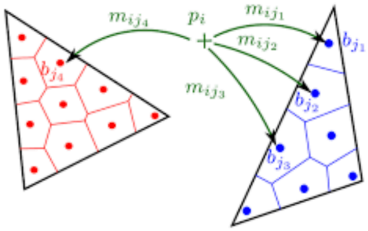
AGENCE NATIONALE DE LA RECHERCHE

ANR

REPAS

RELIABLE AND PRIVACY-AWARE SOFTWARE SYSTEMS



Deliverable D2.b

Differential Logical Relations
Part I: The Simply-Typed Case

Abstract

We introduce a new form of logical relation which, in the spirit of metric relations, allows us to assign each pair of programs a quantity measuring their distance, rather than a boolean value standing for their being equivalent. The novelty of differential logical relations consists in measuring the distance between terms not (necessarily) by a numerical value, but by a mathematical object which somehow reflects the interactive complexity, i.e. the type, of the compared terms. We exemplify this concept in the simply-typed lambda-calculus, and show a form of soundness theorem. We also see how ordinary logical relations and metric relations can be seen as instances of differential logical relations. Finally, we show that differential logical relations can be organised in a cartesian closed category, contrarily to metric relations, which are well-known *not* to have such a structure, but only that of a monoidal closed category.

1 Introduction

Modern software systems tend to be heterogeneous and complex, and this is reflected in the analysis methodologies we use to tame their complexity. Indeed, in many cases the only way to go is to make use of compositional kinds of analysis, in which *parts* of a large system can be analysed in isolation, without having to care about the rest of the system, the *environment*. As an example, one could consider a component A and replace it with another (e.g. more efficient) component B without looking at the context $\mathcal{C}$ in which A and B are supposed to operate, see Figure 1. Of course, for this program transformation to be safe, A should be *equivalent* to B or, at least, B should be a *refinement* of A.

Program equivalences and refinements, indeed, are the cruxes of program semantics, and have been investigated in many different programming paradigms. When programs have an interactive behaviour, like in concurrent or higher-order languages, even *defining* a notion of program equivalence is not trivial, while coming out with handy methodologies for *proving* concrete programs to be equivalent can be quite challenging, and has been one of the major research topics in programming language theory, stimulating the development of techniques like logical relations [20, 17], applicative bisimilarity [1], and to some extent denotational semantics [23, 24] itself.

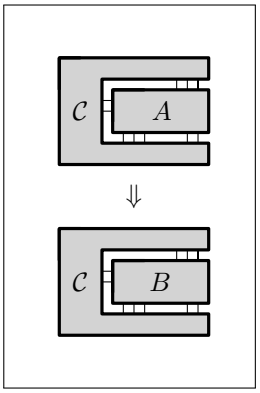


Figure 1: Replacing A with B.

Coming back to our example, may we say anything about the case in which A and B are *not* equivalent, although behaving very similarly? Is there anything classic program semantics can say about this situation? Actually, the answer is negative: the program transformation turning such an A into B cannot be justified, simply because there is no guarantee about what the possible negative effects that turning A into B could have on the overall system formed by $\mathcal{C}$ and A. There are, however, many cases in which program transformations like the one we just described are indeed of interest, and thus desirable. Many examples can be, for instance, drawn from the field of *approximate computing* [18], in which equivalence-breaking program transformations are considered as beneficial *provided* the overall behaviour of the program is not affected too much by the transformation, while its intensional behaviour, e.g. its performance, is significantly improved.

One partial solution to the problem above consists in considering program *metrics* rather than program *equivalences*. This way, any pair of programs are dubbed being at a certain numerical distance rather than being merely equivalent (or not). This, for example, can be useful in the context of differential privacy [21, 5, 29] and has also been studied in the realms of domain theory [10, 4, 11, 13, 3] (see also [25] for an introduction to the subject) and coinduction [27, 26, 12, 7]. The common denominator among all these approaches is that on the one hand, the notion of a congruence, crucial for compositional reasoning, is replaced by the one of a *Lipschitz-continuous* map: any context should not amplify (too much) the distance between any pair of terms, when it is fed with either the former or the latter:

$$\delta(C[M], C[N]) \leq c \cdot \delta(M, N).$$

This enforces compositionality, and naturally leads us to consider metric spaces and Lipschitz functions as the underlying category. As is well known, this is not a cartesian closed category, and thus does *not* form a model of typed λ-calculi, unless one adopts linear type systems, or type systems in which the number of uses of each variable is kept track of, like FUZZ [21]. This somehow limits the compositionality of the metric approach [10, 14].

Even if one considers affine calculi, there are program transformations which are intrinsically unjustifiable in the metric approach. Consider the following two programs of type $REAL \to REAL$

$$M_{SIN} := \lambda x.\mathtt{sin}(x) \qquad\qquad M_{ID} := \lambda x.x.$$

The two terms compute two very different functions on the real numbers, namely the sine trigonometric function and the identity on $\mathbb{R}$, respectively. The euclidean distance $|\sin x - x|$ is unbounded when x ranges over $\mathbb{R}$. As a consequence, comparing M_{SIN} and M_{ID} using the so-called sup metric[1] as it is usually done in metric logical relations [21, 10] and applicative distances [14, 8], we see that their distance is infinite, and that the program transformation turning M_{SIN} into M_{ID} cannot be justified this way, for very good reasons. As highlighted by Westbrook and Chaudhuri [28], this is not the end of the story, at least if the environment in which M_{SIN} and M_{ID} operate feed either of them *only with* real numbers close to 0. If this is the case, M_{SIN} can be substituted with M_{ID} without affecting *too much* the overall behaviour of the system.

The key insight by Westbrook and Chaudhuri is that justifying program transformations like the one above requires taking the difference $\delta(M_{SIN}, M_{ID})$ between M_{SIN} and M_{ID} not merely as a number, but as a more structured object. What they suggest is to take $\delta(M_{SIN}, M_{ID})$ as *yet another program*, which however describes the difference between M_{SIN} and M_{ID}:

$$\delta(M_{SIN}, M_{ID}) := \lambda x.\lambda\varepsilon.|\sin x - x| + \varepsilon.$$

This reflects the fact that the distance between M_{SIN} and M_{ID}, namely the discrepancy between their output, depends not only on the discrepancy on the input, namely on ε, but also *on the input itself*, namely on x. It both x and ε are close to 0, $\delta(M_{SIN}, M_{ID})$ is itself close to 0.

In this paper, we develop Westbrook and Chaudhuri's ideas, and turn them into a framework of *differential logical relations*. We will do all this in a simply-typed λ-calculus with real numbers as the only base type. Starting from such a minimal calculus has at least two advantages: on the one hand one can talk about meaningful examples like the one above, and on the other hand the induced metatheory is simple enough to highlight the key concepts.

The contributions of this paper can be summarised as follows:

- After introducing our calculus $ST^{\lambda}_{\mathbb{R}}$, we define differential logical relations inductively on types, as ternary relations between pairs of programs and *differences*. The latter are mere set theoretic entities here, and the nature of differences between terms depends on terms' types.
- We prove a soundness theorem for differential logical relations, which allows us to justify compositional reasoning about terms' differences. We also prove a *finite difference theorem*, which stipulates that the distance between two simply-typed λ-terms is finite if mild conditions hold on the underlying set of function symbols.

[1] Recall that given (pseudo)metric spaces (X, d_X), (Y, d_Y) we can give the set Y^X of non-expansive maps between X and Y a (pseudo)metric space structure setting $d_{Y^X}(f, g) = \sup_{x \in X} d_Y(f(x), g(x))$

$$\frac{x:\tau\in\Gamma}{\Gamma\vdash x:\tau} \qquad \frac{}{\Gamma\vdash r:REAL} \qquad \frac{f_n\in\mathcal{F}_n}{\Gamma\vdash f_n:REAL^n\to REAL} \qquad \frac{\Gamma,x:\tau\vdash M:\rho}{\Gamma\vdash\lambda x.M:\tau\to\rho}$$

$$\frac{\Gamma\vdash M:\tau\to\rho \quad \Gamma\vdash N:\tau}{\Gamma\vdash MN:\rho} \qquad \frac{\Gamma\vdash M:\tau \quad \Gamma\vdash N:\rho}{\Gamma\vdash\langle M,N\rangle:\tau\times\rho} \qquad \frac{}{\Gamma\vdash\pi_1:\tau\times\rho\to\tau} \qquad \frac{}{\Gamma\vdash\pi_2:\tau\times\rho\to\rho}$$

$$\frac{\Gamma\vdash M:\tau \quad \Gamma\vdash N:\tau}{\Gamma\vdash \texttt{iflz}\ M\ \texttt{else}\ N:REAL\to\tau} \qquad \frac{\Gamma\vdash M:\tau\to\tau \quad \Gamma\vdash N:\tau}{\Gamma\vdash \texttt{iter}\ M\ \texttt{base}\ N:REAL\to\tau}$$

Figure 2: Typing rules for $ST^{\lambda}_{\mathbb{R}}$.

- We give embeddings of logical and metric relations into differential logical relations. This witnesses that the latter are a generalisation of the former two.
- Finally, we show that generalised metric domains, the mathematical structure underlying differential logical relations, form a cartesian closed category, contrarily to the category of metric spaces, which is well known not to have the same property.

2 A Simply-Typed λ-Calculus with Real Numbers

In this section, we introduce a simply-typed λ-calculus in which the only base type is the one of real numbers, and constructs for iteration and conditional are natively available. The choice of this language as the reference calculus in this paper has been made for the sake of simplicity, allowing us to concentrate on the most crucial aspects, at the same time guaranteeing a minimal expressive power.

Terms and Types $ST^{\lambda}_{\mathbb{R}}$ is a typed λ-calculus, so its definition starts by giving the language of *types*, which is defined as follows:

$$\tau,\rho ::= REAL \mid \tau\to\rho \mid \tau\times\rho.$$

The expression τ^n stands for $\underbrace{\tau\times\cdots\times\tau}_{n \text{ times}}$. The set of *terms* is defined as follows:

$$M,N ::= x \mid r \mid f_n \mid \lambda x.M \mid MN \mid \langle M,N\rangle \mid \pi_1 \mid \pi_2 \mid \texttt{iflz}\ M\ \texttt{else}\ N \mid \texttt{iter}\ M\ \texttt{base}\ N$$

where x ranges over a set $\mathbb{V}$ of variables, r ranges over the set $\mathbb{R}$ of real numbers, n is a natural number and f_n ranges over a set $\mathcal{F}_n$ of total real functions of arity n. We do not make any assumption on $\{\mathcal{F}_n\}_{n\in\mathbb{N}}$, apart from the predecessor $pred_1$ being part of $\mathcal{F}_1$. The family, in particular, could in principle contain non-continuous functions. The expression $\langle M_1,\ldots,M_n\rangle$ is simply a shortcut for $\langle\ldots\langle\langle M_1,M_2\rangle,M_3\rangle\ldots,M_n\rangle$. All constructs are self-explanatory, except for the `iflz` and `iter` operators, which are conditional and iterator combinators, respectively. An *environment* Γ is a set of assignments of types to variables in $\mathbb{V}$ where each variable occurs at most once. A *type judgment* has the form $\Gamma\vdash M:\tau$ where Γ is an environment, M is a term, and τ is a type. Rules for deriving correct typing judgments are in Figure 2, and are standard. The set of terms M for which $\cdot\vdash M:\tau$ is derivable is indicated as $CT(\tau)$.

Call-by-Value Operational Semantics A static semantics is of course not enough to give meaning to a paradigmatic programming language, the dynamic aspects being captured only once an *operational* semantics is defined. The latter turns out to be very natural. *Values* are defined as follows:

$$V,W ::= r \mid f_n \mid \lambda x.M \mid \langle M,N\rangle \mid \pi_1 \mid \pi_2 \mid \texttt{iflz}\ M\ \texttt{else}\ N \mid \texttt{iter}\ M\ \texttt{base}\ N.$$

The set of closed values of type τ is $CV(\tau)\subseteq CT(\tau)$, and the evaluation of $M\in CT(\tau)$ produces a value $V\in CV(\tau)$, as formalised by the rules in Figure 3, through the judgment $M\Downarrow V$. We write

$$\frac{}{V \Downarrow V} \qquad \frac{M \Downarrow f_n \quad N \Downarrow \langle L_1, \ldots, L_n \rangle \quad L_i \Downarrow r_i}{MN \Downarrow f(r_1, \ldots, r_n)} \qquad \frac{M \Downarrow \lambda x.L \quad N \Downarrow V \quad L\{V/x\} \Downarrow W}{MN \Downarrow W}$$

$$\frac{M \Downarrow \pi_1 \quad N \Downarrow \langle L, P \rangle \quad L \Downarrow V}{MN \Downarrow V} \qquad \frac{M \Downarrow \pi_2 \quad N \Downarrow \langle L, P \rangle \quad P \Downarrow V}{MN \Downarrow V}$$

$$\frac{M \Downarrow \texttt{iflz}\ L\ \texttt{else}\ P \quad N \Downarrow r \quad r < 0 \quad L \Downarrow V}{MN \Downarrow V} \qquad \frac{M \Downarrow \texttt{iflz}\ L\ \texttt{else}\ P \quad N \Downarrow r \quad r \geq 0 \quad P \Downarrow V}{MN \Downarrow V}$$

$$\frac{M \Downarrow \texttt{iter}\ L\ \texttt{base}\ P \quad N \Downarrow r \quad r < 0 \quad P \Downarrow V}{MN \Downarrow V}$$

$$\frac{M \Downarrow \texttt{iter}\ L\ \texttt{base}\ P \quad N \Downarrow r \quad r \geq 0 \quad L((\texttt{iter}\ L\ \texttt{base}\ P)(pred_1(r)) \Downarrow V}{MN \Downarrow V}$$

Figure 3: Operational semantics for $ST^{\lambda}_{\mathbb{R}}$.

$M \Downarrow$ if $M \Downarrow V$ is derivable *for some* V. The absence of full recursion has the nice consequence of guaranteeing a form of termination:

Thoerem 1. *The calculus $ST^{\lambda}_{\mathbb{R}}$ is terminating: if $\cdot \vdash M : \tau$ then $M \Downarrow$.*

We show the normalisation theorem using the standard reducibility candidate argument.

Definition 2. *We define RED_τ as follows.*

$$\begin{aligned} RED_\tau &= \{M \mid M \Downarrow V \wedge V \in VRED_\tau\} \\ VRED_{REAL} &= \mathbb{R} \\ VRED_{\tau\to\rho} &= \{V \mid \forall W \in VRED_\tau . VW \in RED_\rho\} \\ VRED_{\tau\times\rho} &= \{\langle M, N\rangle \mid M \in RED_\tau \wedge N \in RED_\rho\} \end{aligned}$$

Then we show the two lemmas that prove Theorem 1 together:

Lemma 3. *If $\cdot \vdash M : \tau$, then $M \in RED_\tau$.*

Proof. The following strengthening of the statement can be proved by induction on the structure of M: whenever $x_1 : \rho_1, \ldots, x_n : \rho_n \vdash M : \tau$ and whenever $V_i \in VRED_{\rho_i}$ it holds that

$$M\{V_1/x_1, \ldots, V_n/x_n\} \in RED_\tau.$$

All inductive cases are standard. One that deserves a little bit of attention is the case of abstractions, in which one needs to deduce that $(\lambda x.M)V \in RED_\tau$ iff $M\{x/V\} \in RED_\tau$. But this is of course easy to prove, because the former evaluated to any value W iff the latter evaluates to W. Another delicate case is the one of $\texttt{iter}\ M\ \texttt{base}\ N$, which requires a further induction. □

Please observe that, by definition, if $M \in RED_\tau$, then $M \Downarrow$. As a consequence, one easily gets termination from Lemma 3.

Corollary 4. *If $\cdot \vdash M : REAL$ then there exists a unique $r \in \mathbb{R}$ satisfying $M \Downarrow r$, which we indicate as $NF(M)$.*

Proof. By Theorem 1 there exists a value V satisfying $M \Downarrow V$. The only form of value of type $REAL$ is $r \in \mathbb{R}$. Moreover, the fact that such a r is unique is a consequence of the following, slightly more general result: if $M \Downarrow V$ and $M \Downarrow W$, then V is syntactically equal to W. This can be proved by a straightforward induction on the structure of the proof that, e.g., $M \Downarrow V$. □

Context Equivalence A *context* C is nothing more than a term containing a single occurrence of a placeholder $[\cdot]$. Given a context C, $C[M]$ indicates the term one obtains by substituting M for the occurrence of $[\cdot]$ in C. Typing rules in Figure 2 can be lifted to contexts by generalising judgments to the form $\Gamma \vdash C[\Delta \vdash \cdot : \tau] : \rho$, by which one captures that whenever $\Delta \vdash M : \tau$, it holds that $\Gamma \vdash C[M] : \rho$. Two terms M and N such that $\Gamma \vdash M, N : \tau$ are said to be *context equivalent* [19] when for every C such that $\emptyset \vdash C[\Gamma \vdash \cdot : \tau] : REAL$ it holds that $NF(C[M]) = NF(C[N])$. Context equivalence is the largest adequate congruence, and is thus considered as the coarsest "reasonable" equivalence between terms. It can also be turned into a pseudometric [9, 8] — called *context distance* — by stipulating that

$$\delta(M, N) = \sup_{\emptyset \vdash C[\Gamma \vdash \cdot : \tau] : REAL} |NF(C[M]) - NF(C[M])|.$$

The obtained notion of distance, however, is bound to trivialise [9], given that $ST^{\lambda}_{\mathbb{R}}$ is not affine. Trivialisation of context distance highlights an important limit of the metric approach to program difference which, ultimately, can be identified with the fact that program distances are sensitive to interactions with the environment. Our notion of a differential logical relation tackles such a problem from a different perspective, namely refining the concept of a program difference which is not just a number, but is now able to take into account interactions with the environment.

Set-Theoretic Semantics Before introducing differential logical relations, it is useful to remark that we can give $ST^{\lambda}_{\mathbb{R}}$ a standard set-theoretic semantics. To any type τ we associate the set $[\![\tau]\!]$, the latter being defined by induction on the structure of τ as follows:

$$[\![REAL]\!] = \mathbb{R}; \qquad [\![\tau \to \rho]\!] = [\![\tau]\!] \to [\![\rho]\!]; \qquad [\![\tau \times \rho]\!] = [\![\tau]\!] \times [\![\rho]\!].$$

This way, any closed term $M \in CT(\tau)$ is interpreted as an element $[\![M]\!]$ of $[\![\tau]\!]$ in a natural way (see, e.g. [17]). Up to now, everything we have said about $ST^{\lambda}_{\mathbb{R}}$ is absolutely standard, and only serves to set the stage for the next sections.

3 Making Logical Relations Differential

Logical relations can be seen as one of the *many* ways of defining when two programs are to be considered equivalent. Their definition is type driven, i.e., they can be seen as a *family* $\{\delta_\tau\}_\tau$ of binary relations indexed by types such that $\delta_\tau \subseteq CT(\tau) \times CT(\tau)$. This section is devoted to showing how all this can be made into differential logical relations.

The first thing that needs to be discussed is how to define the space of *differences* between programs. These are just boolean values in logical relations, become real numbers in ordinary metrics, and is type-dependent itself. A function $(\!|\cdot|\!)$ that assigns a set to each type is defined as follows:

$$(\!|REAL|\!) = \mathbb{R}^{\infty}_{\geq 0}; \qquad (\!|\tau \to \rho|\!) = [\![\tau]\!] \times (\!|\tau|\!) \to (\!|\rho|\!); \qquad (\!|\tau \times \rho|\!) = (\!|\tau|\!) \times (\!|\rho|\!);$$

where $\mathbb{R}^{\infty}_{\geq 0} = \mathbb{R}_{\geq 0} \cup \{\infty\}$. The set $(\!|\tau|\!)$ is said to be the *difference space* for the type τ and is meant to model the outcome of comparisons between closed programs of type τ. As an example, when τ is $REAL \to REAL$, we have that $(\!|\tau|\!) = \mathbb{R} \times \mathbb{R}^{\infty}_{\geq 0} \to \mathbb{R}^{\infty}_{\geq 0}$. This is the type of the function $\delta(M, N)$ we used to compare the two programs described in the Introduction.

Now, which structure could we endow $(\!|\tau|\!)$ with? First of all, we can define a partial order $\leq_\tau$ over $(\!|\tau|\!)$ for each type τ as follows:

$$\begin{array}{rl} r \leq_{REAL} s & \text{if } r \leq s \text{ as the usual order over } \mathbb{R}^{\infty}_{\geq 0}; \\ f \leq_{\tau \to \rho} g & \text{if } \forall x \in [\![\tau]\!]. \forall t \in (\!|\tau|\!). f(x, t) \leq_\rho g(x, t); \\ (t, u) \leq_{\tau \times \rho} (s, r) & \text{if } t \leq_\tau s \text{ and } u \leq_\rho r. \end{array}$$

This order has least upper bounds and greater lower bounds, thanks to the nice structure of $\mathbb{R}^{\infty}_{\geq 0}$:

Proposition 5. *For each type τ, $(\llparenthesis\tau\rrparenthesis, \leq_\tau)$ forms a complete lattice.*

Proof. We show that each $\llparenthesis\tau\rrparenthesis$ has suprema by induction on types.

- Case *REAL*. Then $(\llparenthesis\tau\rrparenthesis, \leq_\tau) = (\mathbb{R}^\infty_{\geq 0}, \leq)$ is clearly complete.
- Case $\tau \to \rho$. Given a subset $A \subseteq \llparenthesis\tau \to \rho\rrparenthesis$, we define $s_A \in \llparenthesis\tau \to \rho\rrparenthesis$ as:

$$s_A(V,t) = \sup_{f \in A} f(V,t),$$

  where the supremum on the right-hand side exists by induction hypothesis (on the type ρ). This s_A serves as the supremum of A because:
  - (**Upperbound**.) For any $g \in A$, by definition of supremum it holds that: $\forall V \in CV(\tau).\forall t \in \llparenthesis\tau\rrparenthesis. g(V,t) \leq_\tau \sup_{f\in A} f(V,t) = s_A(V,t)$. Hence $g \leq_{\tau\to\rho} s_A$.
  - (**Leastness**.) Suppose that s' is an upperbound of A, i.e. $\forall f \in A. f \leq_{\tau\to\rho} s'$. Then, it by definition means that: $\forall f \in A.\forall V \in CV(\tau).\forall t \in \llparenthesis\tau\rrparenthesis. f(V,t) \leq_\rho s'(V,t)$. Therefore $s'(V,t)$ is an upperbound of the set $\{f(V,t)\}_{f\in A}$ for each V, t. Thus by definition of supremum, $s_A(V,t) = \sup_{f\in A} f(V,t) \leq_\rho s'(V,t)$ for each V, t. Hence $s_A \leq_{\tau\to\rho} s'$ holds by definition of $\leq_{\tau\to\rho}$.
- Case $\tau \times \rho$. Given a subset $A \subseteq \llparenthesis\tau \times \rho\rrparenthesis$, we define $s_A = (\sup \boldsymbol{\pi_1} A, \sup \boldsymbol{\pi_2} A) \in \llparenthesis\tau \times \rho\rrparenthesis$, where $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ are meta-level projections and the suprema on the right-hand side exist by induction hypothesis (on the types τ and ρ). One can verify that s_A is the supremum of A in a straightforward way:
  - (**Upperbound**.) For any $(t,u) \in A$, by definition of supremum $t \leq_\tau \sup \boldsymbol{\pi_1} A$ and $u \leq_\rho \sup \boldsymbol{\pi_2} A$ hold. Hence $(t,u) \leq_{\tau\times\rho} (\sup \boldsymbol{\pi_1} A, \sup \boldsymbol{\pi_2} A) = s_A$ by definition of $\leq_{\tau\times\rho}$.
  - (**Leastness**.) Suppose that (s'_1, s'_2) is an upperbound of A, i.e. $\forall (t_1,t_2) \in A.(t_1,t_2) \leq_{\tau\times\rho} (s'_1, s'_2)$. It by definition means that $\forall t_1 \in \boldsymbol{\pi_1} A. t_1 \leq_\tau s'_1$ and $\forall t_2 \in \boldsymbol{\pi_2} A. t_2 \leq_\rho s'_2$. Therefore s'_1 (resp. s'_2) is an upperbound of the set $\boldsymbol{\pi_1} A$ (resp. $\boldsymbol{\pi_2} A$). Thus by definition of supremum, $\sup \boldsymbol{\pi_1} A \leq_\tau s'_1$ (resp. $\sup \boldsymbol{\pi_2} A \leq_\rho s'_2$). Hence $(\sup \boldsymbol{\pi_1} A, \sup \boldsymbol{\pi_2} A) \leq_{\tau\times\rho} (s'_1, s'_2)$ holds by definition of $\leq_{\tau\times\rho}$.

□

The fact that $\llparenthesis\tau\rrparenthesis$ has a nice order-theoretic structure is not the end of the story. For every type τ, we define a binary operation $*_\tau$ as follows:

$$r *_{REAL} s = r + s \text{ if } r, s \in \mathbb{R}_{\geq 0}; \qquad (f *_{\tau\to\rho} g)(V,t) = f(V,t) *_\rho g(V,t);$$
$$r *_{REAL} s = \infty \text{ if } r = \infty \vee s = \infty; \qquad (t,s) *_{\tau\times\rho} (u,r) = (t *_\tau u, s *_\rho r).$$

This is precisely what it is needed to turn $\llparenthesis\tau\rrparenthesis$ into a *quantale*[2] [22].

Proposition 6. *For each type τ, $\llparenthesis\tau\rrparenthesis$ forms a commutative unital non-idempotent quantale. That is, the following holds for any τ:*

- *$t *_\tau u = u *_\tau t$ for all $t, u \in \llparenthesis\tau\rrparenthesis$,*
- *$t *_\tau (\sup_{i\in I} u_i) = \sup_{i\in I}(t *_\tau u_i)$ for all $t, u_i \in \llparenthesis\tau\rrparenthesis$ where I is an arbitrary index set,*
- *there exists an element $e_\tau \in \llparenthesis\tau\rrparenthesis$ satisfying $e_\tau *_\tau t = t$ for all $t \in \llparenthesis\tau\rrparenthesis$,*
- *$*_\tau$ does not necessarily satisfy $t *_\tau t = t$.*

Proof. By induction on τ.

- Case *REAL*. The multiplication $*_{REAL}$ is clearly commutative and satisfies $r *_\tau (\sup_{i\in I} s_i) = \sup_{i\in I}(r *_\tau s_i)$ for all $r, s_i \in \llparenthesis REAL\rrparenthesis = \mathbb{R}^\infty_{\geq 0}$. The unit e_{REAL} is 0; the multiplication is obviously non-idempotent.
- Case $\tau \to \rho$. It holds that $(f *_{\tau\to\rho} g) = (g *_{\tau\to\rho} f)$ because

$$\begin{aligned}(f *_{\tau\to\rho} g)(V,t) &= f(V,t) *_\rho g(V,t)\\ &\overset{\text{I.H.}}{=} g(V,t) *_\rho f(V,t)\\ &= (g *_{\tau\to\rho} f)(V,t)\end{aligned}$$

[2]Recall that a quantale $\mathbb{Q} = (Q, \leq_Q, 0_Q, *_Q)$ consists of a complete lattice $(Q, \leq_Q)$ and a monoid $(Q, 0_Q, *_Q)$ such that the lattice and monoid structures properly interact (meaning that monoid multiplication distributes over joins). We refer to [22, 15] for details.

and $f *_{\tau\to\rho} (\sup_{i\in I}(g_i)) = \sup_{i\in I}(f *_{\tau\to\rho} g_i)$ because

$$\begin{aligned}(f *_{\tau\to\rho} (\sup_{i\in I}(g_i)))(V,t) &= f(V,t) *_\rho (\sup_{i\in I} g_i)(V,t)\\ &= f(V,t) *_\rho (\sup_{i\in I}(g_i(V,t)))\\ &\overset{\text{I.H.}}{=} \sup_{i\in I}(f(V,t) *_\rho g_i(V,t))\\ &= \sup_{i\in I}((f *_{\tau\to\rho} g_i)(V,t))\\ &= (\sup_{i\in I}(f *_{\tau\to\rho} g_i))(V,t).\end{aligned}$$

The unit $e_{\tau\to\rho}$ is the constant e_ρ function: $e_{\tau\to\rho}(V,t) = e_\rho$ for all V, t.

- Case $\tau\times\rho$. Then

$$\begin{aligned}(t,t') *_{\tau\times\rho} (u,u') &= (t *_\tau u, t' *_\rho u')\\ &\overset{\text{I.H.}}{=} (u *_\tau t, u' *_\rho t')\\ &= (u,u') *_{\tau\times\rho} (t,t')\end{aligned}$$

and

$$\begin{aligned}(t,t') *_{\tau\times\rho} (\sup_{i\in I}(u_i,u_i')) &= (t,t') *_{\tau\times\rho} (\sup_{i\in I} u_i, \sup_{i\in I} u_i')\\ &= (t *_\tau (\sup_{i\in I} u_i), t' *_\tau (\sup_{i\in I} u_i'))\\ &\overset{\text{I.H.}}{=} (\sup_{i\in I}(t *_\tau u_i), \sup_{i\in I}(t' *_\tau u_i'))\\ &= \sup_{i\in I}(t *_\tau u_i, t' *_\tau u_i')\\ &= \sup_{i\in I} ((t,t') *_{\tau\times\rho} (u_i,u_i')).\end{aligned}$$

The unit $e_{\tau\times\rho}$ is (e_τ, e_ρ).

□

The fact that $(\!|\tau|\!)$ is a quantale means that it has, e.g., the right structure to be the codomain of generalised metrics [16, 15]. Actually, a more general structure is needed for our purposes, namely the one of a generalised metric domain, which will be thoroughly discussed in Section 6 below. For the moment, let us concentrate our attention to programs:

Definition 7 (Differential Logical Relations)**.** *We define a* differential logical relation $\{\delta_\tau \subseteq \Lambda_\tau \times (\!|\tau|\!) \times \Lambda_\tau\}_\tau$ *as a set of ternary relations indexed by types satisfying*

$$\begin{aligned}\delta_{REAL}(M,r,N) &\Leftrightarrow |NF(M) - NF(N)| \leq r;\\ \delta_{\tau\times\rho}(M,(d_1,d_2),N) &\Leftrightarrow \delta_\tau(\pi_1 M, d_1, \pi_1 N) \wedge \delta_\rho(\pi_2 M, d_2, \pi_2 N)\\ \delta_{\tau\to\rho}(M,d,N) &\Leftrightarrow (\forall V \in CV(\tau).\ \forall x \in (\!|\tau|\!).\ \forall W \in CV(\tau).\\ &\qquad \delta_\tau(V,x,W) \Rightarrow \delta_\rho(MV, d([\![V]\!],x), NW) \wedge \delta_\rho(MW, d([\![V]\!],x), NV)).\end{aligned}$$

An intuition behind the condition required for $\delta_{\tau\to\rho}(M,d,N)$ is that $d([\![V]\!],y)$ overapproximates both the "distance" between MV and NW and the one between MW and NV, this *whenever* W is within the error x from V.

Some basic facts about differential logical relations, which will be useful in the following are now in order.

Lemma 8. *For every τ, M, N, it holds that $\delta_\tau(M,d,N)$ if and only if $\delta_\tau(N,d,M)$.*

Proof. By induction on types. □

Lemma 9. *Let $\cdot \vdash M, N : \tau$ and $d \in (\!|\tau|\!)$. Assume that $\delta_{REAL}(M,d,N)$ and $\delta_{REAL}(N,e,L)$ implies $\delta_{REAL}(M,d+e,L)$. Then $\delta_\tau(M,d,N)$ and $\delta_\tau(N,e,L)$ implies $\delta_\tau(M,d+e,L)$.*

Proof. By induction on types. □

Lemma 10. *Let $\cdot \vdash M, N : \tau$ and $d \in (\!|\tau|\!)$. Assume that $\delta_{REAL}(M,d,N)$ and $d \leq e$ implies $\delta_{REAL}(M,e,N)$. Then $\delta_\tau(M,d,N)$ and $d \leq e$ implies $\delta_\tau(M,e,N)$.*

Proof. By induction on types. □

3.1 A Fundamental Lemma

Usually, the main result about any system of logical relations is the so-called *Fundamental Lemma*, which states that any typable term is in relation *with itself*. But how would the Fundamental Lemma look like here? Should any term be at *somehow minimal distance* to itself, in the spirit of what happens, e.g. with metrics [21, 10]? Actually, there is no hope to prove anything like that for differential logical relations, as the following example shows.

Example 11. *Consider again the term $M_{ID} = \lambda x.x$, which can be given type $\tau = REAL \to REAL$ in the empty context. Please recall that $(\!|\tau|\!) = \mathbb{R} \times \mathbb{R}^{\infty}_{\geq 0} \to \mathbb{R}^{\infty}_{\geq 0}$. Could we prove that $\delta_\tau(M_{ID}, 0_\tau, M_{ID})$, where 0_τ is the constant-0 function? The answer is negative: given two real numbers r and s at distance ε, the terms $M_{ID}r$ and $M_{ID}s$ are themselves ε apart, thus at nonnull distance. The best one can say, then, is that $\delta_\tau(M_{ID}, f, M_{ID})$, where $f(x, \varepsilon) = \varepsilon$.*

As the previous example suggests, a term M being at self-distance d is a witness of M being *sensitive to changes* to the environment according to d. Indeed, the only terms which are at self-distance 0 are the constant functions. This makes the underlying theory more general than the one of logical or metric relations, although the latter can be proved to be captured by differential logical relations, as we will see in the next section.

Coming back to the question with which we opened the section, we can formulate a suitable fundamental lemma for differential logical relations by stating that for any closed term M of type τ there exists $d \in (\!|\tau|\!)$ such that $(M, d, M) \in \delta_\tau$. In order to prove such result, however, we need to prove something stronger, namely the extension of the above statement to arbitrary (and thus possibly open) terms. Doing so, requires to extend differential logical relations to arbitrary sequents $\Gamma \vdash \tau$. Let us begin extending the maps $[\![\cdot]\!]$ and $(\!|\cdot|\!)$ to environments.

Definition 12. *Given an environment Γ, define:*

$$[\![\Gamma]\!] = \prod_{(x:\tau)\in\Gamma} [\![\tau]\!]; \qquad (\!|\Gamma|\!) = \prod_{(x:\tau)\in\Gamma} (\!|\tau|\!).$$

An element in e.g. $(\!|\Gamma|\!)$ is thus a family $\alpha \in \prod_{(x:\tau)\in\Gamma}$, meaning that for any $(x : \tau) \in \Gamma$, $\alpha(x) \in (\!|\tau|\!)$. The syntactic counterparts of such families is given by families $\mathbf{V} \in \prod_{(x:\tau)\in\Gamma} CV(\tau)$. We refer to $\mathbf{V}$ as a Γ-*family of values*. Indeed, such a Γ-family of values can naturally be seen as a substitution mapping each variable $(x : \tau) \in \Gamma$ to $\mathbf{V}(x) \in CV(\tau)$. As it is customary, for a term $\Gamma \vdash M : \tau$ we write $M\mathbf{V}$ for the closed term of type τ obtained applying the substitution $\mathbf{V}$ to M. We denote by $CV(\Gamma)$ the set of all Γ-family of values.

We can now extend a differential logical relation $\{\delta_\tau\}_\tau$ to environments stipulating that the family $\{\delta_\Gamma \subseteq CV(\Gamma) \times (\!|\Gamma|\!) \times CV(\Gamma)\}_\Gamma$ is a differential logical relation if

$$\delta_\Gamma(\mathbf{V}, \alpha, \mathbf{W}) \iff \forall (x : \tau) \in \Gamma.\ \delta_\tau(\mathbf{V}(x), \alpha(x), \mathbf{W}(x)).$$

Next, we extend our framework to arbitrary sequents $\Gamma \vdash \tau$. First of all, we define:

$$[\![\Gamma \vdash \tau]\!] = [\![\tau]\!]^{[\![\Gamma]\!]}; \qquad (\!|\Gamma \vdash \tau|\!) = (\!|\tau|\!)^{[\![\Gamma]\!]\times(\!|\Gamma|\!)}.$$

It is then natural to extend $\{\delta_\tau\}_\tau$ to arbitrary sequents by stipulating that $\{\delta_{\Gamma\vdash\tau} \subseteq \Lambda_{\Gamma\vdash\tau} \times (\!|\Gamma \vdash \tau|\!) \times \Lambda_{\Gamma\vdash\tau}\}_{\Gamma\vdash\tau}$, where $\Lambda_{\Gamma\vdash\tau}$ denotes the set of sequents typable within the sequent $\Gamma \vdash \tau$, is a differential logical relation if $\delta_{\Gamma\vdash\tau}(M, d, N)$ holds if and only if

$$\delta_\Gamma(\mathbf{V}, \alpha, \mathbf{W}) \implies \delta_\tau(M\mathbf{V}, d([\![\mathbf{V}]\!], \alpha), N\mathbf{W}).$$

This definition as it is, however, does not work well, as it does not take into account possible alternations of the substitutions $\mathbf{V}$ and $\mathbf{W}$. To solve this issue we introduce the following notation. Given a boolean-valued map $B \in \{0, 1\}^\Gamma$, and two substitutions $\mathbf{V}, \mathbf{W} \in CV(\Gamma)$, define the substitution $B^{\mathbf{V}}_{\mathbf{W}} \in CV(\Gamma)$ as:

$$B^{\mathbf{V}}_{\mathbf{W}}(x) = \begin{cases} \mathbf{V}(x) & \text{if } b(x) = 0 \\ \mathbf{W}(x) & \text{if } b(x) = 1. \end{cases}$$

We can now extend differential logical relations to arbitrary terms.

Definition 13. *Given a differential logical relations* $\{\delta_\tau\}_\tau$*, define* $\{\delta_{\Gamma\vdash\tau} \subseteq \Lambda_{\Gamma\vdash\tau} \times (\!|\Gamma \vdash \tau|\!) \times \Lambda_{\Gamma\vdash\tau}\}_{\Gamma\vdash\tau}$ *stipulating that* $\delta_{\Gamma\vdash\tau}(M, d, N)$ *holds if and only if*

$$\delta_\Gamma(\mathbf{V}, \alpha, \mathbf{W}) \implies \forall B \in \{0,1\}^\Gamma \delta_\tau(MB^{\mathbf{V}}_{\mathbf{W}}, d([\![\mathbf{V}]\!], \alpha), NB^{\mathbf{W}}_{\mathbf{V}}).$$

Before proving the desired strengthening of the fundamental lemma, it is useful to observe the following useful result, where we use the notation $NF(M)$ to denote the (unique) value a well-typed closed term M evaluates to (cf. Theorem 1).

Lemma 14. *For all terms* $\cdot \vdash M, N : \tau$*, we have* $\delta_\tau(M, d, N) \iff \delta_\tau(NF(M), d, NF(N))$.

Proof. First observe that if $\delta_\tau(M', d, N)$ and $M \to_\beta M'$ (where $\to_\beta$ is the obvious small-step semantics relation associated to $\Downarrow$), then $\delta_\tau(M, d, N)$ holds (a similar statement holds for N). By Theorem 1 we thus infer the right-to-left implication. For the other implication, we proceed by induction on τ observing that $NF(NF(M)V) = NF(MV)$. □

Lemma 15. *For any* $\Gamma \vdash M : \tau$*, there exists* $d \in (\!|\Gamma \vdash \tau|\!)$ *such that* $\delta_{\Gamma\vdash\tau}(M, d, M)$.

Proof. The proof is by induction on $\Gamma \vdash M : \tau$.

- Suppose $\Gamma \vdash x : \tau$, meaning that $x \in \Gamma$. We simply define $d : [\![\Gamma]\!] \times (\!|\Gamma|\!) \to (\!|\tau|\!)$ as $d(g, \alpha) = \alpha(x)$.
- Suppose $\Gamma \vdash r : \mathit{REAL}$. Define $d : [\![\Gamma]\!] \times (\!|\Gamma|\!) \to \mathbb{R}^\infty_{\geq 0}$ as $d(g, \alpha) = 0$.
- Suppose $\Gamma \vdash f : \mathit{REAL}^n \to \mathit{REAL}$. For simplicity, we show the case for $n = 1$ (the case for $n > 1$ follows the same structure). We have to find $d \in (\!|\mathit{REAL} \to \mathit{REAL}|\!)^{[\![\Gamma]\!]\times(\!|\Gamma|\!)}$ such that $\delta_\Gamma(\mathbf{V}, \alpha, \mathbf{W})$ implies $\delta_{\mathit{REAL}\to\mathit{REAL}}(f, d([\![\mathbf{V}]\!], \alpha), f)$. The latter means, that for all values $\cdot \vdash V, W \vdash \mathit{REAL}$ (for simplicity, we denote by V both the numeral V and the number $[\![V]\!]$) and $e \in \mathbb{R}^\infty_{\geq 0}$, $|V - W| \leq e$ implies $|NF(f(V)) - NF(f(W))| \leq d([\![\mathbf{V}]\!], \alpha)(V, e)$. Define:

  $$A = \bigcup_{e' \in \mathbb{R}, e' \leq e} [V - e', V + e']; \qquad d([\![\mathbf{V}]\!], \alpha)([\![V]\!], e) = \mathit{diam}(f(A)),$$

  where the diameter $\mathit{diam}(X)$ of a set $X \subseteq \mathbb{R}$ is defined as $\sup_{x,y\in X} |x - y|$. Notice that a set can have diameter ∞. We conclude the wished thesis observing that $|V - W| \leq e$ implies $V, W \in A$ (recall that V, W being real numbers, so is $|V - W|$), and thus $f(V), f(W) \in f(A)$. As a consequence, $|f(V) - f(W)| \leq \mathit{diam}(f(A))$, and thus we are done.
- Suppose $\dfrac{\Gamma \vdash M : \rho \to \tau \quad \Gamma \vdash N : \rho}{\Gamma \vdash MN : \tau}$. By induction hypothesis we have:
  1. There exists $d_1 \in (\!|\rho \to \tau|\!)^{[\![\Gamma]\!]\times(\!|\Gamma|\!)}$ such that $\delta_\Gamma(\mathbf{V}, \alpha, W)$ implies for any $B \in \{0,1\}^\Gamma$, for all $V, W \in CV(\rho)$, and for any $x \in (\!|\rho|\!)$:

     $$\delta_\rho(V, x, W) \implies \delta_\tau(MB^{\mathbf{V}}_{\mathbf{W}}V, d_1([\![\mathbf{V}]\!], \alpha)([\![V]\!], x), MB^{\mathbf{W}}_{\mathbf{V}}W).$$

  2. There exists $d_2 \in (\!|\rho|\!)^{[\![\Gamma]\!]\times(\!|\Gamma|\!)}$ such that $\delta_\Gamma(\mathbf{V}, \alpha, W)$ implies for any $B \in \{0,1\}^\Gamma$:

     $$\delta_\rho(NB^{\mathbf{V}}_{\mathbf{W}}, d_2([\![\mathbf{V}]\!], \alpha), NB^{\mathbf{W}}_{\mathbf{V}}W).$$

  We define the wished d as $d([\![\mathbf{V}]\!], \alpha) = \sup_V d_1([\![\mathbf{V}]\!], \alpha)([\![V]\!], d_2([\![\mathbf{V}]\!], \alpha))$. We conclude the wished thesis instantiating V as $NF(NB^{\mathbf{V}}_{\mathbf{W}})$ relying on Lemma 14.
- Suppose $\dfrac{\Gamma, x : \tau \vdash M : \rho}{\Gamma \vdash \lambda x.M : \tau \to \rho}$. The thesis directly follows from the induction hypothesis.

□

As an immediate corollary we obtain the wished result.

Thoerem 16 (Fundamental Lemma, Version I)**.** *For every $\cdot \vdash M : \tau$ there is a $d \in (\!|\tau|\!)$ such that $(M, d, M) \in \delta_\tau$.*

But what do we gain from Theorem 16? In the classic theory of logical relations, the Fundamental Lemma has, as an easy corollary, that logical relations are compatible: it suffices to invoke the theorem with any context C *seen as a term* $C[x]$, such that $x : \tau, \Gamma \vdash C[x] : \rho$. Thus, ultimately, logical relations are proved to be a *compositional* methodology for program equivalence, in the following sense: if M and N are equivalent, then $C[M]$ and $C[N]$ are equivalent, too.

In the realm of differential logical relations, the Fundamental Lemma plays a similar role, although with a different, *quantitative* flavor: once C has been proved sensitive to changes according to d, and V, W are proved to be at distance e, then, e.g., the impact of substituting V with W in C can be measured by composing d and e (and $[\![V]\!]$), i.e. by computing $d([\![V]\!], e)$. Notice that the sensitivity analysis on C and the relational analysis on V and W are decoupled. What the Fundamental Lemma tells you is that d and e can *always* be found.

3.2 Our Running Example, Revisited

It is now time to revisit the example we talked about in the Introduction. Consider the following two programs, both closed and of type $REAL \to REAL$:

$$M_{SIN} = \lambda x.sin_1(x); \qquad M_{ID} = \lambda x.x.$$

First of all, let us observe that, as already remarked, comparing M_{SIN} and M_{ID} using the sup metric on $\mathbb{R} \to \mathbb{R}$, as it is done in metric logical relations and applicative distances, naturally assigns them distance ∞, the euclidean distance $|x - sin(x)|$ being unbounded when x ranges over $\mathbb{R}$.

Let us prove that $(M_{SIN}, f, M_{ID}) \in \delta_{REAL \to REAL}$, where $f(x, y) = y + |x - \sin x|$. Consider any pair of real numbers $r, s \in \mathbb{R}$ such that $|r - s| \leq \varepsilon$, where $\varepsilon \in \mathbb{R}^\infty_{\geq 0}$. We have that:

$$\begin{aligned} |\sin r - s| &= |\sin r - r + r - s| \leq |\sin r - r| + |r - s| \leq |\sin r - r| + \varepsilon = f(r, \varepsilon) \\ |\sin s - r| &= |\sin s - \sin r + \sin r - r| \leq |\sin s - \sin r| + |\sin r - r| \leq |s - r| + |\sin r - r| \\ &\leq \varepsilon + |\sin r - r| = f(r, \varepsilon). \end{aligned}$$

The fact that $|\sin s - \sin r| \leq |s - r|$ is a consequence of sin being 1-Lipschitz continuous. This can be proved, e.g., by way of Lagrange Theorem:

Thoerem 17 (Lagrange)**.** *Let $f : [a, b] \to \mathbb{R}$ a function continuous in $[a, b]$ and differentiable in (a, b). Then there exists a point $c \in (a, b)$ such that*

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

The following is an easy corollary

Proposition 18. *For each ϑ, φ, $|\sin(\vartheta) - \sin(\varphi)| \leq |\vartheta - \varphi|$.*

Proof. If $\vartheta = \varphi$ the result is trivial. Then without loss of generality we consider $\varphi < \vartheta$. We apply Lagrange Theorem to the interval $[\varphi, \vartheta]$. In particular, there exists a point $\psi \in (\varphi, \vartheta)$ such that

$$\frac{\sin(\vartheta) - \sin(\varphi)}{\vartheta - \phi} = \sin'(\psi) = \cos(\psi).$$

Since $-1 \leq \cos(\psi) \leq 1$,

$$\left| \frac{\sin(\vartheta) - \sin(\varphi)}{\vartheta - \phi} \right| \leq 1$$

from which follows $|\sin(\vartheta) - \sin(\varphi)| \leq |\vartheta - \varphi|$. □

Now, consider a context C which makes use of either M_{SIN} or M_{ID} by feeding them with a value close to 0, call it θ. Such a context could be, e.g., $C = (\lambda x.x(x\theta))[\cdot]$. C can be seen as a term having type $\tau = (REAL \to REAL) \to REAL$. A self-distance d for C can thus be defined as an element of

$$(\!|\tau|\!) = [\![REAL \to REAL]\!] \times (\!|REAL \to REAL|\!) \to \mathbb{R}^{\infty}_{\geq 0}.$$

namely $F = \lambda\!\!\lambda\langle g, h\rangle.h(g(\theta), h(\theta, 0))$. This allows for compositional reasoning about program distances: the overall impact of replacing M_{SIN} by M_{ID} can be evaluated by computing $F([\![M_{SIN}]\!], f)$. Of course the context C needs to be taken into account, but *once and for all*: the functional F can be built without any access to either M_{SIN} or M_{ID}.

4 Logical and Metric Relations as DLRs

The previous section should have convinced the reader about the peculiar characteristics of differential logical relations compared to (standard) metric and logical relations. In this section we show that despite the apparent differences, logical and metric relations can somehow be retrieved as specific kinds of program differences. This is, however, bound to be nontrivial. The naïve attempt, namely seeing program equivalence as being captured by *minimal* distances in logical relations, fails: the distance between a program *and itself* can be nonnull.

How should we proceed, then? Isolating those distances which witness program equivalence is indeed possible, but requires a bit of an effort. In particular, the sets of those distances can be, again, defined by induction on τ. For every τ, we give $(\!|\tau|\!)^0 \subseteq (\!|\tau|\!)$ by induction on the structure of τ:

$$(\!|REAL|\!)^0 = \{0\} \qquad (\!|\tau \times \rho|\!)^0 = (\!|\tau|\!)^0 \times (\!|\rho|\!)^0$$
$$(\!|\tau \to \rho|\!)^0 = \{f \mid \forall x \in [\![\tau]\!].\forall y \in (\!|\tau|\!)^0.f(x, y) \in (\!|\rho|\!)^0\}$$

Lemma 19. *$(\!|\tau|\!)^0$ is complete. That is, $\forall A \subseteq (\!|\tau|\!)^0.\sup A \in (\!|\tau|\!)^0$.*

Proof. By induction on types.

- Case $REAL$. Obvious: $\sup \emptyset = \sup \{0\} = 0 \in (\!|REAL|\!)^0$.
- Case $\tau \to \rho$. Let $A \subseteq (\!|\tau \to \rho|\!)^0$. Note that $\forall f \in A.\forall x \in CV(\tau).\forall d \in (\!|\tau|\!)^0.f(x, d) \in (\!|\rho|\!)^0$. The function $s = \sup A$: $CV(\tau) \times (\!|\tau|\!) \to (\!|\rho|\!)$ is defined by $s(x, d) = \sup\{f(x, d) \mid f \in A\}$. We verify that $\forall x \in CV(\tau).\forall d \in (\!|\tau|\!)^0.s(x, d) \in (\!|\rho|\!)^0$. This is true since given $x \in CV(\tau)$ and $d \in (\!|\tau|\!)^0$, $f(x, d)$ is in $(\!|\rho|\!)^0$, and thus $s(x, d) = \sup\{f(x, d) \mid f \in A\} \in (\!|\rho|\!)^0$ by I.H.
- Let $A \subseteq (\!|\tau \times \rho|\!)^0$. Then $\sup A = (\sup(\pi_1 A), \sup(\pi_2 A)) \in (\!|\tau|\!)^0 \times (\!|\rho|\!)^0 = (\!|\tau \times \rho|\!)^0$ by I.H.

□

Lemma 20. *Let $d, d' \in (\!|\tau|\!)^0$ and $d \leq_\tau d'$. Let $\{\delta_\rho\}_\rho$ be a differential logical relation. If $\delta_\tau(M, d, N)$ then $\delta_\tau(M, d', N)$.*

Proof. By induction on types.

- Case $REAL$. Obvious, since $(\!|REAL|\!)^0 = \{0\}$.
- Case $\tau \to \rho$. Let $\delta_{\tau\to\rho}(M, f, N)$ and $f \leq f'$. Then $\forall x \in CV(\tau).\forall d \in (\!|\tau|\!).\forall x \in CV(\tau)$.

$$\begin{array}{rcl} \delta_\tau(x, d, y) & \Rightarrow & \delta_\rho(Mx, f(x, d), Ny) \wedge \delta_\rho(My, f(x, d), Nx) \\ & \Rightarrow & \delta_\rho(Mx, f'(x, d), Ny) \wedge \delta_\rho(My, f'(x, d), Nx) \\ & & \text{by } f(x, d) \leq f'(x, d) \text{ and I.H.} \end{array}$$

  Thus $\delta_{\tau\to\rho}(M, f', N)$.
- Case $\tau \times \rho$. Let $\delta_{\tau\times\rho}(M, (d_1, d_2), N)$ and $(d_1, d_2) \leq (d'_1, d'_2)$. By definition $\delta_\tau(\pi_1 M, d_1, \pi_1 N)$, $\delta_\rho(\pi_2 M, d_2, \pi_2 N)$, $d_1 \leq d'_1$, and $d_2 \leq d'_2$. Thus by I.H. $\delta_\tau(\pi_1 M, d'_1, \pi_1 N)$ and $\delta_\rho(\pi_2 M, d'_2, \pi_2 N)$ hold, hence $\delta_{\tau\times\rho}(M, (d'_1, d'_2), N)$.

□

Notice that $(\!|\tau \to \rho|\!)^0$ is not defined as $[\![\tau]\!] \times (\!|\tau|\!)^0 \to (\!|\rho|\!)^0$ (doing so would violate $(\!|\tau \to \rho|\!)^0 \subseteq (\!|\tau \to \rho|\!)$). The following requires some effort, and testifies that, indeed, program equivalence in the sense of logical relations precisely corresponds to being at a distance in $(\!|\tau|\!)^0$:

Thoerem 21. *Let $\{\mathcal{L}_\tau\}_\tau$ be a logical relation. There exists a differential logical relation $\{\delta_\tau\}_\tau$ satisfying $\mathcal{L}_\tau(M,N) \iff \exists d \in (\!|\tau|\!)^0.\delta_\tau(M,d,N)$.*

Proof. By induction on types.

- Case *REAL*. Define δ_{REAL} by $\delta_{REAL}(M,0,N)$ if and only if $\mathcal{L}_\tau(M,N)$ or $\mathcal{L}_\tau(N,M)$.
- Case $\tau \to \rho$.
  $\Leftarrow$. Assume that there exists $f \in (\!|\tau \to \rho|\!)^0$ satisfying $\delta_{\tau\to\rho}(M,f,N)$. Then for all M', N' of type τ,
  $$\begin{array}{rcl} \mathcal{L}_\tau(M',N') & \overset{\text{I.H.}}{\Leftrightarrow} & \exists d' \in (\!|\tau|\!)^0.\delta_\tau(M',d',N') \\ & \Rightarrow & \delta_\rho(MM', f(M',d'), NN') \\ & \overset{\text{I.H.}}{\Leftrightarrow} & \mathcal{L}_\rho(MM', NN'). \end{array}$$
  Thus $\mathcal{L}_{\tau\to\rho}(M,N)$ holds.
  $\Rightarrow$. Assume $\mathcal{L}_{\tau\to\rho}(M,N)$. Define a function $f^{M,N}\colon CV(\tau) \times (\!|\tau|\!) \to (\!|\rho|\!)$ by:
  $$f^{M,N}(M',d) = \sup \bigcup_{N'\colon \delta_\tau(M',d,N')} \{d' \in (\!|\rho|\!)^0 \;\mid\; \delta_\rho(MM', d', NN')\}.$$
  We show that
  - (I) $f^{M,N} \in (\!|\tau \to \rho|\!)^0$
  - (II) $\delta_{\tau\to\rho}(M, f^{M,N}, N)$.

  (I) is immediate since the right-hand side of the definition of $f^{M,N}(M',d)$ is always contained by $(\!|\rho|\!)^0$ by Lemma 19. (II) is equivalent to the following by definition for each $M' \in CV(\tau)$ and $d \in (\!|\tau|\!)$:
  $$\forall N' \in CV(\rho).\delta_\tau(M',d,N') \Rightarrow \delta_\rho(MM', f^{M,N}(M,d), NN') \wedge \delta_\rho(MN', f^{M,N}(M,d), NM').$$
  Fix N' arbitrarily. If $\delta_\tau(M',d,N')$ does not hold, the implication vacuously holds. Assume $\delta_\tau(M',d,N')$ holds. Then we have
  $$\begin{array}{rcl} \delta_\tau(M',d,N') & \overset{\text{I.H.}}{\Leftrightarrow} & \mathcal{L}_\tau(M',N') \\ & \Rightarrow & \mathcal{L}_\rho(MM', NN') \\ & \overset{\text{I.H.}}{\Leftrightarrow} & \exists d' \in (\!|\rho|\!)^0.\delta_\rho(MM', d', NN'). \end{array}$$
  By definition $d' \leq_\rho f^{M,N}(M',d)$ for such $d' \in (\!|\rho|\!)^0$. Thus $\delta_\rho(MM', f^{M,N}(M',d), NN')$ also holds by Lemma 20. Similarly $\delta_\rho(MN', f^{M,N}(M',d), NM')$. Hence $\delta_{\tau\to\rho}(M, f^{M,N}, N)$.
- Case $\tau \times \rho$. Let $\mathcal{L}_{\tau\times\rho}(M,N)$. By definition of logical relations, $\mathcal{L}_\tau(\pi_1 M, \pi_1 N)$ and $\mathcal{L}_\rho(\pi_2 M, \pi_2 N)$ hold. By I.H. there exist $d_1 \in (\!|\tau|\!)^0$ and $d_2 \in (\!|\rho|\!)^0$ that satisfy $\delta_\tau(\pi_1 M, d_1, \pi_1 N)$ and $\delta_\rho(\pi_2 M, d_2, \pi_2 N)$; thus $\delta_{\tau\times\rho}(M, (d_1,d_2), N)$ holds for $(d_1,d_2) \in (\!|\tau \times \rho|\!)^0$. The other direction also holds by I.H.

□

What if we want to generalise the argument above to metric relations, as introduced, e.g., by Reed and Pierce [21]. The set $(\!|\tau|\!)^0$ becomes a set of distances parametrised by a single real number:

$$(\!|REAL|\!)^r = \{r\} \qquad (\!|\tau \times \rho|\!)^r = (\!|\tau|\!)^r \times (\!|\rho|\!)^r$$
$$(\!|\tau \to \rho|\!)^r = \{f \mid \forall x \in [\![\tau]\!].\forall y \in (\!|\tau|\!)^s.f(x,y) \in (\!|\rho|\!)^{r+s}\}$$

5 Strengthening the Fundamental Theorem through Finite Distances

Let us now ask ourselves the following question: given any term $M \in CT(\tau)$, what can we say about its sensitivity, i.e., about the values $d \in (\!|\tau|\!)$ such that $\delta_\tau(M, d, M)$? Two of the results we have proved about $ST^\lambda_{\mathbb{R}}$ indeed give partial answers to the aforementioned question. On the one hand, Theorem 16 states that such a d can *always* be found. On the other hand, Theorem 21 tells us that such a d can be taken in $(\!|\tau|\!)^0$. Both these answers are not particularly informative, however. The mere existence of such a $d \in (\!|\tau|\!)$, for example, is trivial since d can always be taken as d_∞, the maximal element of the underlying quantale. The fact that such a d can be taken from $(\!|\tau|\!)^0$ tells us that, e.g. when $\tau = \rho \to \xi$, M returns equivalent terms when fed with equivalent arguments: there is no quantitative guarantee about the behaviour of the term when fed with non-equivalent arguments.

Is this the best one can get about the sensitivity of $ST^\lambda_{\mathbb{R}}$ terms? The absence of full recursion suggests that we could hope to prove that infinite distances, although part of the underlying quantale, can in fact be useless. In other words, we are implicitly suggesting that self-distances could be elements of $(\!|\tau|\!)^{<\infty} \subset (\!|\tau|\!)$, defined as follows:

$$(\!|REAL|\!)^{<\infty} = \mathbb{R}_{\geq 0}; \qquad (\!|\tau \times \rho|\!)^{<\infty} = (\!|\tau|\!)^{<\infty} \times (\!|\rho|\!)^{<\infty};$$

$$(\!|\tau \to \rho|\!)^{<\infty} = \{f \in (\!|\tau \to \rho|\!) \mid \forall x \in [\![\tau]\!].\forall t \in (\!|\tau|\!)^{<\infty}.f(x,t) \in (\!|\rho|\!)^{<\infty}\}.$$

Please observe that $(\!|\tau|\!)^{<\infty}$ is in general a much larger set of differences than $\bigcup_{r \in \mathbb{R}^\infty_{\geq 0}} (\!|\tau|\!)^r$: the former equals the latter only when τ is $REAL$. Already when τ is $REAL \to REAL$, the former includes, say, functions like $f(r, \varepsilon) = (r + \varepsilon)^2$, while the latter does not.

Unfortunately, there are terms in $ST^\lambda_{\mathbb{R}}$ which cannot be proved to be at self-distance in $(\!|\tau|\!)^{<\infty}$, and, surprisingly, this is *not* due to the higher-order features of $ST^\lambda_{\mathbb{R}}$, but to $\{\mathcal{F}_n\}_{n \in \mathbb{N}}$ being arbitrary, and containing functions which do not map finite distances to finite distances, like

$$h(r) = \begin{cases} 0 & \text{if } r = 0 \\ \frac{1}{r} & \text{otherwise} \end{cases}$$

(see Figure 4). Is this phenomenon *solely* responsible for the necessity of finite self-distances in $ST^\lambda_{\mathbb{R}}$? The answer is positive, and the rest of this section is devoted precisely to formalising and proving the aforementioned conjecture.

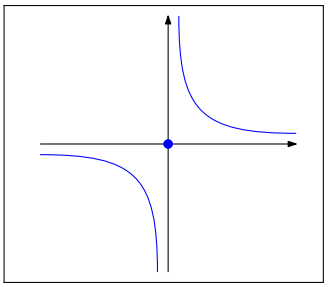


Figure 4: A total, but highly discontinuous, function.

First of all, we need to appropriately axiomatise the absence of unbounded discontinuities from $\{\mathcal{F}_n\}_{n \in \mathbb{N}}$. A not-so-restrictive but sufficient axiom turns out to be weak boundedness: a function $f_n : \mathbb{R}^n \to \mathbb{R}$ is said to be *weakly bounded* if and only if it maps bounded subsets of $\mathbb{R}^n$ into bounded subsets of $\mathbb{R}$. As an example, the function h above is *not* weakly bounded, because $h([-\varepsilon, \varepsilon])$ is

$$\left(-\infty, -\frac{1}{\varepsilon}\right] \cup \{0\} \cup \left[\frac{1}{\varepsilon}, \infty\right)$$

which is unbounded for any as $\varepsilon > 0$. Any term M is said to be weakly bounded iff any function symbol f_n occurring in M is itself weakly bounded. Actually, this is precisely what one needs to get the strengthening of the Fundamental Theorem we are looking for.

Lemma 22. *Let $\cdot \vdash M, N : \tau$ and $M \Downarrow V$. Then $\delta^\tau(M, N) = \delta^\tau(V, N)$.*

Proof. By induction on type τ; do case analysis for each type constructor. □

Lemma 23. *Let τ be a type and $t \in (\!|\tau|\!)^{<\infty}$. If $t' \leq_\tau t$ then $t' \in (\!|\tau|\!)^{<\infty}$.*

Proof. By induction on type τ. Straightforward. □

Thoerem 24 (Fundamental Theorem, Version II)**.** *For any weakly bounded term $\cdot \vdash M : \tau$, there is $d \in (\!|\tau|\!)^{<\infty}$ such that $(M, d, M) \in \delta_\tau$.*

Proof. By induction on derivation of $\Gamma \vdash M : \tau$. In order not to make the proof too unreadable, we prove it for the case $n = 1$, meaning $\Gamma = w\colon \rho$. It is straightforward (but tedious) to extend it to an arbitrarily large environment.

- Case
$$\frac{w : \rho \in \Gamma}{\Gamma \vdash w : \rho.}$$
Then
$$\begin{aligned}
\delta^\rho_\Gamma(w, w) &= \delta^{\rho\to\rho}(\lambda w.w, \lambda w.w)\\
&= \lambda\!\!\lambda \langle x^{CV(\rho)}, y^{(\!|\rho|\!)}\rangle.\sup_{z\colon \delta^\rho(z,x)\le y}\{\delta^\rho((\lambda w.w)x, (\lambda w.w)z), \delta^\rho((\lambda w.w)z, (\lambda w.w)x)\}\\
&= \lambda\!\!\lambda \langle x^{CV(\rho)}, y^{(\!|\rho|\!)}\rangle.\sup_{z\colon \delta^\rho(z,x)\le y}\{\delta^\rho(x, z), \delta^\rho(z, x)\} \text{ by Lemma 22}\\
&= \lambda\!\!\lambda \langle x^{CV(\rho)}, y^{(\!|\rho|\!)}\rangle.\sup_{z\colon \delta^\rho(z,x)\le y}\delta^\rho(z, x) \text{ by Lemma 8}\\
&\le \lambda\!\!\lambda \langle x^{CV(\rho)}, y^{(\!|\rho|\!)}\rangle.y \in (\!|\rho \to \rho|\!)^{<\infty}.
\end{aligned}$$
Hence $\delta^\rho_\Gamma(w, w) \in (\!|\rho \to \rho|\!)^{<\infty}$ by Lemma 23.
- Case
$$\frac{}{\Gamma \vdash r : \mathit{REAL}.}$$
Easy.
- Case
$$\frac{}{\Gamma \vdash f_n : \mathit{REAL}^n \to \mathit{REAL}.}$$
Straightforward.
- Case
$$\frac{\Gamma, x : \tau \vdash M : \rho}{\Gamma \vdash \lambda x.M : \tau \to \rho.}$$
By induction hypothesis.
- Case
$$\frac{\Gamma \vdash M : \tau_1 \to \tau_2 \quad \Gamma \vdash N : \tau_1}{\Gamma \vdash MN : \tau_2}.$$
Induction hypothesis in this case can be written down as:

$\forall x_1 \in CV(\rho).\forall y_1 \in (\!|\rho|\!)^{<\infty}.\forall x_2 \in CV(\tau_1).\forall y_2 \in (\!|\tau_1|\!)^{<\infty}.$
$\sup_{z_1\colon \delta^\rho(z_1,x_1)\le y_1}\sup_{z_2\colon \delta^\rho(z_2,x_2)\le y_2}\{\delta^{\tau_2}(M\{x_1/w\}x_2, M\{z_1/w\}z_2), \delta^{\tau_2}(M\{x_1/w\}z_2, M\{z_1/w\}x_2)\} \in (\!|\tau_2|\!)^{<\infty}$
$\cdots$ (I)

$\forall x_1 \in CV(\rho).\forall y_1 \in (\!|\rho|\!)^{<\infty}.$
$\sup_{z_1\colon \delta^\rho(z_1,x_1)\le y_1}\delta^{\tau_2}(N\{x_1/w\}, N\{z_1/w\}) \in (\!|\tau_1|\!)^{<\infty}$ $\cdots$ (II)

We show that $\delta^{\tau_2}_\Gamma(MN, MN) \in (\!|\tau_2|\!)^{<\infty}$, i.e. $\delta^{\tau_2}(\lambda w.MN, \lambda w.MN) \in (\!|\rho \to \tau_2|\!)^{<\infty}$. By definition we must show that

$\forall x_1 \in CV(\rho).\forall y_1 \in (\!|\rho|\!)^{<\infty}.$
$\sup_{z\colon \delta^\rho(z,x_1)\le y_1}\{\delta^{\tau_2}((\lambda w.MN)x_1, (\lambda w.MN)z), \delta^{\tau_2}((\lambda w.MN)z, (\lambda w.MN)x_1)\}$
$= \sup_{z\colon \delta^\rho(z,x_1)\le y_1}\delta^{\tau_2}((\lambda w.MN)z, (\lambda w.MN)x_1)$ by Lemma 8
$= \sup_{z\colon \delta^\rho(z,x_1)\le y_1}\delta^{\tau_2}(M\{z/w\}N\{z/w\}, M\{x_1/w\}N\{x_1/w\})$ by Lemma 22
$\in (\!|\tau_2|\!)^{<\infty}.$

By definition of sup the following inequality holds for all $x_1 \in CV(\rho)$ and $y_1 \in (\!|\rho|\!)^{<\infty}$:

$\sup_{z_1\colon \delta^\rho(z_1,x_1)\le y_1}\delta^{\tau_2}(M\{z_1/w\}N\{z_1/w\}, M\{x_1/w\}N\{x_1/w\})$
$\le \sup_{z_1\colon \delta^\rho(z_1,x_1)\le y_1}\{\delta^{\tau_2}(M\{x_1/w\}N\{x_1/w\}, M\{z_1/w\}N\{z_1/w\}), \delta^{\tau_2}(M\{x_1/w\}N\{z_1/w\}, M\{z_1/w\}N\{x_1/w\})\}$
$\le \sup_{z_1\colon \delta^\rho(z_1,x_1)\le y_1}\sup_{z_2\colon \delta^\rho(z_1,N\{x_1/w\})\le s}$
$\{\delta^{\tau_2}(M\{x_1/w\}N\{x_1/w\}, M\{z_1/w\}z_2), \delta^{\tau_2}(M\{x_1/w\}z_2, M\{z_1/w\}N\{x_1/w\})\},$

where $s = \sup_{z_1 \,:\, \delta^\rho(z_1,x_1)\leq y_1} \delta^{\tau_2}(N\{x_1/w\}, N\{z/w\})$.
Thus by Lemma 23 it suffices show that

$$\sup_{z_1 \,:\, \delta^\rho(z_1,x_1)\leq y_1} \sup_{z_2 \,:\, \delta^\rho(z_1,N\{x_1/w\})\leq s} \{\delta^{\tau_2}(M\{x_1/w\}N\{x_1/w\}, M\{z_1/w\}z_2), \delta^{\tau_2}(M\{x_1/w\}z_2, M\{z_1/w\}N\{x_1/w\})\} \in (\!|\tau_2|\!)^{<\infty}.$$

By I.H. (I), this holds if $N\{x_1/w\} \in CV(\tau_2)$ and $s = \sup_{z_1 \,:\, \delta^\rho(z_1,x_1)\leq y_1} \delta^{\tau_2}(N\{x_1/w\}, N\{z/w\}) \in (\!|\tau_2|\!)^{<\infty}$; the latter holds by I.H. (II).

- Case
$$\frac{\Gamma \vdash M : \tau \quad \Gamma \vdash N : \rho}{\Gamma \vdash \langle M, N\rangle : \tau \times \rho} .$$
Straightforward using induction hypothesis.
- Case
$$\frac{}{\Gamma \vdash \pi_1 : \tau \times \rho \to \tau.}$$
Straightforward.
- Case
$$\frac{}{\Gamma \vdash \pi_2 : \tau \times \rho \to \rho.}$$
Straightforward, similar to the case of π_1.

□

The reader may have wondered about how restrictive a condition weak boundedness really is. In particular, whether it corresponds to some form of continuity. In fact, the introduced condition only rules out unbounded discontinuities. In other words, weak boundedness can be equivalently defined by imposing local boundedness *at any point* in the domain $\mathbb{R}$. This is weaker than asking for boundedness, which requires the existence of a global bound.

6 A Categorical Perspective

Up to now, differential logical relations have been treated very concretely, without looking at them through the lens of category theory. This is in contrast to, e.g., the treatment of metric relations from [10], in which soundness of metric relations for FUZZ is obtained as a byproduct of a proof of symmetric monoidal closedness for the category **MET** of pseudometric spaces and Lipschitz functions.

But what could take the place of pseudometric spaces in a categorical framework capturing differential logical relations? The notion of a metric needs to be relaxed along at least two axes. On the one hand, the codomain of the "metric" δ is not necessarily the set of real numbers, but a more general structure, namely a quantale. On the other, as we already noticed, it is not necessarily true that equality implies indistancy, but rather than indistancy implies inequality. What comes out of these observations is, quite naturally, the notion of a generalized metric domain, itself a generalisation of partial metrics [6]. The rest of this section is devoted to proving that the category of generalised metric domains is indeed cartesian closed, thus forming a model of simply typed λ-calculi.

Formally, given a quantale $\mathbb{Q} = (Q, \leq_Q, 0_Q, *_Q)$[3], a *generalised metric domain* on $\mathbb{Q}$ is a pair (A, δ_A), where A is a set and δ_A is a subset of $A \times \mathbb{Q} \times A$ satisfying some axioms akin to those of a metric domain:

$$\delta_A(x, 0_Q, y) \Rightarrow x = y; \qquad \text{(Indistancy Implies Equality)}$$
$$\delta_A(x, d, y) \Rightarrow \delta_A(y, d, x); \qquad \text{(Symmetry)}$$
$$\delta_A(x, d, y) \wedge \delta_A(y, e, y) \wedge \delta_A(y, f, z) \Rightarrow \delta_A(x, d * e * f, z). \qquad \text{(Triangularity)}$$

Please observe that δ_A is a *relation* rather than a function. Moreover, the first axiom is dual to the one typically found in, say, pseudometrics. The third axiom, instead, resembles the usual

[3]When unambiguous, we will omit subscripts in $\leq_Q$, 0_Q, and $*_Q$.

triangle inequality for pseudometrics, but with the crucial difference that since objects can have non-null self-distance, such a distance has to be taken into account. Requiring equality to imply indistancy (and thus $\delta_A(x, 0_Q, y) \Leftrightarrow x = y$), we see that (Triangularity) gives exactly the usual triangle inequality (properly generalised to quantale and relations [15, 16]).

In this section we show that generalised metric domains form a cartesian closed category, unlike that of metric spaces (which is known to be non-cartesian closed). As a consequence, we obtain a firm categorical basis of differential logical relations. The category of generalised metric domain, denoted by **GMD**.

Definition 25. *The category* **GMD** *has the following data.*

- *An object* $\mathcal{A}$ *is a triple* $(A, \mathbb{Q}, \delta)$ *where* $\mathbb{Q}$ *is a quantale and* (A, δ) *is a generalized metric domain on* $\mathbb{Q}$.
- *An arrow* $(A, \mathbb{Q}, \delta) \to (B, \mathbb{S}, \rho)$ *is a pair* (f, ζ) *consisting of a function* $f \colon A \to B$ *and another function* $\zeta \colon Q \times A \to S$ *satisfying* $\forall a, a' \in A. \forall q \in Q. \delta(a, q, a') \Rightarrow \rho(f(a), \zeta(q, a), f(a'))$ *and* $\rho(f(a), \zeta(q, a'), f(a'))$.

We can indeed give **GMD** the structure of a category. In fact, the identity on the object $\mathcal{A} = (A, \mathbb{Q}, \delta)$ in **GMD** is given by $(\mathrm{id}_{\mathcal{A}}, \mathrm{id}'_{\mathcal{A}})$ where $\mathrm{id}_{\mathcal{A}} \colon A \to A$ is the set-theoretic identity on A and $\mathrm{id}'_{\mathcal{A}} \colon Q \times A \to Q$ is defined by $\mathrm{id}'_{\mathcal{A}}(q, a) = q$. The composition of two arrows $(f, \zeta) \colon (A, \mathbb{Q}, \delta) \to (B, \mathbb{S}, \rho)$ and $(g, \eta) \colon (B, \mathbb{S}, \rho) \to (C, \mathbb{T}, \nu)$ is the pair (h, θ) where $h \colon A \to C$ is given by the function composition $g \circ f \colon A \to C$ and $h \colon Q \times A \to T$ is given by $\theta(q, a) = \eta(\zeta(q, a), f(a))$. Straightforward calculations show that composition is associative, and that the identity arrow behaves as its neutral element.

Lemma 26. **GMD** *is a category.*

Proof. The identity on the object $\mathcal{A} = (A, \mathbb{Q}, \delta)$ in **GMD** is given by $(\mathrm{id}_{\mathcal{A}}, \mathrm{id}'_{\mathcal{A}})$ where $\mathrm{id}_{\mathcal{A}} \colon A \to A$ is the set-theoretic ideneity on A and $\mathrm{id}'_{\mathcal{A}} \colon Q \times A \to Q$ is defined by $\mathrm{id}'_{\mathcal{A}}(q, a) = q$. The composition of two arrows $(f, \zeta) \colon (A, \mathbb{Q}, \delta) \to (B, \mathbb{S}, \rho)$ and $(g, \eta) \colon (B, \mathbb{S}, \rho) \to (C, \mathbb{T}, \nu)$ is the pair (h, θ) where $h \colon A \to C$ is given by the function composition $g \circ f \colon A \to C$ and $h \colon Q \times A \to T$ is given by $\theta(q, a) = \eta(\zeta(q, a), f(a))$. The fact that every identity arrow and every composition are again arrows in **GMD** can be checked straightforwardly: $\mathrm{id}_{\mathcal{A}}$ clearly satisfies $\delta(a, q, a') \Rightarrow \delta(\mathrm{id}(a), \mathrm{id}'(q, a), \mathrm{id}(a'))$ and $\delta(\mathrm{id}(a), \mathrm{id}'(q, a'), id(a'))$ since the right-hand side is by definition $\delta(a, q, a)$. We have to check that (h, θ) satisfies $\delta(a, q, a') \Rightarrow \nu(h(a), \theta(q, a), h(a'))$ (and its symmetric part). Indeed, we have $\delta(f(a), \zeta(q, a), f(a'))$ since (f, ζ) is an arrow in **GMD**; and $\nu(g(f(a)), \eta(\zeta(q, a), f(a)), g(f(a')))$, which is equivalent to $\nu(h(a), \theta(q, a), h(a'))$ by definition, holds since (g, η) is an arrow in **GMD**. (Similarly for the symmetric part.) □

The construction of (finite) products in **GMD** is mostly straightforward:

Lemma 27. *The category* **GMD** *has a terminal object and binary products.*

Proof. The terminal object **GMD** is defined as $(\{*\}, \mathbb{0}, \delta_0)$, where $\mathbb{0}$ is the one-element quantale $\{0\}$, and $\delta_0 = \{(*, 0, *)\}$. Clearly, $(\{*\}, \delta_0)$ is a generaliszed metric domain on $\mathbb{0}$ which behaves as a terminal object. Next, we show that **GMD** has binary products. Given two objects $\mathcal{A}$ and $\mathcal{B}$, their binary product $\mathcal{A} \times \mathcal{B}$ is given by a triple $(A \times B, \mathbb{Q} \times \mathbb{S}, \delta \times \rho)$. The projection from $\mathcal{A} \times \mathcal{B}$ to $\mathcal{A}$ is the pair (π_1, π'_1) given by $\pi_1(a, b) = a$ and $\pi'_1((q, s), (a, b)) = q$ (similarly for π_2).

Given objects $\mathcal{A}, \mathcal{B}, \mathcal{C}$ and arrows $(f, \zeta) \colon \mathcal{C} \to \mathcal{A}, (g, \eta) \colon \mathcal{C} \to \mathcal{B}$, the mediating arrow $\mathcal{C} \to \mathcal{A} \times \mathcal{B}$ is given by a pair (h, θ) where $h \colon C \to A \times B$ is a function $h(c) = (f(c), g(c))$ and $\theta \colon T \times C \to Q \times S$ is a function $\theta(t, c) = (\zeta(t, c), \eta(t, c))$. This satisfies $(\pi_1, \pi'_1) \circ (h, \theta) = (f, \zeta)$: on the first component, $(\pi_1 \circ h)(c) = \pi_1(g(c), h(c)) = g(c)$. On the second, $(\pi'_1 \circ \theta)(t, c) = \pi'_1(\theta(t, c), h(c)) = \pi'_1((\zeta(t, c), \eta(t, c)), h(c)) = \zeta(t, c)$ (similarly $(\pi_2, \pi'_2) \circ (h, \theta) = (g, \eta)$ holds). □

Lemma 28. *The category* **GMD** *has exponential objects.*

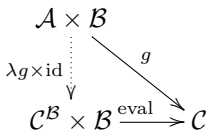
Proof. The exponential object $\mathcal{C}^{\mathcal{B}}$ is given by a triple $(C^B, \mathbb{T}^{\mathbb{S} \times B}, \nu^{\rho})$ where C^B is the function space $\{f \mid f \colon B \to C\}$, $\mathbb{T}^{\mathbb{S} \times B}$ is the exponential quantale, and ν^{ρ} is a ternary relation over $C^B \times$

$T^{S\times B} \times C^B$ defined by: if $\rho(b, s, b')$ then $\nu(f(b), d(s, b), f'(b'))$ and $\nu(f(b), d(s, b'), \zeta(b'))$. The relation ν^ρ is indeed a differential logical relation.

Then given three objects $\mathcal{A}, \mathcal{B}, \mathcal{C}$ and an arrow $g\colon \mathcal{A}\times\mathcal{B} \to \mathcal{C}$, the abstraction $\lambda g\colon \mathcal{A} \to \mathcal{C}^\mathcal{B}$ of g is given by a pair $(\lambda g, \lambda\eta)$ where $\lambda g\colon A \to C^B$ is defined by $\lambda g(a)(b) = g(a, b)$ and $\lambda\eta\colon Q\times A \to T^{S\times B}$ is defined by $\lambda\eta(q, a)(s, b) = \eta((q, s), (a, b))$.

Last, $\mathrm{eval}\colon \mathcal{C}^\mathcal{B} \times \mathcal{B} \to \mathcal{C}$ is given by a pair $(\mathrm{eval}, \mathrm{eval}')$ where $\mathrm{eval}\colon C^B \times B \to C$ is defined by $\mathrm{eval}(f, b) = f(b)$ and $\mathrm{eval}'\colon (T^{S\times B} \times S) \times (C^B \times B) \to T$ is defined by $\mathrm{eval}'((d, s), (f, b)) = d(s, b)$.

The fact that these arrows makes the diagram



commute can be checked componentwise. Let (h, θ) be the pair comprising the composition $\mathrm{eval}\circ(\lambda g \times \mathrm{id})\colon \mathcal{A}\times\mathcal{B} \to \mathcal{C}$. On the first component, we have $h((a, b)) = \mathrm{eval}((\lambda g \times \mathrm{id})(a, b)) = \mathrm{eval}((\lambda g(a), b)) = \lambda g(a)(b) = g(a, b)$. On the second, $\theta((q, s), (a, b)) = \mathrm{eval}'((\lambda\eta\times\mathrm{id}')(q, s)(a, b), (\lambda g\times \mathrm{id})(a, b)) = \mathrm{eval}'((\lambda\eta(q, a), \mathrm{id}'(s, b)), (\lambda g(a), b)) = \mathrm{eval}'((\lambda\eta(q, a), s), (\lambda g(a), b)) = \lambda\eta(q, a)(s, b) = \eta((q, s), (a, b))$.

□

Joining together 27 and and 28 we obtain the wished result.

Corollary 29. *The category* **GMD** *is cartesian closed.*

Interestingly, the constructions of product and exponential objects closely match the definition of a differential logical relation. In other words, differential logical relations as given in Definition 7 can be seen as providing a denotational model of $ST^\lambda_\mathbb{R}$ in which base types are interpreted by the generalised metric domain corresponding to the Euclidean distance.

7 Conclusion

In this paper, we introduced differential logical relations as a novel methodology to evaluate the "distance" between programs of higher-order calculi akin to the λ-calculus. We have been strongly inspired by some unpublished work by Westbrook and Chaudhuri [28], who were the first to realise that evaluating differences between interactive programs requires going beyond mere real numbers. We indeed borrowed our running examples from the aforementioned work.

This paper's contribution, then consists in giving a simple definition of differential logical relations, together with some results about their underlying metatheory: two formulations of the Fundamental Lemma, a result relating differential logical relations and ordinary logical relations, a categorical framework in which generalised metric domains — the metric structure corresponding to differential logical relations — are proved to form a cartesian closed category. Such results give evidence that, besides being *more expressive* than metric relations, differential logical relations are somehow *more canonical*, naturally forming a model of simply-typed λ-calculi.

As the title of this paper suggests, we see the contributions above just as a very first step towards understanding the nature of differences in a logical environment. In particular, at least two directions deserve to be further explored.

- The first one concerns *language features*: admittedly, the calculus $ST^\lambda_\mathbb{R}$ we consider here is very poor in terms of its expressive power, lacking full higher-order recursion and thus not being universal. Moreover, $ST^\lambda_\mathbb{R}$ does not feature any form of effect, including probabilistic choices, in which evaluating differences between programs would be very helpful. Addressing such issues seems to require to impose a domain structure on generalised metric domain, on one hand, and to look at monads on **GMD**, on the other hand (for the latter, the literature on monadic lifting for quantale-valued relations might serve as a guide [15]).

- The second one is about *abstract differences*: defining differences as functions with *the same rank* as that of the compared programs implies that reasoning about them is complex. Abstracting differences so as to facilitate differential reasoning could be the way out, given that deep connections exist between logical relations and abstract interpretation [2].

References

[1] S. Abramsky. The lazy lambda calculus. In D. Turner, editor, *Research Topics in Functional Programming*, pages 65–117. Addison Wesley, 1990.

[2] Samson Abramsky. Abstract interpretation, logical relations and Kan extensions. *J. Log. Comput.*, 1(1):5–40, 1990.

[3] A. Arnold and M. Nivat. Metric interpretations of infinite trees and semantics of non deterministic recursive programs. *Theor. Comput. Sci.*, 11:181–205, 1980.

[4] C. Baier and M.E. Majster-Cederbaum. Denotational semantics in the CPO and metric approach. *Theor. Comput. Sci.*, 135(2):171–220, 1994.

[5] Gilles Barthe, Marco Gaboardi, Justin Hsu, and Benjamin C. Pierce. Programming language techniques for differential privacy. *SIGLOG News*, 3(1):34–53, 2016.

[6] Michael A. Bukatin, Ralph Kopperman, Steve Matthews, and Homeira Pajoohesh. Partial metric spaces. *The American Mathematical Monthly*, 116(8):708–718, 2009.

[7] Konstantinos Chatzikokolakis, Daniel Gebler, Catuscia Palamidessi, and Lili Xu. Generalized bisimulation metrics. In *CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings*, pages 32–46, 2014.

[8] Raphaëlle Crubillé and Ugo Dal Lago. Metric reasoning about λ-terms: The affine case. In *Proc. of LICS 2015*, pages 633–644, 2015.

[9] Raphaëlle Crubillé and Ugo Dal Lago. Metric reasoning about λ-terms: The general case. In *Proc. of ESOP 2017*, pages 341–367, 2017.

[10] A.A. de Amorim, M. Gaboardi, J. Hsu, S. Katsumata, and I. Cherigui. A semantic account of metric preservation. In *Proc. of POPL 2017*, pages 545–556, 2017.

[11] J.W. de Bakker and J.I. Zucker. Denotational semantics of concurrency. In *STOC*, pages 153–158, 1982.

[12] Josee Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004.

[13] M.H. Escardo. A metric model of pcf. In *Workshop on Realizability Semantics and Applications*, 1999.

[14] Francesco Gavazzo. Quantitative behavioural reasoning for higher-order effectful programs: Applicative distances. In *Proc. of LICS 2018*, pages 452–461, 2018.

[15] D. Hofmann, G.J. Seal, and W. Tholen, editors. *Monoidal Topology. A Categorical Approach to Order, Metric, and Topology.* Number 153 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2014.

[16] F.W. Lawvere. Metric spaces, generalized logic, and closed categories. *Rend. Sem. Mat. Fis. Milano*, 43:135–166, 1973.

[17] John C. Mitchell. *Foundations for Programming Languages.* MIT Press, 1996.

[18] Sparsh Mittal. A survey of techniques for approximate computing. *ACM Comput. Surv.*, 48(4), 2016.

[19] J. Morris. *Lambda Calculus Models of Programming Languages*. PhD thesis, MIT, 1969.

[20] Gordon D. Plotkin. Lambda-definability and logical relations. Memorandum SAI-RM-4, University of Edinburgh, 1973.

[21] J. Reed and B.C. Pierce. Distance makes the types grow stronger: a calculus for differential privacy. In *Proc. of ICFP 2010*, pages 157–168, 2010.

[22] K.I. Rosenthal. *Quantales and their applications*. Pitman research notes in mathematics series. Longman Scientific & Technical, 1990.

[23] Dana Scott. Outline of a mathematical theory of computation. Technical Report PRG02, OUCL, November 1970.

[24] Dana Scott and Christopher Strachey. Toward a mathematical semantics for computer languages. Technical Report PRG06, OUCL, August 1971.

[25] F. Van Breugel. An introduction to metric semantics: operational and denotational models for programming and specification languages. *Theor. Comput. Sci.*, 258(1-2):1–98, 2001.

[26] F. Van Breugel and J. Worrell. A behavioural pseudometric for probabilistic transition systems. *Theor. Comput. Sci.*, 331(1):115–142, 2005.

[27] Franck van Breugel and James Worrell. Towards quantitative verification of probabilistic transition systems. In *Proc. of ICALP 2001*, pages 421–432, 2001.

[28] Edwin M. Westbrook and Swarat Chaudhuri. A semantics for approximate program transformations. *CoRR*, abs/1304.5531, 2013. URL: `http://arxiv.org/abs/1304.5531`.

[29] Lili Xu, Konstantinos Chatzikokolakis, and Huimin Lin. Metrics for differential privacy in concurrent systems. In *Proc. of FORTE 2014*, pages 199–215, 2014.