > 0\ \exists\ \delta \forall y\ \ (0 < \|y - x\| < \delta \to (y - x) - (y - x) \cdot 1 < \xi\|y - x\|)$. By QE and CQ, reduces to $\xi > 0 \wedge 0 < \|y - x\| < \delta \to 0 < \xi\|y - x\|$ which proves by QE. Then applying $(\theta)'$, have $(x)' = x' \cdot 1$, and by QE and CQ again, $(x)' = x'$.
- $((+)')$ $\mathsf{E}((f(x))') \wedge \mathsf{E}((g(x))') \to (f(x)+g(x))' = (f(x))' + (g(x))'$ We unpack the differentials $(f(x))'$ and $(g(x))'$, which exist by assumption, introducing new variables M_1 and M_2 which uniquely satisfy

$$\begin{aligned}\forall \xi > 0\ \exists\ \delta \forall y\ \big(&0 < \|y - x\| < \delta \to \\ &(f(y) - f(x)) - (y - x) \cdot M_1 < \xi\|y - x\|\big)\end{aligned} \quad (1)$$

  and

$$\begin{aligned}\forall \xi > 0\ \exists\ \delta \forall y\ \big(&0 < \|y - x\| < \delta \to \\ &(g(y) - g(x)) - (y - x) \cdot M_2 < \xi\|y - x\|\big)\end{aligned} \quad (2)$$

  this allows to prove that $M_1 + M_2$ satisifies

$$\begin{aligned}\forall \xi > 0\ \exists\ \delta \forall y\ \big(&0 < \|y - x\| < \delta \to \\ &((f(y) + g(y)) - (f(x) + g(x)) - (y - x) \cdot (M_1 + M_2)) < \xi\|y - x\|\big)\end{aligned} \quad (0)$$

which will suffice to show the axiom by Prop. 2, since any differential is the unique differential.

Begin the proof of (0) by applying $\forall$ to (0), fixing $\xi > 0$. Apply $\forall I$ to (1) and (2) with $\xi_1 = \xi_2 = \frac{\xi}{2}$, then apply $\forall$, fixing δ_1, δ_2. Apply (the dual of) $\forall I$ to (0) with $\delta = \min(\delta_1, \delta_2)$, then apply $\forall$, fixing y s.t. (3)$0 < \|y - x\| < \delta$. By QE and (3) have (4a) $0 < |y-x| < \delta_1$ and (4b) $0 < |y-x| < \delta_2$. Apply MP to (1) and (2) with (4a) and (4b) finally yielding (5a) $(f(y)-f(x))-(y-x)\cdot M_1 < \xi\|y-x\|$ and (5b) $(g(y)-g(x))-(y-x)\cdot M_2 < \xi\|y-x\|$. By QE have (6) $((f(y)+g(y))-(f(x)+g(x))-(y-x)\cdot(M_1+M_2)) < \xi\|y-x\|$ since

$$\begin{aligned}&\|(f+g)(y)-(f+g)(x)-(y-x)\cdot(M_1+M_2)\|\\ \leq&\|f(y)-f(x)-(y-x)\cdot M_1\| + \|g(y)-g(x)\| - (y-x)\cdot M_2\\ \leq&2\varepsilon\|y-x\|\end{aligned}$$

proving (0).

– $((\cdot)')$ $\mathsf{E}((f(x))') \wedge \mathsf{E}((g(x))') \rightarrow (f(x)\cdot g(x))' = (g(x))'\cdot f(x) + (g(x))'\cdot f(x)$
For the sake of simplicity, we focus on the case where x is real-valued. Rather than a direct $\epsilon\delta$ proof, a proof by limits is simpler for axiom $(\cdot)'$. Fortunately, limits are definable in dL_ι:

$$\lim_{y\to x} f(y) \equiv \iota L\ \forall \xi > 0\ \exists\delta\forall y\ \ (0 < \|y-x\| < \delta \rightarrow \|f(y) - L\| < \xi)$$

Because the sum and product rules for limits are standard, we assume them here without proof:

Lemma 4 (Sums of limits). *Formula* $\mathsf{E}(\lim_{y\to x} f(x)) \wedge \mathsf{E}(\lim_{y\to x} g(x)) \rightarrow \lim_{y\to x}(f(x)+g(x)) = \lim_{y\to x} f(x) + \lim_{y\to x} g(x)$ *is valid.*

Lemma 5 (Products of limits). *Formula* $\mathsf{E}(\lim_{y\to x} f(x)) \wedge \mathsf{E}(\lim_{y\to x} g(x)) \rightarrow \lim_{y\to x}(f(x)\cdot g(x)) = \lim_{y\to x} f(x)\cdot\lim_{y\to x} g(x)$ *is valid.*

Lemma 6. *Formula* $\mathsf{E}((f(x))') \rightarrow \lim_{y\to x} f(y) = f(x)$ *is valid.*

We also note that our definition of differential is equivalent to the limit definition of differential:

Lemma 7 (Differential as limit). *Formula* $(f(x))' = x'\cdot\lim_{y\to x}\frac{f(y)-f(x)}{y-x}$ *is valid when* x *and* y *are reals.*

Then we prove $(\cdot)'$ as a chain of equalities. Each equality step assumes at least one side of the equality exists. It is easiest to show this is the case by working backwards from the final step: because axiom $(\cdot)'$ assumes $(f(x))'$ and $(g(x))'$ exist, then $(f(x))'\cdot g(x) + (g(x))'\cdot f(x)$ because $f(x)$ exists any

time $(f(x))'$ does and because addition and multiplication preserve existence.

$$
\begin{aligned}
&(f(x)\cdot g(x))'\\
=&x'\cdot\lim_{y\to x}\frac{f(y)\cdot g(y)-f(x)\cdot g(x)}{y-x} && \text{[Lem. 7]}\\
=&x'\cdot\lim_{y\to x}\frac{f(y)\cdot g(y)-f(x)\cdot g(y)+f(x)\cdot g(y)-f(x)\cdot g(x)}{y-x} && \text{[QE]}\\
=&x'\cdot\lim_{y\to x}\frac{(f(y)-f(x))\cdot g(y)+f(x)\,(g(y)-g(x))}{y-x} && \text{[QE]}\\
=&x'\cdot\lim_{y\to x}\frac{(f(y)-f(x))\cdot g(y)}{y-x}+x'\cdot\lim_{y\to x}\frac{f(x)\cdot(g(y)-g(x))}{y-x} && \text{[Lem. 4]}\\
=&x'\cdot\lim_{y\to x}\frac{(f(y)-f(x))}{y-x}\cdot\lim_{y\to x}g(y)+x'\cdot\lim_{y\to x}\frac{(g(y)-g(x))}{y-x}\cdot\lim_{y\to x}f(x) && \text{[Lem. 4]}\\
=&(f(x))'\cdot\lim_{y\to x}g(y)+(g(x))'\cdot\lim_{y\to x}f(x) && \text{[Lem. 7]}\\
=&(f(x))'\cdot g(x)+(g(x))'\cdot f(x) && \text{[Lem. 6]}
\end{aligned}
$$

C.4 Rules

Non-substitution rules

G $\dfrac{P}{[a]P}$ Assume $I\nu[\![P]\!]=\oplus$ for all ν (validity). Let ω arbitrary. Then $I\mu[\![P]\!]=\oplus$ also for all $\mu \mid (\omega,\mu)\in I[\![a]\!]$ so $I\omega[\![[a]P]\!]=\oplus$ regardless of ω, so $[a]P$ is valid, and thus the rule is sound.

∀ $\dfrac{p(x}{\forall x p(x)}$ Assume $I\nu[\![p(x)]\!]{=}p\oplus$, all ν. Fix ω, then $I\omega[\![\forall x p(x)]\!]{=}\sqcap_{t\in\mathbf{Tree}(\mathbb{R})} I\omega^t_x[\![p(x)]\!]$. By the assumption, $\sqcap_{t\in\mathbf{Tree}(\mathbb{R})}I\omega^t_x[\![p(x)]\!]=\sqcap_{t\in\mathbf{Tree}(\mathbb{R})}\oplus=\oplus$, so the conclusion is valid, and the rule is sound.

MP $\dfrac{P\to Q\quad P}{Q}$ Assume $I\nu[\![P]\!]=\oplus$ and $I\nu[\![P\to Q]\!]=\oplus$ for all ν so also $I\nu[\![P]\!]\le I\nu[\![Q]\!]$. Fix ω. By assumptions $\oplus=I\omega[\![P]\!]\le I\omega[\![Q]\!]$, i.e., $I\omega[\![Q]\!]=\oplus$ for all ω so the conclusion is valid, and the rule is sound.

CQ $\dfrac{f(x)=g(x)\quad \mathsf{E}(\mathrm{h}(f(x)))\wedge\mathsf{E}(\mathrm{h}(g(x)))}{\mathrm{h}(f(x))=\mathrm{h}(g(x))}$ (For $I\omega[\![f(x)]\!],I\omega[\![g(x)]\!]\in\mathbf{Tree}(\mathbb{R})\cup\bot$) Assume $I\omega[\![f(x)=g(x)]\!]=\oplus$, by inversion $I\omega[\![f(x)]\!]=I\omega[\![g(x)]\!]\in\mathbf{Tree}(\mathbb{R})$ (since $f(x)=g(x)$ takes value $\bigoplus$ if either side is $\bot$). By second premiss, assume also have $I\omega[\![\mathsf{E}(\mathrm{h}(f(x)))\wedge\mathsf{E}(\mathrm{h}(g(x)))]\!]=\oplus$. By inversion, $I\omega[\![\mathrm{h}(f(x))]\!],I\omega[\![\mathrm{h}(g(x))]\!]\in\mathbf{Tree}(\mathbb{R})$ then $I\omega[\![\mathrm{h}(f(x))]\!]=I(\mathrm{h})(I(f)(\omega(x)))=I(\mathrm{h})(I(g)(\omega(x)))=I\omega[\![\mathrm{h}(g(x))]\!]$, so $I\omega[\![\mathrm{h}(f(x))=\mathrm{h}(g(x))]\!]=\oplus$, so the conclusion is valid, so the rule is sound.

CE $\dfrac{P\leftrightarrow Q}{C(P)\leftrightarrow C(Q)}$ Assume $P\leftrightarrow Q$ is valid, i.e., $I[\![P\leftrightarrow Q]\!]=\oplus$. Then by inversion $I[\![P]\!]=I[\![Q]\!]$. Then $I\omega[\![C(P)]\!]=I(C)(I[\![P]\!])=I(C)(I[\![Q]\!])=I\omega[\![C(Q)]\!]$. Then the conclusion is valid, and the rule sound.

C.5 Equiexpressivity Proof

Theorem 5 (Reducible).
There exists a computable function T such that for all dL_ι formulas ϕ, the dL formula $T(\phi)$ is valid in dL iff ϕ is in dL_ι.

Proof. We take an indirect reduction $\mathsf{dL}_\iota \to \mathsf{dL}_1 \to \mathsf{dL}_C \to \mathsf{dL}$, where dL_1 is dL_ι without tuples, dL_C is dL with all rigid symbols limited to interpretations as continuous functions, and dL is dL without such symbols.

Eliminate Tuples By analogy to the dL-definable bijection between $\mathbb{R}$ and $\mathbb{R}^k$ for any k [20, Lem. A.1], there is a dL-definable bijection between finite trees of reals and reals. First, observe a real nomber in dL can be considered as an infinite string of bits by taking the fractional and interval parts in base 2, each an infinite string of bits, and interleaving them. The first tag of each typed value is a tag bit: 0 for a real number, in which case the following bits are the bits of the real number, or else 1 to indicate a pair, in which case the following bits are alternating bits of each component. Given a tree, one can easily write a hybrid program for post-order traversal, from which $\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$ is easily implemented. The exception is systems of ODE's, but systems of ODE's are allowed in dL anyway.

Eliminate Definite Descriptions The challenging case is when definite descriptions occur on the right-hand-side of an ODE. In every other context, a definite description $\iota z\ \phi$ by introducing a fresh variable x and an assumption $[z := x]\phi \wedge \forall y\,([z := y]\phi \to y = x)$. Because the meaning of ϕ and likewise $\iota x\ \phi$ typically depends on variables other than x as well, it is essential that a distinct fresh variable is introduced for *each* occurrence of even syntactically identical definite descriptions, and that the assumption $p(x) \wedge \forall y\,([x := y]\phi \to y = x)$ is made in the *same* context as the definite description term appears. For example: $[y := 3](\iota z\ z + y = 0) < 0$ expands to $[y := 3](([z := x]z + y = 0) \wedge \forall y\,(([z := y]z + y = 0) \to y = x) \to z < 0)$ which are both true.

This translation doesn't quite work in the differential equation case because the bound variables of the ODE are bound *continuously*, thus the value of the variable x encoding the definite description would have to change continuously to keep up. The only mechanism offered by dL for modifying x continuously is to add additional dimensions to the ODE, which are not general enough to express all possible definite descriptions, e.g. those that are not differentiable and thus could not themselves be the solution of a differential equation.[2]

The differential equation case is addressed by axiomatizing the ODE system using a continuous function symbol. The main sticking point is that the ODEs of dL are polynomial ODEs with guaranteed unique solution, whereas ODEs of dL_ι are not. It thus does not suffice to reduce to FOD (first-order logic with

[2] If our target language featured differential games, for example, we could introduce a new continuously changing x, but alas it does not.

differential equations) of prior work [17]. Rather we reduce to dL with function symbols whose interpretations are restricted to continuous functions. Specifically, we build on prior work that shows an embedding of the dL reachability modality $\langle\alpha\rangle\phi$ can be embedded in FOD [14, Lem. 5]. Instead, we embed from dL_1 into dL_C by redefining the translation for systems of ODEs:

$$\langle x' = f(x)\,\&\,q(x)\rangle p(x) \leftrightarrow x = \mathsf{sol}(0) \land \forall t(\forall 0{\leq}s{\leq}t(q(\mathsf{sol}(s)) \land \mathsf{sol}' = \theta \to p(x)))$$

Where sol is a fresh continuous function symbol. If we wished to semantically impose the constraint that the interpretation of the function symbol sol is not only continuous but also differentiable, then this step would be done. However, this is an unnecessary restriction, as we can axiomatize sol' as a new function symbol (call it d) with the following assumptions, which we arrive at by combining the reduction for discrete definite descriptions, axiom $(\theta)'$, and Prop. 2:

$$\forall s\,\forall \xi{>}0\ \exists \delta\ \forall y\ \ (0{<}\|\,(y{-}x)\,\|{<}\delta \to (\mathsf{sol}(y){-}\mathsf{sol}(x)){-}d(s)\cdot(y{-}x){<}\xi\|\,(y{-}x)\,\|)$$

Eliminate Continuous Function Symbols To eliminate continuous function symbols, we reuse the reduction from previous work [20, Corr. A.4]: a bijection between reals $\mathbb{R}$ and continuous functions on the reals $C(\mathbb{R},\mathbb{R})$ has previously been established, reducing dL_C to dL. The reduction exploits the fact that continuous functions $C(\mathbb{R},\mathbb{R})$ can be uniquely characterized by their values on rational-valued inputs.

C.6 Conservativity Proof

Theorem 6. *There exists a reduction $T(\phi)$ (or α, or θ) that reduces dL to dL_ι in linear time and space. For all states ω, interpretations I, terms θ, formulas ϕ, programs α of dL:*

- $I\omega[\![T(\theta)]\!] = I\omega[\![\theta]\!]_{\mathsf{dL}}$
- $I\omega[\![T(\phi)]\!] = I\omega[\![\phi]\!]_{\mathsf{dL}}$ *where* $I\omega[\![\phi]\!]_{\mathsf{dL}} = \oplus$ *if* $\omega \in I[\![\phi]\!]_{\mathsf{dL}}$ *or* $I\omega[\![\phi]\!]_{\mathsf{dL}} = \ominus$ *if* $\omega \notin I[\![\phi]\!]_{\mathsf{dL}}$.
- $I[\![T(\alpha)]\!] = I[\![\alpha]\!]_{\mathsf{dL}}$

where $I\omega[\![\cdot]\!]_{\mathsf{dL}}$ is the dL semantics.

First define a suitable reduction T. The only sense in which dL_ι is not conservative vs. dL is that quantifiers and variables range over trees of reals in dL_ι while they range only over reals in dL. The key case is:

$$T(\forall x\,\phi) = (\forall x\,(\mathsf{in}\mathbb{R}(x) \to S(\phi)))$$

while all other cases map through homomorphically.

Proof of conservation of semantics:

1. $I\omega[\![T(q)]\!] = I\omega[\![q]\!] = q = I\omega[\![q]\!]_{\mathsf{dL}}$ for literal $q \in \mathbb{Q}$.

2. $I\omega[\![T(x)]\!] = I\omega[\![x]\!] = \omega(x) \in \mathbb{R}$ since we assumed ω was a dL state. Then $\omega(x) = I\omega[\![x]\!]_{\mathsf{dL}}$ since $\mathbb{R} \subseteq \mathbf{Tree}(\mathbb{R})$.
3. $I\omega[\![T(\theta_1{+}\theta_2)]\!] = I\omega[\![T(\theta_1)]\!]{+}I\omega[\![T(\theta_2)]\!] =_{\text{IH}} I\omega[\![\theta_1]\!]_{\mathsf{dL}}{+}I\omega[\![\theta_2]\!]_{\mathsf{dL}} = I\omega[\![\theta_1+\theta_2]\!]_{\mathsf{dL}}$.
4. $I\omega[\![T(\theta_1{\cdot}\theta_2)]\!] = I\omega[\![T(\theta_1)]\!]{\cdot}I\omega[\![T(\theta_2)]\!] =_{\text{IH}} I\omega[\![\theta_1]\!]_{\mathsf{dL}}{\cdot}I\omega[\![\theta_2]\!]_{\mathsf{dL}} = I\omega[\![\theta_1\cdot\theta_2]\!]_{\mathsf{dL}}$.
5. $I\omega[\![T((\theta)')]\!] = \sum_{x\in\mathcal{V}} \omega(x')\frac{\partial I\omega[\![T(\theta)]\!]}{\partial x} = \sum_{x\in\mathcal{V}} \omega(x')\frac{\partial I\omega[\![\theta]\!]_{\mathsf{dL}}}{\partial x} = I\omega[\![(\theta)']\!]_{\mathsf{dL}}$.

Let ϕ be a formula of dL. Let ω be a dL state (for all variables x, $\omega(x) \in \mathbb{R}$). Then $I\omega[\![T(\phi)]\!]_{\mathsf{dL}} = \oplus$ if $I\omega[\![\phi]\!] = \oplus$ and $I\omega[\![T(\phi)]\!]_{\mathsf{dL}} = \ominus$ if $I\omega[\![\phi]\!] = \ominus$.

1. $I\omega[\![T(\theta_1 \geq \theta_2)]\!] = (I\omega[\![T(\theta_1)]\!] \geq I\omega[\![T(\theta_2)]\!]) = (I\omega[\![\theta_1]\!]_{\mathsf{dL}} \geq I\omega[\![\theta_2]\!]_{\mathsf{dL}}) = I\omega[\![\theta_1 \geq \theta_2]\!]_{\mathsf{dL}}$.
2. $I\omega[\![T(\phi \wedge \psi)]\!] = I\omega[\![T(\phi)]\!] \sqcap I\omega[\![T(\psi)]\!] = I\omega[\![\phi]\!]_{\mathsf{dL}} \sqcap I\omega[\![\psi]\!]_{\mathsf{dL}} = I\omega[\![\phi \wedge \psi]\!]_{\mathsf{dL}}$.
3. $I\omega[\![T(\neg\phi)]\!] = \overline{I\omega[\![T(\phi)]\!]} = \overline{I\omega[\![\phi]\!]_{\mathsf{dL}}} = I\omega[\![\neg\phi]\!]_{\mathsf{dL}}$.
4. $I\omega[\![T(\forall x\, \phi)]\!]$. Because the domain of quantification differs between dL and dL_ι, this case of the reduction T enforce that x varies only over reals: $I\omega[\![T(\forall x\, \phi)]\!] = I\omega[\![\forall x\, (\mathsf{in}\mathbb{R}(x) \to T(\phi))]\!] = \sqcap_{t\in\mathbf{Tree}(\mathbb{R})} I\omega^t_x[\![\mathsf{in}\mathbb{R}(x) \to T(\phi)]\!] = \sqcap_{r\in\mathbb{R}} I\omega^r_x[\![T(\phi)]\!] = \sqcap_{r\in\mathbb{R}} I\omega^r_x[\![\phi]\!]_{\mathsf{dL}} = I\omega[\![\forall x\, \phi]\!]_{\mathsf{dL}}$
5. $I\omega[\![[\alpha]\phi]\!] = \bigsqcap_{(\omega,\nu)\in I[\![\alpha]\!]} I\nu[\![\phi]\!] = \bigsqcap_{(\omega,\nu)\in I[\![\alpha]\!]_{\mathsf{dL}}} I\nu[\![\phi]\!]_{\mathsf{dL}} = I\omega[\![[\alpha]\phi]\!]_{\mathsf{dL}}$. Note the IH is applicable here because whenever $(\omega,\nu) \in I[\![\alpha]\!]$ for dL program α and dL state ω then ν is also a dL state. This can be proven by another induction on the program α.

Programs:

1. $I[\![T(x := \theta)]\!] = \{(\omega, \omega^r_x) \mid r = I\omega[\![\theta]\!], r \in \mathbb{R}\} = \{(\omega, \omega^r_x) \mid r = I\omega[\![\theta]\!]_{\mathsf{dL}}\} = I[\![x := \theta; ?\mathsf{in}\mathbb{R}(x)]\!]_{\mathsf{dL}}$.
2. $I[\![T(?\psi)]\!] = \{(\omega,\omega) \mid I\omega[\![T(\psi)]\!]\} = \{(\omega,\omega) \mid I\omega[\![\psi]\!]_{\mathsf{dL}}\} = I[\![?\psi]\!]_{\mathsf{dL}}$
3. $I[\![T(\alpha \cup \beta)]\!] = I[\![T(\alpha)]\!] \cup I[\![T(\beta)]\!] = I[\![\alpha]\!]_{\mathsf{dL}} \cup I[\![\beta]\!]_{\mathsf{dL}} = I[\![\alpha \cup \beta]\!]_{\mathsf{dL}}$.
4. $I[\![T(\alpha;\beta)]\!] = I[\![T(\alpha)]\!] \circ I[\![T(\beta)]\!] = I[\![\alpha]\!]_{\mathsf{dL}} \circ I[\![\beta]\!]_{\mathsf{dL}} = I[\![\alpha;\beta]\!]$.
5. $I[\![T(\alpha^*)]\!] = I[\![T(\alpha)]\!]^* = I[\![\alpha]\!]^*_{\mathsf{dL}} = I[\![\alpha^*]\!]_{\mathsf{dL}}$.
6. $I[\![T(x' = \theta \,\&\, \psi)]\!] = \{(\omega, \varphi(r)) \mid$ exist solution φ and $r \in \mathbb{R}_{\geq 0}$ and for all $s \in [0,r]$ have $I\varphi(s)[\![T(\phi)]\!] = \oplus$ and $\varphi'(s)(x) = I\varphi(s)[\![T(\theta)]\!]$ and $\omega = \varphi(0)$ on $\{x'\}^C\}$. Then for the same φ and r and for all $s \in [0,r]$ by the IH have $I\varphi(s)[\![T(\phi)]\!] = I\varphi(s)[\![\phi]\!]_{\mathsf{dL}} = \oplus$ and $I\varphi(s)[\![T(\theta)]\!] = I\varphi(s)[\![\theta]\!]_{\mathsf{dL}}$ so $\{(\omega, \varphi(r)) \mid$ exist solution φ and $r \in \mathbb{R}_{\geq 0}$ and for all $s \in [0,r]$ have $I\varphi(s)[\![T(\phi)]\!] = \oplus$ and $\varphi'(s)(x) = I\varphi(s)[\![T(\theta)]\!]$ and $\omega = \varphi(0)$ on $\{x'\}^C\} = \{(\omega, \varphi(r)) \mid$ exist solution φ and $r \in \mathbb{R}_{\geq 0}$ and for all $s \in [0,r]$ have $I\varphi(s)[\![\phi]\!]_{\mathsf{dL}} = \oplus$ and $\varphi'(s)(x) = I\varphi(s)[\![\theta]\!]_{\mathsf{dL}}$ and $\omega = \varphi(0)$ on $\{x'\}^C\} = I[\![x' = \theta \,\&\, \psi]\!]_{\mathsf{dL}}$ as desired.

C.7 Coincidence proof

The proof of coincidence follows the general structure of the coincidence proof in [19]. For all terms θ, formulas ϕ, programs α, for all interpretations I, J that agree on $\Sigma(\phi$ or α or $\theta)$, have:

- If $\omega, \tilde{\omega}$ agree on $\mathrm{FV}(\theta)$, then $I\omega[\![\theta]\!] = J\tilde{\omega}[\![\theta]\!]$
- If $\omega, \tilde{\omega}$ agree on $\mathrm{FV}(\phi)$, then $I\omega[\![\phi]\!] = J\tilde{\omega}[\![\phi]\!]$
- If $\omega, \tilde{\omega}$ agree on $V \supseteq \mathrm{FV}(\alpha)$ then for $(\omega, \nu) \in I[\![\alpha]\!]$ exists $\tilde{\nu}$ s.t. $(\tilde{\omega}, \tilde{\nu}) \in I[\![\alpha]\!]$ and $\nu, \tilde{\nu}$ agree on $V \cup \mathrm{MBV}(\alpha)$.

The signature $\Sigma(\phi)$ is defined in Fig. 8 of App. B.

By mutual induction on terms, formulas, programs. We consider $\mathsf{shape}(\theta)$ structurally simpler $(\theta)'$ in the induction.

- **case** $\theta = q$: $I\omega[\![q]\!] = q = J\tilde{\omega}[\![q]\!]$
- **case** $\theta = x$: $I\omega[\![x]\!] = \omega(x) = \tilde{\omega}(x) = J\tilde{\omega}[\![x]\!]$ since $x \in \mathrm{FV}(x)$
- **case** $\theta = \theta_1 + \theta_2$ when both denote reals : $I\omega[\![\theta_1 + \theta_2]\!] = I\omega[\![\theta_1]\!] + I\omega[\![\theta_2]\!] =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_1]\!] + J\tilde{\omega}[\![\theta_2]\!] = J\tilde{\omega}[\![\theta_1 + \theta_2]\!]$
- **case** $\theta = \theta_1 + \theta_2$ error on left : $I\omega[\![\theta_1 + \theta_2]\!] = \bot$ and $I\omega[\![\theta_1]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_1]\!] = J\tilde{\omega}[\![\theta_1 + \theta_2]\!]$
- **case** $\theta = \theta_1 + \theta_2$ error on right : $I\omega[\![\theta_1 + \theta_2]\!] = \bot$ and $I\omega[\![\theta_2]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_2]\!] = J\tilde{\omega}[\![\theta_1 + \theta_2]\!]$
- **case** $\theta = \theta_1 \cdot \theta_2$ when both denote reals : $I\omega[\![\theta_1 \cdot \theta_2]\!] = I\omega[\![\theta_1]\!] \cdot I\omega[\![\theta_2]\!] =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_1]\!] \cdot J\tilde{\omega}[\![\theta_2]\!] = J\tilde{\omega}[\![\theta_1 \cdot \theta_2]\!]$
- **case** $\theta = \theta_1 \cdot \theta_2$ error on left : $I\omega[\![\theta_1 \cdot \theta_2]\!] = \bot$ and $I\omega[\![\theta_1]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_1]\!] = J\tilde{\omega}[\![\theta_1 \cdot \theta_2]\!]$
- **case** $\theta = \theta_1 \cdot \theta_2$ error on right : $I\omega[\![\theta_1 \cdot \theta_2]\!] = \bot$ and $I\omega[\![\theta_2]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_2]\!] = J\tilde{\omega}[\![\theta_1 \cdot \theta_2]\!]$
- **case** $\theta = (\theta_1, \theta_2)$ when both denote reals : $I\omega[\![(\theta_1, \theta_2)]\!] = (I\omega[\![\theta_1]\!], I\omega[\![\theta_2]\!]) =_{\mathrm{IH}}$ $(J\tilde{\omega}[\![\theta_1]\!], J\tilde{\omega}[\![\theta_2]\!]) = J\tilde{\omega}[\![(\theta_1, \theta_2)]\!]$
- **case** $\theta = (\theta_1, \theta_2)$ error on left : $I\omega[\![(\theta_1, \theta_2)]\!] = \bot$ and $I\omega[\![\theta_1]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_1]\!] = J\tilde{\omega}[\![(\theta_1, \theta_2)]\!]$
- **case** $\theta = (\theta_1, \theta_2)$ error on right : $I\omega[\![(\theta_1, \theta_2)]\!] = \bot$ and $I\omega[\![\theta_2]\!] = \bot =_{\mathrm{IH}}$ $J\tilde{\omega}[\![\theta_2]\!] = J\tilde{\omega}[\![(\theta_1, \theta_2)]\!]$
- **case** $\theta = \iota x\ \phi$ exists unique : $I\omega[\![\iota x\ \phi]\!] =$ unique $t \in \mathbf{Tree}(\mathbb{R})$ s.t. $\omega_x^t[\![\phi]\!] = \oplus$. Then for *all* $s \in \mathbf{Tree}(\mathbb{R})$ by IH have $I\omega_x^s[\![\phi]\!] = J\tilde{\omega}_x^s[\![\phi]\!]$ since ω_x^s and $\tilde{\omega}_x^s$ agree both on x and on $\mathrm{FV}(\iota x\ \phi) = \mathrm{FV}(\phi) \setminus \{x\}$, thus they agree on $\mathrm{FV}(\phi)$. This holds both for s and all other t so s is also unique s where $J\tilde{\omega}_x^t[\![\phi]\!] = \oplus$ so $s = J\tilde{\omega}[\![\iota x\ \phi]\!]$.
- **case** $\theta = \iota x\ \phi$ not exists unique : $I\omega[\![\iota x\ \phi]\!] = \bot$, does not exist exactly one $t \in \mathbf{Tree}(\mathbb{R})$ s.t. $\omega_x^t[\![\phi]\!] = \oplus$. Then for *all* $s \in \mathbf{Tree}(\mathbb{R})$ by IH have $I\omega_x^s[\![\phi]\!] = J\tilde{\omega}_x^s[\![\phi]\!]$ since ω_x^s and $\tilde{\omega}_x^s$ agree both on x and on $\mathrm{FV}(\iota x\ \phi) = \mathrm{FV}(\phi) \setminus \{x\}$, thus they agree on $\mathrm{FV}(\phi)$. This holds both for all s so there is no unique t where $J\tilde{\omega}_x^t[\![\phi]\!] = \oplus$ so $J\tilde{\omega}[\![\iota x\ \phi]\!] = \bot$.
- **case** $\theta = \mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$ Proceed by a nested induction on the value $I\omega[\![\theta_1]\!]$.
  - **case** Base case $\bot$: Then $I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!] = \bot = J\tilde{\omega}[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!]$ since by outer IH $I\omega[\![\theta_1]\!] = J\tilde{\omega}[\![\theta_1]\!]$
  - **case** Base case $r \in \mathbb{R}$: Then $I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!] = \mathsf{Fold}(\omega[\![\theta_1]\!], s\ \theta_2, lr\ \theta_3, \omega) = I\omega_s^{I\omega[\![\theta_1]\!]}[\![\theta_2]\!]$

  - **case** $\theta = \mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$ tuple case : Then $I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!] = \mathsf{Fold}(\omega[\![\theta_1]\!], s\ \theta_2, lr\ \theta_3, \omega) = \mathsf{Fold}((v_L, v_R), s\ \theta_2, lr\ \theta_3, \omega) I\omega_{l,r}^{L,R}[\![\theta_3]\!]$ for $L, R = \mathsf{Fold}(v_L, s\ \theta_2, lr\ \theta_3, I\omega), \mathsf{Fold}(v_R, s\ \theta_2, lr\ \theta_3, I\omega) =_{\text{inner IH}}$ $\mathsf{Fold}(v_L, s\,\theta_2, lr\,\theta_3, J\tilde{\omega}), \mathsf{Fold}(v_R, s\,\theta_2, lr\,\theta_3, J\tilde{\omega})$ so $I\omega_{l,r}^{L,R}[\![\theta_3]\!] = I\omega_{l,r}^{L,R}[\![\theta_3]\!] = \mathsf{Fold}((v_L, v_R), s\ \theta_2, lr\ \theta_3, J\tilde{\omega}) = J\tilde{\omega}[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!]$.

– **case** $(\theta)'$ exists : Then $I\omega[\![(\theta)']\!] = \sum_{x\in\mathcal{V}} \frac{\partial I\omega[\![\theta]\!]}{\partial x}\omega'(x) = \sum_{x\in\mathcal{V}} \frac{\partial I\omega[\![\theta]\!]}{\partial x}\tilde{\omega}'(x) =_{\text{IH}}$ $\sum_{x\in\mathcal{V}} \frac{\partial J\tilde{\omega}[\![\theta]\!]}{\partial x}\tilde{\omega}'(x) = J\tilde{\omega}[\![(\theta)']\!]$ since $\omega = \tilde{\omega}$ on $\mathrm{FV}((\theta)')$ which includes x' for each $x \in \mathrm{FV}(\theta)$ and thus x' for every nonzero term of the sum since the partial with respect to any $y \notin \mathrm{FV}(\theta)$ is 0. Furthermore the IH applies since θ is simpler than $(\theta)'$ and $\mathrm{FV}(\theta) \subseteq \mathrm{FV}((\theta)')$. The partial derivatives by X of $I\omega_x^X[\![\theta]\!]$ and $J\tilde{\omega}_x^X[\![\theta]\!]$ agree since by IH $I\omega_x^X[\![\theta]\!] = J\tilde{\omega}_x^X[\![\theta]\!]$ for *all* X since $\omega_x^X = \tilde{\omega}_x^X$ on $\{x\} \cup \mathrm{FV}(\theta)$ since x is assigned X in both states and $\omega = \tilde{\omega}$ on $\mathrm{FV}(\theta)$.

– **case** $(\theta)'$ doesn't exist : the partial derivative $\frac{\partial I\omega[\![\theta]\!]}{\partial x}$ is $\bot$ if the shape of $I\omega[\![\theta]\!]$ varies in every neighborhood of ω, while the product $\omega(x')\frac{\partial I\omega[\![\theta]\!]}{\partial x}$ is the sum of elementwise products. It is $\bot$ when either factor is $\bot$, with the exception that it is 0 when either factor consists entirely of zeroes. In this case then either

  1. $\omega(x)$ and $\omega(x')$ differ in shape for some $\|\frac{\partial I\omega[\![\theta]\!]}{\partial x}\| > 0$. Then $x \in \mathrm{FV}(\theta)$ because nonfree variables have partial derivative 0, and $\{x, x'\} \subseteq \mathrm{FV}((\theta)')$. Then $\omega = \tilde{\omega}$ on $\{x, x'\}$ by assumption. By IH $\|\frac{\partial J\tilde{\omega}[\![\theta]\!]}{\partial x}\| = \|\frac{\partial I\omega[\![\theta]\!]}{\partial x}\| > 0$ and $\tilde{\omega}(x)$ and $\tilde{\omega}x'$ differ in shape, so $J\tilde{\omega}[\![(\theta)']\!] = \bot$.
  2. For every neighborhood $\mathcal{N}_\epsilon = \{\nu \mid \|\nu - \omega\| < \epsilon\}$ exist $\nu, \mu \in \mathcal{N}_\epsilon$ where $I\nu[\![\mathsf{shape}(\theta)]\!] \neq I\mu[\![\mathsf{shape}(\theta)]\!]$. Since $\mathrm{FV}(\mathsf{shape}(\theta)) = \mathrm{FV}(\theta)$ then by IH on $\mathsf{shape}(\theta)$ (see induction metric) assume without loss of generality that $\nu = \mu = \omega$ on $\{\mathrm{FV}(\theta)\}^C$ and that $I\nu[\![\theta]\!] = J\tilde{\nu}[\![\theta]\!]$ and $I\mu[\![\theta]\!] = J\tilde{\mu}[\![\theta]\!]$ for $\tilde{\mu} = \mu$ on $\mathrm{FV}(\theta)$ and $\tilde{\mu} = \tilde{\omega}$ on $\mathrm{FV}(\theta)^C$, likewise for $\tilde{\nu}$. Because $\tilde{\omega} = \omega$ on $\mathrm{FV}(\theta)$ to begin with, then $\|\tilde{\mu} - \tilde{\omega}\| \leq \|\mu - \omega\|$ and $\|\tilde{\nu} - \tilde{\omega}\| \leq \|\nu - \omega\|$, so $\{\tilde{nu}, \tilde{\mu}\} \subseteq \tilde{\mathcal{N}}_\epsilon = \{\nu \mid \|\nu - \tilde{\omega}\| < \epsilon\}$. Because this argument is generic in ϵ then every neighborhood of $\tilde{\omega}$ has $\tilde{\nu}, \tilde{\mu}$ where the shape of θ differs, so $J\tilde{\omega}[\![(\theta)']\!] = \bot$.
  3. $I[\![\theta]\!]$ is not differentiable at ω. In this case it is easiest to work with definition of differential as a limit, where we write $(I[\![\theta]\!])'(\omega)$ for the differential of $I[\![\theta]\!]$ at ω. Analogously to Lem. 7, the differential expressed as a limit is $(I[\![\theta]\!])'(\omega) = \lim_{\nu\to\omega} \frac{\|I\nu[\![\theta]\!] - I\omega[\![\theta]\!]\|}{\|\nu-\omega\|}$. If $(I[\![\theta]\!])'(\omega)$ does not exist, then the limit $\lim_{\nu\to\omega} \frac{\|I\nu[\![\theta]\!] - I\omega[\![\theta]\!]\|}{\|\nu-\omega\|}$ does not exist. Observe $\lim_{\nu\to\omega} \frac{\|I\nu[\![\theta]\!] - I\omega[\![\theta]\!]\|}{\|\nu-\omega\|} = \lim_{\nu\to\tilde{\omega}} \frac{\|J\nu[\![\theta]\!] - I\tilde{\omega}[\![\theta]\!]\|}{\|\nu-\tilde{\omega}\|}$ by applying the IH on θ inside the limit, i.e., for every ν we know $I\nu[\![\theta]\!] = J\tilde{\nu}[\![\theta]\!]$ where $\tilde{\nu} = \nu$ on $\mathrm{FV}(\theta)$ and $\tilde{\nu} = \tilde{\omega}$ on $\mathrm{FV}(\theta)^C$. Because these limits are equal, then $\lim_{\nu\to\tilde{\omega}} \frac{\|J\nu[\![\theta]\!] - I\tilde{\omega}[\![\theta]\!]\|}{\|\nu-\tilde{\omega}\|}$ does not exist so $J\tilde{\omega}[\![(')[\!]]\!] = \bot$ as desired.

– **case** $f(\theta) : I\omega[\![f(\theta)]\!] = I(f)(I\omega[\![\theta]\!]) =_{\text{assump}} J(f)(I\omega[\![\theta]\!]) =_{\text{IH}} J(f)(J\tilde{\omega}[\![\theta]\!]) = I\omega[\![f(\theta)]\!]$.

- **case** $\theta_1 \geq \theta_2$ both exist: $I\omega[\![\theta_1 \geq \theta_2]\!] = \mathsf{Geq}(v_1, v_2) I\omega$ where $v_i = I\omega[\![\theta_i]\!]$. Then by IH $v_i = J\tilde{\omega}[\![\theta_i]\!]$ so by functionality of $\mathsf{Geq}(,)$, have $\mathsf{Geq}(v_1, v_2) = J\tilde{\omega}[\![\theta_1 \geq \theta_2]\!]$.
- **case** $\theta_1 \geq \theta_2$ not both exist: Then have some $I\omega[\![\theta_i]\!] = \bot$, so by IH $J\tilde{\omega}[\![\theta_i]\!] = \bot$ and $J\tilde{\omega}[\![\theta_1 \geq \theta_2]\!] = \bot$
- **case** $p(\theta)$: $I\omega[\![p(\theta)]\!] = I(p)(I\omega[\![\theta]\!]) =_{\text{assump}} J(p)(I\omega[\![\theta]\!]) =_{\text{IH}} J(p)(J\tilde{\omega}[\![\theta]\!]) = J\tilde{\omega}[\![p(\theta)]\!]$.
- **case** $C(\phi)$: Note $\omega = \tilde{\omega}$ since $\text{FV}(C(\phi)) = \mathcal{V} \cup \mathcal{V}'$. We write the partial application $I[\![\phi]\!] : \mathcal{S} \to \{\oplus, \textcircled{\oplus}, \ominus\}$ is shorthand for the function mapping each ω to $I\omega[\![\phi]\!]$, or likewise $I[\![\phi]\!] = J[\![\phi]\!]$ to say that for all μ, by IH have $I\mu[\![\phi]\!] = J\mu[\![\phi]\!]$. $I\omega[\![C(\phi)]\!] = I(C)(I[\![\phi]\!]) =_{\text{assump}} J(C)(I[\![\phi]\!]) =_{\text{note}} J(C)(J[\![\phi]\!]) = J\tilde{\omega}[\![C(\phi)]\!]$.
- **case** $\neg\phi$: $I\omega[\![\neg\phi]\!] = \overline{I\omega[\![\phi]\!]} = \overline{J\tilde{\omega}[\![\phi]\!]} = J\tilde{\omega}[\![\neg\phi]\!]$
- **case** $\phi \wedge \psi$: $I\omega[\![\phi \wedge \psi]\!] = I\omega[\![\phi]\!] \sqcap I\omega[\![\psi]\!] = J\tilde{\omega}[\![\phi]\!] \sqcap J\tilde{\omega}[\![\psi]\!] = J\tilde{\omega}[\![\phi \wedge \psi]\!]$
- **case** $\forall x\, \phi$: $I\omega[\![\forall x\, \phi]\!] = \sqcap_{t \in \mathbf{Tree}(\mathbb{R})} I\omega^t_x[\![\phi]\!] =_{\text{IH}} \sqcap_{t \in \mathbf{Tree}(\mathbb{R})} J\tilde{\omega}^d_x[\![\phi]\!] = J\tilde{\omega}[\![\forall x\, \phi]\!]$.
- **case** $[\alpha]\phi$: $I\omega[\![[\alpha]\phi]\!] = \sqcap_{\nu \mid (\omega,\nu) \in I[\![\alpha]\!]} I\nu[\![\phi]\!] =_{\text{IH}} \sqcap_{\tilde{\nu} \mid (\tilde{\omega},\tilde{\nu}) \in J[\![\alpha]\!]} J\tilde{\nu}[\![\phi]\!] = J\tilde{\omega}[\![[\alpha]\phi]\!]$.
- **case** a for program constant a: Have $I(a) = J(a)$ by assumption and since $\text{FV}(a) = \mathcal{V} \cup \mathcal{V}'$ have $\omega = \tilde{\omega}$. Then $(\omega, \nu) \in I[\![a]\!]$ iff $(\omega, \nu) \in I(a)$ iff $(\omega, \nu) \in J(a)$ iff $(\tilde{\omega}, \tilde{\nu}) \in J(a)$ letting every $\tilde{\nu} = \nu$.
- **case** $x := \theta : (\omega, \nu) \in I[\![x := \theta]\!]$ so $\nu = \omega^{I\omega[\![\theta]\!]}_x$ then by IH $I\omega[\![\theta]\!] = J\tilde{\omega}[\![\theta]\!]$. Now let $\tilde{\nu} = \tilde{\omega}^{J\tilde{\omega}[\![\theta]\!]}_x$ and observe $(\tilde{\omega}, \tilde{\nu}) \in J\tilde{\omega}[\![x := \theta]\!]$ by definition and that ν agrees with $\tilde{\nu}$ on the must-bound $\{x\}$ by IH above and agrees also on V by agreement between ω and $\tilde{\omega}$.
- **case** $?\phi : (\omega, \nu) \in I[\![?\phi]\!]$ so $\omega = \nu$, and $I\omega[\![\phi]\!] = \oplus$ then let $\tilde{\nu} = \tilde{\omega}$ and since ω and $\tilde{\omega}$ agree on $\text{FV}(\phi)$ then $J\tilde{\omega}[\![\phi]\!] = \oplus$ by IH so $(\tilde{\omega}, \tilde{\nu}) \in J[\![?\phi]\!]$. Lastly observe ν and $\tilde{\nu}$ agree on V trivially since $\text{BV}(?\phi) = \emptyset$
- **case** $x' = \theta \,\&\, \psi$: $(\omega, \nu) \in I[\![x' = \theta \,\&\, \psi]\!]$, let r be such that $\varphi(r) = \nu$ and $\varphi(0) = \omega$ on $\{x'\}^C$. Now define $\tilde{\varphi}(s) = \varphi(s)$ on $\{x, x'\}$ and $\tilde{\varphi}(s) = \tilde{\nu}(s)$ on $\{x, x'\}^C$. Letting $\tilde{\nu} = \tilde{\varphi}(r)$ we will now show $(\tilde{\omega}, \tilde{\nu}) \in J[\![x' = \theta \,\&\, \psi]\!]$ since for every $0 \leq s \leq r$ we have $I\varphi(s)[\![\theta]\!] = J\tilde{\varphi(s)}[\![\theta]\!]$ and $I\varphi(s)[\![\psi]\!] = J\tilde{\varphi}(s)[\![\psi]\!] = \oplus$, both by IH's, and moreover since $I\varphi[\![\theta]\!]$ and $J\tilde{\varphi}[\![\theta]\!]$ are the same function of time, they have the same solution and thus $s \mapsto J\tilde{\varphi}(s)[\![\theta]\!]$ is the time-derivative of $s \mapsto \tilde{\varphi}(s)(x)$ as desired. Lastly, φ and $\tilde{\varphi}$ agree on $\{x, x'\}$ by construction and agree for the other V by assumption that ω and $\tilde{\omega}$ agree on V and since $\omega = \varphi(s)$ on $\{x, x'\}^C$ and $\tilde{\omega} = \tilde{\varphi}(s)$ on the same, by construction.
- **case** $\alpha \cup \beta$: From $(\omega, \nu) \in I[\![\alpha \cup \beta]\!]$ have either $(\omega, \nu) \in I[\![\alpha]\!]$ or $(\omega, \nu) \in I[\![\beta]\!]$. Since $\text{FV}(\alpha), \text{FV}(\beta) \subseteq \text{FV}(\alpha \cup \beta)$, then by IH exists in each case $\tilde{\nu}$ such that either $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha]\!]$ with $\tilde{\nu}$ agreeing with ν on $V \cup \text{MBV}(\alpha)$ (where the must-bound variables $\text{MBV}(\alpha)$ are bound on every execution of α) or $(\tilde{\omega}, \tilde{\nu}) \in I[\![\beta]\!]$ with $\tilde{\nu}$ agreeing with ν on $V \cup \text{MBV}(\beta)$, respectively. In each case $\text{MBV}(\alpha), \text{MBV}(\beta) \supseteq \text{MBV}(\alpha \cup \beta)$ so ν and $\tilde{\nu}$ agree on $\text{MBV}(\alpha \cup \beta) \cup V$ and also $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha \cup \beta]\!]$ since $J[\![\alpha]\!], J[\![\beta]\!] \subseteq J[\![\alpha \cup \beta]\!]$.
- **case** $\alpha;\ \beta$: From $(\omega, \nu) \in I[\![\alpha;\ \beta]\!]$ have μ s.t. $(\omega, \mu) \in I[\![\alpha]\!]$ and $(\mu, \nu) \in I[\![\beta]\!]$. Since $\text{FV}(\alpha) \subseteq \text{FV}(\alpha;\ \beta)$ IH1 is applicable. By IH1 exists $\tilde{\mu}$ s.t. $(\tilde{\omega}, \tilde{\mu}) \in J[\![\alpha]\!]$ where $\tilde{\mu}$ agrees with μ on $V \cup \text{MBV}(\alpha)$. Since $V \supseteq \text{FV}(\alpha;\ \beta)$ then $V \cup$

$\mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\alpha;\beta) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) \cup \mathrm{MBV}(\alpha) \subseteq \mathrm{FV}(\beta)$. Then by IH2 have $\tilde{\nu}$ s.t. $(\tilde{\mu}, \tilde{\nu}) \in J[\![\beta]\!]$ and $\omega = \tilde{\omega}$ on $(V \cup \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\beta) = V \cup \mathrm{MBV}(\alpha;\ \beta)$. On

- **case** α^* : Recall α^n is considered structurally simpler than α^*. Have $(\omega, \nu) \in I[\![\alpha^*]\!]$ iff exists $n \in \mathbb{N}$ s.t. $(\omega, \nu) \in I[\![\alpha^n]\!]$. The case $n = 0$ follows immediately from the assumptions on ω and $\tilde{\omega}$ since $\nu = \omega$ (let $\tilde{\nu} = \nu$) and since $\mathrm{MBV}(\alpha^*) = \emptyset$. In the case $n > 0$ apply the induction hypothesis on structurally simpler α^n, then there exists $\tilde{\nu}$ where $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha^n]\!]$ and $\tilde{\nu} = \nu$ on $V \cup \mathrm{MBV}(\alpha^n) \supseteq V \cup \mathrm{MBV}(\alpha^*) = V$. This concludes the proof since $J[\![\alpha^n]\!] \subseteq J[\![\alpha^*]\!]$.

C.8 Bound effect lemma proof

This lemma is not discussed in the main paper for the sake of space. It will be used in the substitution soundness proof. If $(\omega, \nu) \in I[\![\alpha]\!]$ then $\omega = \nu$ on $\mathrm{BV}(\alpha)^C$.

- **case** a: Vacuous since $\mathrm{BV}(a)^C = (\mathcal{V} \cup \mathcal{V}')^C = \emptyset$
- **case** $x := \theta$: $(\omega, \nu) \in I[\![x ::= \theta]\!]$ iff $\nu = \omega_x^{I\omega[\![\theta]\!]}$ so $\nu = \omega$ except on $\{x\} = \mathrm{BV}(x := \theta)$
- **case** $?\phi$: $(\omega, \nu) \in I[\![?\phi]\!]$ iff $\omega = \nu$ and $I\omega[\![\phi]\!] = \oplus$, so $\omega = \nu$ on $\mathcal{V} \cup \mathcal{V}'$ as desired for $\mathrm{BV}(?\phi) = \emptyset$.
- **case** $x' = \theta \,\&\, \psi$ implies $\omega = \varphi(0)$ on $\{x, x'\}^C$ and $\nu = \varphi(r)$ for solution φ of duration at least r. Then $\varphi(s) = \omega$ on $\{x, x'\}^C$ for all s in its domain. So $\omega = \nu$ on $\{x, x'\}^C = \mathrm{BV}(x' = \theta \,\&\, \psi)^C$ as desired.
- **case** $\alpha \cup \beta$: $(\omega, \nu) \in I[\![\alpha \cup \beta]\!]$ implies $(\omega, \nu) \in I[\![\alpha]\!]$ or $(\omega, \nu) \in I[\![\beta]\!]$; in each case by IH $\omega = \nu$ on either $\mathrm{BV}(\alpha)^C$ or $\mathrm{BV}(\beta)^C$ and thus in both cases on $\mathrm{BV}(\alpha)^C \cap \mathrm{BV}(\beta)^C = \mathrm{BV}(\alpha \cup \beta)^C$.
- **case** $\alpha;\beta$: $(\omega, \nu) \in I[\![\alpha;\beta]\!]$ iff exists μ where $(\omega, \mu) \in I[\![\alpha]\!]$ and $(\mu, \nu) \in I[\![\beta]\!]$ so by IH's $\omega = \mu$ on $\mathrm{BV}(\alpha)^C$ and $\mu = \nu$ on $\mathrm{BV}(\beta)^C$ so by transitivity $\omega = \nu$ on $\mathrm{BV}(\alpha)^C \cap \mathrm{BV}(\beta)^C = \mathrm{BV}(\alpha;\ \beta)^C$.
- **case** α^*: $(\omega, \nu) \in I[\![\alpha^*]\!] = \bigcup_{n \in \mathbb{N}} I[\![\alpha^n]\!]$ follows by induction on natural number n.

C.9 Adjoint lemma proof

Definition 6 (Adjoint interpretation). *For any interpretation I, state ω, and admissible susbstitution σ, the adjoint interpretation $\sigma^*_\omega I$ is defined by:*

$$\sigma^*_\omega I(f) : (\mathbf{Tree}(\mathbb{R}) \cup \{\bot\}) \to (\mathbf{Tree}(\mathbb{R}) \cup \{\bot\}); d \mapsto I^d_{\cdot}\omega[\![\sigma f(\cdot)]\!]$$
$$\sigma^*_\omega I(p) : (\mathbf{Tree}(\mathbb{R}) \cup \{\bot\}) \to \{\oplus, \textcircled{\oplus}, \ominus\}; d \mapsto I^d_{\cdot}\omega[\![\sigma p(\cdot)]\!]$$
$$\sigma^*_\omega I(C) : (\mathcal{S} \to \{\oplus, \textcircled{\oplus}, \ominus\}) \to (\mathcal{S} \to \{\oplus, \textcircled{\oplus}, \ominus\}); R \mapsto I^R_{\_}[\![\sigma C(\_)]\!]$$
$$\sigma^*_\omega I(a) = I[\![\sigma a]\!]$$

Lemma 8 (Adjoint agreement). *If $\omega = \nu$ on $FV(\sigma)$ then $\sigma^*_\omega I = \sigma^*_\nu I$. If σ is U-admissible for ϕ or θ or α and $\omega = \nu$ and $\omega = \nu$ on U^C then for all states μ:*

$$\sigma^*_\omega I\mu[\![\theta]\!] = \sigma^*_\nu I\mu[\![\theta]\!]$$
$$\sigma^*_\omega I\mu[\![\phi]\!] = \sigma^*_\nu I\mu[\![\phi]\!]$$
$$\sigma^*_\omega I[\![\alpha]\!] = \sigma^*_\nu I[\![\alpha]\!]$$

Proof. First, $\sigma^*_\omega I(a) = I[\![\sigma a]\!] = \sigma^*_\nu I(a)$ because the adjoint to σ for I and ω in the case of programs is independent of ω. Likewise $\sigma^*_\omega I(C) = \sigma^*_\nu IC$ for quantifier symbols C. By Lem. 2, $\cdot^*_d I\omega[\![\sigma f(\cdot)]\!] = \cdot^*_d I\nu[\![\sigma f(\cdot)]\!]$ when $\omega = \nu$ on $\mathrm{FV}(\sigma f(\cdot)) \subseteq \mathrm{FV}(\sigma)$. Also by Lem. 2, $\cdot^*_d I\omega[\![\sigma p(\cdot)]\!] = \cdot^*_d I\nu[\![\sigma p(\cdot)]\!]$ on $\mathrm{FV}(\sigma p(\cdot)) \subseteq \mathrm{FV}(\sigma)$. Thus $\sigma^*_\omega I = \sigma^*_\nu I$ when $\omega = \nu$ on $\mathrm{FV}(\sigma)$.

If σ is U-admissible for ϕ, θ, α then $\mathrm{FV}(\sigma f(\cdot)) \cap U = \emptyset$ and thus $\mathrm{FV}(\sigma f(\cdot)) \subseteq U^C$ for every function symbol f and (likewise predicate p) in $\Sigma(\phi, \theta, \alpha)$. We need not concern ourselves with $C(\phi)$ or a since $\sigma^*_\omega I(C)$ and $\sigma^*_\omega I(a)$ are independent of ω anyway. Since $\omega = \nu$ on U^C then $\sigma^*_\omega I = \sigma^*_\nu I$ on $\Sigma(\phi, \theta, \alpha)$.

Then by Lem. 2 (for all possible states μ) have $\sigma^*_\omega I\mu[\![\theta]\!] = \sigma^*_\nu I\mu[\![\theta]\!]$ and $\sigma^*_\omega I\mu[\![\phi]\!] = \sigma^*_\nu I\mu[\![\phi]\!]$ and $\sigma^*_\omega I[\![\alpha]\!] = \sigma^*_\nu I[\![\alpha]\!]$. □

C.10 Substitution lemma proof

For all $\phi, \theta, \alpha, \omega$ and admissible σ:

1. $I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$
2. $I\omega[\![\sigma(\phi)]\!] = \sigma^*_\omega I\omega[\![\phi]\!]$
3. $I[\![\sigma(\alpha)]\!] = \sigma^*_I I[\![\alpha]\!]$

- **case** q: $I\omega[\![\sigma(q)]\!] = I\omega[\![q]\!] = q = \sigma^*_I I\omega[\![q]\!]$
- **case** x: $I\omega[\![\sigma(x)]\!] = I\omega[\![x]\!] = \omega(x) = \sigma^*_I I\omega[\![x]\!]$
- **case** $\theta_1 + \theta_2$ exists: $I\omega[\![\sigma(\theta_1 + \theta_2)]\!] = I\omega[\![\sigma(\theta_1)]\!] + I\omega[\![\sigma(\theta_2)]\!] = \sigma^*_I I\omega[\![\theta_1]\!] + \sigma^*_I I\omega[\![\theta_2]\!] = \sigma^*_I I\omega[\![\theta_1 + \theta_2]\!]$
- **case** $\theta_1 + \theta_2$ doesn't exist: Then for some i, have $I\omega[\![\sigma(\theta_i)]\!] = \bot$ so by IH $\sigma^*_I I\omega[\![\theta_i]\!] = \bot$ and $\sigma^*_I I\omega[\![\theta_1 + \theta_2]\!]$
- **case** $\theta_1 \cdot \theta_2$ exists: $I\omega[\![\sigma(\theta_1 \cdot \theta_2)]\!] = I\omega[\![\sigma(\theta_1)]\!] \cdot I\omega[\![\sigma(\theta_2)]\!] = \sigma^*_I I\omega[\![\theta_1]\!] \cdot \sigma^*_I I\omega[\![\theta_2]\!] = \sigma^*_I I\omega[\![\theta_1 \cdot \theta_2]\!]$
- **case** $\theta_1 \cdot \theta_2$ doesn't exist: Then for some i, have $I\omega[\![\sigma(\theta_i)]\!] = \bot$ so by IH $\sigma^*_I I\omega[\![\theta_i]\!] = \bot$ and $\sigma^*_I I\omega[\![\theta_1 \cdot \theta_2]\!]$
- **case** (θ_1, θ_2) exists: $I\omega[\![\sigma((\theta_1, \theta_2))]\!] = (I\omega[\![\sigma(\theta_1)]\!], I\omega[\![\sigma(\theta_2)]\!])$ $= (\sigma^*_I I\omega[\![\theta_1]\!], \sigma^*_I I\omega[\![\theta_2]\!]) = \sigma^*_I I\omega[\![(\theta_1, \theta_2)]\!]$
- **case** (θ_1, θ_2) doesn't exist: Then for some i, have $I\omega[\![\sigma(\theta_i)]\!] = \bot$ so by IH $\sigma^*_I I\omega[\![\theta_i]\!] = \bot$ and $\sigma^*_I I\omega[\![(\theta_1, \theta_2)]\!]$
- **case** $\iota x\ \phi$: Then $I\omega[\![\sigma(\iota x\ \phi)]\!] =$ the unique $t \in \mathbf{Tree}(\mathbb{R})$ s.t. $\omega^t_x[\![\sigma(\phi)]\!] = \oplus$. For each $s \in \mathbf{Tree}(\mathbb{R})$, apply IH and have $\omega^t_x[\![\phi]\!] = \sigma^*_{\omega^t_x} I\omega^t_x[\![\phi]\!]$. Then by $\{x\}$-admissibility and since ω agrees with ω^t_x on $\{x\}^C$ have $\sigma^*_{\omega^t_x} I\omega^t_x[\![\phi]\!] = \sigma^*_\omega I\omega^t_x[\![\phi]\!]$. Since this was for all s, then uniqueness is preserved, so t is the *unique* t such that $\sigma^*_\omega I\omega^t_x[\![\phi]\!] = \oplus$ so $t = \sigma^*_\omega I\omega[\![\iota x\ \phi]\!]$.

- **case** $\iota x\ \phi$ doesn't exist: In this case there are either 0 or multiple $t \in \mathbf{Tree}(\mathbb{R})$ s.t. $I\omega^t_x[\![\sigma(\phi)]\!] = \oplus$. By IH, admissibility, and Lem. 8, for each such t have $\omega^t_x[\![\sigma(\phi)]\!] = \sigma^*_\omega I\omega^t_x[\![\phi]\!]$, so non-uniqueness and non-existence are preserved, so $\sigma^*_\omega I\omega[\![\iota x\ \phi]\!] = \bot$ as desired.
- **case** $\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)$ doesn't exist: Then $I\omega[\![\sigma(\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3))]\!]$ and $I\omega[\![\sigma(\theta_1)]\!] = \bot$ so by IH $\cdots = \sigma^*_\omega I\omega[\![\theta_1]\!]$ and $\sigma^*_\omega I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!] = \bot$ as desired.
- **case** $\mathsf{red}(\theta_1, s\,\theta_2, lr\,\theta_3)$ base: Then $I\omega[\![\sigma(\mathsf{red}(\theta_1, s\,\theta_2, lr\,\theta_3))]\!] = I\omega_s^{I\omega[\![\sigma(\theta_1)]\!]}[\![\sigma(\theta_2)]\!]$. By first IH, $\cdots = I\omega_s^{\sigma^*_\omega I\omega[\![\theta_1]\!]}[\![\theta_2]\!]$ and by second IH $\cdots = \sigma^*_{\omega_s^{\sigma^*_\omega I\omega[\![\theta_1]\!]}} I\omega_s^{\sigma^*_\omega I\omega[\![\theta_1]\!]}[\![\theta_2]\!]$. Then by admissibility $I\omega_s^{\sigma^*_\omega I\omega[\![\theta_1]\!]}$ agrees with ω on $\{s\}^C$ so by Lem. 8 have $\cdots = \sigma^*_\omega I\omega_s^{\sigma^*_\omega I\omega[\![\theta_1]\!]}[\![\theta_2]\!]$ Which is then $\cdots = \sigma^*_\omega I\omega[\![\mathsf{red}(\theta_1, s\ \theta_2, lr\ \theta_3)]\!]$ as desired.
- **case** $\mathsf{red}(\theta_1, s\,\theta_2, lr\,\theta_3)$ inductive: Then $I\omega[\![\sigma(\mathsf{red}(\theta_1, s\,\theta_2, lr\,\theta_3))]\!] = I\omega^{L,R}_{l,r}[\![\sigma(\theta_3)]\!]$ for $L, R = \mathsf{Fold}(v_L, s\ \theta_2, lr\ \theta_3, I\omega), \mathsf{Fold}(v_R, s\ \theta_2, lr\ \theta_3, I\omega)$ and $(v_L, v_R) = I\omega[\![\sigma(\theta_1)]\!] = \sigma^*_\omega I\omega[\![\theta_1]\!]$ by IH. Then by IH 3 $I\omega^{L,R}_{l,r}[\![\sigma(\theta_3)]\!] = \sigma^*_{\omega^{L,R}_{l,r}} I\omega^{L,R}_{l,r}[\![\theta_3]\!]$ which by admissibility condition is $\cdots = \sigma^*_\omega I\omega^{L,R}_{l,r}[\![\theta_3]\!]$ which by definition is $\mathsf{Fold}(\sigma^*_\omega I\omega[\![\theta_1]\!], s\,\theta_2, lr\,\theta_3, \sigma^*_\omega I\omega)$ which is $\sigma^*_\omega I\omega[\![\mathsf{red}(\theta_1, s\,\theta_2, lr\,\theta_3)]\!]$ as desired.
- **case** $(\theta)'$ exists: $I\omega[\![\sigma((\theta)')]\!] = \sum_{x\in\mathcal{V}} \frac{\partial I\omega[\![\sigma(\theta)]\!]}{\partial x}(\omega)' = \sum_{x\in\mathcal{V}} \frac{\partial \sigma^*_\omega I\omega[\![\theta]\!]}{\partial x}(\omega)'$ by IH and because by $\mathcal{V}\cup\mathcal{V}'$-admissibility have $\sigma^*_\omega I = \sigma^*_\mu I$ for any state whatsoever, as encountered while forming the partial derivative. Then $\cdots = \sigma^*_\omega I\omega[\![(\theta)']\!]$ as desired.
- **case** $(\theta)'$ doesn't exist: $I\omega[\![\sigma((\theta)')]\!] = \bot$ when $I[\![\sigma((\theta)')]\!]$ is non differentiable at ω. Since $I[\![\sigma((\theta)')]\!]$ is the same function as $\sigma^*_\omega I[\![(\theta)']\!]$ (which follows from the IH on θ and because by the admissibility condition $\sigma^*_\omega I = \sigma^*_\nu I$ for all states ν) then it follows that it is also not differentiable at ω so $\sigma^*_\omega I\omega[\![(\theta)']\!] = \bot$ as desired.
- **case** $f(\theta)$ in σ: $I\omega[\![\sigma(f(\theta))]\!] = I\omega[\![\{\cdot \mapsto \sigma(\theta)\}\sigma f]\!] = I_{\cdot}^d[\![\sigma f]\!] = \sigma^*_\omega I(f)(d) = \sigma^*_\omega I(f)(\sigma^*_\omega I\omega[\![\theta]\!]) = \sigma^*_\omega I\omega[\![f(\theta)]\!]$ (by IH) where $d = I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$ (by other IH). In the first case note the term is not strictly smaller but the substitution is lower-order, so substitution is well-founded.
- **case** $f(\theta)$ not in σ: $I\omega[\![\sigma(f(\theta))]\!] = I\omega[\![f(\sigma(\theta))]\!] = \sigma^*_\omega I\omega[\![f(\theta)]\!]$ by IH.
- **case** $\theta_1 \geq \theta_2$ both exist: $I\omega[\![\sigma(\theta_1 \geq \theta_2)]\!] = \mathsf{Geq}(I\omega[\![\sigma(\theta_1)]\!], I\omega[\![\sigma(\theta_2)]\!])I\omega = \mathsf{Geq}(\sigma^*_\omega I\omega[\![\theta_1]\!], \sigma^*_\omega I\omega[\![\theta_2]\!])I\omega = \sigma^*_\omega I\omega[\![\theta_1 \geq \theta_2]\!]$
- **case** $\theta_1 \geq \theta_2$ not both exist: Then some $I\omega[\![\sigma(\theta_i)]\!] = \bot$ so by IH $\sigma^*_\omega I\omega[\![\theta_i]\!] = \bot$ so $\sigma^*_\omega I\omega[\![\theta_1 \geq \theta_2]\!] = \bigoplus$ as desired.
- **case** $p(\theta)$ subst case: $I\omega[\![\sigma(p(\theta))]\!] = I\omega[\![\{\cdot \mapsto \sigma(\theta)\}\sigma p]\!] = I_{\cdot}^d[\![\sigma p]\!] = \sigma^*_\omega I(p)(d) = \sigma^*_\omega I(p)(\sigma^*_\omega I\omega[\![\theta]\!]) = \sigma^*_\omega I\omega[\![p(\theta)]\!]$ (by IH) where $d = I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$ (by other IH). In the first case note the expression is not strictly smaller but the substitution is lower-order, so substitution is well-founded.
- **case** $p(\theta)$ no subst case: $I\omega[\![\sigma(p(\theta))]\!] = I\omega[\![p(\sigma(\theta))]\!] = \sigma^*_\omega I\omega[\![p(\theta)]\!]$ by IH.
- **case** $C(\phi)$ in subst case: $I\omega[\![\sigma(C(\phi))]\!] = I\omega[\![\{\cdot \mapsto \sigma(\phi)\}\sigma C]\!] = I_{\cdot}^d\omega[\![\sigma C]\!] = \sigma^*_\omega I(C)(d) = \sigma^*_\omega I(C)(\sigma^*_\omega I[\![\phi]\!]) = \sigma^*_\omega I\omega[\![C(\phi)]\!]$ (by IH) where $d = I[\![\sigma(\phi)]\!] = \sigma^*_\omega I[\![\phi]\!]$ (by other IH).
- **case** $C(\phi)$ no subst case: $I\omega[\![\sigma(C(\phi))]\!] = I\omega[\![C(\sigma(\phi))]\!] = \sigma^*_\omega I\omega[\![C(\phi)]\!]$

- **case** $\neg\phi$: $I\omega[\![\sigma(\neg\phi)]\!] = \overline{I\omega[\![\sigma(\phi)]\!]} = \overline{\sigma^*_\omega I\omega[\![\phi]\!]} = \sigma^*_\omega I\omega[\![\neg\phi]\!]$
- **case** $\phi\wedge\psi$: $I\omega[\![\sigma(\phi\wedge\psi)]\!] = I\omega[\![\sigma(\phi)]\!] \sqcap I\omega[\![\sigma(\psi)]\!] =_{\text{IH}} \sigma^*_\omega I\omega[\![\phi]\!] \sqcap \sigma^*_\omega I\omega[\![\psi]\!] = \sigma^*_\omega I\omega[\![\phi\wedge\psi]\!]$
- **case** $\forall x\,\phi$: $I\omega[\![\sigma(\forall x\,\phi)]\!] = \sqcap_{d\in\mathbf{Tree}(\mathbb{R})} I\omega^d_x[\![\sigma(\phi)]\!] =_{\text{IH}} \sqcap_{d\in\mathbf{Tree}(\mathbb{R})}\sigma^*_{\omega^d_x} I\omega^d_x[\![\phi]\!]$ $=_{\text{Lem. 8}} \sqcap_{d\in\mathbf{Tree}(\mathbb{R})}\sigma^*_\omega I\omega^d_x[\![\phi]\!] = \sigma^*_\omega I\omega[\![\forall x\,\phi]\!]$
- **case** $[\alpha]\phi$: Then we have that $I\omega[\![\sigma([\alpha]\phi)]\!] = \sqcap_{\nu\ |\ (\omega,\nu)\in I[\![\sigma(\alpha)]\!]} I\omega[\![\sigma(\phi)]\!] =_{\text{IH}}$ $\sqcap_{\nu\ |\ (\omega,\nu)\in\sigma^*_\omega I[\![\alpha]\!]}\sigma^*_\nu I\omega[\![\phi]\!] =_{\text{Lem. 8}} \sqcap_{\nu\ |\ (\omega,\nu)\in\sigma^*_\omega I[\![\alpha]\!]}\sigma^*_\omega I\omega[\![\phi]\!] = \sigma^*_\omega I\omega[\![[\alpha]\phi]\!]$
- **case** a: Have $I[\![\sigma(a)]\!] = I[\![\sigma a]\!] = \sigma^*_\omega I(a) = \sigma^*_{om} I[\![a]\!]$ for $a\in\sigma$, likewise for $a\notin\sigma$.
- **case** $x := \theta$: Have $(\omega,\nu)\in I[\![\sigma(x:=\theta)]\!] = I[\![x:=\sigma(\theta)]\!]$ iff $\nu = \omega^{I\omega[\![\sigma(\theta)]\!]}_x = \omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_x$ by IH, where $I\omega[\![\sigma(\theta)]\!]\neq\bot$ by semantics case. Then by definition $(\omega,\nu)\in\sigma^*_\omega I[\![x:=\theta]\!]$ as well.
- **case** $?\phi$: Have $(\omega,\nu)\in I\omega[\![\sigma(?\phi)]\!]$ iff $\omega=\nu$ and $I\omega[\![\sigma(\phi)]\!] = \oplus$ iff (by IH) $\sigma^*_\omega I\omega[\![\phi]\!] = \oplus$ iff $(\omega,\nu)\in\sigma^*_\omega I[\![?\phi]\!]$.
- **case** $\{x' = \theta\&\psi\}$: Have $(\omega,\nu)\in I[\![\sigma(x'=\theta\,\&\,\psi)]\!]$ (for $\{x,x'\}$-admissible σ for θ,ψ) iff $\exists\varphi : [0,T]\to\mathcal{S}$ with $\varphi(0)=\omega$ on $\{x'\}^C$, $\varphi(T)=\nu$ and for all $t\geq 0$ $\varphi'(t) = I[\![\sigma(\theta)]\!] = \sigma^*_{\varphi(t)} I[\![\theta]\!]$ by IH1 and $I\varphi(t)[\![\sigma(\psi)]\!] = \oplus$ which by IH2 is equivalent to $\sigma^*_{\varphi(t)} I\varphi(t)[\![\psi]\!]$.

  Then $(\omega,\nu)\in\sigma^*_\omega I[\![x'=\theta\,\&\,\psi]\!]$ iff $\exists\varphi : [0,T]\to\mathcal{S}$ with $\varphi(0)=\omega$ on $\{x'\}^C$, $\varphi(T)=\nu$ and for all $t\geq 0$ $\varphi'(t) = \sigma^*_\omega I\varphi(t)[\![\theta]\!]$ and $\sigma^*_\omega I\varphi(t)[\![\psi]\!] = \oplus$, which holds since $\sigma^*_\omega I[\![\theta]\!] = \sigma^*_{\varphi(t)} I[\![\theta]\!]$ and $\sigma^*_\omega I[\![\psi]\!] = \sigma^*_\psi I[\![\psi]\!]$ by Lem. 8 because σ is assumed $\{x,x'\}$-admissible for both and by bound effect, $\varphi(t)$ and ω agree on $\{x,x'\}^C$.
- **case** $\alpha\ \cup\ \beta$: Have $(\omega,\nu)\in I[\![\sigma(\alpha\ \cup\ \beta)]\!] = I[\![\sigma(\alpha)]\!]\cup I[\![\sigma(\beta)]\!] =_{\text{IH}} \sigma^*_\omega I[\![\alpha]\!]\cup \sigma^*_\omega I[\![\beta]\!] = \sigma^*_\omega I[\![\alpha\ \cup\ \beta]\!]$
- **case** $\alpha;\ \beta$: Have $(\omega,\nu)\in I[\![\sigma(\alpha;\ \beta)]\!]$ iff exists μ where $(\omega,\mu)\in I[\![\sigma(\alpha)]\!]$ and $(\mu,\nu)\in I[\![\sigma(\beta)]\!]$ then by IH1 $(\omega,\nu)\in\sigma^*_\omega I[\![\alpha]\!]$ and by IH2 $(\mu,\nu)\in\sigma^*_\mu I[\![\beta]\!]$. Then $\sigma^*_\mu I[\![\beta]\!] = \sigma^*_\omega I[\![\beta]\!]$ by Lem. 8 and because σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for β by this case of substitution and $\omega=\nu$ on $\mathrm{BV}(\sigma(\alpha))^C$ by bound variables lemma. This gives $(\omega,\nu)\in\sigma^*_\omega I[\![\alpha;\ \beta]\!]$ as desired.
- **case** α^*: Have $(\omega,\nu)\in I[\![\sigma(\alpha^*)]\!]$ iff exists $n\in\mathbb{N}$ such that $(\omega,\nu)\in I[\![\sigma(\alpha)^n]\!]$, i.e., there are $\omega_0=\omega,\ldots,\omega_n=\nu$ s.t. $(\omega_i,\omega_{i+1})\in I[\![\sigma(\alpha)]\!]$ for each $i<n$. By applying the IH to each, $(\omega_i,\omega_{i+1})\in\sigma^*_{\omega_i} I[\![\alpha]\!]$. Then by Lem. 8 $\sigma^*_{\omega_i} I = \sigma^*_\omega I$ for all i since σ is $\mathrm{BV}(\sigma(\alpha))$-admissible by case and since $\omega_i = \omega_{i+1}$ on $\mathrm{BV}(\sigma(\alpha))^C$ by bound effect. Then each $(\omega_i,\omega_{i+1})\in\sigma^*_\omega I[\![\alpha]\!]$ and $(\omega,\nu)\in\sigma^*_\omega I[\![\alpha^*]\!]$.

D A Note on the Semantics of Differential Terms

This appendix discusses the semantics of differential terms and why we require existence of a total differential.

To state the semantics of the differential term precisely, we first introduce some notation. We write $\omega(d)$ to index the state ω by a *path* d: analogously to accessing the valuation $\omega(x)$ we write $\omega(d.0)$ and $\omega(d.1)$ to access the values of the left or right component of d assuming $\omega(d)$ is a pair, or $\bot$ if $\omega(d)$ is a real. Then the interpretation is:

$$I\omega[\![(]\!](\theta))' = \sum_{d\in\mathsf{Dim}(\theta)} \omega(d')\frac{\partial I\omega[\![\theta]\!]}{\partial d} \text{ if } I[\![\theta]\!] \text{ is totally differentiable at } \omega$$

and $\bot$ otherwise, where $\mathsf{Dim}(\omega) = \{d \mid \omega(d) \in \mathbb{R} \text{ and } \omega(x') \in \mathbb{R} \text{ and } \frac{\partial I\omega[\![\theta]\!]}{\partial d} \neq 0\}$. Summing over $\mathsf{Dim}(\omega)$ serves two purposes:

- It makes precise the meaning of partial differentials over variable x when x is a tuple. We make precise the intuitive idea that for example when x contains a two-dimensional tuple, we treat their elements as two real-valued variables which we vary independently.
- It makes clear the interactions between the shape of $\omega(x)$ and $\omega(x')$ and specifically resolves them in a way that makes Lem. 2 true. The subtlety is that the semantics should be $\bot$ if $\omega(x)$ and $\omega(x')$ differ in shape: while this can only occur if an adversarial user goes out of their way to write a troublesome formula, we must handle it soundly. At the same time, coincidence demands that the meaning should only depend on variables that are mentioned. To reconcile these demands we sum only over variables that even influenced the meaning (so in $(x)'$ it's fine if $\omega(y)$ and $\omega(y')$ have different shapes), but the mentioned variables must have the correct shape, else the differential is $\bot$.

The notion of *totally differentiable* here also deserves a note. As mentioned in the proof of axiom $(\theta)'$, we do not vary the shape of $\omega(y)$ for any y when taking the differential, and if the shape of θ varies even when the shape of ω remains constant, then it is not considered differentiable. The formal justification for this notion of differentiation is if we define the sets $A_x \subset \mathbf{Tree}(\mathbb{R}) = \{v \mid v \text{ has the same shape as } \omega(x)\}$ and $A = \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$ and $B \subset \mathbf{Tree}(\mathbb{R}) = \{v \mid v \text{ has the same shape as } I\omega[\![\theta]\!]\}$ then the A_i's and A and B are all real-normed vector spaces under the Euclidean norm where A describes the values that ω takes on as it varies in the derivative and B the values that $I[\![\theta]\!]$ may take on in the derivative.

A canonical function demonstrating the need for total differentials is:

$$z(x,y) = \begin{cases} 0 & x = y = 0 \\ \frac{xy}{x^2+y^2} & \text{otherwise} \end{cases}$$

Because at point $(0,0)$, both partial derivatives exist but the total differential does not. Notably, both partial derivatives are 0 at point $(0,0)$, and also are 0

so long as we remain on the line $x = y$. This means that we could "prove" $z = 0$ as an invariant as we move from the origin along $x = y$. This is quite a serious soundness issue, as $z = 1/2$ everywhere on that line except the origin.

Let $\alpha \equiv x := 0; y := 0; x' = 1, y' = 1$. Then we can prove the invalid formula:

$$[\alpha](\iota z\ x = y = z = 0 \lor ((x \neq 0 \lor y \neq 0) \land z = \frac{xy}{x^2 + y^2})) = 0$$

This proves first by a DC which easily proves $x = y$ by DI, then by a direct DI, which, for its initial condition, observes

$$(\iota z\ x = y = z = 0 \lor ((x \neq 0 \lor y \neq 0) \land z = \frac{xy}{x^2 + y^2})) = 0$$

holds when $x = y = 0$ and for its inductive step observes

$$((\iota z\ x = y = z = 0 \lor ((x \neq 0 \lor y \neq 0) \land z = \frac{xy}{x^2 + y^2})))' = 0$$

by the partial-differential definition.

Thus it was important that we require full differentiability. Such a differential does not exist for function z and so rule DI is inapplicable in our system, ruling out this unsound application. The application fails specifically because the axiom $(\theta)'$ requires a differential that exists for *every* element of an open neighborhood around (x, y). This problematic case was exactly the line $x = y$, which is not caught when taking the partials along the x or y-axis.