dL$_\iota$: Definite Descriptions in Differential Dynamic Logic

Brandon Bohrer **Manuel Fernández**
André Platzer

November 2019
CMU-CS-19-111

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

A version of this work [3] appears in the 27th International Conference on Automated Deduction (CADE) 2019.

This research was sponsored by NDSEG, the AFOSR under grant number FA9550-16-1-0288, and the Alexander von Humboldt Foundation.

Keywords: dynamic logic, definite description, hybrid systems, theorem proving, uniform substitution, partial functions

Abstract

We introduce dL$_\iota$, which extends differential dynamic logic (dL) for hybrid systems with definite descriptions and tuples, thus enabling its theoretical foundations to catch up with its implementation 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. Unlike in vanilla dL, definite descriptions enable non-locally-Lipschitz terms, so our differential equation (ODE) axioms now make their continuity requirements explicit. Tuples are simple when considered in isolation, but in the context of hybrid systems they demand that differentials are treated in full generality. The addition of definite descriptions also makes dL$_\iota$ a free logic; we investigate the interaction of free logic and the ODEs of dL, showing that this combination is sound, and characterize its expressiveness. We give an example system that can be defined and verified using these extensions.

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) [19, 23, 24] is a logic for formal verification of *hybrid systems* [10], 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 [12, 15, 16] using the KeYmaera X [9] theorem prover, and for its strong foundations, as evidenced by its completeness results [19, 23, 24, 26] and a formal proof of soundness in both Isabelle/HOL and Coq [4].

However, there is a tension between the goals of practical applicability and rigorous foundations. In practice, multiple theorem prover implementations have demanded new features which were not anticipated in theory. Formalizations of KeYmaera X [5], 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 [13], 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 multiple ad-hoc extensions as they arise. To that end, this paper addresses the challenge of how best to reimagine the foundation of dL to support the features needed in practice without any ad-hoc concessions.

This paper identifies *definite descriptions* as a feature which can enrich dL with a variety of new term constructs, including the partial and discontinuous terms used in practice. We extend vanilla dL to a new dialect dL_ι with terms $\iota x\,\phi$ that denote the unique x for which ϕ holds iff there is exactly one such x. It is not surprising that partiality and continuity are pain points for dL: differential equations are the defining feature of dL, and interfacing differential equations with partial or discontinuous terms is known to require care. It is pleasantly surprising however that definite descriptions allow us to confront the questions of partiality and continuity just once and reap the benefits of many new definable term constructs. Certainly, adding definite description requires confronting continuity and partiality because many choices of $\iota x\,\phi$ do not have a unique solution x in every state, or have solutions that are not continuous as a function of the other state variables. Rather, the pleasant surprise is that existing practical extensions like divisions θ_1/θ_2, roots $\sqrt[n]{\theta}$, and the functions $\min(\theta_1,\theta_2)$, $\max(\theta_1,\theta_2)$, and $|\theta|$ are all definable from one core feature: definite description. Even better, useful *new* features like trigonometric functions are definable as well. Because vectoriality has also proven a crucial feature in practice, dL_ι also extends dL with pairs (θ,η), which enable differential equation (ODE) *systems*. Desirable new features definable from pairs include vectors and matrices, which arise frequently in physical applications. The combination of definite descriptions with pairs also gives new, general axiomatizations for existing features like differential terms $(\theta)'$. Our new axiomatization has a practical impact of future-proofing dL_ι's differential reasoning rules: when a user of dL_ι defines a new term construct, they can employ user-level proofs to build a corresponding differentiation rule, without further extensions to the dL_ι core.

The term $\iota x\,\phi$ is the definite (i.e., requiring unique existence) counterpart of Hilbert's choice

$\varepsilon x\,\phi$; both have seen success in HOL-style theorem provers [17, 27]. We chose definite $\iota x\,\phi$ over $\varepsilon x\,\phi$ because uniqueness significantly simplifies continuity and differential reasoning. In adopting definite descriptions and tuples in dL_ι, we solve the novel challenges of integrating them with differential equations, dL's distinguishing feature. Definite descriptions allow partiality, discontinuity, and nondifferentiability, all of which interact subtly with sound ODE reasoning. Multidimensional systems, enabled by tuples, demand a general treatment of differentials and expose subtle variable dependencies in some advanced ODE reasoning principles.

An example demonstrates the power of definite description: definite descriptions allow non-polynomial terms and thus non-polynomial ODEs, which need not have unique solutions. While non-polynomial ODEs (and all of dL_ι) are reducible to dL in theory, the reduction of $\iota x\,\phi$ is completely impractical, which justifies our choice to develop a calculus for proving dL_ι formulas directly. Expressiveness comes with deep semantic changes: 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 with additional definedness conditions. We develop the theory of dL_ι, show that the proof calculus is sound and show the nontrivial reduction from dL_ι to dL.

2 Syntax

We present the core syntax of dL_ι, which extends dL with definite descriptions, tuples, null-terminators, and primitive recursors. We describe the constructs informally here, deferring formal semantics to Sec. 3. As a free logic [8], dL_ι contains terms that do not denote and formulas whose truth values are unknown or uncertain (definite truth is indicated $\oplus$, definite falsehood by $\ominus$, and uncertainty by $\oslash$); this is a major point of difference between our semantics and proof calculus vs. those of dL. Our calculus uses uniform substitution [6, §35,§40], where symbols ranging over predicates, programs, etc. are explicitly represented in the syntax, because it has simplified the construction of dL calculi [24], implementations [9], and machine-checked correctness proofs [4]. This will ease implementing dL_ι and mechanizing the soundness proof in future work. The syntax of dL_ι is divided into terms, programs, and formulas, whose definitions, unlike in dL, are all mutually recursive. The terms θ (also η, ζ, γ) of dL_ι extend the terms of dL with definite descriptions, nullary and binary pairs, and reductions:

$$\theta, \eta, \zeta, \gamma \;::=\; q \mid x \mid f(\theta) \mid \theta + \eta \mid \theta \cdot \eta \mid (\theta)' \mid \iota x\,\phi \mid \;() \mid (\theta, \eta) \mid \mathsf{mr}(\theta, \eta, s\;\zeta, lr\;\gamma)$$

for literal $q \in \mathbb{Q}$ and variable $x \in \mathcal{V}$, where $\mathcal{V}$ is the (at most countable) set of all base variable names, f is a function symbol, and ϕ is a formula. The set of variables x' corresponding to each x is written $\mathcal{V}'$. The constructors novel to dL_ι are listed in red. The first six cases are as in dL: rational literals q, program variables x, uninterpreted function symbols f applied to arguments θ, sums $\theta + \eta$, products $\theta \cdot \eta$, and differentials $(\theta)'$. Variables are *flexible*: they are modified by quantifiers and programs. Variables x always denote some value and so programs which assign to variables will succeed only when the right-hand side denotes a value. 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. While most *theorem statements* could be expressed without function symbols f, they are essential

for the *axioms* of Sec. 5. 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 a value (since description is definite). Pairs (θ, η) can be nested to arbitrary finite depth, so their eliminator is primitive recursion on finite binary trees with values at the leaves and with null-terminators. When a definite description does not denote any value because it does not have a unique solution, we will write $\bot$ for its denotation. This should not be confused with a notation we will introduce in Sec. 3: $\top$ for the semantic counterpart of $()$.

The nullary tuple $()$ is primarily used as a list terminator in combination with pairs to express Lisp-style lists, which are untyped and nestable. For example the list of 1 and 2 is represented as $(1, (2, ()))$. The primitive recursor can be understood as map-reduce: $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ reduces every null terminator to η, every leaf $t \in \mathbb{R}$ to ζ_s^t, and every pair a, b of recursive results to $\gamma_l^{a\ b}{}_r$, where e_x^y is the capture-avoiding substitution of y for every x in e. We give an example of mr applied to a tree, albeit one which is not a valid (nested) list. If $\theta = ((-1, 2), -3)$, then the reduction $\mathsf{mr}(\theta, ()\,, s\ s^2, lr\ (r, l))$ is the elementwise square of the reverse tree, $(9, (4, 1))$. We remark that $\mathsf{mr}(\theta, \eta, s\,\zeta, lr\,\gamma)$ is not the only elimination construct we could have defined. We made this choice because primitive recursion supports simple arguments for termination and totality, while still enabling many common recursive operations. In Sec. 4 we will see examples of useful recursive functions. We will also see that some of the operations in Sec. 4 have more complex definitions with primitive recursors than with general recursors, but adopting general recursion would have required a much more complex treatment of partiality.

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. For any starting state, a program α might transition to zero, one, or many final states. Whenever a program transitions to zero states, we say it *aborts*.

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

Assignments $x := \theta$ assign the value of term θ to variable x, if θ denotes a value, else they abort. Tests $?\phi$ are no-ops if formula ϕ is true, else they abort execution. 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 $x' = \theta\,\&\,\psi$, which continuously evolve x according to the differential equation $x' = \theta$ for any duration such that term θ denotes and formula ψ is definitely true throughout. Note the core syntax of dL_ι need only contain systems of a single variable x: in Sec. 4 we will derive systems with multiple variables from systems of one variable. Uninterpreted program symbols a range over programs. We parenthesize programs α as $\{\alpha\}$ with braces for disambiguation and readability. dL_ι has the same formula constructors as dL, and the formulas ϕ, ψ of dL_ι are defined inductively:

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

Conjunctions $\phi \wedge \psi$, negations $\neg\phi$, and quantifiers $\forall x\,\phi$ are as in first-order Łukasiewicz [14] logic. In particular, quantifiers range only over the *existing* values because program variables,

unlike function symbols, must always denote something that exists. 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 $\theta \geq \eta$, if terms θ and η both denote reals, those reals are compared, if they both denote tuples they are compared elementwise, and a null terminator is equal only to itself. In all other cases the result is unknown ($\oslash$). 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 argument θ is allowed not to denote, and $p(\theta)$ is likewise allowed to take on the unknown truth value ($\oslash$). The unary *quantifier symbol* $C(\phi)$ is a higher-order predicate symbol which has ϕ as an argument and which binds all program variables. These are primarily used for rigorous formal contextual equivalence reasoning. We also write P, Q for nullary quantifier symbols, i.e., predicate symbols which take *all* variables as arguments. These can be defined as unary quantifier symbols with trivial arguments, i.e., $P \equiv C(\mathsf{true})$. We sometimes write the implication $\phi \to \psi$ as $\psi \leftarrow \phi$ for emphasis on ψ. The always-true and always-false formulas can be defined $\mathsf{true} \equiv 1 \geq 0$ and $\mathsf{false} \equiv 0 \geq 1$. This should not be confused with the notation we will introduce in Sec. 3: $\top$ for the semantic counterpart of `()` and $\bot$ for the denotation of a term with no value.

Our exact requirements regarding definedness may be a stumbling block on a first reading for some. However, our requirements follow a convention which is standard among free logics: flexible symbols always denote a value and range only over the existing values, while rigid symbols range also over $\bot$ for terms or $\oslash$ for formulas. The program variables x which appear in assignments and quantifiers are flexible, while symbols f, p, and C are rigid. A flexible symbol can change its value throughout a formula, while a rigid symbol does not. We will see in Sec. 5 both that rigid symbols are essential to supporting the substitution rule of our uniform substitution calculus, and also that the above convention yields natural rules for assignments and quantifiers.

Example 1 (Robot Water Cooler). A leaky bucket is a textbook example (see Hubbard [11, §4.2]) of a non-Lipschitz ODE, because a leaky bucket is described by an ODE of form $h' = k \cdot \sqrt{h}$ with constant k. In dL_ι, in contrast to dL, non-Lipschitz terms simplify describing a hybrid system with a leaky-bucket ODE. Our example hybrid system extends the leaky-bucket example with a simple discrete controller. 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:

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

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 [7], or rate 0 if the valve is closed. This control process repeats arbitrarily often. The constructs $\sqrt{2gh}$ (root) and $\frac{a}{A}$ (division) are not core dL, but we can rewrite α_B using definite descriptions:

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

This example is representative 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 will combine to make proofs about our example 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. We give an example proposition about the water cooler: the final water height of α_B never exceeds the initial height, so the cooler is *leaky* (or at least is not filling up):

Proposition 1 (Leakiness). The following formula is valid, i.e., definitely true ($\oplus$) in all states:

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

We will prove 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* [8]. We write $\bot$ for the interpretation of a term that does not denote any value, not to be confused with the trivial (i.e. unit tuple) denotation $\top$ for the nullary pair `()`. When a term denotes, it denotes a *finite, binary* tree with real values and/or terminators at the leaves. The terminator $\top$ denotes an empty tree, a scalar denotes a singleton tree, and (arbitrarily nested) pairs denote non-singleton trees. We refer to the set of all real trees as $\mathbf{Tree}(\mathbb{R})$, where for any S, $\mathbf{Tree}(S)$ is the smallest set such that: i) $\top \in \mathbf{Tree}(S)$, ii) $S \subseteq \mathbf{Tree}(S)$, and iii) for any L and $R \in \mathbf{Tree}(S)$, $(L, R) \in \mathbf{Tree}(S)$. We use variable names u and v for arbitrary elements of $\mathbf{Tree}(\mathbb{R})$, names L and R for components, and $r, s, t \in \mathbb{R} \subset \mathbf{Tree}(\mathbb{R})$. Typing is extrinsic, i.e., we do not make typing distinctions between $\mathbb{R}$ and $\mathbf{Tree}(\mathbb{R})$ in the semantics; typing constraints will be expressed explicitly as predicates. To account for non-denoting terms, formulas can take on three truth values: $\oplus$ (definitely true), $\oslash$ (unknown), and $\ominus$ (definitely false). Thus dL_ι is a *3-valued* logic, and first-order connectives use the Łukasiewicz [14] interpretation. We use the Łukasiewicz [14] interpretation both because it is standard and because it yields intuitive interpretations of conjunction, disjunction, and negation. We will sometimes write j, k for metavariables over the truth values $\oplus, \oslash, \ominus$.

The interpretation functions are parameterized by state $\omega : \mathcal{V} \to \mathbf{Tree}(\mathbb{R})$ mapping variables to values, and by an interpretation I mapping function symbols, predicate symbols, and program constants to their interpretation, including the possibility of not denoting a value. Writing $\mathcal{S}$ for the set of all states, we have

$$\begin{aligned}
I(f) &: (\mathbf{Tree}(\mathbb{R}) \cup \bot) && \to (\mathbf{Tree}(\mathbb{R}) \cup \bot) \\
I(p) &: (\mathbf{Tree}(\mathbb{R}) \cup \bot) && \to \{\oplus, \oslash, \ominus\} \\
I(C) &: (\mathcal{S} \to \{\oplus, \oslash, \ominus\}) && \to (\mathcal{S} \to \{\oplus, \oslash, \ominus\} \\
I(a) &: \wp(\mathcal{S} \times \mathcal{S})
\end{aligned}$$

where $\wp(U)$ is the power set of a set U. For a given $t \in \mathbf{Tree}(\mathbb{R})$, we write ω_x^t for the state that is equal to ω except at x, where $\omega_x^t(x) = t$.

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

$$
\begin{aligned}
I\omega[\![q]\!] &= q \quad I\omega[\![x]\!] = \omega(x) \quad I\omega[\![f(\theta)]\!] = I(f)(I\omega[\![\theta]\!]) \quad I\omega[\![\,()\,]\!] = \top \\
I\omega[\![\theta + \eta]\!] &= I\omega[\![\theta]\!] + I\omega[\![\eta]\!] \text{ if } I\omega[\![\theta]\!], I\omega[\![\eta]\!] \in \mathbb{R} \\
I\omega[\![\theta \cdot \eta]\!] &= I\omega[\![\theta]\!] \cdot I\omega[\![\eta]\!] \text{ if } I\omega[\![\theta]\!], I\omega[\![\eta]\!] \in \mathbb{R} \\
I\omega[\![\iota x\, \phi]\!] &= \begin{cases} v & \text{if a unique } v \in \mathbf{Tree}(\mathbb{R}) \text{ has } I\omega_x^v[\![\phi]\!] = \oplus \\ \bot & \text{otherwise} \end{cases} \\
I\omega[\![(\theta, \eta)]\!] &= (I\omega[\![\theta]\!], I\omega[\![\eta]\!]) \text{ if } I\omega[\![\theta]\!], I\omega[\![\eta]\!] \neq \bot \\
I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] &= \mathsf{Reduce}(I\omega[\![\theta]\!], I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega) \text{ if } I\omega[\![\theta]\!] \neq \bot \\
I\omega[\![(\theta)']\!] &= \sum_{x \in \mathcal{V}} \omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x} \text{ if } I[\![\theta]\!] \text{ totally differentiable at } \omega \\
I\omega[\![\theta]\!] &= \bot \textbf{ in all other cases}
\end{aligned}
$$

The partial application $I[\![\theta]\!]$ is a function which expects a state ω. Addition and multiplication denote sums or products when applied to two scalars, else they denote $\bot$. It is occasionally useful (Sec. 4.2) to write, e.g., $u[\![\cdot]\!]v$ for the semantic product of u by v, with dimensionality checking.

Semantics of Differential Terms In this subsection, we devote significant attention to exploring the semantics of differential terms $(\theta)'$ in detail. Compared to prior work [24], differential term semantics in dL_ι are remarkably subtle, because we must consider vector-valued functions of vector-valued inputs. Even handling the error cases grows more complicated, for example when two variables x and x' differ in shape. Our exploration begins by carefully defining the expression $\omega(x')\frac{\partial I\omega[\![\theta]\!]}{\partial x}$ from Def. 1, which is thus far an abuse of notation. When $\omega(x)$ is a tuple, we mean to say that partial derivatives are taken w.r.t. each real-number component of x, scaled by the corresponding component of x'. At a high level, because dL_ι's tuples allow vectorial terms, we wish to support vectorial differentials in our semantics. However, getting the definition just right requires care, because nested tuples can be shaped as arbitrary binary trees, and because there are several notions of vectorial differentials, each of which interacts with partiality in unique ways. This subsection is dedicated to getting these details just right.

Formally, we say a *path* d into a variable x can be either i) a path to the root of x, which is just written x, ii) the left projection $d.0$, or iii) the right projection $d.1$. Paths index the state, so that, e.g., $\omega(d.0)$ is the left projection of $\omega(d)$ assuming $\omega(d)$ is a pair. For a set of variables $S \subseteq \mathcal{V} \cup \mathcal{V}'$, we write $\mathsf{Dim}_\omega(S)$ for the set of all paths into ω which point to a leaf of some variable $x \in S$. Only returns paths which vary in the neighborhood of ω are included, i.e., $\mathsf{Dim}_\omega(S) = \{d \mid \omega(d) \in \mathbb{R}\}$. Likewise for a value v we write $\mathsf{Dim}(v) = \{d \mid v(d) \in \mathbb{R}\}$. We write $\mathsf{FV}(\theta) \subseteq \mathcal{V} \cup \mathcal{V}'$ for the

finite set of variables which influence the meaning of θ, as defined in Sec. 6.1. We can now give a precise semantics for differential terms:

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

In discussing the semantics, we also exploit a formal notion of the *shape* of a term, $\mathsf{shape}(\theta)$, which will be defined in Fig. 2 of Sec. 4, and correspondingly $\mathsf{shape}(t)$ for values t, defined as the smallest relation such that $\mathsf{shape}(I\omega[\![\theta]\!]) = I\omega[\![\mathsf{shape}(\theta)]\!]$ for all θ, I, ω. We remark on the important subtleties in this definition now, and defer additional soundness subtleties to the appendix (App. A):

- A guiding principle of our design, which will be captured in Lem. 36, is that only variables which are explicitly mentioned in an expression should influence its meaning. For this reason, it is essential that only $\mathrm{FV}(\theta)$ contributes to the sum, even if employing the syntactic notion $\mathrm{FV}(\theta)$ in a semantic definition is inelegant. In support of Lem. 36, our semantics for differential terms $(x)'$ permits that $\omega(y)$ and $\omega(y')$ differ in shape, because y is not mentioned. In contrast, if $\omega(x)$ and $\omega(x')$ differ in shape, then $I\omega[\![(x)']\!] = \bot$, as desired.

- $\mathsf{Dim}_\omega(S)$ includes even paths for which only one of $\omega(d)$ or $\omega(d')$ is defined. Thus if x and x' differ in shape for $x \in \mathrm{FV}(\theta)$, then the differential does not exist. It is only when $x \notin \mathrm{FV}(\theta)$ that x and x' are free to differ in shape. The semantics of a differential equation $x' = \theta$ will ensure x and x' have the same shape, so that this edge case does not arise in differential reasoning.

- Formally, the semantics of each differential term $(\theta)'$ can be understood as a total differential on a Euclidean space isomorphic to $\mathbb{R}^k$, where $k = |\mathsf{Dim}_\omega(\mathrm{FV}(\theta))|$. To show this isomorphism, we identify a set of variables $\{x_1, \ldots, x_n\}$ with a sequence of variables $\vec{x}$ under some canonical (e.g. alphabetical) ordering. For each $\vec{x} \subseteq \mathsf{Dom}(\omega)$ such that $\mathsf{shape}(x_i) = \mathsf{shape}(x_i')$ for all $x_i \in \vec{x}$, define $A_{\vec{x}} = \{v \mid \mathsf{shape}(v) = \mathsf{shape}(\omega(x))\} \subset \mathbf{Tree}(\mathbb{R})$, then A_x is a Euclidean space. Specifically, $A_{\vec{x}}$ is isomorphic to $\mathbb{R}^{|\mathsf{Dim}_\omega(\vec{x})|}$ under the isomorphism $f(t) = (\mathsf{Dim}_\omega(\vec{x})(1), \ldots, \mathsf{Dim}_\omega(\vec{x})(n) \mid n = |\mathsf{Dim}_\omega(\vec{x})|)$. Moreover, for any θ, we define $B_\theta = \{v \mid \mathsf{shape}(v) = \mathsf{shape}(I\omega[\![\theta]\!])\} \subset \mathbf{Tree}(\mathbb{R})$, which is a Euclidean space isomorphic to a subspace of $\mathbb{R}^{|\mathsf{Dim}_\omega(\theta)|}$. Specifically, B_θ is isomorphic to $\mathbb{R}^{|\mathsf{Dim}_\omega(\theta)|}$ under the isomorphism $f(t) = \{\mathsf{Dim}_\omega(\theta)(1), \ldots, \mathsf{Dim}_\omega(\theta)(n) \text{ s.t. } n = |\mathsf{Dim}_\omega(\theta)|\}$. In the case that θ is defined in every state, then $A_{\vec{x}} = \mathbb{R}^{|\mathsf{Dim}_\omega(\vec{x})|}$ exactly, else it is a strict subset. The set on which θ is defined must include a neighborhood of ω in order for a total differential to exist. Given these definitions, we note that $I[\![\theta]\!]$ can be restricted in the neighborhood of ω to a function from $A_{\mathrm{FV}(\theta)}$ to B_θ. Because $A_{\mathrm{FV}(\theta)}$ and B_θ are Banach and even Euclidean spaces, the notion of differentiable functions between them is well-defined.

- One notable alternative design choice would be to let the shape of a term vary throughout a differential. The main motivation would be to simplify the mathematical description of

differentials, rather than a practical motivation. It would simplify our intuition if we could say the set of all tree values *were* a Banach space *globally*, rather than each differential ranging over *some* space *locally*. Sadly, the set of all tree values simply *is not* a Banach space, thus we treat differentials locally over some Euclidean space.

$\mathbf{Tree}(\mathbb{R})$ is not a Banach space for the same reason that the eventually-zero sequence space c_{00} is not a Banach space [18]: despite being real-normed vector spaces, neither is complete. A standard counterexample for c_{00} constructs a series of eventually-zero sequences c_i where $c_{ij} = \frac{1}{j}$ for $j \leq i$ and $c_{ij} = 0$ otherwise. Every c_i is in c_{00} because only the first i elements are nonzero, but their limit is the infinite sequence $d(i) = \frac{1}{i}$ which, being infinitely non-zero, is not in c_{00}. Because c_{00} does not contain all its limits, it is not complete and thus not Banach. This example generalizes immediately to $\mathbf{Tree}(\mathbb{R})$ by embedding eventually-zero sequences into trees as finite lists. In each case, a Banach space could be constructed by taking the completion of the real-normed vector space, e.g., the completion of c_{00} is the Banach space c_0, the space of infinite sequences with finite sums. The completion of $\mathbf{Tree}(\mathbb{R})$ is a set of trees which may have infinitely many nodes, so long as all infinite series of node *values* are convergent. For example, if the i'th element of an infinite (1-indexed) list is $\frac{1}{2^i}$, we generate a list whose values sum to finite value, specifically 1. Such an approach should be possible technically, however we deem it excessively complex given its modest benefits.

In conclusion, tuples raise several crucial subtleties. We define differentials as a subtle sum over partial derivatives to account for conflicting shapes in x and x'. With tuples, we must carefully consider competing notions of differential, of which only total differentials suits our soundness needs. Previous formulations of dL [24] did not encounter such nuances because they considered scalar, smooth terms, for which different notions of differentials are interchangeable and for which x and x' are always scalar.

Reduction semantics The semantics of the primitive recursor $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ are given by an inductively-defined helper function: $I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] = \mathsf{Reduce}(I\omega[\![\theta]\!], I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega)$, (for the case $I\omega[\![\theta]\!] \neq \bot$). The helper function $\mathsf{Reduce}(u, v, s\ \theta, lr\ \eta, I\omega)$ evaluates the reduction by primitive recursion on t:

$$\begin{aligned}
\mathsf{Reduce}(\,(\,)\,, v, s\ \theta, lr\ \eta, I\omega) &= v \\
\mathsf{Reduce}(u, v, s\ \theta, lr\ \eta, I\omega) &= I\omega^u_s[\![\theta]\!] \text{ when } u \in \mathbb{R} \\
\mathsf{Reduce}((L, R), v, s\ \theta, lr\ \eta, I\omega) &= I\omega^{K\ S}_{l\ \ r}[\![\eta]\!] \text{ where} \\
&\quad K = \mathsf{Reduce}(L, v, s\ \theta, lr\ \eta, I\omega), S = \mathsf{Reduce}(R, v, s\ \theta, lr\ \eta, I\omega)
\end{aligned}$$

That is, v is returned in the base case, singleton trees u are reduced by binding s to u in θ, and nodes (L, R) are reduced by binding l, r to the reductions of the respective branches in η. The interpretation I and state ω are simply passed along and used to interpret any symbols which appear in θ or η.

Definition 2 (Formula semantics)**.** The formula semantics are 3-valued:

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

$$
\begin{aligned}
\mathsf{Geq}(\top, \top) &= \oplus \\
\mathsf{Geq}(r_1, r_2) &= (r_1 \geq r_2) \text{ if } r_1, r_2 \in \mathbb{R} \\
\mathsf{Geq}((l_1, r_1), (l_2, r_2)) &= \mathsf{Geq}(l_1, l_2) \sqcap \mathsf{Geq}(r_1, r_2) \\
\mathsf{Geq}(u, v) &= \oslash \text{ otherwise}
\end{aligned}
$$

$j \sqcap k$	$k = \oplus$	$\oslash$	$\ominus$
$j = \oplus$	$\oplus$	$\oslash$	$\ominus$
$j = \oslash$	$\oslash$	$\oslash$	$\ominus$
$j = \ominus$	$\ominus$	$\ominus$	$\ominus$

$\overline{j}$	$j = \oplus$	$\oslash$	$\ominus$
	$\ominus$	$\oslash$	$\oplus$

$j \to_{\text{Ł}} k$	$k = \oplus$	$\oslash$	$\ominus$
$j = \oplus$	$\oplus$	$\oslash$	$\ominus$
$j = \oslash$	$\oplus$	$\oplus$	$\oslash$
$j = \ominus$	$\oplus$	$\oplus$	$\oplus$

$j \leftrightarrow_{\text{Ł}} k$	$k = \oplus$	$\oslash$	$\ominus$
$j = \oplus$	$\oplus$	$\oslash$	$\ominus$
$j = \oslash$	$\oslash$	$\oplus$	$\oslash$
$j = \ominus$	$\ominus$	$\oslash$	$\oplus$

Below, let P and Q be formulas and j, k their truth values. Likewise, let θ and η be terms with denotations u, v. We sometimes write the interpretation of connectives as an infix operator, e.g., $p \to_{\text{Ł}} q$ for the interpretation of a formula $P \to Q$. This infix notation is primarily used in proofs, e.g., in Sec. 4.2. Implication $P \to Q$ is interpreted as $j \to_{\text{Ł}} k$, which can be intuited as $j \leq k$, (where $\ominus < \oslash < \oplus$) so $(j \to_{\text{Ł}} k)$ is $\oplus$ even when $j = k = \oslash$. Conjunction $P \wedge Q$ is interpreted as $j \sqcap k$, which takes the minimum value of the arguments, and is unknown $\oslash$ when the least conjunct is $\oslash$. Equivalence $P \leftrightarrow Q$ is interpreted as $j \leftrightarrow_{\text{Ł}} k$, which is reflexive (even $\oslash \leftrightarrow_{\text{Ł}} \oslash = \oplus$), but is $\oslash$ when exactly one argument is $\oslash$. We say a formula ϕ is *valid* if it is definitely-true everywhere, i.e., for all ω and I we have $I\omega[\![\phi]\!] = \oplus$. Comparisons $\theta \geq \eta$ (interpreted $\mathsf{Geq}(u, v)$) are taken elementwise and are unknown ($\oslash$) for differing shapes. Predicates p are interpreted by the interpretation I. In the interpretation of $C(\phi)$, the notation $I[\![\phi]\!]$ denotes the function which computes $I\nu[\![\phi]\!]$ for any argument ν, i.e., the interpretation of $C(\phi)$ is allowed to depend on the truth value of ϕ at each and every state ν, not just the current state ω. The meaning of quantifiers $\forall x\, \phi$ and $[\alpha]\phi$ are taken as conjunctions $\sqcap_S$ over potentially-uncountable index sets S. The value of $\sqcap_S$ is the least truth value of any conjunct under the ordering $\ominus < \oslash < \oplus$. The maximum exists over any index set S and agrees with the supremum over S because there are only three truth values. Note that $\mathsf{Geq}(u, v)$ interacts with equality in the expected way, so that $u = v$ iff $\mathsf{Geq}(u, v) \sqcap \mathsf{Geq}(v, u) = \oplus$.

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

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

$$I[\![x' = \theta \,\&\, \psi]\!] = \{(\omega,\nu) \mid \omega = \varphi(0) \text{ on } \{x'\}^{\complement} \text{ and } \nu = \varphi(r) \text{ for some } r \in \mathbb{R}_{\geq 0}, \varphi : [0,r] \to \mathcal{S}$$
$$\text{which solves } x' = \theta \,\&\, \psi, \text{ i.e., for } s \in [0,r], \frac{d\,\varphi(t)(x)}{dt}(s) = \varphi(s)(x')$$
$$\text{and } I\varphi(s)[\![x' = \theta \wedge \psi]\!] = \oplus \text{ and } \varphi(s) = \varphi(0) \text{ on } \{x,x'\}^{\complement}\}$$

where $X^{\complement}$ is the complement of set X. Assignments $x := \theta$ are strict: they store the value of θ in variable x, or abort if θ does not denote a value. Tests $?\phi$ succeed if ϕ is definitely true ($\oplus$); both the unknown ($\oslash$) and definitely false ($\ominus$) cases abort execution. 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 $I\varphi(s)[\![x' = \theta \wedge \psi]\!] = \oplus$. ODEs $x' = \theta \,\&\, \psi$ are initial value problems: $(\omega,\nu) \in I[\![x' = \theta \,\&\, \psi]\!]$ if some solution φ of some duration $r \in \mathbb{R}_{\geq 0}$ takes ω to ν while satisfying ψ throughout. A solution φ must satisfy $x' = \theta$ as an equation, satisfy constraint ψ, and assign the time-derivative of x to x'. The initial value of x' is overwritten and variables except x, x' are not changed. Note that θ may be either scalar or nonscalar: in the nonscalar case, x' matches the shape of θ and x matches the shape of x' (in ν) since $\frac{d\,\varphi(t)(x)}{dt}(s) = \varphi(s)(x')$. The initial shape of x' in ω is irrelevant since x' is overwritten. In real models, every ODE right-hand side θ is intended to have a constant shape over time. However, if the shape of θ were to change, then $x' = \theta$ will have no solution φ, i.e., $I[\![x' = \theta \,\&\, \psi]\!] = \emptyset$. The proof rules of Sec. 5 are sound even in this degenerate case.

Time differentials agree with (total) spatial differentials throughout on ODE.

Lemma 2 (Differential lemma). Let η such that $\mathrm{FV}(\theta) \subseteq \{x\}$. and let φ solve $x' = \theta \,\&\, \psi$ on $[0,r]$ for $r > 0$. Then all $s \in [0,r]$ satisfy

$$I\varphi(s)[\![(\!|\theta|\!)(\eta))']\!] = \frac{d\,\varphi(t)[\![\eta]\!]}{dt}(s)$$

Proof. Direct proof from the semantics of ODEs, following the proof of [24, Lem. 35]. □

4 Derived Constructs

A key benefit of dL_ι is extensibility: Many term constructs can be defined with definite descriptions $\iota x\,\phi$ and tuples which otherwise require unwieldy encodings as formulas. In this section we reap the benefits of extensibility by defining such new term constructs. The constructs defined in this section can be understood as a prelude or standard library for dL_ι.

4.1 Defining the Standard Library

Arithmetic Operations. In practice, we often wish to use arithmetic operations beyond the core dL operations. Fig. 1 demonstrates basic arithmetic operations which have simple definitions in dL_ι but not as terms in dL: Of these, $\max$, $\min$, and $|\cdot|$ preserve Lipschitz-continuity but not

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

Figure 1: Derived arithmetic operations (for fresh x, t, c, s, z)

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. Since pure dL requires smooth terms [24], even *functions* $\max$ and $\min$ would be encoded as formulas in pure dL.

Types and Definedness. Many of the operations in dL_ι expect, for example, reals or 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 $\mathbb{R}$. Typed quantifiers are definable, e.g., $\forall x:\mathbb{R}\ \phi \equiv \forall x\,(\mathsf{in}\mathbb{R}(x) \rightarrow \phi)$. Whether a term denotes 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:

p	$\oplus$	$\oslash$	$\ominus$
$\mathsf{D}(p)$	$\oplus$	$\ominus$	$\ominus$

$$\mathsf{D}(\phi) \equiv \neg(\phi \rightarrow \neg\phi)$$

That is, $\mathsf{D}(\phi)$ collapses $\oslash$ into $\ominus$. It is also sometimes useful (Sec. 4.2) to write $\mathsf{D}(p)$ for the truth value resulting from applying modality $\mathsf{D}(\cdot)$ to an argument with truth value p. Likewise, $\mathsf{E}(v)$ can be written for the truth value resulting from applying $\mathsf{E}(\cdot)$ to a term whose denotation is v. These constructs are used in the axioms of Sec. 5. In the same spirit, we sometimes need to know that a function $f(x)$ (of any dimension) is continuous, but derive this notion. We write $\mathsf{Con}(f(x))$ to say

that $f(x)$ is continuous as x varies around its current value:

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

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 otherwise exist.

Tuples. We make tuples first-class in dL_ι to simultaneously simplify the treatment of ODEs compared to prior work [19] and provide support for data structures such as vectors, widely used in physical computations. In contrast to the flexible function symbols (think: unbounded arrays) of QdL [21], they are equipped with a primitive recursion operator, making it easier to write sophisticated functional computations. These structures can be used in systems with non-scalar inputs, for example a robot which avoids a list of obstacles [16].

While pairs (θ, η) are core dL_ι constructs, the left and right projections $\pi_1\theta$ and $\pi_2\theta$ are derivable, as are convenience predicates $\mathsf{is}\top(\theta), \mathsf{in}\mathbb{R}(\theta)$, and $\mathsf{isP}(\theta)$ which hold exactly for `()`, for scalars, and for tuples, respectively:

$$\pi_1\theta \equiv \iota l\, \exists r\, (\theta = (l, r)) \qquad \mathsf{is}\top(\theta) \equiv \mathsf{D}(\mathsf{mr}(\theta, 0, s\ 1, lr\ 2) = 0)$$
$$\pi_2\theta \equiv \iota r\, \exists l\, (\theta = (l, r)) \qquad \mathsf{in}\mathbb{R}(\theta) \equiv \mathsf{D}(\mathsf{mr}(\theta, 0, s\ 1, lr\ 2) = 1)$$
$$\mathsf{isP}(\theta) \equiv \mathsf{D}(\mathsf{mr}(\theta, 0, s\ 1, lr\ 2) = 2)$$

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. Lists are represented as right-nested pairs, i.e., trees whose left-projections are never pairs and whose rightmost projection is `()`. We name an argument J, K, L, to indicate its intended use as a list rather than an arbitrary tree. We write M, N for arguments which are intended to be matrices, which are column-major. Note that $(L \times M)$ is vector-matrix multiplication, with L understood as a row vector on the left.

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

$$\{x_1'{=}\theta,\ x_2'{=}\eta\} \ \equiv\ \big(z := (x_1, x_2);\ \{z' = (\theta_{x_j}^{\pi_j z}, \eta_{x_j}^{\pi_j z})\};\ x_1 := \pi_1 z;\ x_2 := \pi_2 z\big)$$

While this encoding is simple, it will enable us in Sec. 5 to support systems of any finite dimension in axiom DG, which implementation experience [9] has shown challenging due to the variable dependencies involved.

4.2 Correctness of the Standard Library

In Sec. 4.1 we defined a standard library of useful constructs in dL_ι. In the present section, we give formal specifications for each construct and prove that the definitions satisfy their specifications. The constructs in our library are common in standard libraries of functional programming

$$
\begin{aligned}
\mathsf{map2}(T, f(x,y)) &= \mathsf{mr}(T,\ (\,)\,, s\ s, lr\ \mathsf{if}(\mathsf{size}(l) = 2)(f(\pi_1 l, \pi_1\pi_2 r), r)\mathsf{else}(l, r)) \\
\mathsf{snoc}(L, x) &= \mathsf{mr}(L, (x,\ (\,)\,), s\ s, lr\ (l, r)) \\
\mathsf{rev}(L) &= \mathsf{mr}(L,\ (\,)\,, s\ s, lr\ \mathsf{snoc}(r, l)) \\
\mathsf{zip}(K, L) &= \pi_2\mathsf{mr}(K, (\mathsf{rev}(L),\ (\,)\,), s\ s, lr\ (\pi_2\pi_1 r, ((l, \pi_1\pi_1 r), \pi_2 r))) \\
\left(K \vec{+} L\right) &= \mathsf{map2}(\mathsf{zip}(K, L), x + y) \\
(K \vec{*} L) &= \mathsf{map2}(\mathsf{zip}(K, L), x \cdot y) \\
K \cdot L &= \mathsf{mr}((K \vec{*} L)\,, 0, s\ s, lr\ l + r) \\
\|L\| &= \sqrt{L \cdot L} \\
\left(K \vec{-} L\right) &= \mathsf{map}(\mathsf{zip}(K, L), \pi_1 x - \pi_2 x) \\
\mathsf{mapc}(M, f(x)) &= \mathsf{mr}(M,\ (\,)\,, s\ s, lr\ \mathsf{if}(\mathsf{in}\mathbb{R}(l))(l, r)\mathsf{else}(f(l), r)) \\
(L \times M) &= \mathsf{mapc}(M, x \cdot L) \\
\mathsf{shape}(T) &= \mathsf{mr}(T, 0, s\ 1, lr\ (l, r)) \\
\mathsf{size}(T) &= \mathsf{mr}(T, 0, s\ 1, lr\ l + r) \\
\mathsf{depth}(T) &= \mathsf{mr}(T, 0, s\ 1, lr\ \max(l, r) + 1) \\
\mathsf{islist}(T) &= (\mathsf{mr}(T, 0, s\ 1, lr\ 1 + r) = \mathsf{size}(T))
\end{aligned}
$$

Figure 2: Example vector and tree functions

languages and in linear algebra libraries. Therefore, some readers may find their specifications standard or their proofs repetitive. However, we provide this section of the report in the interest of comprehensiveness. A few constructs such as $\mathsf{zip}(K, L)$ also have nonstandard proofs because they are implemented with primitive recursion instead of the general recursion which is typical in functional programming languages. Where we have used nonstandard definitions, detailed proofs provide an extra level of confidence.

In this section, it is convenient to use the notation $[x_1, \ldots, x_n] \equiv (x_1, (\cdots, (x_n, ())))$ for the list consisting of scalars x_i, or $\{\!|T_1, \ldots, T_n|\!\} \equiv (T_1, (\cdots, (T_n, ())))$ for a list consisting of T_i which might not be scalars. We also use the word *vector* to refer to nonempty scalar lists, and *matrix* to refer to nonempty rectangular lists of vectors, i.e., a matrix is not empty and does not contain the empty list, and each inner list has identical length, containing only scalars.

Because we are proving the correctness of *derived* constructs, we can employ both semantic proof approaches and syntactic proof approaches using the dL_ι calculus (Sec. 5). In a software implementation, syntactic proof would be preferred in order to minimize the amount of trusted code. Because these are paper proofs and we wish for this section to stand alone from Sec. 5, we primarily use semantic proof, only presenting the proofs in a syntactic style when it poses a readability advantage.

Typing. Below, fix a term θ, state ω, and interpretation I. In every theorem statement of this section, let $v = I\omega[\![\theta]\!]$.

Proposition 3 (Definite truth). If $I\omega[\![\phi]\!] = \oplus$ then $I\omega[\![\mathsf{D}(\phi)]\!] = \oplus$, else $I\omega[\![\mathsf{D}(\phi)]\!] = \ominus$.

Proof. By cases on $I\omega[\![\phi]\!]$.

Case $\oplus$: $I\omega[\![\mathsf{D}(\phi)]\!] = I\omega[\![\neg(\phi \to \neg\phi)]\!] = \overline{\oplus \to_{Ł} \overline{\oplus}} = \overline{\oplus \to_{Ł} \ominus} = \overline{\ominus} = \oplus$

Case $\oslash$: $I\omega[\![\mathsf{D}(\phi)]\!] = I\omega[\![\neg(\phi \to \neg\phi)]\!] = \overline{\oslash \to_{Ł} \overline{\oslash}} = \overline{\oslash \to_{Ł} \oslash} = \overline{\oplus} = \ominus$

Case $\ominus$: $I\omega[\![\mathsf{D}(\phi)]\!] = I\omega[\![\neg(\phi \to \neg\phi)]\!] = \overline{\ominus \to_{Ł} \overline{\ominus}} = \overline{\ominus \to_{Ł} \oplus} = \overline{\oplus} = \ominus$

In each case $\mathsf{D}(\phi)$ has the desired truth value by calculation. □

Proposition 4 (Type inspectors). Recall $v = I\omega[\![\theta]\!]$, then exactly one of the following holds:

- $v = \bot$, $I\omega[\![\mathsf{E}(\theta)]\!] = \ominus$, and $I\omega[\![\mathsf{is}\top(\theta)]\!] = I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!] = I\omega[\![\mathsf{isP}(\theta)]\!] = \oslash$.
- $v = \top$ and $I\omega[\![\mathsf{is}\top(\theta)]\!] = I\omega[\![\mathsf{E}(\theta)]\!] = \oplus$ while $I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!] = I\omega[\![\mathsf{isP}(\theta)]\!] = \ominus$.
- $v \in \mathbb{R}$ and $I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!] = I\omega[\![\mathsf{E}(\theta)]\!] = \oplus$ while $I\omega[\![\mathsf{is}\top(\theta)]\!] = I\omega[\![\mathsf{isP}(\theta)]\!] = \ominus$.
- $v = (L, R)$ and $I\omega[\![\mathsf{isP}(\theta)]\!] = I\omega[\![\mathsf{E}(\theta)]\!] = \oplus$ while $I\omega[\![\mathsf{is}\top(\theta)]\!] = I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!] = \ominus$.

Proof. By cases on v.

First case: $v = \bot$, then $I\omega[\![\mathsf{E}(\theta)]\!] = I\omega[\![\mathsf{D}(\theta = \theta)]\!] = I\omega[\![\neg(\theta = \theta \to \neg(\theta = \theta))]\!] = \overline{I\omega[\![\theta = \theta \to \neg(\theta = \theta)]\!]} = \overline{I\omega[\![\theta = \theta]\!] \to_{Ł} \overline{I\omega[\![(\theta = \theta)]\!]}}$. Then since $v = \bot$, we have $I\omega[\![\theta = \theta]\!] = \mathsf{Geq}(v, v) \sqcap \mathsf{Geq}(v, v) = \oslash$. Then $\overline{I\omega[\![\theta = \theta]\!] \to_{Ł} \overline{I\omega[\![(\theta = \theta)]\!]}} = \overline{\oslash \to_{Ł} \overline{\oslash}} = \overline{\oslash \to_{Ł} \oslash} = \overline{\oplus} = \ominus$ as desired.

We show the second subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{is}\top(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=0)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\bot,0,s\ 1,lr\ 2,I\omega)=0)\\
=&\mathsf{D}(\bot=0)\\
=&\mathsf{D}(\mathsf{Geq}(\bot,0)\sqcap\mathsf{Geq}(0,\bot))\\
=&\mathsf{D}(\oslash)=\ominus.
\end{aligned}$$

We show the third subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=1)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\bot,0,s\ 1,lr\ 2,I\omega)=1)\\
=&\mathsf{D}(\bot=1)\\
=&\mathsf{D}(\mathsf{Geq}(\bot,1)\sqcap\mathsf{Geq}(1,\bot))\\
=&\mathsf{D}(\oslash)=\ominus.
\end{aligned}$$

We show the fourth subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{isP}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=2)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\bot,0,s\ 1,lr\ 2,I\omega)=2)\\
=&\mathsf{D}(\bot=2)\\
=&\mathsf{D}(\mathsf{Geq}(\bot,2)\sqcap\mathsf{Geq}(2,\bot))\\
=&\mathsf{D}(\oslash)=\ominus
\end{aligned}$$

Second case: $v=\top$, then $I\omega[\![\mathsf{E}(\theta)]\!]=I\omega[\![\mathsf{D}(\theta=\theta)]\!]=I\omega[\![\neg(\theta=\theta\to\neg(\theta=\theta))]\!]=\overline{I\omega[\![\theta=\theta\to\neg(\theta=\theta)]\!]}=I\omega[\![\theta=\theta]\!]\to_{\text{Ł}}\overline{I\omega[\![(\theta=\theta)]\!]}$. Then since $v=\top$, we have $I\omega[\![\theta=\theta]\!]=\mathsf{Geq}(v,v)\sqcap\mathsf{Geq}(v,v)=\oplus$. Then $I\omega[\![\theta=\theta]\!]\to_{\text{Ł}}\overline{I\omega[\![(\theta=\theta)]\!]}=\oplus\to_{\text{Ł}}\overline{\oplus}=\oplus\to_{\text{Ł}}\ominus=\overline{\ominus}=\oplus$ as desired.

We show the second subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{is}\top(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=0)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\top,0,s\ 1,lr\ 2,I\omega)=0)\\
=&\mathsf{D}(0=0)\\
=&\mathsf{D}(\mathsf{Geq}(0,0)\sqcap\mathsf{Geq}(0,0))\\
=&\mathsf{D}(\oplus)=\oplus.
\end{aligned}$$

We show the third subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=1)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\top,0,s\ 1,lr\ 2,I\omega)=1)\\
=&\mathsf{D}(0=1)\\
=&\mathsf{D}(\mathsf{Geq}(0,1)\sqcap\mathsf{Geq}(1,0))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

We show the fourth subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{isP}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=2)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(\top,0,s\ 1,lr\ 2,I\omega)=2)\\
=&\mathsf{D}(0=2)\\
=&\mathsf{D}(\mathsf{Geq}(0,2)\sqcap\mathsf{Geq}(2,0))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

Third case: $v\in\mathbb{R}$, then $I\omega[\![\mathsf{E}(\theta)]\!]=I\omega[\![\mathsf{D}(\theta=\theta)]\!]=I\omega[\![\neg(\theta=\theta\to\neg(\theta=\theta))]\!]=\overline{I\omega[\![\theta=\theta\to\neg(\theta=\theta)]\!]}=\overline{I\omega[\![\theta=\theta]\!]\to_{\text{Ł}}\overline{I\omega[\![(\theta=\theta)]\!]}}$. Then since $v\in\mathbb{R}$, we have $I\omega[\![\theta=\theta]\!]=\mathsf{Geq}(v,v)\sqcap\mathsf{Geq}(v,v)=\oplus$. Then $\overline{I\omega[\![\theta=\theta]\!]\to_{\text{Ł}}\overline{I\omega[\![(\theta=\theta)]\!]}}=\overline{\oplus\to_{\text{Ł}}\overline{\oplus}}=\overline{\oplus\to_{\text{Ł}}\ominus}=\overline{\ominus}=\oplus$ as desired.

We show the second subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{is}\top(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=0)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=0)\\
=&\mathsf{D}(1=0)\\
=&\mathsf{D}(\mathsf{Geq}(1,0)\sqcap\mathsf{Geq}(0,1))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

We show the third subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=1)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=1)\\
=&\mathsf{D}(1=1)\\
=&\mathsf{D}(\mathsf{Geq}(1,1)\sqcap\mathsf{Geq}(1,1))\\
=&\mathsf{D}(\oplus)=\oplus.
\end{aligned}$$

We show the fourth subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{isP}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=2)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=2)\\
=&\mathsf{D}(1=2)\\
=&\mathsf{D}(\mathsf{Geq}(1,2)\sqcap\mathsf{Geq}(2,1))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

Fourth case: $v = (L, R)$, then $I\omega[\![\mathsf{E}(\theta)]\!] = I\omega[\![\mathsf{D}(\theta = \theta)]\!] = I\omega[\![\neg(\theta = \theta \to \neg(\theta = \theta))]\!] = \overline{I\omega[\![\theta = \theta \to \neg(\theta = \theta)]\!]} = \overline{I\omega[\![\theta = \theta]\!] \to_{\text{Ł}} \overline{I\omega[\![(\theta = \theta)]\!]}}$. Then since $v = (L, R)$, and since $\mathsf{Geq}(v, v) = \mathsf{Geq}(L, L) \sqcap \mathsf{Geq}(R, R) = \oplus \sqcap \oplus = \oplus$ then we have $I\omega[\![\theta = \theta]\!] = \mathsf{Geq}(v, v) \sqcap \mathsf{Geq}(v, v) = \oplus$. Then $\overline{I\omega[\![\theta = \theta]\!] \to_{\text{Ł}} \overline{I\omega[\![(\theta = \theta)]\!]}} = \overline{\oplus \to_{\text{Ł}} \overline{\oplus}} = \overline{\oplus \to_{\text{Ł}} \ominus} = \overline{\ominus} = \oplus$ as desired.

We show the second subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{is}\top(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=0)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=0)\\
=&\mathsf{D}(2=0)\\
=&\mathsf{D}(\mathsf{Geq}(2,0)\sqcap\mathsf{Geq}(0,2))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

We show the third subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{in}\mathbb{R}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=1)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=1)\\
=&\mathsf{D}(2=1)\\
=&\mathsf{D}(\mathsf{Geq}(2,1)\sqcap\mathsf{Geq}(1,2))\\
=&\mathsf{D}(\ominus)=\ominus.
\end{aligned}$$

We show the fourth subcase:

$$\begin{aligned}
&I\omega[\![\mathsf{isP}(\theta)]\!]\\
=&I\omega[\![\mathsf{D}(\mathsf{mr}(\theta,0,s\ 1,lr\ 2)=2)]\!]\\
=&\mathsf{D}(\mathsf{Reduce}(v,0,s\ 1,lr\ 2,I\omega)=2)\\
=&\mathsf{D}(2=2)\\
=&\mathsf{D}(\mathsf{Geq}(2,2)\sqcap\mathsf{Geq}(2,2))\\
=&\mathsf{D}(\oplus)=\oplus.
\end{aligned}$$

□

Proposition 5 (Projections). Recall $v = I\omega[\![\theta]\!]$. If v has shape (L, R), then $I\omega[\![\pi_1\theta]\!] = L$ and $I\omega[\![\pi_2\theta]\!] = R$, else $I\omega[\![\pi_1\theta]\!] = I\omega[\![\pi_2\theta]\!] = \bot$.

Proof. First note (1) $I\omega[\![\pi_1\theta]\!]$ is the unique $L \in \mathbf{Tree}(\mathbb{R})$ s.t. there exists $R \in \mathbf{Tree}(\mathbb{R})$ s.t. $v = (L, R)$, if unique such L exists. Likewise (2) $I\omega[\![\pi_2\theta]\!]$ is the unique $R \in \mathbf{Tree}(\mathbb{R})$ s.t. there exists $L \in \mathbf{Tree}(\mathbb{R})$ s.t. $v = (L, R)$, if unique such R exists. These facts follow directly by expanding the definitions of $\pi_1\theta$ and $\pi_2\theta$ then expanding the semantics.

We finish the proof by cases on u.

If $v = \bot, v = \top$, or $v \in \mathbb{R}$, then $I\omega[\![\pi_1\theta]\!] = I\omega[\![\pi_2\theta]\!] = \bot$ since the descriptions (1) and (2) have no solutions. Else $v = (L, R)$, then (1) and (2) have L and R as their unique solutions respectively, as desired. □

Proposition 6 (Typed quantifiers). The typed quantifiers obey the equations:

- $I\omega[\![\forall x : \mathbb{R}\ \phi]\!] = \bigsqcap_{v\in\mathbb{R}} I\omega_x^v[\![\phi]\!]$
- $I\omega[\![\exists x : \mathbb{R}\ \phi]\!] = \bigsqcup_{v\in\mathbb{R}} I\omega_x^v[\![\phi]\!]$

Proof. Direct proof. $I\omega[\![\forall x : \mathbb{R}\ \phi]\!] = I\omega[\![\forall x\,(\mathsf{in}\mathbb{R}(x) \to \phi)]\!] = \bigsqcap_{v\in\mathbf{Tree}(\mathbb{R})} I\omega_x^v[\![\mathsf{in}\mathbb{R}(x) \to \phi]\!] =^* \bigsqcap_{v\in\mathbb{R}} I\omega_x^v[\![\phi]\!]$ as desired. The step marked (*) uses the semantics of implication and the fact that $I\omega[\![\mathsf{in}\mathbb{R}(x)]\!] \neq \oslash$ always (Prop. 4).

Likewise, $I\omega[\![\exists x : \mathbb{R}\ \phi]\!] = I\omega[\![\exists x\,(\mathsf{in}\mathbb{R}(x) \wedge \phi)]\!] = \bigsqcup_{v\in\mathbf{Tree}(\mathbb{R})} I\omega_x^v[\![\mathsf{in}\mathbb{R}(x) \wedge \phi]\!] =^* \bigsqcup_{v\in\mathbb{R}} I\omega_x^v[\![\phi]\!]$ as desired. The step marked (*) again uses $I\omega[\![\mathsf{in}\mathbb{R}(x)]\!] \neq \oslash$ (Prop. 4). □

Proposition 7 (Continuity). If $I\omega[\![\mathsf{Con}(f(x))]\!] = \oplus$ then the function $y : \mathbf{Tree}(\mathbb{R}) \mapsto I\omega[\![f(y)]\!]$ is continuous in some neighborhood of $y = x$, else $I\omega[\![\mathsf{Con}(f(x))]\!] = \ominus$.

Proof. Throughout, we consider F which maps every $y : \mathbf{Tree}(\mathbb{R})$ to $I\omega[\![f(y)]\!]$. By Prop. 4, $\mathsf{Con}(f(x)) \neq \oslash$. Formally, the notion of function continuity can be defined for functions between any two metric spaces. As in Sec. 3, we note that the value space $\mathbf{Tree}(\mathbb{R})$ behaves locally as some $\mathbb{R}^k$ when the shape of a tree is fixed. It suffices to show F is (locally) a continuous function between two Euclidean subspaces of $\mathbb{R}^k$ which we call A_x (satisfying $A_x \subseteq \mathbf{Tree}(\mathbb{R})$) and $B_{f(x)}$, again borrowing the notation of Sec. 3. Specifically, $v \in A_x$ iff $\mathsf{shape}(v) = \mathsf{shape}(\omega(x))$ and $v \in B_{f(x)}$ iff $\mathsf{shape}(v) = \mathsf{shape}(I(f)(\omega(x)))$.

Note that in the below, $\mathcal{N}_\xi(\omega(x)) = \{\omega_x^v \mid \|v - \omega(x)\| < \xi\}$. To show local continuity, we show:

- There exists an open ball $\mathcal{N}_\xi(\omega(x))$ of size $\xi > 0$ centered on $\omega(x)$ for which $\mathcal{N}_\xi(\omega(x)) \subseteq A_x$ and the image $F(\mathcal{N}_\xi(\omega(x)))$ of $\mathcal{N}_\xi(\omega(x))$ under F is a subset $F(\mathcal{N}_\xi(\omega(x))) \subseteq B_{f(x)}$.
- The restriction F_ξ of F to $\mathcal{N}_\xi(\omega(x))$ is continuous, i.e., according to the delta-epsilon definition of continuity between metric spaces under the Euclidean metric.

We now show that the definition (0) of $\mathsf{Con}(f(x))$ is equivalent the conjunction of (1) and (2).

First show (0) implies (1) and (2). Assume x and f are such that $I\omega[\![\forall\xi > 0\,\exists\delta > 0\,\forall y\,(0 < \|y - x\| < \delta \wedge \|f(y) - f(x)\| < \xi)]\!] = \oplus$. Then by expanding the semantics, we have for all $\xi > 0$

there exists $\delta > 0$ such that for all y where $\|y - \omega(x)\| \in (0, \delta)$ then $\|I(f)(y) - I(f)(\omega(x))\| < \xi$. To show (1), consider any $\xi > 0$ then fix some $\delta > 0$ where $\forall y\,(0 < \|y - \omega(x)\| < \delta \rightarrow \|I(f)(y) - I(f)(\omega(x))\| < \xi)$. Then $\mathcal{N}_\delta(\omega(x))$ is the desired neighborhood since $\mathcal{N}_\delta(\omega(x)) \subseteq A_x$ and $F(\mathcal{N}_\delta(\omega(x))) \subseteq B_{f(x)}$. Since the norms $\|y - x\|$ and $\|f(y) - f(x)\|$ exist it follows that y has the same shape as x and $f(y)$ the same shape as $f(x)$: the difference of two terms which differ in shape is undefined. Then (2) also holds since $\mathsf{Con}(f(x))$ implies $\lim_{y \to x} f(y) = x$ for y in $\mathcal{N}_\delta(\omega(x))$.

Then show First show (1) and (2) implies (0). In the converse direction, assume x and f such that $I\omega[\![\forall \xi > 0\, \exists \delta > 0\, \forall y\,(0 < \|y - x\| < \delta \wedge \|f(y) - f(x)\| < \xi)]\!] = \ominus \neq \oplus$ (truth value $\oslash$ cannot arise). Then by de Morgan's law, there exists $\xi > 0$ such that for all $\delta > 0$ there exists y such that $\|y - x\| \in (0, \delta)$ where $\|f(y) - f(x)\| < \xi$. Then the limit $\lim_{y \to x} f(y) = x$ does not exist, that is the limits as y approaches x from *each* direction do not exist or do not equal each other, thus f is not continuous at x. □

Arithmetic.

Proposition 8 (Conditional terms). If $I\omega[\![\phi]\!] = \oplus$ then $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = I\omega[\![\theta]\!]$, else if $I\omega[\![\phi]\!] = \ominus$ then $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = I\omega[\![\eta]\!]$, else $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = \bot$.

Proof. Below, we assume x is fresh w.r.t. to ϕ, θ, and η. By the semantics, $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!]$ is the unique $v \in \mathbf{Tree}(\mathbb{R})$ such that $(I\omega^v_x[\![\phi]\!] \sqcap I\omega^v_x[\![x = \theta]\!]) \sqcup (\overline{I\omega^v_x[\![\phi]\!]} \sqcap I\omega^v_x[\![x = \eta]\!]) = \oplus$, which is the unique v such that $(I\omega^v_x[\![\phi]\!] \sqcap I\omega^v_x[\![x = \theta]\!]) = \oplus$ or $(\overline{I\omega^v_x[\![\phi]\!]} \sqcap I\omega^v_x[\![x = \eta]\!]) = \oplus$ (assuming there exists a unique such v). This is the unique v such that $I\omega^v_x[\![\phi]\!] = I\omega^v_x[\![x = \theta]\!] = \oplus$ or $\overline{I\omega^v_x[\![\phi]\!]} = I\omega^v_x[\![x = \eta]\!] = \oplus$.

We proceed by cases on $I\omega^v_x[\![\phi]\!]$, which by Lem. 36 equals $I\omega[\![\phi]\!]$, and seek a unique solution v to the above definite description in each case:

$\oplus$: then by case, have $I\omega^v_x[\![\phi]\!] = \oplus$. Let $v = I\omega[\![\theta]\!] = I\omega^v_x[\![\theta]\!]$ (by Lem. 36). Then if $v \neq \bot$, we have that v is a solution to $I\omega^v_x[\![x = \theta]\!] = \oplus$ by reflexivity. It is trivially the unique such solution as desired. Else $v = \bot$ so $I\omega^v_x[\![x = \theta]\!] = \oslash$. There is no solution v to the definite description so that $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = \bot$, but in this case $I\omega[\![\theta]\!] = \bot$ anyway so $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = I\omega[\![\theta]\!]$ regardless as desired.

$\oslash$: then by case, have $I\omega^v_x[\![\phi]\!] = \oslash = \overline{I\omega^v_x[\![\phi]\!]}$. Since neither $I\omega^v_x[\![\phi]\!] = \oplus$ nor $\overline{I\omega^v_x[\![\phi]\!] = \oplus}$ then the description has no solution. Then $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = \bot$ as desired.

$\ominus$: then by case, have $I\omega^v_x[\![\phi]\!] = \ominus$, i.e., $\overline{I\omega^v_x[\![\phi]\!]} = \oplus$. Let $v = I\omega[\![\eta]\!] = I\omega^v_x[\![\eta]\!]$. Then if $v \neq \bot$, we have that v is a solution to $I\omega^v_x[\![x = \eta]\!] = \oplus$ by reflexivity. It is trivially the unique such solution as desired. Else $v = \bot$ so $I\omega^v_x[\![x = \eta]\!] = \oslash$. There is no solution v to the definite description so that $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = \bot$, but in this case $I\omega[\![\eta]\!] = \bot$ anyway so $I\omega[\![\mathsf{if}(\phi)(\theta)\mathsf{else}(\eta)]\!] = I\omega[\![\eta]\!]$ regardless as desired. □

Proposition 9 (Five-function arithmetic). If $I\omega[\![\theta]\!] \in \mathbb{R}_{\geq 0}$ then $I\omega[\![\sqrt{\theta}]\!] = \sqrt{I\omega[\![\theta]\!]}$, else $I\omega[\![\sqrt{\theta}]\!] = \bot$. If $I\omega[\![\eta]\!] \in \mathbb{R} \setminus \{0\}$ and $I\omega[\![\theta]\!] \in \mathbb{R}$ then $I\omega[\![\theta/\eta]\!] = I\omega[\![\theta]\!]/I\omega[\![\eta]\!]$, else $I\omega[\![\theta/\eta]\!] = \bot$.

Proof. In the first case for $\sqrt{\theta}$, let $r = I\omega[\![\theta]\!] \in \mathbb{R}_{\geq 0}$. Then we need $I\omega[\![\sqrt{\theta}]\!]$ to be some unique v such that $I\omega^t_x[\![x \geq 0 \wedge x \cdot x = \theta]\!] = \oplus$, equivalently some unique $v \in \mathbb{R}$ s.t. $v > 0$ and $v^2 = I\omega[\![\theta]\!]$.

Now let $v = \sqrt{r}$ which is a solution and a unique one. It is a solution because $r \geq 0$ has a square root, because $(\sqrt{r})^2 = r$, and $\sqrt{r} \geq 0$ necessarily. It is the unique solution because the only other solution of $v^2 = r$ is $-\sqrt{r}$, which is not a solution of $v \geq 0$ except at $v = 0$ where $v = -v$ anyway.

In the second case for $\sqrt{\theta}$, let $r = I\omega[\![\theta]\!] \notin \mathbb{R}_{\geq 0}$. Then there is no solution v such that $I\omega^v_x[\![x \geq 0 \wedge x \cdot x = \theta]\!] = \oplus$. Assume for the sake of contradiction such a v exists, then $\mathsf{Geq}(v, 0) = \ominus$ so $v \in \mathbb{R}_{\geq 0}$ but then $v^2 = r \in \mathbb{R}_{\geq 0}$ contradicting $r \notin \mathbb{R}_{\geq 0}$.

In the first case for θ/η, let $r = I\omega[\![\theta]\!] \in \mathbb{R}$ and $s = I\omega[\![\eta]\!] \in \mathbb{R} \setminus \{0\}$. We need $I\omega[\![\theta/\eta]\!]$ to be some unique v such that $I\omega^v_x[\![x \cdot \eta{=}\theta]\!] = \oplus$, i.e., (by Lem. 36) such that $v[\![\cdot]\!]s = r$. Since $r, s \in \mathbb{R}$ it suffices that $vs = r$. Now let $v = r/s$ and since $s \neq 0$ by gradeschool algebra v is a solution. It is unique, also by gradeschool algebra.

In the second case for θ/η, let $r = I\omega[\![\theta]\!] \notin \mathbb{R}$ or $s = I\omega[\![\eta]\!] \notin \mathbb{R} \setminus \{0\}$. If either $r \notin \mathbb{R}$ or $s \notin \mathbb{R}$ then $v[\![\cdot]\!]s = \bot$ so that $I\omega^v_x[\![x \cdot \eta{=}\theta]\!] = \oslash$, thus $I\omega[\![\theta/\eta]\!] = \bot$ as desired. Otherwise $r \in \mathbb{R}$ but $s = 0$. If $r = 0$ as well then *every* $v \in \mathbb{R}$ is a solution $vs = r$, else when $r \neq 0$ then $v \cdot 0 = r$ has no solution. In either case there is no *unique* solution v so in both cases $I\omega[\![\theta/\eta]\!] = \bot$ as desired. □

Proposition 10 (Extremum functions). If $I\omega[\![\theta]\!] = \bot$ or $I\omega[\![\eta]\!]$ are $\bot$ or differ in shape then $I\omega[\![\max(\theta, \eta)]\!] = I\omega[\![\min(\theta, \eta)]\!] = \bot$. If $I\omega[\![\theta]\!] = \bot$ then additionally $I\omega[\![|\theta|]\!] = \bot$. Else $I\omega[\![\max(\theta, \eta)]\!] = \max(I\omega[\![\theta]\!], I\omega[\![\eta]\!])$ and $I\omega[\![\min(\theta, \eta)]\!] = \min(I\omega[\![\theta]\!], I\omega[\![\eta]\!])$ and $I\omega[\![|\theta|]\!] = |I\omega[\![\theta]\!]|$. In the case that θ and η have the same nonscalar shape, the extremum of a pair is a pair of the extrema of the components.

Proof. By cases. Case $\theta = \bot$ (or $\eta = \bot$ for $\max$ and $\min$). Let v stand for the solution of the definite description, if a unique such solution exists. $I\omega^v_x[\![\theta \geq \eta]\!] = I\omega^v_x[\![\eta \geq \theta]\!] = I\omega^v_x[\![x = \theta]\!] = I\omega^v_x[\![x = \eta]\!] = \oslash$. By calculation $I\omega[\![\max(\theta, \eta)]\!] = I\omega[\![\min(\theta, \eta)]\!] = I\omega[\![|\theta|]\!] = \bot$.

Case $\mathsf{shape}(I\omega[\![\theta]\!]) \neq \mathsf{shape}(I\omega[\![\eta]\!])$: Let v stand for the solution of the definite description, if a unique such solution exists. Then still $I\omega^v_x[\![\theta \geq \eta]\!] = I\omega^v_x[\![\eta \geq \theta]\!] = \oslash$ so both disjuncts are $\oslash$ (or possibly $\ominus$) so there is no solution v where $(\theta \geq \eta \wedge x = \theta) \vee (\eta \geq \theta \wedge x = \eta)$ for $\max$ or where $(\theta \geq \eta \wedge x = \eta) \vee (\eta \geq \theta \wedge x = \theta)$ for $\min$, thus $I\omega[\![\max(\theta, \eta)]\!] = I\omega[\![\min(\theta, \eta)]\!] = \bot$ as desired.

Case $\mathsf{shape}(I\omega[\![\theta]\!]) = \mathsf{shape}(I\omega[\![\eta]\!])$: Proceed by subcases for each function, letting $L = I\omega[\![\theta]\!]$ and $R = I\omega[\![\eta]\!]$. For max, let $v = \max(L, R)$ (we write $\max(L, R)$ for componentwise maximum, likewise for $\min(L, R)$ and $|L|$). If $L \geq R$ then $v = L$ so the left disjunct is satisfied $I\omega^v_x[\![\theta \geq \eta \wedge x = \theta]\!]$. The solution is unique by $x = \theta$. Else $L \geq R$ and $v = R$ and right disjunct is satisfied uniquely: $I\omega^v_x[\![\eta \geq \theta \wedge x = \eta]\!] = \oplus$. For min, let $v = \min(L, R)$. If $L \geq R$ then $v = R$ so the left disjunct is satisfied $I\omega^v_x[\![\theta \geq \eta \wedge x = \eta]\!]$. The solution is unique by $x = \eta$. Else $R \geq L$ and $v = L$ and right disjunct is satisfied uniquely: $I\omega^v_x[\![\eta \geq \theta \wedge x = \theta]\!] = \oplus$. For absolute value, let $v = |L| = \max(L, -L)$, then the result follows from the case for $\max$. □

Proposition 11 (Trig. functions). If $I\omega[\![\theta]\!] \in \mathbb{R}_{\geq 0}$ then $I\omega[\![\sin\theta]\!] = \sin I\omega[\![\theta]\!]$ and $I\omega[\![\cos\theta]\!] = \cos I\omega[\![\theta]\!]$.

We assume $\theta \geq 0$ because it simplifies the definitions of $\sin$ and $\cos$. If desired, this assumption can be removed by prefixing the program $z := \theta;\ \{z := z + 2\pi\}^*;\ ?0 \leq z$ to the ODE in the definition of $(\sin, \cos)$ and testing $z{=}\theta$ rather than $t{=}\theta$. Note such a loop is nondeterministic

because multiple positive solutions exist, but all such solutions are congruent modulo 2π and thus have the same sine and cosine.

Proof. We wish to show that $v = (\sin\theta, \cos\theta)$ is the unique value such that we have the equality $I\omega_z^v[\![t := 0; s := 0; c := 1; s'{=}c, c'{=}{-}s, t'{=}1; ?t{=}\theta]z{=}(s,c)]\!] = \oplus$. We abbreviate $\mu = \omega_{z\ t\ s\ c}^{v\ 0\ 0\ 0}$. Now by assignment semantics it suffices to show $v = (\sin I\omega[\![\theta]\!], \cos I\omega[\![\theta]\!])$ is the unique solution of $I\mu[\![s'{=}c, c'{=}{-}s, t'{=}1; ?t{=}\theta]z{=}(s,c)]\!] = \oplus$, i.e., the unique v such that for all $(\mu,\nu) \in I[\![s'{=}c, c'{=}{-}s, t'{=}1]\!]$, if $I\nu[\![?t{=}\theta]\!] = \oplus$ (i.e., $\nu(t) = I\nu[\![\theta]\!]$) then $I\nu[\![z{=}(s,c)]\!] = \oplus$ (i.e., $\nu(z) = (\nu(s), \nu(c))$. By ODE semantics, $(\mu,\nu) \in I[\![s'{=}c, c'{=}{-}s, t'{=}1]\!]$ iff there is some $r \in \mathbb{R}$ and $\varphi : [0,r]$ such that φ solves $s'{=}c, c'{=}{-}s, t'{=}1$ and $\omega = \varphi(0)$ on $\{x'\}^{\complement}$ $\nu = \varphi(r)$. Since the ODE $s'{=}c, c'{=}{-}s, t'{=}1$ is linear, there is even a unique such φ. Specifically, we can define φ by $\varphi(r)(t) = r, \varphi(r)(c) = \cos r, \varphi(r)(s) = \sin r, \varphi(r)(z) = \mu(z)$. We check that our φ is indeed a solution. The initial conditions hold: $\varphi(0)(t) = 0 = \mu(t), \varphi(0)(c) = \cos 0 = 1 = \mu(c), \varphi(0)(s) = \sin 0 = 0 = \mu(s), \varphi(0)(z) = \mu(z) = v$. The ODE is satisfied because $\frac{\partial\varphi(r)(s)}{\partial r} = \varphi(r)(c)$ and $\frac{\partial\varphi(r)(c)}{\partial r} = -\varphi(r)(s)$ (a direct result of the differentiation laws for sine and cosine) and $\frac{\partial\varphi(r)(t)}{\partial r} = 1$. Of the possible durations r, it suffices by the test $?t{=}\theta$ to consider only those where $\nu(t) = I\nu[\![\theta]\!] = I\omega[\![\theta]\!]$ (by Lem. 36 and the assumption that c, s, t, z are fresh). Thus it suffices to consider only $\nu = \varphi(I\omega[\![\theta]\!]) = \omega_t^{I\omega[\![\theta]\!]}{}_c^{\cos I\omega[\![\theta]\!]}{}_s^{\sin I\omega[\![\theta]\!]}{}_z^{v}$. Specifically, for v to be a solution, it suffices to ensure $I\nu[\![z{=}(s,c)]\!]$ or equivalently $v = (\sin I\omega[\![\theta]\!], \cos I\omega[\![\theta]\!])$. This is exactly the solution we chose for v. It is the *unique* solution because equality formulas $I\nu[\![z{=}(s,c)]\!]$ hold for unique values of z only. □

Data structures. In this section, we specify and verify our operations on vectors and matrices. Because the terms that appear here are comparatively large, we knowingly blur the lines between syntax and semantics for the sake of readability. Specifically, if we say that $\theta = \eta$ is a theorem, we mean that $I\omega[\![\theta]\!] = I\omega[\![\eta]\!]$ for all I and ω.

Proposition 12 (map2). Assume T is a list of 2-element lists $T = \{\!|[x_1,y_1], \ldots, [x_n,y_n]|\!\}$. Then $\mathsf{map2}(T, f(x,y)) = \{\!|f(x_1,y_1), \ldots, f(x_n,y_n)|\!\}$.

Proof. By induction on n.

Case $n = 0$ then $T = \texttt{()}$ and

$$\begin{aligned}&\mathsf{map2}(T, f)\\ =&\mathsf{mr}(T, \texttt{()}, s\ s, lr\ \mathsf{if}(\mathsf{size}(l) = 2)(f(\pi_1 l, \pi_1\pi_2 r), r)\mathsf{else}(l,r))\\ =&\texttt{()}.\end{aligned}$$

Case $n = k+1$ then $T = \{\!|[x_1,y_1], \ldots, [x_n,y_n]|\!\} = ([x_1,y_1], \{\!|[x_2,y_2], \ldots, [x_n,y_n]|\!\})$. Then

$$
\begin{aligned}
&\mathsf{map2}(T, f)\\
=&\mathsf{mr}(T,\ \texttt{()}\ , s\ s, lr\ \mathsf{if}(\mathsf{size}(l) = 2)(f(\pi_1 l, \pi_1\pi_2 r), r)\mathsf{else}(l, r))\\
=&\mathsf{if}(\mathsf{size}(\mathsf{map2}([x_1, y_1], f)) = 2)(f(\pi_1 l, \pi_1\pi_2 r), \mathsf{map2}(\{\!|[x_2, y_2], \ldots, [x_n, y_n]|\!\}, f))\mathsf{else}(l, r)\\
=&\mathsf{if}(\mathsf{size}([x_1, y_1]) = 2)(f(\pi_1[x_1, y_1], \pi_1\pi_2[x_1, y_1]), \mathsf{map2}(\{\!|[x_2, y_2], \ldots, [x_n, y_n]|\!\}, f))\mathsf{else}(l, r)\\
=&((f(\pi_1[x_1, y_1], \pi_1\pi_2[x_1, y_1]), \mathsf{map2}(\{\!|[x_2, y_2], \ldots, [x_n, y_n]|\!\}, f))\\
=&(f(x_1, y_1), \mathsf{map2}(\{\!|[x_2, y_2], \ldots, [x_n, y_n]|\!\}, f))\\
\overset{=}{\text{IH}}&(f(x_1, y_1), \{\!|f(x_2, y_2), \ldots, f(x_n, y_n)|\!\})\\
=&\{\!|f(x_1, y_1), \ldots, f(x_n, y_n)|\!\}.
\end{aligned}
$$

□

Proposition 13 (snoc). $\mathsf{snoc}([x_1, \ldots, x_n], y) = [x_1, \ldots, x_n, y]$

Proof. By induction on n.
Case $n = 0$ then $\mathsf{snoc}(\texttt{()}, y) = \mathsf{mr}(\texttt{()}, (y,\ \texttt{()}), s\ s, lr\ (l, r)) = (y,\ \texttt{()}) = [y]$ as desired.
Case $n = k + 1$ then

$$
\begin{aligned}
&\mathsf{snoc}([x_1, \ldots, x_n], y)\\
=&\mathsf{mr}([x_1, \ldots, x_n], (y,\ \texttt{()}), s\ s, lr\ (l, r))\\
=&(x_1, \mathsf{mr}([x_2, \ldots, x_n], (y,\ \texttt{()}), s\ s, lr\ (l, r)))\\
=&(x_1, [x_2, \ldots, x_n, y])\\
=&[x_1, \ldots, x_n, y].
\end{aligned}
$$

□

Proposition 14 (Reverse). $\mathsf{rev}([x_1, \ldots, x_n]) = [x_n, \ldots, x_1]$

Proof. By induction on n.
Case $n = 0$ then $\mathsf{rev}(\texttt{()}) = \mathsf{mr}(\texttt{()}, \texttt{()}, s\ s, lr\ \mathsf{snoc}(r, l)) = \texttt{()}$ as desired.
Case $n = k + 1$ then

$$
\begin{aligned}
&\mathsf{rev}([x_1, \ldots, x_n])\\
=&\mathsf{mr}([x_1, \ldots, x_n],\ \texttt{()}, s\ s, lr\ \mathsf{snoc}(r, l))\\
=&\mathsf{snoc}(\mathsf{rev}([x_2, \ldots, x_n]), x_1)\\
=&\mathsf{snoc}([x_n, \ldots, x_2], x_1)\\
=&[x_n, \ldots, x_1].
\end{aligned}
$$

□

Proposition 15 (zip). $\mathsf{zip}([x_1, \ldots, x_n], [y_1, \ldots, y_n]) = \{\!|[x_1, y_1], \ldots, [x_n, y_n]|\!\}$

Proof. Recall that zip is defined by:

$$\mathsf{zip}(K, L) = \pi_2\mathsf{mr}(K, (\mathsf{rev}(L), \texttt{()}), s\ s, lr\ (\pi_2\pi_1 r, ((l, \pi_1\pi_1 r), \pi_2 r)))$$

We write $\mathsf{zip'}([x_1, \ldots, x_n], [y_1, \ldots, y_n], k)$ for the $k'th$ intermediate step of the main reduction, i.e., $f(x_{n-k+1}, \ldots, f(x_n, ([y_n, \ldots, y_1], \texttt{()})))$ where $f(l, r) = (\pi_2\pi_1 r, ((l, \pi_1\pi_1 r), \pi_2 r))$ By induction on n we show $\mathsf{zip'}([x_1, \ldots, x_n], [y_1, \ldots, y_n], k) = ([y_{n-k}, \ldots, y_1], \{\!|[x_{n-k+1}, y_{n-k+1}], [x_n, y_n]|\!\})$. Setting $k = n$ yields $\mathsf{zip'}([x_1, \ldots, x_n], [y_1, \ldots, y_n], n) = (\texttt{()}, \{\!|[x_1, y_1], [x_n, y_n]|\!\})$, then the theorem follows directly from the "obvious" (i.e., we do not bother presenting a proof) property $\mathsf{zip}([x_1, \ldots, x_n], [y_1, \ldots, y_n]) = \pi_2\mathsf{zip'}(x_1, \ldots, x_n, y_1, \ldots, y_n, n)$.

Case $k = 0$ then

$$\begin{aligned}
&\mathsf{zip'}([x_1, \ldots, x_n], [y_1, \ldots, y_n], 0)\\
=&([y_n, \ldots, y_1], \texttt{()})\\
=&([y_{n-k}, \ldots, y_1], \{\!|[x_{n-k+1}, y_{n-k+1}], [x_n, y_n]|\!\})
\end{aligned}$$

since $\{\!|[x_{n-k+1}, y_{n-k+1}], [x_n, y_n]|\!\} = \{\!|[x_{n+1}, y_{n+1}], [x_n, y_n]|\!\} = \texttt{()}$.

Case $k = j + 1$ then

$$\begin{aligned}
&\mathsf{zip'}([x_1, \ldots, x_n], [y_1, \ldots, y_n], j+1)\\
=&f(x_{n-k+1}, \ldots, f(x_n, ([y_n, \ldots, y_1], \texttt{()})))\\
=&f(x_{n-j}, f(x_{n-j+1}, \ldots, f(x_n, ([y_n, \ldots, y_1], \texttt{()}))))\\
=&f(x_{n-j}, ([y_{n-j}, \ldots, y_1], \{\!|[x_{n-j+1}, y_{n-j+1}], [x_n, y_n]|\!\})\\
=&([y_{n-(j+1)}, \ldots, y_1], \{\!|[x_{n-j}, y_{n-j}], [x_n, y_n]|\!\})
\end{aligned}$$

as desired. □

Proposition 16 (Vector addition). $\left([x_1, \ldots, x_n] \vec{+} [y_1, \ldots, y_n]\right) = [x_1 + y_1, \ldots, x_n + y_n]$

Proof. By direct proof and Prop. 12:

$$\begin{aligned}
&\left([x_1, \ldots, x_n] \vec{+} [y_1, \ldots, y_n]\right)\\
=&[f(x_1, y_1), \ldots, f(x_n, y_n)](\text{for } f(x, y) = x + y)\\
=&[x_1 + y_1, \ldots, x_n + y_n].
\end{aligned}$$

□

Proposition 17 (Vector subtraction). $\left([x_1, \ldots, x_n] \vec{-} [y_1, \ldots, y_n]\right) = [x_1 - y_1, \ldots, x_n - y_n]$

Proof. By direct proof and Prop. 12:

$$\begin{aligned}
&\left([x_1, \ldots, x_n] \vec{-} [y_1, \ldots, y_n]\right)\\
=&[f(x_1, y_1), \ldots, f(x_n, y_n)](\text{for } f(x, y) = x - y)\\
=&[x_1 - y_1, \ldots, x_n - y_n].
\end{aligned}$$

□

Proposition 18 (Vector elementwise multiplication). $([x_1, \ldots, x_n]\vec{*}[y_1, \ldots, y_n]) = [x_1 y_1, \ldots, x_n y_n]$

Proof. By direct proof and Prop. 12:

$$\begin{aligned}&([x_1, \ldots, x_n]\vec{*}[y_1, \ldots, y_n])\\ =&[f(x_1, y_1), \ldots, f(x_n, y_n)](\text{for } f(x, y) = xy)\\ =&[x_1 y_1, \ldots, x_n y_n].\end{aligned}$$

□

Proposition 19 (Dot product). $[x_1, \ldots, x_n] \cdot [y_1, \ldots, y_n] = x_1 y_1 + \cdots + x_n y_n$

Proof. Start by applying Prop. 18:

$$\begin{aligned}&[x_1, \ldots, x_n] \cdot [y_1, \ldots, y_n]\\ =&\mathsf{mr}(([x_1, \ldots, x_n]\vec{*}[y_1, \ldots, y_n]), 0, s\ s, lr\ l + r)\\ =&\mathsf{mr}([x_1 y_1, \ldots, x_n y_n], 0, s\ s, lr\ l + r)\\ =&[x_1 y_1, \ldots, x_n y_n].\end{aligned}$$

To finish the proof, show $\mathsf{mr}([x_1 y_1, \ldots, x_n y_n], 0, s\ s, lr\ l + r) = x_1 y_1 + \cdots + x_n y_n$ by induction:
Case $n = 0$ then $\mathsf{mr}(\texttt{()}, 0, s\ s, lr\ l + r) = 0$.
Case $n = k + 1$ then

$$\begin{aligned}&\mathsf{mr}([x_1 y_1, \ldots, x_n y_n], 0, s\ s, lr\ l + r)\\ =&x_1 y_1 + \mathsf{mr}([x_2 y_2, \ldots, x_n y_n], 0, s\ s, lr\ l + r)\\ =&x_1 y_1 + (x_2 y_2 + \cdots + x_n y_n)\\ =&x_1 y_1 + \cdots + x_n y_n.\end{aligned}$$

□

Proposition 20 (Matrix map). We have that $\mathsf{mapc}(M, f(x)) = \{\!|f(c_1), \ldots, f(c_n)|\!\}$ for all matrices $M = \{\!|c_1, \ldots, c_n|\!\}$.

Proof. By two inductions, first for the columns and then the matrix. By convention we write $m \times n$ for the dimensions of M. We write x_{ij} for the i'th row, j'th column, e.g., $c_j = [x_{1j}, \ldots, x_{mj}]$ since matrices are column-major.

We write $\text{mred}(M)$ for the reduction $\mathsf{mr}(M, \texttt{()}, s\ s, lr\ \mathsf{if}(\mathsf{in}\mathbb{R}(l))(l, r)\mathsf{else}(f(l), r))$ applied to list or matrix M. First for arbitrary $j \in [1, n]$ we show by induction on $k \in [0, m-1]$ that $\text{mred}([c_{j(n-k+1)}], \ldots, c_{jn}) = [c_{j(n-k+1)}, \ldots, c_{jn}]$.

Base case $k = 0$: then $\text{mred}(\texttt{()}) = \texttt{()}$ as desired.

Base case $k > 0$: then

$$\begin{aligned}
&\mathsf{mred}([c_{j(n-k+1)}], \ldots, c_{jn}) \\
=&\mathsf{if}(\mathsf{in}\mathbb{R}(c_{j(n-k+1)}))(c_{j(n-k+1)}, \mathsf{mred}([c_{j(n-k+2)}], \ldots, c_{jn})) \\
&\mathsf{else}(f(c_{j(n-k+1)}), \mathsf{mred}([c_{j(n-k+2)}], \ldots, c_{jn})) \\
=&(c_{j(n-k+1)}, \mathsf{mred}([c_{j(n-k+2)}, \ldots, c_{jn}])) \\
=&(c_{j(n-k+1)}, [c_{j(n-k+2)}, \ldots, c_{jn}]) \\
=&[c_{j(n-k+1)}, \ldots, c_{jn}]
\end{aligned}$$

So letting $k = n$ we get $\mathsf{mred}(c_j) = c_j$.

We now use a second induction to show for arbitrary $k \in [0, n-1]$ that $\mathsf{mred}(\{\!|c_{n-k+1}, \ldots, c_n|\!\}) = \{\!|f(c_{n-k+1}), \ldots, f(c_n)|\!\}$.

Base case $k = 0$: then $\mathsf{mred}(\texttt{()}) = \texttt{()}$.

Base case $k > 0$: then

$$\begin{aligned}
&\mathsf{mred}(\{\!|c_{n-k+1}, \ldots, c_n|\!\}) \\
=&\mathsf{if}(\mathsf{in}\mathbb{R}(\mathsf{mred}(c_{n-k+1})))(\mathsf{mred}(c_{n-k+1}), \mathsf{mred}(\{\!|c_{n-k+2}, \ldots, c_n|\!\})) \\
&\mathsf{else}(f(\mathsf{mred}(c_{n-k+1})), \mathsf{mred}(\{\!|c_{n-k+2}, \ldots, c_n|\!\})) \\
=&(f(\mathsf{mred}(c_{n-k+1})), \mathsf{mred}(\{\!|c_{n-k+2}, \ldots, c_n|\!\})) \\
=&(f(c_{n-k+1}), \mathsf{mred}(\{\!|c_{n-k+2}, \ldots, c_n|\!\})) \\
=&(f(c_{n-k+1}), \{\!|f(c_{n-k+2}), \ldots, f(c_n)|\!\}) \\
=&\{\!|f(c_{n-k+1}), \ldots, f(c_n)|\!\}).
\end{aligned}$$

using the previous result $\mathsf{mred}(c_j) = c_j$ for all j. Now plugging in $k = n$ again, we get $\mathsf{mred}(\{\!|c_1, \ldots, c_n|\!\}) = \{\!|f(c_1), \ldots, f(c_n)|\!\}$, i.e., $\mathsf{mapc}(M, f(x)) = \{\!|f(c_1), \ldots, f(c_n)|\!\}$ as desired. □

Proposition 21 (Row-matrix multiplication). Let L be a row vector and M be a matrix of compatible dimension, then $(L \times M)$ is the matrix product LM, i.e., the result of matrix multiplication where L is treated as a one-row matrix.

Proof. Let $m \times n$ be the dimension of M and m be the dimension of L. Then $M = \{\!|c_1, \ldots, c_n|\!\}$ for some columns c_j. Then $(L \times M) = \mathsf{mapc}(M, x \cdot L) = \mathsf{mapc}(\{\!|c_1, \ldots, c_n|\!\}, x \cdot L)$. Then by Prop. 20 we have $(L \times M) = \{\!|c_1 \cdot L, \ldots, c_n \cdot L|\!\}$ which is the definition of row-matrix product. □

Proposition 22 (Shape). Function $\mathsf{shape}(\theta)$ captures the shape of term θ while ignoring its elements. That is, $\mathsf{shape}(\theta) = \mathsf{shape}(\eta)$ iff θ and η have the same shape, regardless of their elements. Formally we say $I\omega[\![\mathsf{shape}(\theta)]\!] = \mathsf{shape}(I\omega[\![\theta]\!])$ where we inductively define $\mathsf{shape}(v)$ (for $v \in \mathbf{Tree}(\mathbb{R}) \cup \{\bot\}$) as:

- $\mathsf{shape}(\bot) = \bot$
- $\mathsf{shape}(\top) = 0$

- For $v \in \mathbb{R}$, then $\mathsf{shape}(v) = 1$
- For $v = (L, R)$ then $\mathsf{shape}(v) = (\mathsf{shape}(L), \mathsf{shape}(R))$

Proof. By induction on v, with $I\omega[\![\theta]\!] = v$.
Case $v = \bot$ then $I\omega[\![\mathsf{shape}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ (l, r))]\!] = \bot = \mathsf{shape}(\bot)$ as desired.
Case $v = \top$ then $I\omega[\![\mathsf{shape}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ (l, r))]\!] = I\omega[\![0]\!] = 0 = \mathsf{shape}(\top)$ as desired.
Case $v \in \mathbb{R}$ then $I\omega[\![\mathsf{shape}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ (l, r))]\!] = I\omega[\![1]\!] = 1 = \mathsf{shape}(v)$.
Case $v = (L, R)$ then

$$\begin{aligned}
& I\omega[\![\mathsf{shape}(\theta)]\!] \\
=& I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ (l, r))]\!] \\
=& (\mathsf{mr}(\pi_1\theta, 0, s\ 1, lr\ (l, r)), \mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ (l, r))) \\
=& (\mathsf{shape}(L), \mathsf{shape}(R)) \\
=& \mathsf{shape}((L, R)) = \mathsf{shape}(v).
\end{aligned}$$

□

Proposition 23 (Size). The function $\mathsf{size}(\theta)$ computes the number of elements in θ. Formally we say $I\omega[\![\mathsf{size}(\theta)]\!] = \mathsf{size}(I\omega[\![\theta]\!])$ where we define $\mathsf{size}(v)$ inductively by:

- $\mathsf{size}(\bot) = \bot$
- $\mathsf{size}(\top) = 0$
- For $v \in \mathbb{R}$, then $\mathsf{size}(v) = 1$
- For $v = (L, R)$ then $\mathsf{size}((L, R)) = \mathsf{size}(L) + \mathsf{size}(R)$

Proof. By induction on v.
Case $v = \bot$ then $I\omega[\![\mathsf{size}(\bot)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ l + r)]\!] = \bot$ as desired.
Case $v = \top$ then $I\omega[\![\mathsf{size}(\top)]\!] = I\omega[\![\mathsf{mr}(\,(\,), 0, s\ 1, lr\ l + r)]\!] = I\omega[\![0]\!] = 0$ as desired.
Case $v \in \mathbb{R}$ then $I\omega[\![\mathsf{size}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ l + r)]\!] = I\omega[\![1]\!] = 1$ as desired.
Case $v = (L, R)$ then $I\omega[\![\mathsf{size}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ l + r)]\!] = I\omega[\![\mathsf{mr}(\pi_1\theta, 0, s\ 1, lr\ l + r)]\!] + I\omega[\![\mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ l + r)]\!] = \mathsf{size}(L) + \mathsf{size}(R)$. □

Proposition 24 (Depth). The function $\mathsf{depth}(\theta)$ computes the longest root-to-leaf path in θ. Formally we say $I\omega[\![\mathsf{depth}(\theta)]\!] = \mathsf{depth}(I\omega[\![\theta]\!])$, where we define $\mathsf{depth}(v)$ inductively by:

- $\mathsf{depth}(\bot) = \bot$
- $\mathsf{depth}(\top) = 0$
- If $v \in \mathbb{R}$ then $\mathsf{depth}(v) = 1$

- If $v = (L, R)$ then $\mathsf{depth}(v) = \max(\mathsf{depth}(L), \mathsf{depth}(R)) + 1$

Proof. By induction on v.
Case $\bot$ then $I\omega[\![\mathsf{depth}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ \max(l, r) + 1)]\!] = \bot$.
Case $\top$ then $I\omega[\![\mathsf{depth}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ \max(l, r) + 1)]\!] = I\omega[\![0]\!] = 0$.
Case $v \in \mathbb{R}$ then $I\omega[\![\mathsf{depth}(\theta)]\!] = I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ \max(l, r) + 1)]\!] = I\omega[\![1]\!] = 1$.
Case $v = (L, R)$ then

$$\begin{aligned}
&I\omega[\![\mathsf{depth}(\theta)]\!] \\
=&I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ \max(l, r) + 1)]\!] \\
=&I\omega[\![1 + \max(\mathsf{depth}(\pi_1\theta), \mathsf{depth}(\pi_2\theta))]\!] \\
=&1 + \max(\mathsf{depth}(L), \mathsf{depth}(R)) \\
=&\mathsf{depth}(v)
\end{aligned}$$

by Prop. 10 as desired. □

Proposition 25 (Is-list). If $I\omega[\![\theta]\!]$ is of form $[x_1, \ldots, x_n]$ then $I\omega[\![\mathsf{islist}(\theta)]\!] = \oplus$, else if $I\omega[\![\theta]\!] = \bot$ then $I\omega[\![\mathsf{islist}(\theta)]\!] = \oslash$, else $I\omega[\![\mathsf{islist}(\theta)]\!] = \ominus$.

Proof. By cases, induction on n and using Prop. 23.
Case $I\omega[\![\theta]\!] = \bot$, then $I\omega[\![\mathsf{islist}(\theta)]\!] = I\omega[\![\mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ 1 + r)]\!]$.
Case $I\omega[\![\theta]\!]$ is of form $[x_1, \ldots, x_n]$: Show $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] = I\omega[\![\mathsf{size}(\theta)]\!] \neq \bot$.
Subcase $n = 0$ and $I\omega[\![\theta]\!] = \top$ then $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1{+}r)]\!] = 0 = \mathsf{size}(\top) = I\omega[\![\mathsf{size}(\ ()\ )]\!]$.
Subcase $n = k + 1$ and $I\omega[\![\theta]\!] = [x_1, \ldots, x_n]$ then

$$\begin{aligned}
&I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] \\
=&I\omega[\![1 + \mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ 1 + r)]\!] \\
=&1 + I\omega[\![\mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ 1 + r)]\!] \\
=&1 + (\mathsf{size}(\pi_2\theta)) \\
=&1 + (\mathsf{size}([x_2, \ldots, x_n])) \\
=&\mathsf{size}(x_1, \ldots, x_n) \\
=&I\omega[\![\mathsf{size}(\theta)]\!].
\end{aligned}$$

Case $I\omega[\![\theta]\!] \in \mathbf{Tree}(\mathbb{R})$ not of form $[x_1, \ldots, x_n]$: We show $I\omega[\![\mathsf{islist}(\theta)]\!] = \ominus$ by showing $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] \neq I\omega[\![\mathsf{size}(\theta)]\!]$. We show this by assuming (C) $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] = I\omega[\![\mathsf{size}(\theta)]\!]$ and deriving a contradiction. The contradiction proceeds by induction on $I\omega[\![\theta]\!]$.

Case $\top$ or $\mathbb{R}$ then θ is a list, which contradicts the outer case.

Case (L, R) then either (a) $L = \top$ or (b) $L \in \mathbb{R}$ and (c) R is not a list. In case (a) we can assume without loss of generality R is a list. In case (a) then $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] = 1 + I\omega[\![\mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ 1 + r)]\!] = 1 + I\omega[\![\mathsf{size}(\pi_2\theta)]\!] = 1 + I\omega[\![\mathsf{size}(\pi_2\theta)]\!]$ contradicting $I\omega[\![\mathsf{size}(\theta)]\!] = I\omega[\![\mathsf{size}(\pi_2\theta)]\!]$ since $L = \top$.

In case (b) then $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] = 1 + I\omega[\![\mathsf{mr}(\pi_2\theta, 0, s\ 1, lr\ 1 + r)]\!] \neq 1 + I\omega[\![\mathsf{size}(\pi_2\theta)]\!] = I\omega[\![\mathsf{size}(\theta)]\!]$ so by transitivity $I\omega[\![\mathsf{mr}(\theta, 0, s\ 1, lr\ 1 + r)]\!] \neq I\omega[\![\mathsf{size}(\theta)]\!]$ which contradicts (C) as desired. □

Proposition 26 (Euclidean norm). If $I\omega[\![\theta]\!] = [x_1, \ldots, x_n]$ then $I\omega[\![||\theta||]\!] = \sqrt{\sum_{i\in[1,n]} x^2}$.

Proof. Direct proof. Assume $I\omega[\![\theta]\!] = [x_1, \ldots, x_n]$ then $I\omega[\![||\theta||]\!] = I\omega[\![\sqrt{\theta \cdot \theta}]\!] =^* \sqrt{I\omega[\![\theta \cdot \theta]\!]} = \sqrt{\sum_{i\in[1,n]} x^2}$. Step (*) is by Prop. 9 and because $\theta \cdot \theta$ is necessarily nonnegative. □

5 dL$_\iota$ 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 [24][6, §35,§40]: from the validity of ϕ we can conclude validity of $\sigma(\phi)$ where the uniform substitution σ specifies concrete replacements for some or all predicates, functions, and program constants in a formula ϕ:

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

The soundness side-conditions to US about σ are non-trivial, and make up much of its 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 soundness proof of the US rule, and every axiom, which is now an individual concrete dL$_\iota$ 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 [24] for dL to account for non-denoting terms and unknown formulas. Axioms are augmented with definedness conditions whenever multiple occurrences of terms or formulas differ in their tolerance for partiality. The conclusion (in canonical usage) of each axiom is highlighted in blue, while any difference from the dL axioms is highlighted in red. 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 requires the inductive step proved definitely true $\oplus$, but also concludes definite truth. This is necessitated by the subtle semantics of Łukasiewicz implication: two unknown tvm propositions can definitely $\oplus$ imply each other, which is only compatible with repeated applications of the inductive step if we ensure definite truth at each step. 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 ($\mathsf{E}(f())$). Assignments [:=] require the assigned term to denote a value, since program variables x range over values.

Fig. 4 gives the dL$_\iota$ generalizations of dL's axioms for reasoning about differential equations. Interfacing ODEs with partial, discontinuous, or vectorial terms is an important contribution of dL$_\iota$, and we now show that only modest changes are required for ODE axioms, in contrast to the complete rethinking of differential terms. The smooth generalization of ODE axioms owes largely

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

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

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

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

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

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

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

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

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

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

V $p \to [a]p$

G $\dfrac{P}{[a]P}$

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

MP $\dfrac{P \to Q \quad P}{Q}$

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

Figure 3: Discrete dL axioms

DW $[x' = f(x)\&q(x)]q(x)$

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

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

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

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

DS $\big(\forall t : \mathbb{R}\, ((\forall 0 \leq s \leq t\, q(x + f()s)) \to [x := x + f()t]p(x))\big) \to [x' = f()\,\&\,q(x)]p(x)$

$(\theta)'$ $(f(x))' = x' \cdot (\iota M\, \forall \xi > 0\, \exists \delta > 0\, \forall y\, \mathsf{D}(0 < \|y - \vec{x}\| < \delta$
$\quad \to f(y) - f(x) - \big((y - \vec{x}) \cdot M\big) < \xi \|y - \vec{x}\|))$
$\quad \leftarrow \mathsf{in}\mathbb{R}((f(x))') \wedge \mathsf{islist}((x)')$

$\mathsf{E}(')$ $\mathsf{E}((f(x))') \leftarrow \mathsf{E}(x' \cdot (\iota M\, \forall \xi > 0\, \exists \delta > 0\, \forall y\, \mathsf{D}(0 < \|y - \vec{x}\| < \delta)$
$\quad \to f(y) - f(x) - \big((y - \vec{x}) \cdot M\big) < \xi \|y - \vec{x}\|))$

Figure 4: Differential equation axioms and differential axioms

to the modal nature of dynamic logic reasoning: a user of dL_ι might write an ill-behaved ODE where no solution exists for any duration, but axioms such as DC and DW hold vacuously in this case, because they *maintain* the presence or absence of solutions. While $\text{DI}_{\geq}$ is written identically to the corresponding axiom in dL, this is simply because we already confronted the challenges of differential induction reasoning when we defined a new semantics for differential terms in Sec. 3. Of all the ODE axioms, changes appear most explicitly in DG: not all dL_ι terms are continuous, so an explicit assumption ensures continuity throughout the domain constraint. DC is generalized by analogy to $[?]$ to require definite truth and DG is generalized to require continuity, otherwise the axioms carry over unchanged. DW says the domain constraint of an ODE always holds as a postcondition. DC says any postcondition which is proven (definitely) true may be added to the domain constraint. DE says the ODE holds as an equation in the postcondition. $\text{DI}_{\geq}$ is the *differential induction* [20] 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 $\text{DI}_{\geq}$ hold only when $f(x)$ and $g(x)$ are *totally* differentiable within the domain constraint, as required for soundness. DG allows extending a system with an additional ghost dimension, and is used for everything from solving systems to reasoning about exponentially-decaying systems [26]. The new dimension is required to be continuous in existing variables so that solutions exist and is required to be linear in the new variables so that the solutions of the extended system exist as long as those of the initial system. DS says the solution of a constant ODE system is linear. To solve multidimensional systems with DS, interpret $x + f()s$ and $x + f()t$ using pairwise vector sums and products per Fig. 2. Axiom $(\theta)'$ expands a differential $(f(x))'$ according to the definition of total differential. Axiom $(\theta)'$ is clearly long-winded which is not desired for practical proving. However, our design goal for $(\theta)'$ was not to be directly useful in proofs, but to provide future-proofing if users wish to define new term constructs. In contrast to previous axiomatizations [24], $(\theta)'$ expresses differential terms in full generality, so that a user-friendly rule for each construct can be derived from $(\theta)'$, without expanding the list of core axioms. To demonstrate this ability, we use $(\theta)'$ to derive differentiation axioms for the vanilla dL terms in Ex. 2. Rule $(\theta)'$ assumes $\mathsf{E}((f(x))')$ because equalities are not allowed to hold between non-denoting terms; proving the existence assumption is enabled by axiom $\mathsf{E}(')$. In $\mathsf{E}(')$, proving the existence of $(f(x))'$ enables proving the existence of any term which depends on a single variable that need not be scalar. In practice, axioms are derived from $\mathsf{E}(')$ for each case and applied recursively to automatically prove existence, for example:

$$\mathsf{E}((f(x))') \land \mathsf{E}((g(x))') \to \mathsf{E}(((f+g)(x))')$$

is used to show differentials of sums exist. The definition of $(\theta)'$ above is specialized to real-valued x and $f(x)$, because scalar differences $f(y) - f(x)$ and $y - x$ only denote a value when $x, y, f(x)$, and $f(y)$ are reals. We now generalize it to vectorial differentials.

Vector differentials. The semantics of differential terms given in Def. 2 apply equally well to terms of any shape. However, axiomatizing differential terms is a separate challenge from defining their semantics, and is harder in the general case than in the scalar case. Axioms $(\theta)'$ and $\mathsf{E}(')$

were introduced in the conference version [3] of this work, and only implement the differentials of scalar terms. Even in the scalar case, the summation from Def. 2 is nuanced, and axiom $(\theta)'$ must find a way to express it within the limitations of dL_ι syntax. For the sake of keeping a small, clean core language of dL_ι terms, we wish to express differentials using only the existing primitive recursion construct $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ and functions defined from it, rather than general recursion. In this section, we show that $(\theta)'$ and $\mathsf{E}(')$ can be generalized to vectorial axioms $(\theta)'$s and $\mathsf{E}(')$s. The main change required for vectors is to employ vector subtraction $\left(\theta \vec{-} \eta\right)$, vector pairwise multiplication $(\theta \vec{*} \eta)$, and vector-matrix multiplication $(L \times M)$ of which dot product $\theta \cdot \theta$ is a special case.

$$
\begin{array}{ll}
 & (f(x))' = x' \vec{*} (\iota M \, \forall \xi \, \|\xi > 0\| \to \exists \delta > 0 \, \forall y \, \mathsf{D}(0 < \|y \vec{-} x\| < \delta \\
(\theta)'\text{s} & \quad \to f(y) \vec{-} f(x) \vec{-} \left(y \vec{-} x\right) \times M < \xi \vec{*} \left(y \vec{-} x\right)) \\
 & \quad \leftarrow \mathsf{islist}((f(x))') \wedge \mathsf{islist}((x)')) \\
\mathsf{E}(')\text{s} & \mathsf{E}((f(x))') \leftarrow \mathsf{E}(x' \vec{*} (\iota M \, \forall \xi \, \|\xi > 0\| \to \exists \delta \, \forall y \, \mathsf{D}(0 < \|y \vec{-} x\| < \delta \\
 & \quad \to f(y) \vec{-} f(x) \vec{-} \left(y \vec{-} x\right) \times M < \xi \vec{*} \left(y \vec{-} x\right)))))
\end{array}
$$

The semantic definition goes even further and supports arbitrary trees. However, the practical motivations for such generality are weak. Differentials in general only see practical use in:

- differential invariant formulas and
- differential effect (DE) reasoning, i.e., substituting the right side of an ODE for the left.

In the former case, even scalar terms suffice; while vectorial formulas may be more elegant in some cases, the same expression can be rewritten using scalars, at least for fixed-length vectors. In differential effect reasoning, it *is* important to support vector-valued variables and their projections, i.e., it is essential to support *systems* of ODEs. Given these applications, and given that there is no practical value in tree-shaped ODE systems vs. list-shaped ODE systems, there is thus no compelling need for tree-shaped differential terms. While we have not disproved the possibility of an axiom for tree-shaped differentials, we remark that it would be notably harder than the vector case, as it would require a notion of tree-matrix multiplication.

Contextual reasoning. Contextual reasoning (Fig. 5) applies valid equations and equivalences in a context. The rule CQ rewrites equal terms while CE rewrites equivalent formulas. In each case, it is essential for soundness that the equation or equivalence is *valid*, i.e., true everywhere. This is because, for example, the truth value of $C(P)$ at the *current* state is allowed to depend on the truth value of P in arbitrary states. Rule CQ additionally requires as its second premise that terms $f(x)$ and $g(x)$ denote in the context h, since equalities in dL_ι can only hold between terms that denote. Rule CE does not need a similar existence condition because equivalences may hold when both sides are unknown ($\oslash$). In a practical sense, the contextual equivalence rules are not needed for completeness; they are a convenience feature which both improves performance of some proofs and allows more flexible proof approaches. Thus we include discussion of contexts in this report for the sake of a complete technical development, not for the sake of a complete proof calculus.

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

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

Figure 5: Contextual rules

Contextual equivalence reasoning is perhaps best understood by example. When proving formulas with nested modalities (or sequential compositions), it is useful in practice to simplify programs right-to-left, which minimizes the difficulty of arithmetic reasoning at the leaves. Consider the formula $\phi \equiv [x:=x+1][x:=1+1]x>0 \leftrightarrow [x:=x+1]2>0$. Formula ϕ could be one step of a right-to-left proof which simplifies the inner equation first. In the dL_ι calculus, we would prove ϕ thusly:

$$\text{CE}\frac{[:=]\dfrac{\text{QE}\dfrac{*}{1+1>0\leftrightarrow 2>0}}{[x:=1+1]x>0\leftrightarrow 2>0}}{[x:=x+1][x:=1+1]x>0\leftrightarrow[x:=x+1]2>0}$$

In the above application of CE, the context is $C \equiv (\psi \mapsto [x:=x+1]\psi)$, that is the context is a mapping which returns $[x:=x+1]\psi$ for any formula ψ. We rewrite two equivalent formulas ψ in this context C: to show that the formulas $[x:=1+1]x>0$ and $2>0$ are equivalent under context C, it suffices to show they are equivalent everywhere, which we then prove by $[:=]$ and QE. While this proof in the formal calculus is more pedantic than most paper proofs, this level of detail is essential to ensure our calculus is implementable in a theorem prover.

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

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

$$\text{redT}\quad \mathsf{mr}((L(),R()),b(),s\ f(s),lr\ g(l,r)) = g\big(\mathsf{mr}(L(),b(),s\ f(s),lr\ g(l,r)),\mathsf{mr}(R(),b(),s\ f(s),lr\ g(l,r))\big)$$

$$\text{redR}\quad \mathsf{in}\mathbb{R}(r)\to \mathsf{mr}(r(),b(),s\ f(s),lr\ g(l,r)) = f(r())\quad \text{redN}\quad \mathsf{mr}(\,(\,),b(),s\ f(s),lr\ g(l,r)) = b$$

$$\text{TreeI}\quad \mathsf{D}\Big(p(\iota x\,\mathsf{false})\land p(\,(\,)\,)\land\forall s\,\big(\mathsf{in}\mathbb{R}(s)\to p(s)\big)\land\forall lr\,\big(p(l)\land p(r)\to p((l,r))\big)\Big)\to \mathsf{D}(p(f()))$$

$$\text{refl}\quad (\,)=(\,)\quad =\bot\quad \neg(\mathsf{D}(\iota x\,\mathsf{false}=f()))\land\neg(\mathsf{D}(\neg(\iota x\,\mathsf{false}=f())))$$

Figure 6: Axioms for datatypes

Datatype axioms. Fig. 6 gives axioms for 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 ι is an example of an axiom of an axiom which benefits from free-logical quantifiers that do not quantify over $\bot$: we never want $\bot$ to be the solution of a definite description.

Axiom $=$T enables comparisons on tuples. Quantifier elimination rule QE uses the theorem that first-order real arithmetic, a fragment of dL_ι, is decidable [28]. 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 (written $\mathrm{V}(\phi)$) are indeed real-valued. Axioms redT and redR evaluate reductions when their shape is known, and axiom TreeI allows proving a property of an arbitrary value by induction on its shape. In redT, we write $L()$ and $R()$ for (constant) function symbols standing for the components of a pair. The first base case $p(\iota x\,\mathsf{false})$ indicates that induction must consider the case where the argument $f()$ does not denote, which is possible for rigid function symbols. In practice, and especially because TreeI is designed to conclude definite truth, p will often contain an existence test on $f()$. The second and third base cases say the nullary tuple and scalars satisfy the predicate p. The inductive step of TreeI preserves definite truth, which then enables TreeI to conclude definite truth; simple implication is insufficient in the inductive step for the same reasons as it does not suffice in loop induction.

Rules refl and $=\!\bot$ say that the trivial value $()$ equals only itself while the valueless term $\iota x\,\mathsf{false}$ compares indeterminately with everything.

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

$$\mathrm{E}\vee\quad \mathsf{is}\top(f()) \vee \mathsf{in}\mathbb{R}(f()) \vee \mathsf{isP}(f()) \leftarrow \mathsf{E}(f())$$

$$()'\quad () = (())' \qquad \pi_L\quad l = \pi_1(L(),R()) \qquad \pi'_L\quad \pi_1((f(x))') = (\pi_1 f(x))'$$

$$(x)'\quad (x)' = x' \qquad \pi_R\quad R() = \pi_2(L(),R()) \qquad \pi'_R\quad \pi_2((f(x))') = (\pi_2 f(x))'$$

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

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

$$(f())'\quad (f())' = 0 \leftarrow \mathsf{in}\mathbb{R}(f()) \qquad (\theta,\eta)'\quad ((f(x))',(g(x))') = (f(x),g(x))'$$

Figure 7: Some derived axioms

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 these axioms also conclude (by applying axiom $\mathsf{E}(')$) that the differential of the larger term exists, because it equals something. Thus, these axioms are suitable both for showing that differentials exist and what form differentials take.

In proving the axiom schemata for differential terms, we will exploit the following proposition:

Proposition 27 (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 $P(M)$ holds by assumption $P(M)$. 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 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: $(\theta)'$ is primarily used to simplify differential invariants, and the invariants which arise in practice can be rewritten in terms of scalars.

Lemma 28 (Derived axioms). The axioms in Fig. 7 are derivable.

Proof. By cases, one for each axiom. The soundness proofs for many of these axioms, such as the syntactic differentiation axioms, implement standard theorems from multivariate and vector calculus. Our contribution in those cases is that we show standard theorems and their proofs can be expressed in dL_ι.

- π_L

  By axiom ι with $p(x) \equiv x = L()$. Then $(L(), R()) = (L(), R())$ by $=$T and reflexivity. The for-all premiss proves by transitivity.

- π_R

  By axiom ι with $p(x) \equiv x = R()$. Then $(L(), R()) = (L(), R())$ by $=$T and reflexivity. The for-all premiss proves by transitivity.

- E$\vee$

  Apply TreeI with invariant $J(\theta) \equiv \neg\mathsf{E}(\theta) \vee \mathsf{is}\top(\theta) \vee \mathsf{in}\mathbb{R}(\theta) \vee \mathsf{isP}(\theta)$ By propositional rewriting, it suffices to prove J. By TreeI reduces to four cases:

  - In case $J(\iota x\, \mathsf{false})$, it suffices to show $\neg\mathsf{E}(\iota x\, \bot)$. By ι and by $=\bot$ since the right-hand side (RHS) is false everywhere, it does not denote and is not equal to itself.
  - In case $J(\,())$ it suffices to observe $\mathsf{is}\top(\,())$ and apply disjunction elimination.
  - In case $J(v \in \mathbb{R})$ it suffices to observe $\mathsf{in}\mathbb{R}(v)$ and apply disjunction introduction.
  - Case $J((L, R))$ holds by redT.

- $(f())'$

  By Prop. 27 differentials are unique and by axiom $(\theta)'$ the constant 0 is the differential if

$$\forall \xi > 0\ \exists\, \delta \forall y\ \ (0 < \|y - x\| < \delta \to (f() - f()) - (y - x) \cdot 0 < \xi \|y - x\|) \qquad (1)$$

so it suffices to prove the validity of (1). By QE and CQ, reduces to $\xi > 0 \land 0 < \|y - x\| < \delta \to 0 < \xi\|y - x\|$ which proves by QE. CQ is applicable because $\mathsf{E}(f())$ by assumption. Then applying axiom $(\theta)'$, have $\mathsf{E}(f()) \to (f())' = x' \cdot 0$, and by QE and CQ again, $\mathsf{E}(f()) \to (f())' = 0$.

- $(x)'$

  By Prop. 27, it 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 $\xi > 0 \land 0 < \|y - x\| < \delta \to 0 < \xi\|y - x\|$ which proves by QE. Then applying axiom $(\theta)'$, have $(x)' = x' \cdot 1$, and by QE and CQ again, $(x)' = x'$.

- $()'$

  By Prop. 27, differentials are unique and by axiom $(\theta)'$ the constant $\texttt{()}$ is the differential if

$$\forall \xi > 0 \; \exists \, \delta \forall y \; (0 < \|y - x\| < \delta \to (\texttt{()} - \texttt{()}) - (y - x) \cdot \texttt{()} < \xi\|y - x\|) \tag{2}$$

  so it suffices to prove the validity of (2). Assume without loss of generality $y = x = \texttt{()}$ for the argument of a the function $\texttt{()}$, then $(y - x) \cdot \texttt{()} = \texttt{()}$ universally. Then by QE and CQ, it suffices to show $\xi > 0 \land 0 < \|y - x\| < \delta \to 0 < \xi\|y - x\|$ which proves by QE since $\|\texttt{()}\| = 0$ and $\xi > 0$. Then applying axiom $(\theta)'$, have $(\texttt{()})' = \texttt{()}$.

- $(\theta, \eta)'$

  We unpack the differentials $(f(x))'$ and $(g(x))'$, which exist by assumption, introducing new variables M and N which uniquely satisfy

$$\begin{aligned} \forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \to \\ (f(y) - f(x)) - (y - x) \cdot M < \xi\|y - x\|\big) \end{aligned} \tag{1}$$

  and

$$\begin{aligned} \forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \to \\ (g(y) - g(x)) - (y - x) \cdot N < \xi\|y - x\|\big) \end{aligned} \tag{2}$$

  then we show (M, N) satisfies

$$\begin{aligned} \forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \to \\ \big(\big((f(y), g(y)) \vec{-} (f(x), g(x))\big) \vec{-} \big(y \vec{-} x\big) \cdot (M, N)\big) < \xi\|y - x\|\big) \end{aligned} \tag{0}$$

  which will suffice to show the axiom by Prop. 27, since any differential is the unique differential.

- π_L'

We unpack the differential $(f(x))'$ which exists by assumption, introducing new variable M which uniquely satisfies

$$\forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \rightarrow \\ (f(y) - f(x)) - (y - x) \cdot M < \xi \|y - x\|\big) \tag{1}$$

then we show $\pi_1 M$ satisfies

$$\forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \rightarrow \\ \big(\big(\pi_1 f(y) \vec{-} \pi_1 f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot \pi_1 M < \xi \|y - x\|\big) \tag{0}$$

which will suffice to show the axiom by Prop. 27, since any differential is the unique differential.

Begin the proof of (0) by applying rule $\forall$ to (0), fixing $\xi > 0$. Apply rule $\forall i$ to (1) with $\xi_1 = \xi$, then apply $\forall$, fixing δ_1. Apply (the existential dual of) rule $\forall i$ to (0) with $\delta = \delta_1$, then apply $\forall$, fixing y s.t. (2) $0 < \| \big(y \vec{-} x\big) \| < \delta$. By QE and (2) have (3) $0 < \| \big(y \vec{-} x\big) \| < \delta_1$ by definition of δ. Apply MP to (1) with (2) (3) yielding (4) $\big(\big(f(y) \vec{-} f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot M < \xi_1 \| \big(y \vec{-} x\big) \| = \xi \| \big(y \vec{-} x\big) \|$. Lastly we have $\big(\big(\pi_1 f(y) \vec{-} \pi_1 f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot \pi_1 M < \xi \| \big(y \vec{-} x\big) \|$ since

$$\begin{aligned} & \big(\big(\pi_1 f(y) \vec{-} \pi_1 f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot \pi_1 M \\ = \; & \pi_1 \big(\big(f(y) \vec{-} f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot M \\ \leq \; & \big(\big(f(y) \vec{-} f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot M \\ \leq \; & \xi \| \big(y \vec{-} x\big) \| \end{aligned}$$

proving (0).

- π'_R

  We unpack the differential $(f(x))'$ which exists by assumption, introducing new variable M which uniquely satisfies

$$\forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \rightarrow \\ (f(y) - f(x)) - (y - x) \cdot M < \xi \|y - x\|\big) \tag{1}$$

  then we show $\pi_2 M$ satisfies

$$\forall \xi > 0 \; \exists \, \delta \forall y \; \big(0 < \|y - x\| < \delta \rightarrow \\ \big(\big(\pi_2 f(y) \vec{-} \pi_1 f(x)\big) \vec{-} \big(y \vec{-} x\big)\big) \cdot \pi_2 M < \xi \|y - x\|\big) \tag{0}$$

  which will suffice to show the axiom by Prop. 27, 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) with $\xi_1 = \xi$, then apply $\forall$, fixing δ_1. Apply (the existential dual of) $\forall i$ to (0) with $\delta = \delta_1$, then apply $\forall$, fixing

y s.t. (2) $0 < \| \left(y \vec{-} x\right) \| < \delta$. By QE and (2) have (3) $0 < \| \left(y \vec{-} x\right) \| < \delta_1$ by definition of δ. Apply MP to (1) with (2) (3) yielding (4) $\left(\left(f(y) \vec{-} f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot M < \xi_1 \| \left(y \vec{-} x\right) \| = \xi \| \left(y \vec{-} x\right) \|$. Lastly we have $\left(\left(\pi_2 f(y) \vec{-} \pi_2 f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot \pi_2 M < \xi \| \left(y \vec{-} x\right) \|$ since

$$\begin{aligned} & \left(\left(\pi_1 f(y) \vec{-} \pi_1 f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot \pi_2 M \\ = \ & \pi_2 \left(\left(f(y) \vec{-} f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot M \\ \leq \ & \left(\left(f(y) \vec{-} f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot M \\ \leq \ & \xi \| \left(y \vec{-} x\right) \| \end{aligned}$$

proving (0).

- $(+)'$

We unpack the differentials $(f(x))'$ and $(g(x))'$, which exist by assumption, introducing new variables M and N which uniquely satisfy

$$\begin{aligned} \forall \xi > 0 \, \exists \, \delta \forall y \, \big(& 0 < \|y - x\| < \delta \rightarrow \\ & (f(y) - f(x)) - (y - x) \cdot M < \xi \|y - x\| \big) \end{aligned} \tag{1}$$

and

$$\begin{aligned} \forall \xi > 0 \, \exists \, \delta \forall y \, \big(& 0 < \|y - x\| < \delta \rightarrow \\ & (g(y) - g(x)) - (y - x) \cdot N < \xi \|y - x\| \big) \end{aligned} \tag{2}$$

this allows us to prove that $M + N$ satisfies

$$\begin{aligned} \forall \xi > 0 \, \exists \, \delta \forall y \, \big(& 0 < \|y - x\| < \delta \rightarrow \\ & ((f(y) + g(y)) - (f(x) + g(x)) - (y - x) \cdot (M + N)) < \xi \|y - x\| \big) \end{aligned} \tag{0}$$

which will suffice to show the axiom by Prop. 27, 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 existential dual of) $\forall i$ to (0) with $\delta = \min(\delta_1, \delta_2)$, then apply $\forall$, fixing y s.t. (3) $0 < \| \left(y \vec{-} x\right) \| < \delta$. By QE and (3) have (4a) $0 < \| \left(y \vec{-} x\right) \| < \delta_1$ and (4b) $0 < |\left(y \vec{-} x\right)| < \delta_2$ by definition of δ. Apply MP to (1) and (2) with (4a) and (4b) yielding (5a) $\left(\left(f(y) \vec{-} f(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot M < \xi_1 \| \left(y \vec{-} x\right) \|$ and (5b) $\left(\left(g(y) \vec{-} g(x)\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot N < \xi_2 \| \left(y \vec{-} x\right) \|$. Then by the rule QE we have (6) $\left(\left(((f(y), g(y)) \vec{-} (f(x), g(x))\right) \vec{-} \left(y \vec{-} x\right)\right) \cdot (M, N)) < \xi \| \left(y \vec{-} x\right) \|$ since

$$\begin{aligned} & \| \left((f(y), g(y)) \vec{-} (f(x), g(x))\right) \| \cdot (M, N) \\ = & \| \left(\left(f(y) \vec{-} f(x)\right), \left(g(y) \vec{-} g(x)\right)\right) \| \cdot (M, N) \\ = & \| \left(f(y) \vec{-} f(x)\right) \| \cdot M + \| \left(g(y) \vec{-} g(x)\right) \| \cdot N \\ \leq & \xi_1 \| \left(y \vec{-} x\right) \| + \xi_2 \| \left(y \vec{-} x\right) \| \\ = & \varepsilon \| \left(y \vec{-} x\right) \| \end{aligned}$$

proving (0).

- $(\cdot)'$

  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:

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

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

  Lemma 29 (Sums of limits). In any state where $\mathsf{E}(\lim_{y\to x} f(x))$ and $\mathsf{E}(\lim_{y\to x} g(x))$ are definitely true, so is $\lim_{y\to x} (f(x) + g(x)) = \lim_{y\to x} f(x) + \lim_{y\to x} g(x)$.

  Lemma 30 (Products of limits). In any state where $\mathsf{E}(\lim_{y\to x} f(x))$ and $\mathsf{E}(\lim_{y\to x} g(x))$ are definitely true, then so is $\lim_{y\to x} (f(x) \cdot g(x)) = \lim_{y\to x} f(x) \cdot \lim_{y\to x} g(x)$.

  Lemma 31. If function f is differentiable at a point x, then $f(y)$ goes to $f(x)$ as y goes to x. That is, formula $\mathsf{E}((f(x))') \to ((\lim_{y\to x} f(y)) = f(x))$ is valid.

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

  Lemma 32 (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 $(f(x))' \cdot g(x) + (g(x))' \cdot f(x)$ exists because $f(x)$ exists any time $(f(x))'$ does and because addition and multiplication preserve existence.

$$\begin{aligned}
&(f(x) \cdot g(x))' \\
&= x' \cdot \lim_{y\to x} \frac{f(y) \cdot g(y) - f(x) \cdot g(x)}{y - x} && \text{[Lem. 32]} \\
&= x' \cdot \lim_{y\to x} \frac{f(y) \cdot g(y) - f(x) \cdot g(y) + f(x) \cdot g(y) - f(x) \cdot g(x)}{y - x} && \text{[QE]} \\
&= x' \cdot \lim_{y\to x} \frac{(f(y) - f(x)) \cdot g(y) + f(x)\,(g(y) - g(x))}{y - x} && \text{[QE]} \\
&= x' \cdot \lim_{y\to x} \frac{(f(y) - f(x)) \cdot g(y)}{y - x} + x' \cdot \lim_{y\to x} \frac{f(x) \cdot (g(y) - g(x))}{y - x} && \text{[Lem. 29]} \\
&= x' \cdot \lim_{y\to x} \frac{(f(y) - f(x))}{y - x} \cdot \lim_{y\to x} g(y) + x' \cdot \lim_{y\to x} \frac{(g(y) - g(x))}{y - x} \cdot \lim_{y\to x} f(x) && \text{[Lem. 29]} \\
&= (f(x))' \cdot \lim_{y\to x} g(y) + (g(x))' \cdot \lim_{y\to x} f(x) && \text{[Lem. 32]} \\
&= (f(x))' \cdot g(x) + (g(x))' \cdot f(x) && \text{[Lem. 31]}
\end{aligned}$$

  □

Now that we have introduced the core dL_ι calculus and used it to derive a library of derived constructs, we revisit our example system Ex. 1 and show how Prop. 1 is proved using dL_ι axioms.

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

Sketch. By axiom I with loop invariant $P \equiv (g > 0 \land A > 0 \land 0 \leq h \leq h_0)$. 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 $\text{DI}_{\geq}$. Because $h \leq h_0$ holds initially and the ODE is locally Lipschitz-continuous given constraint $h \geq 0$, it suffices to show $(h)' \leq (h_0)' = 0$ throughout. Then $(h)' \leq 0$ iff $-\sqrt{2gh}\frac{a}{A} \leq 0$ iff $\sqrt{h} \geq 0$ by algebra and DE, which is true by DW, showing $h \leq h_0$. □

6 Theory

Now that we have developed a proof calculus in Sec. 5, it remains to evaluate the design of the calculus. Example proofs such as Ex. 3 only show that the proof system is useful in one concrete instance. A full evaluation requires understanding general properties of the calculus. Soundness (Thm. 34) is the sine qua non of proof systems, without which we have no reason to believe that syntactic proofs lead to true theorems. Future implementation work also demands that proofchecking is decidable, to which end we provide a simple but important decidability result. We also give expressiveness results, which help us situate dL_ι in the broader context of the dL family of logics.

Proofchecking is decidable, and provable formulas are valid.

Theorem 33 (Proofchecking decidability). There exists an algorithm which decides whether a derivation $\mathcal{D}$ is a proof of a given dL_ι formula ϕ. Specifically, the proof calculus of Sec. 5 is an effective proof calculus.

Proof. By induction on the structure of derivations. The base cases are the axioms, which are trivially effective because each axiom is a single formula. The inductive cases are the rules, of which G, MP, and $\forall$ are trivially effective because they have no side conditions. Rule QE is effective because its side-condition is the validity of a formula in first-order logic over the reals, which is decidable [28]. Rule US is effective because it is defined by primitive recursion and the side conditions are defined using only primitive-recursive functions. Because every axiom and rule is effective, the calculus is effective. □

Theorem 34 (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 valid conclusions from valid premises). Because dL_ι supports the formula and program connectives of 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 the denotational semantics in an arbitrary state. In the proofs that follow, we will use an equals sign both for comparison of truth values and for calculational chains of reasoning, with these uses distinguished by formatting.

Lemma 35 (Core axioms and rules valid). All the core non-derived axioms are valid formulas of dL_ι. All the non-substitution rules are sound rules of dL_ι.

Proof. By cases. 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 $P \equiv C(\mathsf{true})$ for a fresh quantifier symbol C, i.e., as unary quantifier symbols with constant arguments. In the semantics, we write $I(P)$ for the interpretation $I(C)(I[\![\mathsf{true}]\!])$.

As is commonplace with Łukasiewicz logics, it is sometimes convenient to consider arithmetic operations on truth values, where $\oplus$ is interpreted as 1, $\oslash$ as 0.5, and $\ominus$ as 0. For example, we write $p > q$ if the truth value p is strictly more true than q.

[$\cdot$] Formula $\langle a\rangle P \leftrightarrow \neg[a]\neg P$ is valid in dL_ι. By cases, in each case the LHS and RHS have the same truth value.

Case 1: $\oplus$

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

Case 2: $\ominus$ Symmetric.

Case 3:

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

[:=] Formula $([x := f()]p(x) \leftrightarrow p(f())) \leftarrow \mathsf{E}(f())$ is valid in dL_ι. Assume (1) $I\omega[\![\mathsf{E}(f())]\!] = \oplus$ for some state ω and interpretation I, since the case $I\omega[\![\mathsf{E}(f())]\!] = \ominus$ makes the implication vacuously true, and $I\omega[\![\mathsf{E}(\theta)]\!]$ never assumes value $\oslash$. Then observe $I\omega[\![[x := f()]p(x)]\!] =$

$I\omega[\![p(f())]\!]$ by the chain of equalities

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

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

Case 1: $\oplus$

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

Case 2: $\ominus$

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

Case 3: $\oslash$

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

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

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

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

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

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

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

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

By 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 $n = I\nu[\![Q]\!]$. 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 by the semantics of the box operator we have $k \leq m$ yielding $I\omega[\![[a]P \to [a]Q]\!] = \oplus$ so the axiom has value $\oplus$ in this case.

Case $\oslash$: 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 $j = I\nu[\![P]\!] \leq \oslash + I\nu[\![Q]\!] = 0.5 + n$ 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 $I\omega[\![[a]P \to [a]Q]\!] \geq \oslash$. Since $I\omega[\![A \to B]\!] = \oplus$ when $I\omega[\![A]\!] = I\omega[\![B]\!] = \oslash$, 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., $I\nu[\![P]\!] = \oplus$ for all ν such that $(\omega,\nu) \in I[\![a]\!]^*$ iff $(\omega,\nu) \in I[\![a^n]\!]$ for some $n \in \mathbb{N}$. By induction on the natural number n with induction predicate $P(n)$ defined by "if $(\omega,\nu) \in I[\![a]\!]^n = I[\![a^n]\!]$ then $I\nu[\![P]\!] = \oplus$".

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 ν s.t. $(\omega, \nu) \in I[\![a^{k+1}]\!]$: By definition of composition, we have such a μ and additionally (3)$(\mu, \nu) \in I[\![a]\!]$. Then (4) $I\mu[\![P \rightarrow [a]P]\!] = \oplus$ 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 $p \rightarrow [a]p$

Let $q = I\omega[\![p()]\!] = I(p) = I\nu[\![p()]\!]$ (since p is a nullary predicate, ergo constant) for all ν including ν for which $(\omega, \nu) \in I[\![a]\!]$ so $I\omega[\![[a]p()]\!] = \sqcap_{\nu \mid (\omega,\nu) \in I[\![a]\!]} I\nu[\![p()]\!] = \oplus$ when there exists ν such that $(\omega, \nu) \in I[\![a]\!]$ or $\oplus$ when no such ν exists. In either case the axiom is valid since it has truth value $\oplus$ for all I and ω.

$\forall i$ $(\forall x\, p(x)) \rightarrow (\mathsf{E}(f()) \rightarrow p(f()))$

It suffices to consider the case $I\omega[\![\mathsf{E}(f())]\!] = \oplus$ because the implication is vacuously true when $I\omega[\![\mathsf{E}(f())]\!] = \ominus$ and $I\omega[\![\mathsf{E}(f())]\!]$ is necessarily never $\oslash$. That is, (1) $I(f) \in \mathbf{Tree}(\mathbb{R})$. Assume $I\omega[\![\forall x\, p(x)]\!] = \oplus$ and $I\omega[\![\mathsf{E}(f())]\!] = \oplus$ for all ω, so $I\omega^v_x[\![p(x)]\!] = \oplus$ for all $v \in \mathbf{Tree}(\mathbb{R})$. Now by (1) instantiate $v = I(f) \in \mathbf{Tree}(\mathbb{R})$, and have $\omega_x^{I(f)}[\![p(x)]\!] = \oplus$. That is, $I\omega[\![p(f())]\!] = \oplus$ so the implication holds and the axiom is valid.

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

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

Case $\oslash$: Let $k = \sqcap_{v\, \in\, \mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![p(x)]\!]$. Let $v \in \mathbf{Tree}(\mathbb{R})$, and $j = I\omega^v_x[\![p(x)]\!]$. By definition of $\sqcap$ have $k \leq j$. Let $n = I\omega^v_x[\![q(x)]\!]$. By case, have $I\omega^v_x[\![p(x)]\!] \leq \oslash + I\omega^v_x[\![q(x)]\!]$ (i.e., $j \leq 0.5 + n$) so by transitivity $k \leq 0.5 + n$ for all such v, n. Then let $m = \sqcap_{T\, \in\, \mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![p(x)]\!]$. Since this held for all possible v then also have $k \leq 0.5 + m$ yielding $I\omega[\![(\forall x\, p(x) \rightarrow \forall x\, q(x))]\!] \geq \oslash$. Since $I\omega[\![A \rightarrow B]\!] = \oplus$ when $I\omega[\![A]\!] = I\omega[\![B]\!] = \oslash$, the truth value of the axiom is $\oplus$ in this case.

Case $\ominus$: Implication holds vacuously.

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

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

ι $p(\iota z\, p(z)) \leftrightarrow \exists x p(x) \wedge (\forall y\, p(y) \rightarrow y = x)$

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

=T $(L_1(), R_1()) = (L_2(), R_2()) \leftrightarrow L_1() = L_2() \wedge R_1() = R_2()$ 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 $\mathsf{in}\mathbb{R}(v()) \to \mathsf{mr}(v(), b(), s\ f(s), lr\ g(l, r)) = f(v())$ Assume $I\omega[\![\mathsf{in}\mathbb{R}(h())]\!] = \oplus$ so $I(v) \in \mathbb{R}$, else the implication holds vacuously. Then

$$\begin{aligned}
&I\omega[\![\mathsf{mr}(h(), b(), s\ f(s), lr\ g(l, r))]\!] \\
=&\mathsf{Reduce}(I(v), I\omega[\![b()]\!], s\ f(s), lr\ g(l, r), I\omega) \\
=&I\omega^{I(v)}_s[\![f(s)]\!] \\
=&I(f)(I(v)) = I\omega[\![f(h())]\!].
\end{aligned}$$

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

$$\begin{aligned}
&I\omega[\![\mathsf{mr}(h(), b(), s\ f(s), lr\ g(l, r))]\!] \\
&= \mathsf{Reduce}((L, R), I\omega[\![b()]\!], s\ f(s), lr\ g(l, r), I\omega) \\
&= I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![g(l, r)]\!]
\end{aligned}$$

where $\tilde{L}, \tilde{R} = \mathsf{Reduce}(L, R, I\omega[\![b()]\!], s\ f(s), lr\ g(l, r), I\omega)$ so

$$\begin{aligned}
&I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![g(l, r)]\!] \\
&= I(g)(\mathsf{Reduce}(h(), I\omega[\![b()]\!], s\ f(s), lr\ g(l, r), I\omega)) \\
&= I\omega[\![g(\mathsf{mr}(\pi_1 h(), b(), s\ f(s), lr\ g(l, r))), \mathsf{mr}(\pi_2 h(), b(), s\ f(s), lr\ g(l, r))]\!]
\end{aligned}$$

since $I\omega[\![\mathsf{mr}(\pi_1 h(), b(), s\ f(s), lr\ g(l, r))]\!] = \tilde{L}$ likewise for $\tilde{R}$.

refl $I\omega[\![\,() = ()\,]\!] = \mathsf{Geq}(\top, \top) \wedge \mathsf{Geq}(\top, \top) = \oplus$.

=$\bot$ $I[\![\neg(\mathsf{D}(\iota x\, \mathsf{false} = f())) \wedge \neg(\mathsf{D}(\neg(\iota x\, \mathsf{false} = f())))]\!] = \overline{\mathsf{D}(\oslash)} \sqcap \overline{\mathsf{D}(\overline{\oslash})} = \overline{\mathsf{D}(\oslash)} = \overline{\ominus} = \oplus$ as desired.

TreeI $\mathsf{D}(p(\iota x\,\mathsf{false}) \wedge p(\,()\,) \wedge \forall s(\mathsf{in}\mathbb{R}(s) \to p(s)) \wedge \forall lr(p(l) \wedge p(r) \to p((l,r)))) \to \mathsf{D}(p(h()))$. Note the assumption and conclusion both employ $\mathsf{D}(\cdot)$ for the same reason that the assumptions and conclusions of axiom I do: The inductive step assumption will typically need to be applied multiple times. Assume (0) $I\omega[\![p(\iota x\,\mathsf{false}) \wedge \forall s(\mathsf{in}\mathbb{R}(s) \to p(s)) \wedge \forall lr(p(l) \wedge p(r) \to p((l,r)))]\!] = \oplus$, else the implication holds vacuously. By inversion on (0), have (1a) $I\omega[\![p(\iota x\,\mathsf{false})]\!] = \oplus$ and (2a) $I\omega[\![p(\,()\,)]\!] = \oplus$ and (3a) $I\omega[\![\forall s(\mathsf{in}\mathbb{R}(s) \to p(s))]\!] = \oplus$ and (4a) $I\omega[\![\forall lr(p(l) \wedge p(r) \to p((l,r)))]\!] = \oplus$ which simplify respectively to (1b) $I(p)(\bot) = \oplus$ (since there is no value of x that satisfies falsehood in $\iota x\,\mathsf{false}$) and (2b) $I(p)(\top) = \oplus$ (3b) for all $v \in \mathbb{R}, I(p)(v) = \oplus$ and (4b) 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 $v = I\omega[\![v()]\!] = I(v)$ 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, $v = \top$**:** Using assumption (2b), have $I(p)(v) = I(p)(\top) = \oplus$ as desired.

Base case 3, $v \in \mathbb{R}$**:** Using assumption (3b), 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 (5) $I(p)(L) = \oplus$ and (6) $I(p)(R) = \oplus$. By (5) and (6) and because $L, R \in \mathbf{Tree}(\mathbb{R})$ can apply (4b) 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 $\oplus = I(p)(I(v)) = I\omega[\![p(v())]\!]$ as desired.

$(\theta)'$

$$(f(x))' = x' \cdot \iota M\, \forall \xi{>}0\, \exists \delta{>}0\, \forall y\, \mathsf{D}(0{<}\|y\vec{-}x\|{<}\delta \to f(y){-}f(x){-}\big(\big(y\vec{-}x\big) \cdot M\big){<}\xi\|y\vec{-}x\|)$$
$$\leftarrow \mathsf{in}\mathbb{R}((f(x))') \wedge \mathsf{islist}((x)')$$

In this case, the assumptions $\mathsf{in}\mathbb{R}((x)')$ and $\mathsf{islist}((x)')$ let us assume (by Prop. 4 and Prop. 25) that $f(x)$ is scalar and that x and x' are lists with matching shapes. Here $\|u - v\|$ computes the Euclidean distance between u and v, while $(u \cdot v)$ is the dot product of vectors u and v. We assume (0a) $I\omega[\![\mathsf{in}\mathbb{R}((f(x))')]\!] = \oplus$ and (0b) $I\omega[\![\mathsf{islist}((x)')]\!] = \oplus$, else the implication holds trivially. Assumptions (0a) and (0b) are 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: $I\omega[\![(f(x))']\!] = \sum_{y \in \mathsf{Dim}(\mathsf{FV}(f(x)))} \frac{\partial I\omega[\![f(y)]\!]}{\partial y} \cdot \omega(y') = \sum_{y \in \mathsf{Dim}(\{x\})} \frac{\partial I\omega[\![f(y)]\!]}{\partial y} \cdot \omega(y') = \frac{\partial I\omega[\![f(x)]\!]}{\partial x} \cdot \omega(x') = \frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x')$ 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 gradient multiplied by ω' agrees with the directional derivative $\frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x')$ in direction ω'. that is, $\frac{\partial I(f)(\omega(x))}{\partial x} \cdot \omega(x') = \omega(x') \cdot M$ where $M \in \mathbf{Tree}(\mathbb{R})$ is the gradient at x. To complete the

proof, we note that M in axiom $(\theta)'$ indeed denotes the gradient derivative, because M denotes the unique value such that for all $\xi > 0$ exists $\delta > 0$ such that for all $v \in \mathbf{Tree}(\mathbb{R})$ such that $0 < \| \left(v\vec{-}\omega(x)\right) \| < \delta$ have $I(f)(v) - I(f)(\omega(x)) - (\left(v\vec{-}\omega(x)\right))\cdot M < \xi \| \left(v\vec{-}\omega(x)\right) \|$, which agrees with standard definitions of the gradient. 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.

$\mathsf{E}(')$ It suffices to note the left-hand side of $(\theta)'$ exists exactly when the right-hand side does, i.e., $(f(x))'$ exists exactly when the differential of $f(x)$ does.

$(\theta)'$s This is a straightforward generalization of the $(\theta)'$ soundness proof. The input x is already allowed to be a vector. To generalize the output $f(x)$ to a vector, it suffices to generalize our notion of derivatives from gradients to Jacobian matrices. By Prop. 25 we can assume x and $f(x)$ are a vector, from which we apply Prop. 21, Prop. 19, and Prop. 17 to show that matrix multiplication, dot product, and vector subtraction fulfill their specifications as needed to define total differential $(f(x))'$ as a function of the Jacobian M.

$\mathsf{E}(')$s The argument is analogous to the case for $(\theta)'$s: the differential $(f(x))'$ exists exactly when the construction of differential as limit exists.

DW Fix I, ω and show that $I\omega[\![[x' = f(x) \,\&\, q(x)]q(x)]\!] = \oplus$. Then it suffices to show that $\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]} I\nu[\![q(x)]\!] = \oplus$ and likewise suffices to show for all such ν that $I\nu[\![q(x)]\!] = \oplus$. If no ODE solution should exist then the conjunction $\sqcap_{\nu \mid (\omega,\nu)\in I[\![x'=f(x)\,\&\,q(x)]\!]}$ is empty and trivially its truth value is $\oplus$. Else there exists a solution φ s.t. $\varphi(t) = \nu$ for some $t \in \mathbb{R}_{\geq 0}$ 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 proofs, rather it is used to first derive a more friendly, but equivalent, axiom. Hence several similar axioms are all called DW in the literature.

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 $\rightarrow$ 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 $\{x'\}^{\complement}$. Define set $T = \{\varphi(t) \mid \varphi(t)$ 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):

$$\begin{aligned} & (I\omega[\![[x' = f(x) \,\&\, q(x)]r(x)]\!] = \oplus) \\ \equiv\ & \sqcap_T I\varphi(t)[\![r(x)]\!] = \oplus \\ \equiv\ & I\varphi(t)[\![r(x)]\!] = \oplus \text{ for all } t, \varphi \end{aligned} \tag{3}$$

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:

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

Recall that φ is a solution of the ODE on $t \geq 0$ where for all $0 \leq s \leq t$ we have $I\varphi(s)[\![q(x)]\!] = \oplus$. Then by (3) 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 we continue the chain of equalities

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

DE Fix I, ω and show that

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

to show the equivalence. We start by unpacking the meaning of the left-hand side:

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

By def. each such ν is $\varphi(t)$ for $t \in \mathbb{R}_{\geq 0}$, 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 $I\nu[\![p(x,x')]\!] = I\nu_{x'}^{I\nu[\![f(x)]\!]}[\![p(x,x')]\!]$ so we continue the equality chain

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

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 cases for $>, =, \neq, \wedge$, and $\vee$ generalize in the same fashion from their dL proofs [24]. In this proof, the term $\mathsf{shape}(\cdot)$ is given per its definition in Fig. 2. Fix I and ω, then assume (1) $I\omega[\![[?q(x)][x' = f(x)\&q(x)](g(x))' \geq (h(x))']\!] = \oplus$. We then show that $I\omega[\![[x' = f(x)\&q(x)]g(x) \geq h(x) \leftrightarrow [?q(x)]g(x) \geq h(x)]\!] = \oplus$. By (1), for every solution $\varphi : [0,t] \to \mathbf{Tree}(\mathbb{R})$ (for any $t \geq 0$) we have that (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) for all $t_1, t_2 \in [0,t], I\varphi(t_1)[\![\mathsf{shape}(g(x))]\!] = I\varphi(t_2)[\![\mathsf{shape}(g(x))]\!]$ and $I\varphi(t_1)[\![\mathsf{shape}(h(x))]\!] = I\varphi(t_2)[\![\mathsf{shape}(h(x))]\!]$ as a consequence of the 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 across $[0,t]$. 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 that the formulas $[x' = f(x)\&q(x)]\, g(x) \geq h(x)$ and $[?q(x)]\, g(x) \geq h(x)$ imply each other.

Case 1: Assume (5) $I\omega[\![[x' = f(x)\&q(x)]g(x) \geq h(x)]\!] = \oplus$ 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. 36 because $\omega = \nu$ on $\{x'\}^{\complement} \subseteq \mathrm{FV}(g(x) \geq h(x))$ since $x' \notin \mathrm{FV}(g(x) \geq h(x))$, 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 Lem. 36 have $I\nu[\![q(x)]\!] = \oplus$ yielding $(\omega, \nu) \in I[\![x' = f(x)\&q(x)]\!]$ which with (7) (again by Lem. 36) shows the case.

Else assume $t > 0$. We define a function $\mathrm{rel}(s) = I\varphi(s)[\![g(x)]\!] - I\varphi(s)[\![h(x)]\!]$ with domain $[0,t]$. The function rel is differentiable because it is the difference of two differentiable functions. From (7) we have that (8a) $\mathrm{rel}(0) \geq 0$. By applying Lem. 2 to (1) we learn that $\frac{d\, I\varphi(t)[\![g(x)]\!]}{dt}(s) \geq \frac{d\, I\varphi(t)[\![h(x)]\!]}{dt}(s)$, i.e., (8b) $\frac{d\,\mathrm{rel}(t)}{dt}(s) \geq 0$ for all $s \in [0,t]$. From (8a) and (8b) it follows by mean-value theorem that (9) $\mathrm{rel}(t) \geq 0$ because (reasoning by contradiction) we would else have $\frac{d\,\mathrm{rel}(t)}{dt}(s) < 0$ for some s, contradicting (8b). From (9) it follows immediately that $I\varphi(t)[\![g(x)]\!] \geq I\varphi(t)[\![h(x)]\!]$ which is to say $I\varphi(t)[\![g(x) \geq h(x)]\!] = \oplus$ as desired.

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

DG Fix I and ω. Assume the antecedent, equivalently (by Prop. 3) assume for all $v \in \mathbf{Tree}(\mathbb{R})$ such that $I(q)(v) = \oplus$ that (1) $I\omega_x^v[\![\mathsf{Con}(a(x))]\!] = I\omega_x^v[\![\mathsf{Con}(b(x))]\!] = \oplus$. By Prop. 7 then (cont) $I(a)$ and $I(b)$ are continuous real-valued functions of locally-fixed-shape values v at all values $v \in \mathbf{Tree}(\mathbb{R})$ such that $I(q)(v) = \oplus$. 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 will show this 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

$$\begin{aligned}L &\equiv \{\nu \mid (\omega,\nu) \in I[\![x' = f(x)\&q(x)\,\&\,p(x)]\!]\}\\ R &\equiv \{\nu \mid (\omega_y^v,\nu) \in I[\![z := (x,y);\\ &\qquad z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\&q(\pi_1 z); (x,y) := z]\!], \text{ some } v \in \mathbb{R}\}\end{aligned}$$

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

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

$$\begin{aligned}y(0) &= v\\ y'(t) &= F(t,y(t)) = y(t)(I\varphi(t)[\![a(x(t))]\!]) + I\varphi(t)[\![b(x)]\!]\end{aligned}$$

By Picard-Lindelöf [29, §10.VII], solution $y(t)$ exists. By inversion on assumption (1) and by fact (cont), $a(x(t))$ and $b(x(t))$ are continuous as functions of x and, by composition, as functions of t. Because φ is a solution of an ODE, φ is differentiable and thus continuous. Then F is a composition of continuous functions under smooth operators so the solution $y(t)$ exists uniquely, because F satisfies the Lipschitz condition:

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

where the maximum exists because $[0,t]$ is compact and by assumption (1) $a(x)$ is continuous on $\{\nu \mid I\nu[\![q(x)]\!] = \oplus\} \supseteq \{\nu \mid \nu(t) \in [0,t]\}$. We can now define the modification $\tilde{\varphi}$ as such: It agrees with μ on $\{z,z'\}^{\complement}$, 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 $\pi_2\tilde{\varphi}(y) = v$ 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 $I\varphi(s)[\![f(x)]\!] = I\tilde{\varphi}(s)_x^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}[\![f(x)]\!]$ by Lem. 36, then $I\tilde{\varphi}(s)_x^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}[\![f(x)]\!] = I\tilde{\varphi}(s)[\![f(\pi_1 z)]\!]$ and likewise $I\tilde{\varphi}(s)[\![q(\pi_1 z)]\!] = I\tilde{\varphi}(s)_x^{I\tilde{\varphi}(s)[\![\pi_1 z]\!]}[\![q(x)]\!] = I\varphi(s)[\![q(x)]\!]$ by Lem. 36 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 the *inverse* ghost 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, and even when the initial value of $\pi_2 z$ is arbitrary. Term η is even allowed to be discontinuous, vectorial, or partial: these edge cases only ever *shorten*, not *expand*, the existence interval of an ODE. While discontinuous η could have multiple solutions, they would agree with one another on $\pi_1 z$ so that continuity does not disturb the applicability of inverse-ghosting. Show $\nu \in \{\nu \mid (\omega_y^v, \nu) \in I[\![z := (x,y); z' = (f(\pi_1 z), a(\pi_1 z)\pi_2 z + b(\pi_1 z))\&q(\pi_1 z); (x,y) := z]\!], v \in \mathbb{R}\}$ Consider any term η, any $v \in \mathbf{Tree}(\mathbb{R})$ 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 $\{z'\}^{\complement}$. 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 Lem. 36 $I, \varphi_{|L} \models x' = f(x) \wedge q(x)$ because $\varphi_{|L}(x)$ is defined to match $\varphi(z)$ and $\mathrm{FV}(f(x)) = \{x\}$. This completes the proof that $L \subseteq R$.

Then because the sets L and R are identical on all variables except $\{y, y', z, z'\}$ then by Lem. 36 $I\nu[\![p(x)]\!]$ has the same truth value on every element of $L \cup R$, completing the proof.

DS Fix I and ω. Assume without loss of generality (1) $I(f) \neq \bot$, else $I[\![x' = f()\,\&\,q(x)]\!] = \emptyset$ as $I[\![f()]\!] = \bot$ throughout, in which case the implication is vacuous. Then we show that $I\omega[\![[x' = f()\,\&\,q(x)]p(x)]\!] = I\omega[\![\forall t : \mathbb{R}\ ((\forall 0 \leq s \leq t\, q\left(x \vec{+} f()s\right)) \to [x := x + f()t]p(x))]\!]$. The key of the proof is to observe first that (2) φ as defined by $\varphi(s)(x) = I\omega_t^s[\![x + f()t]\!]$ solves $x' = f()$ on $[0, \infty)$ and that because $f()$, which exists by (1), is trivially Lipschitz, this solution is unique. Note the existence interval of the solution is $[0, \infty)$ because $f()$ is a *constant*: if it exists at any time t, it must exist at every time t. In the following, let the domain D be defined by $D = \{t \mid \text{for all } s \in [0,t], I\varphi(s)[\![q(x)]\!] = \oplus\}$. This is interchangeable with $\{t \mid \text{for all } s \in [0,t], I\omega[\![q(x + f()s)]\!] = \oplus\}$ by construction of φ. Then

$$
\begin{aligned}
& I\omega[\![[x' = f()\,\&\,q(x)]p(x)]\!] \\
= \ & \sqcap_{\nu \mid (\omega,\nu) \in I[\![x' = f()\,\&\,q(x)]\!]} I\nu[\![p(x)]\!] \\
= \ & \sqcap_{r \in D} I\varphi(r)[\![p(x)]\!] \\
= \ & \sqcap_{r \in D} I(p)(\varphi(r)(x)) \\
= \ & \sqcap_{r \in D} I(p)(\omega(x) + I(f)r) \\
= \ & \sqcap_{r \in D} (I\omega_x^{I\omega[\![x]\!]}[\![p(x + f()t)]\!]) \\
= \ & \sqcap_{r \in D} (I\omega[\![[x := x + f()t]p(x)]\!]) \\
= \ & \sqcap_{r:\mathbb{R} \mid I\omega_t^r[\![\forall 0 \leq s \leq t\, q(x+f()s)]\!]} I\omega_t^r[\![[x := x + f()t]p(x)]\!] \\
= \ & I\omega[\![\forall t : \mathbb{R}\ (\forall 0 \leq s \leq t\, q(x + f()s)) \to [x := x + f()t]p(x)]\!].
\end{aligned}
$$

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.

$\forall$ $\dfrac{p(f())}{\forall x\, p(x)}$

Assume $I\nu[\![p(x)]\!]{=}\oplus$, all ν. Fix ω, then $I\omega[\![\forall x p(x)]\!]{=}\sqcap_{v\in\mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![p(x)]\!]$. By the assumption, $\sqcap_{v\in\mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![p(x)]\!] = \sqcap_{v\in\mathbf{Tree}(\mathbb{R})}\oplus = \oplus$, 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 $I\nu[\![P]\!] \leq I\nu[\![Q]\!]$. Fix ω. By assumptions $\oplus = I\omega[\![P]\!] \leq I\omega[\![Q]\!]$, i.e., $I\omega[\![Q]\!] = \oplus$ for all ω so the conclusion is valid, and the rule is sound.

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

(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 $\oslash$ if either side is $\bot$). By second premise, assume also have $I\omega[\![\mathsf{E}(\mathrm{h}(f(x))) \land \mathsf{E}(\mathrm{h}(g(x)))]\!] = \oplus$. 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., $I\omega[\![P \leftrightarrow Q]\!] = \oplus$ for all ω. Then by inversion $I\omega[\![P]\!] = I\omega[\![Q]\!]$. Then $I\omega[\![C(P)]\!] = I(C)(I[\![P]\!]) = I(C)(I[\![Q]\!]) = I\omega[\![C(Q)]\!]$. Then the conclusion is valid, and so the rule is sound. □

This completes the proofs of axioms as well as several proof rules. In order to complete the proof of soundness, we now shift focus to the one remaining rule: uniform substitution.

6.1 Uniform Substitution

Like any uniform substitution calculus, the workhorse of dL_ι is the substitution rule US. All the axioms of dL_ι are single, valid formulas, rather than axiom schemata, a key advantage of uniform substitution which simplifies the soundness proof of each axiom. Simplicity in axiom proofs is achieved by offloading side-condition complexity to the definition of and soundness proof for US as shown in this section. This is to our overall benefit, because complex side conditions need only be handled once.

The uniform substitution proof rule in dL_ι is analogous to that in dL:

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

In dL, the US rule is sound when the substitution σ does not introduce free references (Fig. 8) to bound variables (Fig. 9), in which case we say σ is *admissible* for ϕ. Admissibility can be checked syntactically.

We show that the same holds of dL_ι when adding terms $\iota x\,\phi$, $()$, (θ,η) and $\mathsf{mr}(\theta,\eta,s\;\zeta,lr\;\gamma)$ and generalizing dL to a three-valued semantics. Main novelties of dL_ι substitution include support for vectorial differentials of non-total terms as well as the use of simultaneous induction principles supporting terms that mention formulas.

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 $\mathrm{FV}(\sigma|_{\Sigma(\phi)}) \cap U = \emptyset$ where $\sigma|_{\Sigma(\phi)}$ is the restriction of σ that only replaces symbols that occur in ϕ and $\mathrm{FV}(\sigma) = \bigcup_{f\in\sigma}\mathrm{FV}(\sigma f(\cdot)) \cup \bigcup_{p\in\sigma}\mathrm{FV}(\sigma p(\cdot))$ 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. 11.

In Fig. 11, σf denotes the replacement for symbol f provided by σ.

Admissibility checks employ static semantics consisting of free-variable ($\mathrm{FV}(\cdot)$, Fig. 8), may-bound-variable ($\mathrm{BV}(\cdot)$, Fig. 9), and must-bound-variable ($\mathrm{MBV}(\cdot)$, Fig. 9) computations. Analogously to $\mathrm{FV}(\cdot)$ (Fig. 10), the signature $\Sigma(\cdot)$ indicates all *rigid* symbols which influence the meaning of an expression. In Fig. 10, $\otimes$ is shorthand for an arbitrary operator and e means any expression: term, formula, or program.

Intuitively, 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) contains all variables that influence meaning:

Lemma 36 (Coincidence). 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 $V \cup \mathrm{MBV}(\alpha)$.

Proof. The proof of coincidence follows the general structure of the coincidence proof in [24]. Proceed by simultaneous induction on terms, formulas, and programs. We consider $\mathsf{shape}(\theta)$ structurally simpler than $(\theta)'$ in the induction, and we allow the states ω and $\tilde{\omega}$ to vary when applying inductive hypotheses.

- **case** q: $I\omega[\![q]\!] = q = J\tilde{\omega}[\![q]\!]$.
- **case** x: $I\omega[\![x]\!] = \omega(x) = \tilde{\omega}(x) = J\tilde{\omega}[\![x]\!]$ since $x \in \mathrm{FV}(x)$.
- **case** $\theta+\eta$ when both denote reals: $I\omega[\![\theta+\eta]\!] = I\omega[\![\theta]\!] + I\omega[\![\eta]\!] \overset{=}{\text{IH}} J\tilde{\omega}[\![\theta]\!] + J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\theta+\eta]\!]$.
- **case** $\theta+\eta$, error on left: $I\omega[\![\theta+\eta]\!] = \bot$ and $I\omega[\![\theta]\!] = \bot \overset{=}{\text{IH}} J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\theta+\eta]\!]$.
- **case** $\theta+\eta$, error on right: $I\omega[\![\theta+\eta]\!] = \bot$ and $I\omega[\![\eta]\!] = \bot \overset{=}{\text{IH}} J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\theta+\eta]\!]$.

$$
\begin{aligned}
\mathrm{FV}(()) &= \emptyset \\
\mathrm{FV}(q \in \mathbb{Q}) &= \emptyset \\
\mathrm{FV}(x) &= \{x\} \\
\mathrm{FV}(\theta + \eta) &= \mathrm{FV}(\theta) \cup \mathrm{FV}(\eta) \\
\mathrm{FV}(\theta \cdot \eta) &= \mathrm{FV}(\theta) \cup \mathrm{FV}(\eta) \\
\mathrm{FV}(\iota x\, \phi) &= \mathrm{FV}(\phi) \setminus \{x\} \\
\mathrm{FV}(\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)) &= \mathrm{FV}(\theta) \cup \mathrm{FV}(\eta) \cup (\mathrm{FV}(\zeta) \setminus \{s\}) \cup (\mathrm{FV}(\gamma) \setminus \{l, r\}) \\
\mathrm{FV}(f(\theta)) &= \mathrm{FV}(\theta)
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{FV}(\forall x\, \phi) &= \mathrm{FV}(\phi) \setminus \{x\} \\
\mathrm{FV}(\phi \wedge \psi) &= \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi) \\
\mathrm{FV}(\neg\phi) &= \mathrm{FV}(\phi) \\
\mathrm{FV}(\theta \geq \eta) &= \mathrm{FV}(\theta) \cup \mathrm{FV}(\eta) \\
\mathrm{FV}([\alpha]\phi) &= \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha)) \\
\mathrm{FV}(p(\theta)) &= \mathrm{FV}(\theta) \\
\mathrm{FV}(C(\phi)) &= \mathcal{V} \cup \mathcal{V}'
\end{aligned}
$$

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

Figure 8: Free variable computation

$$
\begin{aligned}
\text{BV}(?\phi) &= \emptyset \\
\text{BV}(x := \theta) &= \{x\} \\
\text{BV}(x' = \theta \,\&\, \psi) &= \{x, x'\} \\
\text{BV}(\alpha \cup \beta) &= \text{BV}(\alpha) \cup \text{BV}(\beta) \\
\text{BV}(\alpha; \beta) &= \text{BV}(\alpha) \cup \text{BV}(\beta) \\
\text{BV}(\alpha^*) &= \text{BV}(\alpha) \\
\text{BV}(a) &= \mathcal{V} \cup \mathcal{V}' \\
\hline
\text{MBV}(\alpha \cup \beta) &= \text{MBV}(\alpha) \cap \text{MBV}(\beta) \\
\text{MBV}(\alpha; \beta) &= \text{MBV}(\alpha) \cup \text{MBV}(\beta) \\
\text{MBV}(a) = \text{MBV}(\alpha^*) &= \emptyset \\
\text{MBV}(\alpha) &= \text{BV}(\alpha) \text{ in all other cases}
\end{aligned}
$$

Figure 9: Bound variable computation

$$
\begin{aligned}
\Sigma(s) &= \{s\} \text{ if } s \text{ is } C, a, f, \text{ or } p \\
\Sigma(\otimes(e_1, \ldots, e_n)) &= \Sigma(e_1) \cup \cdots \cup \Sigma(e_n)
\end{aligned}
$$

Figure 10: Signature computation

- **case** $\theta \cdot \eta$ when both denote reals: $I\omega[\![\theta \cdot \eta]\!] = I\omega[\![\theta]\!] \cdot I\omega[\![\eta]\!] \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\theta]\!] \cdot J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\theta \cdot \eta]\!]$.
- **case** $\theta \cdot \eta$, error on left: $I\omega[\![\theta \cdot \eta]\!] = \bot$ and $I\omega[\![\theta]\!] = \bot \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\theta]\!] = J\tilde{\omega}[\![\theta \cdot \eta]\!]$.
- **case** $\theta = \theta \cdot \eta$, error on right: $I\omega[\![\theta \cdot \eta]\!] = \bot$ and $I\omega[\![\eta]\!] = \bot \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\theta \cdot \eta]\!]$.
- **case** $()$: $I\omega[\![()]\!] = \top = J\tilde{\omega}[\![()]\!]$.
- **case** (θ, η) when both are reals: $I\omega[\![(\theta, \eta)]\!] = (I\omega[\![\theta]\!], I\omega[\![\eta]\!]) \stackrel{=}{\text{IH}} (J\tilde{\omega}[\![\theta]\!], J\tilde{\omega}[\![\eta]\!]) = J\tilde{\omega}[\![(\theta, \eta)]\!]$.
- **case** (θ, η), error on left: $I\omega[\![(\theta, \eta)]\!] = \bot$ and $I\omega[\![\theta]\!] = \bot \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\theta]\!] = J\tilde{\omega}[\![(\theta, \eta)]\!]$.
- **case** (θ, η), error on right: $I\omega[\![(\theta, \eta)]\!] = \bot$ and $I\omega[\![\eta]\!] = \bot \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![(\theta, \eta)]\!]$.
- **case** $\iota x\, \phi$, exists unique: $I\omega[\![\iota x\, \phi]\!] =$ unique $v \in \mathbf{Tree}(\mathbb{R})$ s.t. $\omega^v_x[\![\phi]\!] = \oplus$. We take special care in applying the IH because $\iota x\, \phi$, unlike other term constructors, binds a variable x in ϕ. Because the IH is general in the states, for *all* $u \in \mathbf{Tree}(\mathbb{R})$ we have $I\omega^u_x[\![\phi]\!] = J\tilde{\omega}^u_x[\![\phi]\!]$ since ω^u_x and $\tilde{\omega}^u_x$ agree both on x and on $\text{FV}(\iota x\, \phi) = \text{FV}(\phi) \setminus \{x\}$, thus they agree on $\text{FV}(\phi)$. This holds both for u and all other v so u is also unique u where $J\tilde{\omega}^u_x[\![\phi]\!] = \oplus$ so $u = J\tilde{\omega}[\![\iota x\, \phi]\!]$.
- **case** $\theta = \iota x\, \phi$, does not exist uniquely: Since $I\omega[\![\iota x\, \phi]\!] = \bot$, there are either zero or multiple $v \in \mathbf{Tree}(\mathbb{R})$ such that $\omega^v_x[\![\phi]\!] = \oplus$. Then for *all* $u \in \mathbf{Tree}(\mathbb{R})$ by IH have $I\omega^u_x[\![\phi]\!] = J\tilde{\omega}^u_x[\![\phi]\!]$ since ω^u_x and $\tilde{\omega}^u_x$ agree both on x and on $\text{FV}(\iota x\, \phi) = \text{FV}(\phi) \setminus \{x\}$, thus they agree on $\text{FV}(\phi)$. This holds both for all u so there is no unique v where $J\tilde{\omega}^v_x[\![\phi]\!] = \oplus$ so $J\tilde{\omega}[\![\iota x\, \phi]\!] = \bot$.
- **case** $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$: Proceed by a nested induction on the denotation $v = I\omega[\![\theta]\!]$.
  - **case** Base case $v = \bot$: Then because θ is structurally simpler than $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ we apply the outer IH to θ and prove $I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] = \bot = J\tilde{\omega}[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!]$.
  - **case** Base case $v = ()$: Then

$$I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] = \quad I\omega[\![\eta]\!] \stackrel{=}{\text{IH}} J\tilde{\omega}[\![\eta]\!] = J\tilde{\omega}[\![\mathsf{mr}(\theta, \eta, s\ \gamma, lr\ \zeta)]\!]$$

  - **case** Base case $v \in \mathbb{R}$: Then

$$\begin{aligned}
&I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] \\
=&\mathsf{Reduce}(I\omega[\![\theta]\!], I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega) \\
=_{\text{case}}&I\omega^{I\omega[\![\theta]\!]}_s[\![\zeta]\!] \\
\stackrel{=}{\text{IH}}&I\omega^{J\tilde{\omega}[\![\theta]\!]}_s[\![\zeta]\!] \\
\stackrel{=}{\text{IH}}&J\tilde{\omega}^{J\tilde{\omega}[\![\theta]\!]}_s[\![\zeta]\!] \\
=&\mathsf{Reduce}(J\tilde{\omega}[\![\theta]\!], J\tilde{\omega}[\![\eta]\!], s\ \zeta, lr\ \gamma, J\tilde{\omega}) \\
=&J\tilde{\omega}[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!].
\end{aligned}$$

– **case** Inductive case $v = (L, R)$: Then

$$\begin{aligned} & I\omega[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!] \\ =& \mathsf{Reduce}(I\omega[\![\theta]\!], I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega) \\ =& \mathsf{Reduce}((L, R), I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega) \end{aligned}$$

Then let $\tilde{L} = \mathsf{Reduce}(L, I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega)$ and let $\tilde{R} = \mathsf{Reduce}(R, I\omega[\![\eta]\!], s\ \zeta, lr\ \gamma, I\omega)$ then by the inner IH we have $\tilde{L} = \mathsf{Reduce}(L, J\tilde{\omega}[\![\eta]\!], s\ \zeta, lr\ \gamma, J\tilde{\omega})$ and we have $\tilde{R} = \mathsf{Reduce}(R, J\tilde{\omega}[\![\eta]\!], s\ \zeta, lr\ \gamma, J\tilde{\omega})$.

Then we have $J\tilde{\omega}^{\tilde{L},\tilde{R}}_{l,r}[\![\gamma]\!] = J\tilde{\omega}^{\tilde{L},\tilde{R}}_{l,r}[\![\gamma]\!] = \mathsf{Reduce}((L, R), J\tilde{\omega}[\![\eta]\!], s\ \zeta, lr\ \gamma, J\tilde{\omega}) = J\tilde{\omega}[\![\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)]\!]$.

- **case** $(\theta)'$ exists: Then $I\omega[\![(\theta)']\!] = \sum_{d\in\mathsf{Dim}(\mathrm{FV}(\theta))} \frac{\partial I\omega[\![\theta]\!]}{\partial d}\omega'(d) = \sum_{d\in\mathsf{Dim}(\mathrm{FV}(\theta))} \frac{\partial I\omega[\![\theta]\!]}{\partial d}\tilde{\omega}'(d)$ which by the IH is equal to $\sum_{d\in\mathrm{FV}(\theta)} \frac{\partial J\tilde{\omega}[\![\theta]\!]}{\partial d}\tilde{\omega}'(d) = J\tilde{\omega}[\![(\theta)']\!]$ since $\omega = \tilde{\omega}$ on $\mathrm{FV}((\theta)')$ which includes d' for each $d \in \mathsf{Dim}(\mathrm{FV}(\theta))$ and thus d' for every nonzero term of $\left(\sum_{d\in\mathsf{Dim}(\mathrm{FV}(\theta))}\right)$ since the partial differential of $J\tilde{\omega}[\![\theta]\!]$ with respect to any $d \notin \mathsf{Dim}(\mathrm{FV}(\theta))$ is 0. Furthermore the IH applies since θ is simpler than $(\theta)'$ and $\mathrm{FV}(\theta) \subseteq \mathrm{FV}((\theta)')$. More precisely, to show that the partial derivatives $\frac{\partial I\omega[\![\theta]\!]}{\partial d}\omega'(d)$ and $\frac{\partial J\tilde{\omega}[\![\theta]\!]}{\partial d}\tilde{\omega}'(d)$ agree, we note that they are both taken by varying d among some values $D : \mathbb{R}$ in its neighborhood. We apply the IH for *each* $d \in D$ to show $I\omega^D_d[\![\theta]\!] = J\tilde{\omega}^D_d[\![\theta]\!]$ to get that the partials are equal. Each IH application is allowed since $\omega^D_d = \tilde{\omega}^D_d$ on $\{d\} \cup \mathrm{FV}(\theta)$ and $\omega = \tilde{\omega}$ on $\mathrm{FV}(\theta)$.

- **case** $(\theta)'$ does not exist: This case applies iff $\sum_{d\in\mathsf{Dim}_\omega(\mathrm{FV}(\theta))} \frac{\partial I\omega[\![\theta]\!]}{\partial d}\omega'(d)$ does not exist. Only the following cases are possible:

  1. $\omega(d)$ and $\omega(d')$ differ in shape for some d such that $\|\frac{\partial I\omega[\![\theta]\!]}{\partial d}\| > 0$. Then $d \in \mathsf{Dim}_\omega(\mathrm{FV}(\theta))$ because nonfree variables have partial derivative 0, and $\{d, d'\} \subseteq \mathrm{FV}((\theta)')$. Then $\omega = \tilde{\omega}$ on $\{d, d'\}$ by assumption. By IH $\|\frac{\partial J\tilde{\omega}[\![\theta]\!]}{\partial d}\| = \|\frac{\partial I\omega[\![\theta]\!]}{\partial d}\| > 0$ and $\tilde{\omega}(x)$ and $\tilde{\omega}(x')$ differ in shape, so $J\tilde{\omega}[\![(\theta)']\!] = \bot$. item For every neighborhood $\mathcal{N}_\xi(\omega) = \{\nu \text{ s.t. } \|\nu - \omega\| < \xi\}$ there exist two states $\nu, \mu \in \mathcal{N}_\xi(\omega)$ 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 $\mathsf{shape}(\theta)$ (which is allowable by our choice of induction metric) assume without loss of generality that $\nu = \mu = \omega$ on $\{\mathrm{FV}(\theta)\}^{\complement}$ 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 $\mathrm{FV}(\theta)^{\complement}$, 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 $\{\tilde{\nu}, \tilde{\mu}\} \subseteq \mathcal{N}_\xi(\tilde{\omega}) = \{\nu \mid \|\nu - \tilde{\omega}\| < \xi\}$. Because this argument is generic in ξ then every neighborhood of $\tilde{\omega}$ has $\tilde{\nu}, \tilde{\mu}$ where the shape of θ differs, so $J\tilde{\omega}[\![(\theta)']\!] = \bot$.
  2. $I[\![\theta]\!]$ is not totally 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. 32, 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 $\mathrm{FV}(\theta)^{\complement}$. 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 $J\tilde{\omega}[\![(\theta)']\!] = \bot$ as desired.

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

- **case** $\theta \geq \eta$ both exist: $I\omega[\![\theta \geq \eta]\!] = \mathsf{Geq}(u, v)I\omega$ where $u = I\omega[\![\theta]\!], v = I\omega[\![\eta]\!]$. Then by IH $u = J\tilde{\omega}[\![\theta]\!], v = J\tilde{\omega}[\![\eta]\!]$ so by functionality of $\mathsf{Geq}(\cdot,\cdot)$, have $\mathsf{Geq}(u, v) = J\tilde{\omega}[\![\theta \geq \eta]\!]$.

- **case** $\theta \geq \eta$ not both exist: Then have $u = I\omega[\![\theta]\!] = \bot$, or $v = I\omega[\![\eta]\!] = \bot$, so by IH $J\tilde{\omega}[\![\theta]\!] = \bot$ or $J\tilde{\omega}[\![\eta]\!] = \bot$, so $J\tilde{\omega}[\![\theta \geq \eta]\!] = \bot$.

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

- **case** $C(\phi)$: Note $\omega = \tilde{\omega}$ since $\mathrm{FV}(C(\phi)) = \mathcal{V} \cup \mathcal{V}'$. We write the partial application $I[\![\phi]\!] : \mathcal{S} \to \{\oplus, \oslash, \ominus\}$ as 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** $\forall x\, \phi$: $I\omega[\![\forall x\, \phi]\!] = \sqcap_{v\in\mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![\phi]\!] \overset{=}{\text{IH}} \sqcap_{v\in\mathbf{Tree}(\mathbb{R})} J\tilde{\omega}^d_x[\![\phi]\!] = J\tilde{\omega}[\![\forall x\, \phi]\!]$.

- **case** $[\alpha]\phi$: $I\omega[\![[\alpha]\phi]\!] = \sqcap_{\nu \mid (\omega,\nu)\in I[\![\alpha]\!]} I\nu[\![\phi]\!] \overset{=}{\text{IH}} \sqcap_{\tilde{\nu} \mid (\tilde{\omega},\tilde{\nu})\in J[\![\alpha]\!]} J\tilde{\nu}[\![\phi]\!] = J\tilde{\omega}[\![[\alpha]\phi]\!]$.

- **case** a for program constant a: Have $I(a) = J(a)$ by assumption and since $\mathrm{FV}(a) = \mathcal{V} \cup \mathcal{V}'$ have $\omega = \tilde{\omega}$. Let $\tilde{\nu} = nu$, then $(\omega, \nu) \in I[\![a]\!]$ iff $(\omega, \nu) \in I(a)$ iff $(\omega, \nu) \in J(a)$ iff $(\tilde{\omega}, \tilde{\nu}) \in J(a)$.

- **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 $\{x\} = \mathrm{MBV}(x := \theta)$ by IH above and agrees also on $V \setminus \{x\}$ 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 $\mathrm{FV}(\phi)$ 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 $\mathrm{BV}(?\phi) = \emptyset$.

- **case** $x' = \theta \,\&\, \psi$: $(\omega, \nu) \in I[\![x' = \theta \,\&\, \psi]\!]$, let r be such that $\varphi(r) = \nu$ and $\varphi(0) = \omega$ on $\{x'\}^{\complement}$. Now define $\tilde{\varphi}(s) = \varphi(s)$ on $\{x, x'\}$ and $\tilde{\varphi}(s) = \tilde{\nu}(s)$ on $\{x, x'\}^{\complement}$. 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 the inductive hypotheses, 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 $\{x, x'\}^{\complement}$ and $\tilde{\omega} = \tilde{\varphi}(s)$ on the same, by construction.

- **case** $\alpha \cup \beta$: Recall that $\mathrm{MBV}(\alpha)$ are the variables which are bound on every execution of α. From $(\omega, \nu) \in I[\![\alpha \cup \beta]\!]$ have either (1a) $(\omega, \nu) \in I[\![\alpha]\!]$ or (1b)$(\omega, \nu) \in I[\![\beta]\!]$. Since $\mathrm{FV}(\alpha) \subseteq \mathrm{FV}(\alpha \cup \beta)$, and $\mathrm{FV}(\beta) \subseteq \mathrm{FV}(\alpha \cup \beta)$ we can apply the IH in both case (1a) and case (1b). Then there exists $\tilde{\nu}$ such that either (2a) $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha]\!]$ and $\tilde{\nu}$ agrees with ν on $V \cup \mathrm{MBV}(\alpha)$, or (2b) $(\tilde{\omega}, \tilde{\nu}) \in I[\![\beta]\!]$ and $\tilde{\nu}$ agrees with ν on $V \cup \mathrm{MBV}(\beta)$. In case (2a) $\mathrm{MBV}(\alpha) \supseteq \mathrm{MBV}(\alpha \cup \beta)$ and in case (2b) $\mathrm{MBV}(\beta) \supseteq \mathrm{MBV}(\alpha \cup \beta)$, so in each case (3) ν and $\tilde{\nu}$ agree on $\mathrm{MBV}(\alpha \cup \beta) \cup V$. In each case respectively (4a) $J[\![\alpha]\!] \subseteq J[\![\alpha \cup \beta]\!]$ or (4b) $J[\![\beta]\!] \subseteq J[\![\alpha \cup \beta]\!]$. In each case, it follows from (3) that (5) $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha \cup \beta]\!]$.

- **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 $\mathrm{FV}(\alpha) \subseteq \mathrm{FV}(\alpha; \beta)$, the IH on α is applicable. By the IH on α, there exists $\tilde{\mu}$ s.t. (X1) $(\tilde{\omega}, \tilde{\mu}) \in J[\![\alpha]\!]$ where $\tilde{\mu}$ agrees with μ on $V \cup \mathrm{MBV}(\alpha)$. Since $V \supseteq \mathrm{FV}(\alpha; \beta)$ then $V \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\alpha; \beta) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\beta)$. Then by the IH on β there exists some $\tilde{\nu}$ s.t. (X2) $(\tilde{\mu}, \tilde{\nu}) \in J[\![\beta]\!]$ and $\nu = \tilde{\nu}$ on $(V \cup \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\beta) = V \cup \mathrm{MBV}(\alpha; \beta)$. From (X1) and (X2) we have $(\tilde{\omega}, \tilde{\nu}) \in J[\![\alpha; \beta]\!]$ which completes the case since we just showed $\nu = \tilde{\nu}$ on $V \cup \mathrm{MBV}(\alpha; \beta)$.

- **case** α^*: Recall α^n is structurally simpler than α^*. Have $(\omega, \nu) \in I[\![\alpha^*]\!]$ iff exists $n \in \mathbb{N}$ s.t. $(\omega, \nu) \in I[\![\alpha^n]\!]$. In case $n = 0$ then $\nu = \omega$, so we likewise let $\tilde{\nu} = \tilde{\omega}$. The case follows from the fact $\mathrm{MBV}(\alpha^*) = \emptyset$ and the agreement of ω with $\tilde{\omega}$. 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 $J[\![\alpha^n]\!] \subseteq J[\![\alpha^*]\!]$.

□

For substitution in programs, we will also need a *bound effect* lemma saying that only bound variables of a program will change during its execution.

Lemma 37 (Bound effect). If $(\omega, \nu) \in I[\![\alpha]\!]$ then $\omega = \nu$ on $\mathrm{BV}(\alpha)^{\complement}$.

Proof. By induction on α.

- **case** a: This case is vacuous since $\mathrm{BV}(a)^{\complement} = (\mathcal{V} \cup \mathcal{V}')^{\complement} = \emptyset$.

- **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 $\{x, x'\}^{\complement}$ and $\nu = \varphi(r)$ for solution φ of duration at least r. Then $\varphi(s) = \omega$ on $\{x, x'\}^{\complement}$ for all s in its domain. So $\omega = \nu$ on $\{x, x'\}^{\complement} = \mathrm{BV}(x' = \theta \,\&\, \psi)^{\complement}$ 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 $\mathrm{BV}(\alpha)^{\complement}$ or $\mathrm{BV}(\beta)^{\complement}$ and thus in both cases on $\mathrm{BV}(\alpha)^{\complement} \cap \mathrm{BV}(\beta)^{\complement} = \mathrm{BV}(\alpha \cup \beta)^{\complement}$.

- **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 IHs $\omega = \mu$ on $\mathrm{BV}(\alpha)^{\complement}$ and $\mu = \nu$ on $\mathrm{BV}(\beta)^{\complement}$ so by transitivity $\omega = \nu$ on $\mathrm{BV}(\alpha)^{\complement} \cap \mathrm{BV}(\beta)^{\complement} = \mathrm{BV}(\alpha;\ \beta)^{\complement}$.

- **case** α^*: $(\omega,\nu) \in I[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}} I[\![\alpha^n]\!]$, i.e., there exists $n \in \mathbb{N}$ and $\omega_0,\ldots,\omega_n$ such that $\omega = \omega_0, \nu = \omega_n$ and for all $(k \in [0,n-1])$ have $(\omega_k,\omega_{k+1}) \in I[\![\alpha]\!]$. We proceed by induction on n.

  In the case $n = 0$ then $\omega = \omega_0 = \omega_k = \nu$, so trivially ω and ν agree on $\mathcal{V} \cup \mathcal{V}' \supseteq \mathrm{BV}(\alpha^*)^{\complement}$.

  Else $n = k+1$ for some $k \in \mathbb{N}$. Then $(\omega_0,\omega_1) \in I[\![\alpha]\!]$ and $(\omega_1,\omega_k) \in I[\![\alpha]\!]$ for some ω_1 and for $\omega = \omega_0, \nu = \omega_k$. By the outer IH, $\omega_0 = \omega_1$ on $\mathrm{BV}(\alpha)^{\complement} = \mathrm{BV}(\alpha^*)^{\complement}$. By the inner IH, $\omega_1 = \omega_k$ on $\mathrm{BV}(\alpha^*)^{\complement}$. By transitivity, $\omega = \nu$ on $\mathrm{BV}(\alpha^*)^{\complement}$ as desired.

□

We give the substitution algorithm in Fig. 11. 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 occurrences of the variables bound at that constructor. Admissibility conditions are checked recursively during the substitution algorithm proper (Fig. 11). Recall the definition of $U-$admissibility from Def. 4:

> 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 $\mathrm{FV}(\sigma|_{\Sigma(\phi)}) \cap U = \emptyset$ where $\sigma|_{\Sigma(\phi)}$ is the restriction of σ that only replaces symbols that occur in ϕ and $\mathrm{FV}(\sigma) = \bigcup_{f\in\sigma} \mathrm{FV}(\sigma f(\cdot)) \cup \bigcup_{p\in\sigma} \mathrm{FV}(\sigma p(\cdot))$ 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. 11.

U-admissibility makes the admissibility conditions precise. Note also in Fig. 11 that the symbol $\cdot$ is a reserved nullary function symbol standing for an argument term and $\_$ is a reserved nullary predicate symbol standing for an argument predicate.

To assist in proving the soundness of substitutions, we also define *adjoint interpretations* $\sigma^*_\omega I$ which capture the effect of a substitution σ on the interpretation I at state ω.

6.2 Adjoint lemma proof

Definition 5 (Adjoint interpretation)**.** For any interpretation I, state ω, and admissible substitution σ, the adjoint interpretation $\sigma^*_\omega I$ is defined by:

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

where $\cdot$ is a reserved function symbol and $\_$ is a reserved predicate symbol.

Case	Replacement	Admissible when:
$\sigma(())$	$= ()$	
$\sigma(q)$	$= q$	
$\sigma(x)$	$= x$	
$\sigma(\theta+\eta)$	$= \sigma(\theta)+\sigma(\eta)$	
$\sigma(\theta\cdot\eta)$	$= \sigma(\theta)\cdot\sigma(\eta)$	
$\sigma(f(\theta))$	$= \{\cdot\mapsto\sigma(\theta)\}(\sigma f)$ if $f\in\sigma$, else $f(\sigma(\theta))$	
$\sigma(\iota x\,\phi)$	$= \iota x\,\sigma(\phi)$	σ is $\{x\}$-admissible in ϕ
$\sigma((\theta,\eta))$	$= (\sigma(\theta),\sigma(\eta))$	
$\sigma(\mathsf{mr}(\theta,\eta,s\;\zeta,lr\;\gamma))$	$= \mathsf{mr}(\sigma(\theta),\sigma(\eta),s\;\sigma(\zeta),lr\;\sigma(\gamma))$	σ is $\{s\}$-admissible in ζ σ is $\{l,r\}$-admissible in γ
$\sigma(x:=\theta)$	$= x:=\sigma(\theta)$	
$\sigma(\{x'=\theta\,\&\,\psi\})$	$= \{x'=\sigma(\theta)\,\&\,\sigma(\psi)\}$	σ is $\{x,x'\}$-admissible in θ,ψ
$\sigma(?(\phi))$	$=?(\sigma(\phi))$	
$\sigma(\alpha;\beta)$	$= \sigma(\alpha);\sigma(\beta)$	σ is $\mathrm{BV}(\sigma(\alpha))$-admissible in β
$\sigma(\alpha\cup\beta)$	$= \sigma(\alpha)\cup\sigma(\beta)$	
$\sigma(\alpha^*)$	$= \sigma(\alpha)^*$	σ is $\mathrm{BV}(\sigma(\alpha))$-admissible in α
$\sigma(a)$	$= \sigma a$ if $a\in\sigma$, else a	
$\sigma(\theta\geq\eta)$	$= \sigma(\theta)\geq\sigma(\eta)$	
$\sigma(p(\theta))$	$= \{\cdot\mapsto\sigma(\theta)\}(\sigma p)$ if $p\in\sigma$, else $p(\sigma(\theta))$	
$\sigma(C(\phi))$	$= \{\_\mapsto\sigma(\phi)\}(\sigma C)$ if $C\in\sigma$, else $C(\sigma(\phi))$	σ is $\mathcal{V}\cup\mathcal{V}'$-admissible in ϕ
$\sigma(\neg\phi)$	$= \neg\sigma(\phi)$	
$\sigma(\phi\wedge\psi)$	$= \sigma(\phi)\wedge\sigma(\psi)$	
$\sigma(\forall x\,\phi)$	$= \forall x\,\sigma(\phi)$	σ is $\{x\}$-admissible in ϕ
$\sigma([\alpha]\phi)$	$= [\sigma(\alpha)]\sigma(\phi)$	σ is $\mathrm{BV}(\sigma(\alpha))$-admissible in ϕ

Figure 11: Uniform substitution algorithm

Lemma 38 (Adjoint agreement). If $\omega = \nu$ on $\mathrm{FV}(\sigma)$ 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 $U^{\complement}$ 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. 36, $\cdot^*_d I\omega[\![\sigma f(\cdot)]\!] = \cdot^*_d I\nu[\![\sigma f(\cdot)]\!]$ when $\omega = \nu$ on $\mathrm{FV}(\sigma f(\cdot)) \subseteq \mathrm{FV}(\sigma)$. Also by Lem. 36, $\cdot^*_d I\omega[\![\sigma p(\cdot)]\!] = \cdot^*_d I\nu[\![\sigma p(\cdot)]\!]$ 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 $\mathrm{FV}(\sigma f(\cdot)) \subseteq U^{\complement}$ for every function symbol f and (likewise predicate p) in $\Sigma(\phi$ or θ or $\alpha)$. 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 $U^{\complement}$ then $\sigma^*_\omega I = \sigma^*_\nu I$ on $\Sigma(\phi, \theta, \alpha)$.

Then by Lem. 36 (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 $\sigma^*_\omega I[\![\alpha]\!] = \sigma^*_\nu I[\![\alpha]\!]$. □

Using adjoint interpretations, we state and prove a *substitution lemma* syntactic substitution has the same effect as taking an adjoint semantically. Soundness will be a short corollary of this lemma.

Lemma 39 (Substitutions). 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. $I[\![\sigma(\alpha)]\!] = \sigma^*_\omega I[\![\alpha]\!]$

Proof. We proceed by cases.

- **case** q: $I\omega[\![\sigma(q)]\!] = I\omega[\![q]\!] = q = \sigma^*_\omega I\omega[\![q]\!]$.
- **case** x: $I\omega[\![\sigma(x)]\!] = I\omega[\![x]\!] = \omega(x) = \sigma^*_\omega I\omega[\![x]\!]$.
- **case** $\theta+\eta$ exists: $I\omega[\![\sigma(\theta+\eta)]\!] = I\omega[\![\sigma(\theta)]\!]+I\omega[\![\sigma(\eta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]+\sigma^*_\omega I\omega[\![\eta]\!] = \sigma^*_\omega I\omega[\![\theta+\eta]\!]$.
- **case** $\theta + \eta$ does not exist: Then have $I\omega[\![\sigma(\theta)]\!] = \bot$ or $I\omega[\![\sigma(\eta)]\!] = \bot$, so by IH either $\sigma^*_\omega I\omega[\![\theta]\!] = \bot$ or $\sigma^*_\omega I\omega[\![\eta]\!] = \bot$ thus $\sigma^*_\omega I\omega[\![\theta+\eta]\!]$.
- **case** $\theta \cdot \eta$ exists: $I\omega[\![\sigma(\theta \cdot \eta)]\!] = I\omega[\![\sigma(\theta)]\!] \cdot I\omega[\![\sigma(\eta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!] \cdot \sigma^*_\omega I\omega[\![\eta]\!] = \sigma^*_\omega I\omega[\![\theta \cdot \eta]\!]$.
- **case** $\theta \cdot \eta$ does not exist: Then $I\omega[\![\sigma(\theta)]\!] = \bot$ or $I\omega[\![\sigma(\eta)]\!] = \bot$, so by IH either $\sigma^*_\omega I\omega[\![\theta]\!] = \bot$ or $\sigma^*_\omega I\omega[\![\eta]\!] = \bot$ thus $\sigma^*_\omega I\omega[\![\theta \cdot \eta]\!]$.

- **case** $()$: $I\omega[\![\sigma(\,())]\!] = I\omega[\![\,()\,]\!] = \top = \sigma^*_\omega I\omega[\![\,()\,]\!]$.

- **case** (θ, η) exists: $I\omega[\![\sigma((\theta,\eta))]\!] = (I\omega[\![\sigma(\theta)]\!], I\omega[\![\sigma(\eta)]\!])$
$= (\sigma^*_\omega I\omega[\![\theta]\!], \sigma^*_\omega I\omega[\![\eta]\!]) = \sigma^*_\omega I\omega[\![(\theta,\eta)]\!]$.

- **case** (θ, η) does not exist: Then have $I\omega[\![\sigma(\theta)]\!] = \bot$ or $I\omega[\![\sigma(\eta)]\!] = \bot$ so by IH either $\sigma^*_\omega I\omega[\![\theta]\!] = \bot$ or $\sigma^*_\omega I\omega[\![\eta]\!]$ thus $\sigma^*_\omega I\omega[\![(\theta,\eta)]\!] = \bot$.

- **case** $\iota x\, \phi$: Then $I\omega[\![\sigma(\iota x\, \phi)]\!] =$ the unique $v \in \mathbf{Tree}(\mathbb{R})$ s.t. $\omega^v_x[\![\sigma(\phi)]\!] = \oplus$. For each $u \in \mathbf{Tree}(\mathbb{R})$, apply IH and have $\omega^u_x[\![\phi]\!] = \sigma^*_{\omega^u_x} I\omega^u_x[\![\phi]\!]$. Then by $\{x\}$-admissibility and since ω agrees with ω^v_x on $\{x\}^\complement$ have $\sigma^*_{\omega^v_x} I\omega^v_x[\![\phi]\!] = \sigma^*_\omega I\omega^v_x[\![\phi]\!]$. Since this was for all s, then uniqueness is preserved, so v is the ***unique*** v such that $\sigma^*_\omega I\omega^v_x[\![\phi]\!] = \oplus$ so $v = \sigma^*_\omega I\omega[\![\iota x\, \phi]\!]$.

- **case** $\iota x\, \phi$ does not exist: In this case there are 0 or multiple $v \in \mathbf{Tree}(\mathbb{R})$ s.t. $I\omega^v_x[\![\sigma(\phi)]\!] = \oplus$. By IH, admissibility, and Lem. 38, for each such v have $\omega^v_x[\![\sigma(\phi)]\!] = \sigma^*_\omega I\omega^v_x[\![\phi]\!]$, so non-uniqueness and non-existence are preserved, so $\sigma^*_\omega I\omega[\![\iota x\, \phi]\!] = \bot$ as desired.

- **case** $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ does not exist: Then $I\omega[\![\sigma(\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma))]\!]$ and $I\omega[\![\sigma(\theta)]\!] = \bot$ so by IH $\cdots = \sigma^*_\omega I\omega[\![\theta]\!]$ and $\sigma^*_\omega I\omega[\![\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma)]\!] = \bot$ as desired.

- **case** $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ first base case: In this case we first have the chain of equivalences $I\omega[\![\sigma(\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma))]\!] = I\omega[\![\mathsf{mr}(\sigma(\theta),\sigma(\eta),s\ \sigma(\zeta), lr\ \sigma(\gamma))]\!] = I\omega[\![\sigma(\eta)]\!]$ then by IH $\cdots = \sigma^*_\omega I\omega[\![\eta]\!]$.

- **case** $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ second base case: Then $I\omega[\![\sigma(\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma))]\!] = I\omega^{I\omega[\![\sigma(\theta)]\!]}_u[\![\sigma(\zeta)]\!]$. By first IH, $\cdots = I\omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_u[\![\eta]\!]$ and by second IH $\cdots = \sigma^*_{\omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_u} I\omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_u[\![\eta]\!]$. Then by admissibility $I\omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_u$ agrees with ω on $\{u\}^\complement$ so by Lem. 38 have $\cdots = \sigma^*_\omega I\omega^{\sigma^*_\omega I\omega[\![\theta]\!]}_u[\![\eta]\!]$ Which is then $\cdots = \sigma^*_\omega I\omega[\![\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma)]\!]$ as desired.

- **case** $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ inductive: Then $I\omega[\![\sigma(\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma))]\!] = I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![\sigma(\gamma)]\!]$ for $\tilde{L}, \tilde{R} = \mathsf{Reduce}(L, \eta, s\ \zeta, lr\ \gamma, I\omega), \mathsf{Reduce}(R, \eta, s\ \zeta, lr\ \gamma, I\omega)$ and $(L, R) = I\omega[\![\sigma(\theta)]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$ by IH. Then by IH 4 $I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![\sigma(\gamma)]\!] = \sigma^*_{\omega^{\tilde{L},\tilde{R}}_{l,r}} I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![\gamma]\!]$ which by admissibility condition is $\cdots = \sigma^*_\omega I\omega^{\tilde{L},\tilde{R}}_{l,r}[\![\gamma]\!]$ which by definition is $\mathsf{Reduce}(\sigma^*_\omega I\omega[\![\theta]\!], \eta, s\ \zeta, lr\ \gamma, \sigma^*_\omega I\omega)$ which is $\sigma^*_\omega I\omega[\![\mathsf{mr}(\theta,\eta,s\ \zeta, lr\ \gamma)]\!]$ 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** $(\theta)'$ does not 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:

$$\begin{aligned}&I\omega[\![\sigma(f(\theta))]\!]\\=&I\omega[\![\{\cdot\mapsto\sigma(\theta)\}\sigma f]\!]\\=&I^d_\cdot[\![\sigma f]\!]\\=&\sigma^*_\omega I(f)(d)\\=&\sigma^*_\omega I(f)(\sigma^*_\omega I\omega[\![\theta]\!])\\=&\sigma^*_\omega I\omega[\![f(\theta)]\!]\end{aligned}$$

  (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** $\theta \geq \eta$ both exist:

$$\begin{aligned}&I\omega[\![\sigma(\theta\geq\eta)]\!]\\=&\mathsf{Geq}(I\omega[\![\sigma(\theta)]\!],I\omega[\![\sigma(\eta)]\!])I\omega\\=&\mathsf{Geq}(\sigma^*_\omega I\omega[\![\theta]\!],\sigma^*_\omega I\omega[\![\eta]\!])I\omega\\=&\sigma^*_\omega I\omega[\![\theta\geq\eta]\!]\end{aligned}$$

- **case** $\theta \geq \eta$ not both exist: Then $I\omega[\![\sigma(\theta)]\!] = \bot$ or $I\omega[\![\sigma(\eta)]\!]$ so by IH either $\sigma^*_\omega I\omega[\![\theta]\!] = \bot$ or $\sigma^*_\omega I\omega[\![\eta]\!]$ so $\sigma^*_\omega I\omega[\![\theta \geq \eta]\!] = \oslash$ as desired.

- **case** $p(\theta)$ for $p \in \sigma$: $I\omega[\![\sigma(p(\theta))]\!] = I\omega[\![\{\cdot \mapsto \sigma(\theta)\}\sigma p]\!] = I^d_\cdot[\![\sigma p]\!] = \sigma^*_\omega I(p)(d) = \sigma^*_\omega I(p)(\sigma^*_\omega I\omega[\![\theta]\!]) = \sigma^*_\omega I\omega[\![p(\theta)]\!]$ (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** $p(\theta)$ for $p \notin \sigma$: $I\omega[\![\sigma(p(\theta))]\!] = I\omega[\![p(\sigma(\theta))]\!] = \sigma^*_\omega I\omega[\![p(\theta)]\!]$ by IH.

- **case** $C(\phi)$ for $C \in \sigma$: We reason by a chain of equalities: $I\omega[\![\sigma(C(\phi))]\!] = I\omega[\![\{\_ \mapsto \sigma(\phi)\}\sigma C]\!] = I^d_\_\omega[\![\sigma C]\!] =_1 (\sigma^*_\omega I)(C)(d)(\omega) =_2 (\sigma^*_\omega I)(C)(\mu \mapsto \sigma^*_\omega I\mu[\![\phi]\!])(\omega) = \sigma^*_\omega I\omega[\![C(\phi)]\!]$ (by IH on ϕ) where we define d as the map $\mu \mapsto I\mu[\![\sigma(\phi)]\!] = \sigma^*_\mu I\mu[\![\phi]\!]$ by IH on ϕ. The step marked (1) uses the definition of adjoints while the step marked (2) uses the fact that for all μ, $\sigma^*_\omega I\omega[\![\phi]\!] = \sigma^*_\mu I\omega[\![\phi]\!]$ by Lem. 38, which is applicable using the assumption that σ is $\mathcal{V} \cup \mathcal{V}'$-admissible in ϕ.

- **case** $C(\phi)$ for $C \notin \sigma$: $I\omega[\![\sigma(C(\phi))]\!] = I\omega[\![C(\sigma(\phi))]\!] = \sigma^*_\omega I\omega[\![C(\phi)]\!]$.

- **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** $\phi \wedge \psi$: $I\omega[\![\sigma(\phi \wedge \psi)]\!] = I\omega[\![\sigma(\phi)]\!] \sqcap I\omega[\![\sigma(\psi)]\!] \overset{=}{\text{IH}} \sigma^*_\omega I\omega[\![\phi]\!] \sqcap \sigma^*_\omega I\omega[\![\psi]\!] = \sigma^*_\omega I\omega[\![\phi \wedge \psi]\!]$.

- **case** $\forall x\, \phi$:

$$\begin{aligned}
&I\omega[\![\sigma(\forall x\, \phi)]\!]\\
=&\sqcap_{v\in\mathbf{Tree}(\mathbb{R})} I\omega^v_x[\![\sigma(\phi)]\!]\\
\overset{=}{\text{IH}}&\sqcap_{v\in\mathbf{Tree}(\mathbb{R})} \sigma^*_{\omega^v_x} I\omega^v_x[\![\phi]\!]\\
=_{Lem.\,38}&\sqcap_{v\in\mathbf{Tree}(\mathbb{R})} \sigma^*_\omega I\omega^v_x[\![\phi]\!]\\
=&\sigma^*_\omega I\omega[\![\forall x\, \phi]\!].
\end{aligned}$$

- **case** $[\alpha]\phi$: Then we have that

$$\begin{aligned}
&I\omega[\![\sigma([\alpha]\phi)]\!]\\
=&\sqcap_{\nu\ |\ (\omega,\nu)\in I[\![\sigma(\alpha)]\!]} I\omega[\![\sigma(\phi)]\!]\\
=&\overset{=}{\text{IH}}\sqcap_{\nu\ |\ (\omega,\nu)\in\sigma^*_\omega I[\![\alpha]\!]}\sigma^*_\nu I\omega[\![\phi]\!]\\
=_{Lem.\,38}&\sqcap_{\nu\ |\ (\omega,\nu)\in\sigma^*_\omega I[\![\alpha]\!]}\ \sigma^*_\omega I\omega[\![\phi]\!]\\
=&\sigma^*_\omega I\omega[\![[\alpha]\phi]\!].
\end{aligned}$$

- **case** a: Have $I[\![\sigma(a)]\!] = I[\![\sigma a]\!] = \sigma^*_\omega I(a) = \sigma^*_\omega I[\![a]\!]$ 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 there exists duration $r \in \mathbb{R}_{\geq 0}$ and exists $\varphi : [0,r] \to \mathcal{S}$ with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, $\varphi(r) = \nu$ and for all $t \in [0,r]$ $\varphi'(t) = I\varphi(t)[\![\sigma(\theta)]\!] = \sigma^*_{\varphi(t)} I\varphi(t)[\![\theta]\!]$ 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 $r \in \mathbb{R}_{\geq 0}$ and exists $\varphi : [0,r] \to \mathcal{S}$ with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, $\varphi(r) = \nu$ and for all $t \in [0,r]$ $\varphi'(t) = \sigma^*_\omega I\varphi(t)[\![\theta]\!]$ and $\sigma^*_\omega I\varphi(t)[\![\psi]\!] = \oplus$, which holds since $\sigma^*_\omega I\varphi(t)[\![\theta]\!] = \sigma^*_{\varphi(t)} I\varphi(t)[\![\theta]\!]$ and $\sigma^*_\omega I\omega[\![\psi]\!] = \sigma^*_{\varphi(t)} I\omega[\![\psi]\!]$ by Lem. 38 as σ is assumed $\{x,x'\}$-admissible for both. By Lem. 37, $\varphi(t)$ and ω agree on $\{x,x'\}^{\complement}$.

- **case** $\alpha \cup \beta$: Have $(\omega,\nu) \in I[\![\sigma(\alpha \cup \beta)]\!] = I[\![\sigma(\alpha)]\!] \cup I[\![\sigma(\beta)]\!] \overset{=}{\text{IH}} \sigma^*_\omega I[\![\alpha]\!] \cup \sigma^*_\omega I[\![\beta]\!] = \sigma^*_\omega I[\![\alpha \cup \beta]\!]$.

- **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. 38 and because σ is $\mathrm{BV}(\sigma(\alpha))$-admissible for β by this case of substitution and $\omega = \nu$ on $\mathrm{BV}(\sigma(\alpha))^{\complement}$ by Lem. 37 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. 38 $\sigma^*_{\omega_i} I = \sigma^*_\omega I$ for all i since σ is $\mathrm{BV}(\sigma(\alpha))$-admissible by case and since $\omega_i = \omega_{i+1}$ on $\mathrm{BV}(\sigma(\alpha))^\complement$ by Lem. 37. Then each $(\omega_i, \omega_{i+1}) \in \sigma^*_\omega I[\![\alpha]\!]$ and $(\omega,\nu) \in \sigma^*_\omega I[\![\alpha^*]\!]$.

□

Theorem 40 (Uniform substitution). Rule US is sound.

Proof. Assume ϕ is valid, so that for all I and ω, we have $I\omega[\![\phi]\!] = \oplus$. Since $\sigma^*_\omega I$ is also an interpretation, then for I and ω we have $\sigma^*_\omega I\omega[\![\phi]\!] = \oplus$. By Lem. 39, we have $I\omega[\![\sigma(\phi)]\!] = \oplus$. Because the argument was generic, then $\sigma(\phi)$ is desired. □

Soundness of the proof system then follows from validity of the axioms and soundness of US and of the other proof rules. Together, soundness and decidability show that formulas proved with the dL_ι calculus are indeed true and that the calculus is amenable to implementation.

6.3 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 41 (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 not conserved, because it is true for all real values of x, but fails when x is a tuple such as $(0,0)$, outside the domain of multiplication. This is why rule QE requires $\mathsf{in}\mathbb{R}(x)$ for each mentioned x. □

We transform dL quantifiers to real-valued dL_ι quantifiers to close the gap:

Theorem 42 (Converse reducibility). 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.

Proof. 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.

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. $I\omega[\![T(\theta+\eta)]\!] = I\omega[\![T(\theta)]\!] + I\omega[\![T(\eta)]\!] \overset{=}{\text{IH}} I\omega[\![\theta]\!]_{\mathsf{dL}} + I\omega[\![\eta]\!]_{\mathsf{dL}} = I\omega[\![\theta+\eta]\!]_{\mathsf{dL}}$.
4. $I\omega[\![T(\theta\cdot\eta)]\!] = I\omega[\![T(\theta)]\!] \cdot I\omega[\![T(\eta)]\!] \overset{=}{\text{IH}} I\omega[\![\theta]\!]_{\mathsf{dL}} \cdot I\omega[\![\eta]\!]_{\mathsf{dL}} = I\omega[\![\theta\cdot\eta]\!]_{\mathsf{dL}}$.
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. $I\omega[\![T(\theta \geq \eta)]\!] = (I\omega[\![T(\theta)]\!] \geq I\omega[\![T(\eta)]\!]) = (I\omega[\![\theta]\!]_{\mathsf{dL}} \geq I\omega[\![\eta]\!]_{\mathsf{dL}}) = I\omega[\![\theta \geq \eta]\!]_{\mathsf{dL}}$.
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:

$$\begin{aligned} & I\omega[\![T(\forall x\, \phi)]\!] \\ =& I\omega[\![\forall x\, (\mathsf{in}\mathbb{R}(x) \to T(\phi))]\!] \\ =& \sqcap_{v\in\mathbf{Tree}(\mathbb{R})}\, I\omega^v_x[\![\mathsf{in}\mathbb{R}(x) \to T(\phi)]\!] \\ =& \sqcap_{r\in\mathbb{R}}\, I\omega^r_x[\![T(\phi)]\!] \\ =& \sqcap_{r\in\mathbb{R}}\, I\omega^r_x[\![\phi]\!]_{\mathsf{dL}} \\ =& I\omega[\![\forall x\, \phi]\!]_{\mathsf{dL}}. \end{aligned}$$

5. $I\omega[\![[\alpha]\phi]\!] = \sqcap_{(\omega,\nu)\in I[\![\alpha]\!]} I\nu[\![\phi]\!] = \sqcap_{(\omega,\nu)\in I[\![\alpha]\!]_{\mathsf{dL}}} I\nu[\![\phi]\!]_{\mathsf{dL}} = I\omega[\![[\alpha]\phi]\!]_{\mathsf{dL}}$. 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. $I[\![T(x := \theta)]\!] = \{(\omega, \omega_x^v) \mid r = I\omega[\![\theta]\!], r \in \mathbb{R}\} = \{(\omega, \omega_x^v) \mid r = I\omega[\![\theta]\!]_{\mathsf{dL}}\} = I[\![x := \theta; ?\mathsf{in}\mathbb{R}(x)]\!]_{\mathsf{dL}}$.
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. $$\begin{aligned} & I[\![T(x' = \theta \,\&\, \psi)]\!] \\ =& \{(\omega, \varphi(r)) \mid \text{ exist solution } \varphi \text{ and } r \in \mathbb{R}_{\geq 0} \\ & \text{and for all } s \in [0, r] \text{ have } I\varphi(s)[\![T(\phi)]\!] = \oplus \text{ and } \varphi'(s)(x) = I\varphi(s)[\![T(\theta)]\!] \\ & \text{and } \omega = \varphi(0) \text{ on } \{x'\}^{\complement}\}. \end{aligned}$$

   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

   $$\begin{aligned} & \{(\omega, \varphi(r)) \mid \text{ exist solution } \varphi \text{ and } r \in \mathbb{R}_{\geq 0} \\ & \text{and for all } s \in [0, r] \text{ have } I\varphi(s)[\![T(\phi)]\!] = \oplus \text{ and } \varphi'(s)(x) = I\varphi(s)[\![T(\theta)]\!] \\ & \text{and } \omega = \varphi(0) \text{ on } \{x'\}^{\complement}\} \\ =& \{(\omega, \varphi(r)) \mid \text{ exist solution } \varphi \text{ and } r \in \mathbb{R}_{\geq 0} \\ & \text{and for all } s \in [0, r] \text{ have } I\varphi(s)[\![\phi]\!]_{\mathsf{dL}} = \oplus \text{ and } \varphi'(s)(x) = I\varphi(s)[\![\theta]\!]_{\mathsf{dL}} \\ & \text{and } \omega = \varphi(0) \text{ on } \{x'\}^{\complement}\} \\ =& I[\![x' = \theta \,\&\, \psi]\!]_{\mathsf{dL}} \end{aligned}$$

   as desired.

□

The greater challenge is to show that dL also suffices to express all dL_ι formulas and thus dL and dL_ι are equiexpressive:

Theorem 43 (Reducibility). There is a computable T s.t. for all formulas ϕ, interpretations I, and states ω in dL_ι, $I\omega[\![\phi]\!] = \oplus$ in dL_ι iff $I\omega[\![T(\phi)]\!] = \oplus$ in dL.

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_1 with all rigid symbols limited to interpretations as continuous functions, and dL is dL_C without such symbols.

6.3.1 Eliminate Tuples

By analogy to the dL-definable bijection between $\mathbb{R}$ and $\mathbb{R}^k$ for any k [25, Lem. A.1], there is a dL-definable bijection between finite trees of reals and reals. First, observe a real number 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 $\mathsf{mr}(\theta, \eta, s\ \zeta, lr\ \gamma)$ is easily implemented. The exception is systems of ODE's, but systems of ODE's are allowed in dL anyway.

6.3.2 Eliminate Definite Descriptions

Special care must be taken 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 (i.e., discrete ghost) variable x and an assumption $[z := x]\phi \wedge \forall y\, ([z := y]\phi \rightarrow y = x)$. 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 $p(x) \wedge \forall y\, ([x := y]\phi \rightarrow y = x)$ is made in the *same* context as the definite description term appears. For example:
$[y := 3](\iota z\, z + y = 0) < 0$ expands to $[y := 3](([z := x]z + y = 0) \wedge \forall y\, (([z := y]z + y = 0) \rightarrow y = x) \rightarrow z < 0)$ which are both true. Discrete ghost variables are insufficient 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 often to keep up. In an ODE in dL, the only way to change x continuously is to add dimensions to the ODE. Additional dimensions cannot express every definite description, because some descriptions are not differentiable and thus must not be the solution of any differential equation. While some generalizations of dL also support differential games [25] which enable richer continuous changes in variables, this would defeat our purpose of reducing to vanilla dL.

Instead, the differential equation case is addressed by axiomatizing the ODE system using a continuous function symbol. The main hurdle is that the ODEs of dL are polynomial ODEs with guaranteed unique solutions, whereas the ODEs of dL_ι need not be polynomial. It thus does not suffice to reduce to FOD (first-order logic with differential equations) of prior work [22]. Rather we reduce ODEs to dL by introducing function symbols whose interpretations are restricted to continuous functions. Specifically, we build on prior work that shows the dL reachability modality $\langle\alpha\rangle\phi$ can be embedded in FOD [19, Lem. 5]. Instead, we embed from dL_1 into dL_C by redefining the translation for systems of ODEs:

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

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. 27:

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

6.3.3 Eliminate Continuous Function Symbols

To eliminate continuous function symbols, we reuse a previous reduction [25, 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. □

While this result might be misread to suggest that dL_ι is not truly necessary, definite descriptions enable us to define constructs that have no description as terms in dL, even if they can be expressed through a sufficiently complex formula translation. The key is that the reduction from dL_ι to dL is indeed complex, exploiting for example Gödel encodings for tuples and continuous functions [25, 22]. On the contrary, the complexity of the reduction shows that native support for definite descriptions is essential for practical proving. The equiexpressiveness result is of theoretical interest because it allows us to inherit results from dL [19]:

Theorem 44 (Completeness and decidability). dL_ι is reducible to dL, and therefore semidecidable relative to properties of differential equations.

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

7 Conclusion and Future Work

In this paper we developed dL_ι, 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_ι 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_ι, including semantics, a proof calculus, and soundness and expressiveness proofs. We apply dL_ι 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 non-differentiable and partially defined operators with systems of differential equations, an interaction which does not occur for dL's simpler language where all terms are smooth. 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. In future work, implementing dL_ι 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.

Acknowledgements. We thank Martin Giese for discussions on the use of definite descriptions in the KeY theorem prover and the CADE referees for their thoughtful feedback.

References

[1] Abhishek Anand and Vincent Rahli. Towards a formally verified proof assistant. In Gerwin Klein and Ruben Gamboa, editors, *ITP*, volume 8558 of *LNCS*, pages 27–44. Springer, 2014.

[2] Bruno Barras. Sets in Coq, Coq in sets. *J. Formalized Reasoning*, 3(1):29–48, 2010.

[3] Brandon Bohrer, Manuel Fernandez, and André Platzer. dL_ι: Definite descriptions in differential dynamic logic. In *CADE*, LNCS. Springer, 2019.

[4] Brandon Bohrer, Vincent Rahli, Ivana Vukotic, Marcus Völp, and André Platzer. Formally verified differential dynamic logic. In Yves Bertot and Viktor Vafeiadis, editors, *CPP*, pages 208–221. ACM, 2017.

[5] Brandon Bohrer, Yong Kiam Tan, Stefan Mitsch, Magnus O. Myreen, and André Platzer. VeriPhy: Verified controller executables from verified cyber-physical system models. In Dan Grossman, editor, *PLDI*, pages 617–630. ACM, 2018.

[6] Alonzo Church. *Introduction to Mathematical Logic*. Princeton University Press, 1956.

[7] RD Driver. Torricelli's law: An ideal example of an elementary ODE. *Amer. Math. Monthly*, 105(5):453–455, 1998.

[8] Melvin Fitting and Richard L. Mendelsohn. *First-Order Modal Logic*. Kluwer, Norwell, MA, USA, 1999.

[9] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In Amy P. Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 527–538. Springer, 2015.

[10] Thomas A. Henzinger. The theory of hybrid automata. In *LICS*. IEEE, 1996.

[11] John H. Hubbard and Beverly H. West. *Differential equations: A dynamical systems approach*. Springer, 1991.

[12] Jean-Baptiste Jeannin, Khalil Ghorbal, Yanni Kouskoulas, Aurora Schmidt, Ryan Gardner, Stefan Mitsch, and André Platzer. A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system. *STTT*, 19(6):717–741, 2017.

[13] Ramana Kumar, Rob Arthan, Magnus O. Myreen, and Scott Owens. Self-formalisation of higher-order logic: Semantics, soundness, and a verified implementation. *J. Autom. Reas.*, 56(3):221–259, 2016.

[14] Jan Łukasiewicz. O logice trojwartościowej (on 3-valued logic). *Ruch Filozoficzny*, (5):169–171, 1920.

[15] Stefan Mitsch, Marco Gario, Christof J. Budnik, Michael Golm, and André Platzer. Formal verification of train control with air pressure brakes. In Alessandro Fantechi, Thierry Lecomte, and Alexander Romanovsky, editors, *RSSRail*, volume 10598 of *LNCS*, pages 173–191. Springer, 2017.

[16] Stefan Mitsch, Khalil Ghorbal, David Vogelbacher, and André Platzer. Formal verification of obstacle avoidance and navigation of ground robots. *I. J. Robotics Res.*, 36(12):1312–1340, 2017.

[17] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.

[18] Albrecht Pietsch. About the Banach envelope of $\ell_{1,\infty}$. *Rev. Mat. Comput*, 22(1):209–226, 2009.

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

[20] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010.

[21] André Platzer. A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems. *Log. Meth. Comput. Sci.*, 8(4):1–44, 2012. Special issue for selected papers from CSL'10.

[22] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE, 2012.

[23] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24. IEEE, 2012.

[24] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.*, 59(2):219–265, 2017.

[25] André Platzer. Differential hybrid games. *ACM Trans. Comput. Log.*, 18(3):19:1–19:44, 2017.

[26] André Platzer and Yong Kiam Tan. Differential equation axiomatization: The impressive power of differential ghosts. In Anuj Dawar and Erich Grädel, editors, *LICS*, pages 819–828, New York, 2018. ACM.

[27] Konrad Slind and Michael Norrish. A brief overview of HOL4. In Otmane Aït Mohamed, César A. Muñoz, and Sofiène Tahar, editors, *TPHOLs*, volume 5170 of *LNCS*, pages 28–32. Springer, 2008.

[28] Alfred Tarski. A decision method for elementary algebra and geometry. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 24–84. Springer, 1998.

[29] Wolfgang Walter. Ordinary differential equations. 1998.

A Note on Total Differentials

The existence of a total differential implies the existence of all partial derivatives, but the converse implication does not hold universally. We now show that our choice to require the stronger condition of total differentiability was a necessary choice. We consider states containing variables x, y, z and study the following function, which is a textbook example of a function where all partials exist, but the total differential does not:

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

Let $\omega = \{x \mapsto 0, y \mapsto 0, z \mapsto 0\}$. Now both partials are zero in the neighborhood of ω: $\frac{\partial f(x,y)}{\partial \omega(x)} = \frac{\partial f(x,y)}{\partial \omega(y)} = 0$. In contrast, the directional derivative along $x = y$ is 0.5, whereas the partial derivatives would "imply" that every directional derivative were 0. Because the directional derivatives disagree with the partial derivatives in this fashion, we say that the *total* differential of $f(x,y)$ does not exist at ω.

We conclusively justify our total differential requirement by temporarily removing the total differentiability requirement in (only!) the remainder of this appendix for the sake of argument. We then derive a falsehood.

We will use the proof calculus of Sec. 5 in this example. The primary use of differential terms is the *differential induction* rule. Axiom $\text{DI}_{\geq}$ implements the $\geq$ case, from which the $=$ case can be derived. If two terms θ and η are equal initially with equal differentials throughout an ODE, then θ and η are equal throughout. Both cases are sound when "differential" means "total differential," but neither is sound when "differential" means "sum of partial derivatives".

To construct our example, we first give definitions: $f(x,y)$ can be expressed as a definite description. The line $x = y$ can be traversed a program α containing an ODE, while J is an invariant candidate used in the proof.

$$\begin{aligned} f(x,y) &\equiv \left(\iota z\, x = y = z = 0 \vee \left((x \neq 0 \vee y \neq 0) \wedge z = \frac{xy}{x^2+y^2}\right)\right) \\ ODE &\equiv x' = 1, y' = 1 \\ \alpha &= x := 0; y := 0; ODE \\ J &\equiv (f(x,y) = 0) \end{aligned}$$

The piecewise function f is modeled with a disjunction inside a description. The differential invariant candidate J will demonstrate the main soundness issue: J is not an invariant of ODE, but the partial derivatives suggest it is. We "prove" the formula $[\alpha]J$, which is a falsehood because $f(x,y) = 1/2$ everywhere in ODE except the initial point.

The "proof" begins with a lemma $\mathcal{D}$ showing that $x = y$ is an invariant:

$$\text{DI}\frac{\text{QE}\dfrac{*}{x = 0, y = 0 \to x = y} \quad \text{DE}\dfrac{\text{QE}\dfrac{*}{1 = 1}}{x = 0, y = 0 \to [ODE]x' = y'}}{x = 0, y = 0 \to [ODE]x = y}$$

The full proof cuts in $\mathcal{D}$, then proves J with a second differential induction:

$$\text{[:],[:=]}\dfrac{\text{DC}\dfrac{\dfrac{\mathcal{D}}{x=0,y=0\to[ODE]x=y}\quad\text{DI}\dfrac{\dfrac{*}{x=0,y=0\to f(x,y)=0}\text{QE}\quad\dfrac{\dfrac{*}{[ODE\,\&\,x=y]0=0}\text{DW}}{[ODE\,\&\,x=y](f(x,y))'=0}\,1}{x=0,y=0\to[ODE\,\&\,x=y]f(x,y)=0}}{x=0,y=0\to[ODE]J}}{[\alpha]J}$$

The step marked (1) contains several steps. We apply $(\theta)'$ to expand $(f(x,y))'$: the axiom $(\theta)'$ differentiates an arbitrary term including $f(x,y)$ which is defined with a definite description. The general-purpose rule $(\theta)'$ requires us to prove that the differential exists, which is done by applying $\mathsf{E}(')$. The resulting goal is reduced to first-order real arithmetic by applying ι, then closed with QE. Crucially, this QE invocation *only* closes if we define differentials by partials and define axiom $\mathsf{E}(')$ accordingly. Under the total differential requirement, $(\theta)'$ would require a differential that exists and agrees in *every* direction in some open ball around (x,y).

The ODE $x'=1,y'=1$ is itself trivial, it is the differential of $f(x,y)$ which requires care, and in fact ought not exist. If it did, this proof would close. Because it does not, this proof cannot be done with the real dL_ι calculus.

In review, what was the main problem? In isolation, our semantic definition of $(\theta)'$ cannot cause unsoundness, because unsoundness arises from disagreement between semantics and proof calculus. However, the main application of $(\theta)'$ is rule $\text{DI}_{\geq}$, and any definition of $(\theta)'$ which is not conducive to stating a sound $\text{DI}_{\geq}$ axiom is useless. The natural statement of $\text{DI}_{\geq}$ is that initially equal terms are equal throughout when their differentials are equal. The fundamental issue is that this is not always the case when "differential" is read as partial derivative, only when it is read as total or directional derivative. In short, we must ensure that Lem. 2 holds. Intuitively, we demand that $\text{DI}_{\geq}$ considers the *time* differential of θ *as an ODE flows*, and it is the *directional* derivative which always agrees with the time derivative, when it exists. In contrast to the directional derivative, $f(x,y)$ has partial derivatives of 0. The dot product $(0,0)\cdot(x',y')$ is then 0 which disagrees with the time derivative of 0.5. That being said, the reading as *partial* derivative simplifies some rules such as DE, so the best approach is to first check that directional and partial derivatives agree (i.e., total differential exists), after which the different notions of differential may be used interchangeably. Specifically, the check $\mathsf{E}((\theta)')$ prohibits applying $\text{DI}_{\geq}$ to terms such as $f(x,y)$ where the readings of "differential" as partial or total are in disagreement. While our example considered the equality case of differential induction, this issue is not specific to the equality case. If we wish to prove an invariant $\theta>\eta$, it still does not suffice to consider partial derivatives of θ and η if they disagree with the time derivative.