# Relating Distances and Abstractions
## An Abstract Interpretation Perspective

Marco Campion[1][0000−0002−1099−3494], Isabella Mastroeni[2][0000−0003−1213−536X], and Caterina Urban[1][0000−0002−8127−9642]

[1] Inria & ENS | PSL, Paris, France
{marco.campion,caterina.urban}@inria.fr
[2] University of Verona, Department of Computer Science, Verona, Italy
isabella.mastroeni@univr.it

**Abstract.** We establish a formal relation between quantitative and semantic approximations—formalized by pre-metrics and upper closure operators (ucos), respectively—by means of Galois connections. This connection reveals that it is far from trivial for a pre-metric to uniquely identify a uco, highlighting the structural constraints and, more generally, the distinct identity inherent to semantic approximations.
Building on this foundation, we introduce a general composition of semantic and quantitative approximations. This allows us to define a new confidentiality property, called Partial Abstract Non-Interference, that measures bounded variations in program behavior over abstract properties of data. We then relate this property to Partial Completeness in abstract interpretation, revealing a deeper connection between static analysis precision and security guarantees.

**Keywords:** Distances · Abstractions · Abstract Interpretation · Partial Abstract Non-Interference · Partial Completeness

## 1 Introduction

Understanding the behavior of programs is a fundamental challenge in computer science. Due to inherent undecidability, some degree of approximation is unavoidable, both in how we observe program behavior and in how we formalize the properties we aim to analyze. Broadly speaking, we can distinguish between two main paradigms of approximation: semantic and quantitative. *Semantic* approximations capture qualitative properties of data and computations, often abstracting over irrelevant details to retain logical or behavioral correctness. *Quantitative* approximations, on the other hand, measure similarity or closeness between elements using metrics or more relaxed forms of distances.

These two perspectives can be pursued *independently*, or *combined* for a unified approach to approximation. Semantic approximations are at the heart of abstract interpretation [14,16], a foundational framework for soundly approximating program behavior through *abstractions*. They are also intrinsic to properties such as Abstract Non-Interference [24], a relaxation of classic Non-Interference [27] that captures variations in the semantic properties that may

influence program computations. In contrast, quantitative approximations underpin distance-based properties, useful when reasoning about approximations in a meaningful distance space. Notable examples include Approximate Non-Interference [18], which permits some exactly quantified leakage of information, as well as Program Continuity and Robustness [9,11,10], which ensure that arbitrarily small changes to inputs only cause arbitrarily small changes to program outputs, and Differential Privacy [20], which formalizes privacy loss as a bounded statistical difference in output distributions. In some cases, semantic and quantitative perspectives are *combined* to define a more general approximation approach. For instance, Partial Completeness in abstract interpretation [5] leverages pre-metrics compatible with the underlying domain structure to quantify precision loss in program analysis [8]. Similarly, Abstract Robustness [25], characterizes the robustness of deep neural networks against adversarial attacks by combining a distance over inputs with an abstraction of the outputs.

In general, semantic and quantitative approaches offer distinct perspectives on the problem of approximation, each relying on different formal frameworks to capture its nuances. In this work, we aim to explore whether and how these two methodologies relate:

> *Are they fundamentally distinct tools for approximations, or can one be systematically derived from the other?*
>
> *Can we formalize a way to combine their respective advantages into a unifying approximation framework?*

***Our Contribution.*** We explore a formal correspondence between semantic approximations, modeled here as *upper closure operators* (ucos), and quantitative approximations, modeled here as *pre-metrics*. We show how semantic approximations can be derived from distance functions (and vice versa), through a process of abstractions using Galois connections. On the one hand, this connection confirms that ucos can be viewed as particular instances of pre-metrics—specifically, those that assign a distance of zero to elements sharing the same abstraction. On the other hand, however, it is far from trivial for a pre-metric to uniquely identify a uco, highlighting the structural constraints and, more generally, the distinct identity inherent to semantic approximations.

Building on this foundation, we formalize a *composition* operator of pre-metrics that first selects the domain of comparison and then measures distances within this selected domain, thereby enabling a form of layered abstraction. Such a composition, when involving a distance characterizing a semantic abstraction and a distance characterizing a quantitative abstraction, defines a new form of approximation, called *general approximation*, combining semantic and quantitative approaches while keeping the two types of approximations distinct.

This approach allows us to define a new confidentiality property, called *Partial Abstract Non-Interference*, that generalizes both Abstract Non-Interference and Approximate Non-Interference in a unifying view by combining both semantic and quantitative approximations. Partial Abstract Non-Interference allows bounded variations in the abstract program behavior over inputs sharing

a similar abstract property. We then relate this property to Partial Completeness in abstract interpretation, revealing a deeper connection between bounded (im)precision in abstract interpretation and security guarantees.

***Structure of the paper.*** In Sec. 2 we formalize semantic approximations via upper closure operators, and quantitative approximations by pre-metrics, recalling their respective definitions from the literature. Sec. 3 establishes a formal relation between the two forms of approximations. This consists in an abstraction process—formalized by a series of Galois connections—from the domain of pre-metrics to the domain of ucos by passing through equivalence relations. Sec. 4 formally defines a possible way to combine pre-metrics, characterizing quantitative approximations, with distances characterizing semantic abstractions. This will form a general approximation framework which will be used in Sec. 6 to define a new confidentiality property based on the notion of Abstract Non-Interference, called Partial Abstract Non-Interference that quantifies semantic variations in the output domain. This newly defined property is then compared with the Partial Completeness property to establish a relation between them. A background on the Partial Completeness notion in abstract interpretation, and the Abstract Non-Interference property, is provided in Sec. 5.

## 2 Abstractions and Distances

In many domains, approximations are a fundamental tool for simplifying reasoning while retaining essential properties. Broadly speaking, we can distinguish between *semantic* (or *qualitative*) approximations, and *quantitative* approximations. Here we formalize semantic approximations via *upper closure operators* and quantitative approximations by means of *pre-metrics*.

### 2.1 Semantic Approximations via Upper Closure Operators

Qualitative or semantic approximations preserve certain *semantic properties* of the approximated data. Semantic approximations are at the hearth of *abstract interpretation* [14,16], which offers a general methodology for approximating computations by evaluating functions (e.g., program semantics) over an abstract domain $\mathtt{A}$ instead of the concrete domain $\mathtt{C}$. This approach is especially valuable when exact analysis is computationally infeasible or undecidable, trading precision for decidability. In this setting, $\mathtt{A}$ is referred to as an *abstraction* of $\mathtt{C}$ whenever there is a *Galois Connection* (GC), or a *Galois Insertion* (GI), between the two domains. More formally, given a partially ordered set (poset, for short) $\langle \mathtt{C}, \leq_{\mathtt{C}} \rangle$, called the concrete domain, and a poset $\langle \mathtt{A}, \leq_{\mathtt{A}} \rangle$, called the abstract domain, a GC is denoted by $\langle \mathtt{C}, \leq_{\mathtt{C}} \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathtt{A}, \leq_{\mathtt{A}} \rangle$ where $\alpha \colon \mathtt{C} \to \mathtt{A}$ is the (monotone) abstraction function, sometimes referred to as the lower adjoint, and $\gamma \colon \mathtt{A} \to \mathtt{C}$ is the (monotone) concretization function, also referred to as the upper adjoint, both satisfying the following condition $\forall a \in \mathtt{A}$ and $\forall c \in \mathtt{C}$:

$$\alpha(c) \leq_{\mathtt{A}} a \Leftrightarrow c \leq_{\mathtt{C}} \gamma(a)$$

A GC is a GI, denoted by $\langle \mathtt{C}, \leq_{\mathtt{c}} \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathtt{A}, \leq_{\mathtt{A}} \rangle$, when $\alpha \circ \gamma = \iota$, namely when their composition is the identity function ($\iota \stackrel{\text{def}}{=} \lambda x.\, x$). An essential property of a GC is that an upper/lower adjoint of a GC uniquely determines the other: $\alpha(c)$ is the least element $a$ with $c \leq_{\mathtt{c}} \gamma(a)$, and $\gamma(a)$ is the largest element $c$ with $\alpha(c) \leq_{\mathtt{A}} a$. In particular, when both $\langle \mathtt{C}, \leq_{\mathtt{c}} \rangle$ and $\langle \mathtt{A}, \leq_{\mathtt{A}} \rangle$ are complete lattices, respectively $\langle \mathtt{C}, \leq_{\mathtt{c}}, \vee_{\mathtt{c}}, \wedge_{\mathtt{c}}, \top_{\mathtt{c}}, \bot_{\mathtt{c}} \rangle$ and $\langle \mathtt{A}, \leq_{\mathtt{A}}, \vee_{\mathtt{A}}, \wedge_{\mathtt{A}}, \top_{\mathtt{A}}, \bot_{\mathtt{A}} \rangle$, then $\alpha(c) = \wedge_{\mathtt{A}}\{a \in \mathtt{A} \mid c \leq_{\mathtt{c}} \gamma(a)\}$ and $\gamma(a) = \vee_{\mathtt{c}}\{c \in \mathtt{C} \mid \alpha(c) \leq_{\mathtt{A}} a\}$. It turns out that $\alpha$ is a complete join-morphism (sometimes also referred to as an additive function), namely for all $S \subseteq \mathtt{C}$ : $\alpha(\vee_{\mathtt{c}} S) = \vee_{\mathtt{A}}\{\alpha(c) \mid c \in S\}$, dually $\gamma$ is a complete meet-morphism (co-additive function), namely for all $S \in \mathtt{A}$ : $\gamma(\wedge_{\mathtt{A}} S) = \wedge_{\mathtt{A}}\{\gamma(a) \mid a \in S\}$.

Galois connections/insertions can be equivalently formulated in terms of upper closure operators [16] (ucos or closures, for short).

**Definition 1 (Upper Closure Operator).** *An* upper closure operator *on a poset $\langle \mathtt{C}, \leq_{\mathtt{c}} \rangle$ is a function $\rho \colon \mathtt{C} \to \mathtt{C}$ with the following properties $\forall c, c' \in \mathtt{C}$:*

*(i)* $c \leq_{\mathtt{c}} c' \Rightarrow \rho(c) \leq_{\mathtt{c}} \rho(c')$; *(monotonicity)*

*(ii)* $c \leq_{\mathtt{c}} \rho(c)$; *(extensivity)*

*(iii)* $\rho(\rho(c)) = \rho(c)$. *(idempotence)*

Ucos are uniquely determined by the set of their fixpoints: $\rho(C) = \{c \in \mathtt{C} \mid \rho(c) = c\}$. For instance, the composition $\gamma \circ \alpha$ is a uco of $\mathtt{C}$. In the following, the set of all upper closure operators on a poset $\mathtt{C}$ is denoted by $\mathit{Uco}(\mathtt{C})$.

*Example 1 (Sign and Parity Abstractions).* The closure $\mathsf{Sign} \in \mathit{Uco}(\wp(\mathbb{Z}))$ abstracts a set of integers by discarding all information except the sign of its values. It corresponds to the identity function when applied to the empty set or in case the set contains the value zero only. The closure is defined by the set of fixpoints:

$$\mathsf{Sign}(\wp(\mathbb{Z})) \stackrel{\text{def}}{=} \{\varnothing, \{0\}, \{z \in \mathbb{Z} \mid z \leq 0\}, \{z \in \mathbb{Z} \mid z \geq 0\}, \mathbb{Z}\}$$

Similarly, we can define the parity abstraction closure $\mathsf{Par} \in \mathit{Uco}(\wp(\mathbb{Z}))$ as:

$$\mathsf{Par} \stackrel{\text{def}}{=} \{\varnothing, \mathit{Even} \stackrel{\text{def}}{=} \{n \in \mathbb{Z} \mid n \bmod 2 = 0\}, \mathit{Odd} \stackrel{\text{def}}{=} \{n \in \mathbb{Z} \mid n \bmod 2 = 1\}, \mathbb{Z}\} \quad \triangleleft$$

Whenever $\mathtt{C}$ is a complete lattice, then also $\mathit{Uco}(\mathtt{C})$, ordered point-wise, is a complete lattice denoted by $\langle \mathit{Uco}(\mathtt{C}), \sqsubseteq, \sqcup, \sqcap, \lambda x.x, \lambda x.\top \rangle$. Here, for every $\rho, \eta \in \mathit{Uco}(\mathtt{C})$, $\{\rho_i\}_{i \in I} \subseteq \mathit{Uco}(\mathtt{C})$ where $I$ is an index set of ucos, and $x \in \mathtt{C}$: $\rho \sqsubseteq \eta$ iff $\forall c \in \mathtt{C}\,.\, \rho(c) \leq_{\mathtt{c}} \eta(c)$ iff $\eta(\mathtt{C}) \subseteq \rho(\mathtt{C})$; $(\sqcap_{i \in I} \rho_i)(c) = \wedge_{i \in I} \rho_i(c)$; and $(\sqcup_{i \in I} \rho_i)(c) = c \Leftrightarrow \forall i \in I\,.\, \rho_i(c) = c$. Then, $\mathit{Uco}(\mathtt{C})$ is the so-called *lattice of abstractions* of $\mathtt{C}$ [16], i.e., the complete lattice of all possible abstractions (up to isomorphic representation of their objects) of the concrete domain $\mathtt{C}$.

Henceforth, we formally model semantic approximation through ucos:

**Definition 2 (Semantic Approximation).** *Given a poset $\langle \mathtt{C}, \leq_{\mathtt{c}} \rangle$ and the abstraction $\rho \in \mathit{Uco}(\mathtt{C})$, an element $x \in \mathtt{C}$ is* semantically approximated *by $\rho(x)$, and the set $\{y \in \mathtt{C} \mid \rho(y) = \rho(x)\}$ represents all elements in $\mathtt{C}$ sharing the same semantic approximation as $x$.*

| | **pre-** | **quasisemi-** | **semi-** | **quasi-** | **pseudo-** | **metric** |
|---|---|---|---|---|---|---|
| (*non-negativity*) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| (*if-identity*) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| (*iff-identity*) | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| (*symmetry*) | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ |
| (*triangle-inequality*) | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |

Fig. 1: Metrics and their relaxed forms.

*Example 2.* Let $\mathsf{Int}\colon \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$ map a set of integers $S \in \wp(\mathbb{Z})$ to the smallest interval $[l, u] \stackrel{\text{def}}{=} \{i \in \mathbb{Z} \mid l \leq i \leq u\}$ that contains it, namely such that $S \subseteq [l, u]$, where $l \in \mathbb{Z} \cup \{-\infty\}$, $u \in \mathbb{Z} \cup \{+\infty\}$ and $l \leq u$. This is the well known interval abstraction $\mathsf{Int} \in \mathit{Uco}(\wp(\mathbb{Z}))$ [13]. So, for instance, the set of integers $\{0, 1, 4\}$ can be semantically approximated by the interval $[0, 4]$ through $\mathsf{Int}$. Moreover, the set {{0,4}, {0,1,4}, {0,2,4}, {0,3,4}, {0,1,2,4}, {0,1,3,4}, {0,1,2,3,4}} contains all sets of integers $S$ such that $\mathsf{Int}(S) = [0, 4]$. ◁

### 2.2 Quantitative Approximations via Pre-Metrics

Quantitative approximations preserve *closeness* of the approximated data, typically measured through a distance function in a suitable topological space. Here, we model distance functions using (pre-)metrics.

Let $\mathbb{R}^\infty$ be the set of real numbers extended with the infinite symbol $\infty$, such that for all $r \in \mathbb{R}$, $r < \infty$. Let $\mathbb{R}_{\geq n}$ be the restriction of $\mathbb{R}$ to values greater or equal than $n \in \mathbb{N}$. For instance, $\mathbb{R}^\infty_{\geq 0} \stackrel{\text{def}}{=} \{r \in \mathbb{R} \mid r \geq 0\} \cup \{\infty\}$.

**Definition 3 (Metric).** *Given a non-empty set $L$, a* metric *is a binary function $\delta : L \times L \to \mathbb{R}^\infty$ with the following properties $\forall x, y, z \in L$:*

(1) $\delta(x, y) \geq 0$; *(non-negativity)*

(2) $x = y \;\Leftrightarrow\; \delta(x, y) = 0$; *(iff-identity)*

(3) $\delta(x, y) = \delta(y, x)$; *(symmetry)*

(4) $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$. *(triangle-inequality)*

*The pair $\langle L, \delta \rangle$ is called a metric space.*

A classic metric example is the Euclidean distance measuring the distance between two real values as the absolute value of their difference.

Due to their axioms, metrics are among the strongest types of distances. However, depending on what we want to measure and on which domain, a distance function may not satisfy all axioms of a metric, but only, e.g., (*non-negativity*) and (*if-identity*), thereby being a pre-metric instead (cf. Fig. 1). As we will see in Sec. 6, understanding the type of distance function we are manipulating is essential for proving some implications between properties of programs (such as between Partial Completeness and Partial Abstract Non-Interference in Sec. 6).

In particular, a metric that does not satisfy symmetry is called a *quasi-metric*, while a metric that does not satisfy the $\Leftarrow$ implication of (*iff-identity*) is called a *pseudo-metric*. Semi-metrics satisfy all the axioms except for the triangle inequality. The function $\delta$ is called a *pre-metric* [17,8] if it only satisfies (*non-negativity*) and the $\Rightarrow$ implication of the (*iff-identity*), i.e., the (*if-identity*) axiom. All the other metric axioms are not required, making the definition of pre-metric one of the weakest possible distance function. By composing the words pseudo-, quasi- and semi- we obtain different distance flavors by simply keeping the axioms that are satisfied by all the combined words. For instance, a quasisemi-metric is a pre-metric that additionally satisfies the (*iff-identity*). Fig. 1 summarizes the above distance notions and their properties. We will occasionally use the subscript $\delta_{\mathrm{L}}$ in cases where the set $L$ may not be immediately clear from the context. From this point forward, whenever we say that a function $\delta$ is a distance, we assume that it satisfies, at least, the axioms of a pre-metric.

*Example 3 (Size Distance).* Consider the powerset $\wp(L)$ of a set $L$. We write $\mathit{Count}(S)$ for the number of elements in the set $S \in \wp(L)$. We define the distance $\delta_{\mathit{siz}} \colon \wp(L) \times \wp(L) \to \mathbb{R}^{\infty}$ between two sets $S_1, S_2 \in \wp(L)$ as the absolute value of the difference in their size, i.e., $\delta_{\mathit{siz}}(S_1, S_2) \stackrel{\text{def}}{=} |\mathit{Count}(S_2) - \mathit{Count}(S_1)|$. Note that $\delta_{\mathit{siz}}$ is not a metric, but a pseudo-metric since it does not satisfy the (*iff-identity*) axiom: two sets may have the same size yet being different.

In program analysis, $\delta_{\mathit{siz}}$ could be used to count, for instance, the number of spurious elements added by an abstract sound computation with respect to the abstraction of a concrete computation. For instance, if $[0, 0]$ is the (interval abstraction of the) strongest numerical invariant of a program variable $x$ at certain program point, while $[0, 10]$ is the abstract invariant generated by an abstract interpretation over $\mathsf{Int}$, then $\delta^{\mathsf{Int}}_{\mathit{siz}}([0, 0], [0, 10]) = 10$ indicates that the abstract interpretation added 10 spurious values with respect to the (interval abstraction of the) concrete execution. A similar example can be considered when counting the false positives generated by a static analysis while checking an abstract specification (e.g, whether $x \in [0, 0]$). ◁

*Example 4 (Volume Distance).* Let us consider the ordered domain of convex octagons $(\mathsf{Oct}, \leq_{\mathsf{Oct}})$ [39]. We define the distance

$$\delta_{\mathit{Vol}}(o_1, o_2) \stackrel{\text{def}}{=} \mathit{Av}(\mathit{Vol}(o_1) - \mathit{Vol}(o_2))$$

calculating the absolute value of the difference between the volume of two convex octagons $o_1, o_2 \in \mathsf{Oct}$. The volume function $\mathit{Vol} \colon \mathsf{Oct} \to \mathbb{R}^{\infty}_{\geq 0}$ could be a monotone (namely, if $\gamma(o_1) \subseteq \gamma(o_2)$ then $\mathit{Vol}(o_1) \leq \mathit{Vol}(o_2)$) overapproximation of the exact volume computation. $\delta_{\mathit{Vol}}$ satisfies all the axioms of a metric except for (*iff-identity*) since two octagons may have they same volume yet not representing the same octagon. Thus, $\delta_{\mathit{Vol}}$ qualifies as a pseudo-metric. In program analysis, $\delta_{\mathit{Vol}}$ could be used to quantify the difference between the (numerical) invariants of program variables generated by the abstraction of a concrete computation with respect to an abstract computation. ◁

For additional examples of pre-metrics and their applications in domains used within the context of program analysis, we refer to [8].

We formally define quantitative approximations via pre-metrics as follows:

**Definition 4 (Quantitative Approximation).** *Given a pre-metric space* $\langle \mathtt{C}, \delta \rangle$ *and a fixed constant* $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$*, an element* $x \in \mathtt{C}$ *is* quantitatively approximated *by any element in the set* $\{y \in \mathtt{C} \mid \delta(x, y) \leq \varepsilon\}$.

*Example 5.* Continuing Ex. 2, we may approximate sets of integer numbers by the size distance $\delta_{siz}$ defined in Ex. 3. For instance, $\{0, 1, 4\}$ can be quantitatively approximated by any set of integers whose maximum distance from it is at most $\varepsilon = 1$. Examples of such approximations include sets $\{0, 1\}$ and $\{5, 6, 8, 10\}$. ◁

Here, the admitted noise concerns elements that are topologically close to the original one but that may share no semantic property.

## 3 From Pre-Metrics to Upper Closure Operators

Semantic and quantitative approaches offer distinct perspectives on the problem of approximation, relying on different formal frameworks to capture its nuances. This naturally raises the question: are these two perspectives entirely orthogonal, or is there a deeper *relation* between them? Understanding this connection is the main goal of this section. Specifically, in the following, we establish a formal relation between quantitative and semantic approximations—formalized by pre-metrics and ucos, respectively—by means of Galois connections.

Let us start by assuming to work with a complete lattice $\langle \mathtt{C}, \leq_{\mathtt{c}}, \vee_{\mathtt{c}}, \wedge_{\mathtt{c}}, \top_{\mathtt{c}}, \bot_{\mathtt{c}} \rangle$. Pre-metrics provide a quantitative measure of the difference between elements in $\mathtt{C}$. Such distances cannot be derived from the order structure alone, they must be explicitly defined. As a result, the only viable approach to relate pre-metrics and ucos is to derive the latter as abstractions of the former. The abstraction process moves from pre-metrics to ucos by passing through *equivalence relations*:

$$\text{Pre-Metrics} \longrightarrow \text{Equivalence Relations} \longrightarrow \text{Uco}$$

More in detail, we first identify a subset of pre-metrics (called 0-*pseudo-metrics*) on which we can obtain equivalence relations as an abstraction. The underlying intuition is that we can represent a semantic approximation $\rho \in \mathit{Uco}(\mathtt{C})$ by means of a pre-metric $\delta$ that assigns distance 0 to elements $x, y \in \mathtt{C}$ with the same abstraction $\rho(x) = \rho(y)$, and assigns distance $\infty$ otherwise. Elements assigned with a distance of zero are the equivalence classes of the equivalence relation induced by the 0-pseudo-metrics. On the other hand, ucos satisfy structural properties—monotonicity, extensivity, idempotence—that are not automatically satisfied by pre-metrics, 0-pseudo-metrics, or equivalence relations. These properties have to be enforced through suitable constraints imposed by the abstractions. We derive ucos in two further steps: forcing *extensivity* first, and *monotonicity* and *idempotence* afterward, leveraging [15].

### 3.1 The Domain $\mathtt{M}(\mathtt{C})$ of Pre-Metrics

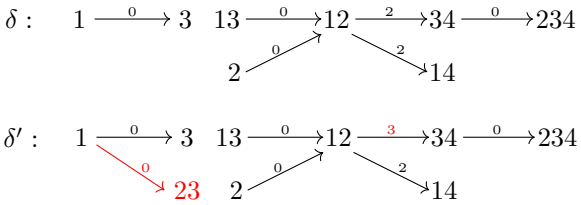
The first step in formalizing the abstraction process from pre-metrics to ucos is to define the underlying domain on which the construction operates. In the following, we introduce the domain of pre-metrics. In the next subsections, we progressively derive the domain of ucos as an abstraction.

Let $\mathtt{M}(\mathtt{C})$ be the set of all pre-metrics $\delta : \mathtt{C} \times \mathtt{C} \longrightarrow \mathbb{R}^\infty$ defined on $\mathtt{C}$, i.e, $\mathtt{M}(\mathtt{C}) \stackrel{\text{def}}{=} \{\delta \mid \delta \text{ is a pre-metric on } \mathtt{C}\}$. We equip $\mathtt{M}(\mathtt{C})$ with a partial order $\sqsubseteq_{\mathtt{m}}$ that compares pre-metrics based on the cardinality of sets of pairs of elements with a distance of zero. Formally, for $\delta_1, \delta_2 \in \mathtt{M}(\mathtt{C})$, we define:

$$\delta_1 \sqsubseteq_{\mathtt{m}} \delta_2 \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \forall x, y \in \mathtt{C} \,.\, \delta_2(x,y) = 0 \vee (\delta_1(x,y) \neq 0 \wedge \delta_1(x,y) \leq \delta_2(x,y))$$

Intuitively, moving upward in the ordering corresponds to enlarging the sets of pairs of elements that are assigned a distance of zero: pairs of elements that are distinguished (assigned a non-zero distance) by a more concrete pre-metric $\delta_1$ may become indistinguishable (assigned a zero distance) by a more abstract pre-metric $\delta_2$. The distance between elements that remain distinguishable in $\delta_2$ may stretch, possibly to $\infty$, reflecting the underlying intuition mentioned above.

*Example 6.* Suppose $\mathtt{C} = \wp(\{1,2,3,4\})$[3]. Let $\delta$ and $\delta'$ be pre-metrics on $\mathtt{C}$ such that $\delta(1,3) = \delta(13,12) = \delta(2,12) = \delta(34,234) = 0$, $\delta(12,14) = 2$, $\delta(12,34) = 2$ while all the other elements are at distance $\infty$, and $\delta' = \delta$ except for $\delta'(1,23) = 0$ ($\delta(1,23) = \infty$) and $\delta'(12,34) = 3 > 2 = \delta(12,34)$, graphically:




(The distances not depicted above are $\infty$. The differences are colored in red.) We clearly have $\delta \sqsubseteq_{\mathtt{m}} \delta'$. ◁

Let $N \subseteq \mathbb{N}$ and $x, y \in \mathtt{C}$. We define the join and meet operators, $\bigsqcup_{\mathtt{m}}$ and $\bigsqcap_{\mathtt{m}}$, over sets of pre-metrics $\{\delta_i(x,y) \in \mathtt{M}(\mathtt{C}) \mid i \in N\}$ as follows:

$$\bigsqcup\nolimits_{\mathtt{m}} \{\delta_i\}_{i \in N} \stackrel{\text{def}}{=} \lambda(x,y). \begin{cases} \max\{\delta_i(x,y) \mid i \in N\} & \forall i \in N \colon \delta_i(x,y) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\bigsqcap\nolimits_{\mathtt{m}} \{\delta_i\}_{i \in N} \stackrel{\text{def}}{=} \lambda(x,y). \begin{cases} m & m = \min\{\delta_i(x,y) \mid i \in N\} \neq \bot \\ \text{undefined} & \text{otherwise} \end{cases}$$

[3] For the sake of readability, in the following, we represent sets of numbers by the sequences of their elements without separators, e.g., $\{1,2\}$ is represented by 12.

where the max and min operators:

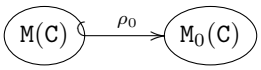
$$\max\{\delta_i(x,y) \mid i \in N\} \stackrel{\text{def}}{=} \begin{cases} d & \exists m \in N\colon \forall i \in N\colon \infty \neq d = \delta_m(x,y) \geq \delta_i(x,y) \\ \infty & \text{otherwise} \end{cases}$$

$$\min\{\delta_i(x,y) \mid i \in N\} \stackrel{\text{def}}{=} \begin{cases} 0 & \forall i \in N\colon \delta_i(x,y) = 0 \\ d & \exists m \in N\colon \forall i \in N\colon 0 < d = \delta_m(x,y) \leq \delta_i(x,y)) \\ \bot & \text{otherwise} \end{cases}$$

find the distances within the given set of pre-metrics that are largest (but different from $\infty$) and smallest (possibly equal to $\infty$), respectively. It is clear that the bottom element of $\mathtt{M}(\mathtt{C})$ does not exist in general. It is $\delta_\bot$ such that $\forall x, y \in \mathtt{C}\colon \delta_\bot(x,y) \stackrel{\text{def}}{=} 1$, if pre-metrics are restricted to assign discrete distances over natural numbers. The top element of $\mathtt{M}(\mathtt{C})$ is $\delta_\top$ such that $\forall x, y \in \mathtt{C}\colon \delta_\top(x,y) \stackrel{\text{def}}{=} 0$.

**Proposition 1.** *$\langle \mathtt{M}(\mathtt{C}), \sqsubseteq_{\mathtt{m}}, \sqcup_{\mathtt{m}}, \sqcap_{\mathtt{m}}, \delta_\top \rangle$ is a join-complete semi-lattice.*

### 3.2 The Domain $\mathtt{M_0}(\mathtt{C})$ of 0-Pseudo-Metrics




We observe that not all pre-metrics in $\mathtt{M}(\mathtt{C})$ are meaningful representations of semantic approximations. For instance, the pre-metric in Ex. 6 is not a meaningful semantic approximation because it is neither symmetric nor transitive between elements at distance zero, e.g., $\delta$ identifies a semantic equivalence between 1 and 3 ($\delta(1,3) = 0$) but not between 3 and 1 ($\delta(3,1) = \infty$).

*The domain* $\mathtt{M_0}(\mathtt{C})$. We define a restriction of pre-metrics—called 0-pseudo-metrics—satisfying symmetry and transitivity between elements that are assigned a distance of zero.

**Definition 5 (0-Pseudo-Metrics).** *A* 0-pseudo-metric $\delta\colon \mathtt{C} \times \mathtt{C} \to \mathbb{R}^\infty$ *is a pre-metric that additionally satisfies the following conditions, for all* $x, y, z \in \mathtt{C}$*:*

1. $\delta(x,y) = 0 \;\Rightarrow\; \delta(y,x) = 0$; *(0-distance symmetry)*
2. $(\delta(x,y) = 0 \;\wedge\; \delta(y,z) = 0) \;\Rightarrow\; \delta(x,z) = 0$ *(0-distance transitivity)*

Let $\mathtt{M_0}(\mathtt{C})$ be the set of all 0-pseudo-metrics defined on $\mathtt{C}$. It is clear that, by definition, $\mathtt{M_0}(\mathtt{C}) \subset \mathtt{M}(\mathtt{C})$, hence $\langle \mathtt{M_0}(\mathtt{C}), \sqsubseteq_{\mathtt{m}} \rangle$, i.e., the domain of 0-pseudo-metrics, is still a poset preserving the same characteristics as $\mathtt{M}(\mathtt{C})$.

**Proposition 2.** *$\langle \mathtt{M_0}(\mathtt{C}), \sqsubseteq_{\mathtt{m}}, \sqcup_{\mathtt{m}}, \sqcap_{\mathtt{m}}, \delta_\top \rangle$ is a join-complete semi-lattice.*

*Abstracting pre-metrics into* 0*-pseudo-metrics.* We show here that 0-pseudo metrics can be obtained from pre-metrics by forcing both symmetry and transitivity between elements assigned with a distance of zero.

Let $\mathbb{S}\colon \mathtt{M}(\mathtt{C}) \to \mathtt{M}(\mathtt{C})$ be the operator forcing symmetry only between the elements with distance zero:

$$\mathbb{S}(\delta) \stackrel{\text{def}}{=} \lambda(x,y).\ \begin{cases} 0 & \delta(y,x) = 0 \\ \delta(x,y) & \text{otherwise} \end{cases}$$

Clearly, if a pre-metric $\delta$ is already symmetric, then $\mathbb{S}(\delta) = \delta$.

Similarly, we define the operator $\mathbb{T}\colon \mathtt{M}(\mathtt{C}) \to \mathtt{M}(\mathtt{C})$ forcing transitivity, again only between elements with distance zero:

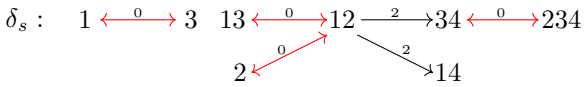
$$\mathbb{T}(\delta) \stackrel{\text{def}}{=} \mathit{lfp}^{\sqsubseteq_{\mathbb{m}}}_{\delta}\, \mathbb{t}$$
$$\mathbb{t}(\delta) \stackrel{\text{def}}{=} \lambda(x,y).\ \begin{cases} 0 & \exists z \in \mathtt{C}\colon \delta(x,z) = 0 \wedge \delta(z,y) = 0 \\ \delta(x,y) & \text{otherwise} \end{cases}$$

Note that, if a pre-metric $\delta$ satisfies the triangle inequality, then $\mathbb{T}(\delta) = \delta$.

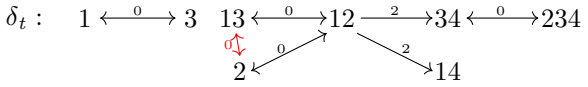
Let $\rho_0 \stackrel{\text{def}}{=} \mathbb{T} \circ \mathbb{S}$. By construction, given a pre-metric $\delta \in \mathtt{M}(\mathtt{C})$, we have that $\rho_0(\delta) \in \mathtt{M}_0(\mathtt{C})$ is a 0-pseudo-metric. More generally, $\rho_0$ is a uco on $\mathtt{M}(\mathtt{C})$ and $\mathtt{M}_0(\mathtt{C})$ is the set of its fixpoints $\rho_0(\mathtt{M}(\mathtt{C}))$.

**Theorem 1.** *$\rho_0 \in \mathit{Uco}(\mathtt{M}(\mathtt{C}))$ and $\mathtt{M}_0(\mathtt{C}) = \rho_0(\mathtt{M}(\mathtt{C}))$.*

*Example 7.* Suppose $\mathtt{C} = \wp(\{1,2,3,4\})$ and consider $\delta$ of Ex. 6. Let $\delta_s \stackrel{\text{def}}{=} \mathbb{S}(\delta)$, such that $\delta_s = \delta$ except for $\delta_s(3,1) = \delta_s(12,13) = \delta_s(12,2) = \delta_s(234,34) = 0$.

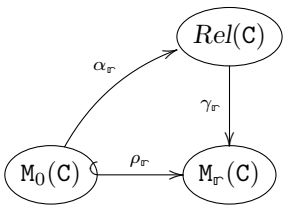



Note that $\delta_s$ is not transitive, e.g., $\delta_s(2,12) = 0 = \delta_s(12,13)$, but $\delta_s(2,13) = \delta(2,13) = \infty$. Let us consider now $\delta_t = \mathbb{T}(\delta_s)$ (which preserves symmetry).




After one iteration of $\mathbb{t}$ we reach the fix-point and $\delta_t(2,13) = \delta_t(13,2) = 0$. Note that the triangle inequality does not hold among elements with a distance greater than zero, e.g., $\delta_t(2,14) = \infty$ while $\delta_t(2,12) = 0$ and $\delta_t(12,14) = 2$. ◁

### 3.3 From $\mathtt{M}_0(\mathtt{C})$ to Equivalence Relations: The Domain $\mathtt{M}_{\mathbb{r}}(\mathtt{C})$



At this point we can observe that 0-pseudo-metrics naturally induce an equivalence relation between elements with a distance of zero. In this section, we thus abstract 0-pseudo-metrics into the equivalence relations induced by them.

Let $\mathit{Rel}(\mathtt{C})$ be the set of equivalence relations on $\mathtt{C}$. In the following, given an element $x \in \mathtt{C}$ and an equivalence relation $\mathtt{R} \in \mathit{Rel}(\mathtt{C})$, $[x]_{\mathtt{R}}$ denotes the equivalence class of $x$ induced by $\mathtt{R}$, i.e., $[x]_{\mathtt{R}} \stackrel{\text{def}}{=} \{y \in \mathtt{C} \mid y\,\mathtt{R}\,x\}$. We define a partial order $\preccurlyeq$ on $\mathit{Rel}(\mathtt{C})$ such that, for any $\mathtt{R}, \mathtt{S} \in \mathit{Rel}(\mathtt{C})$, $\mathtt{R} \preccurlyeq \mathtt{S}$ if and only if $\forall x \in \mathtt{C}\colon [x]_{\mathtt{R}} \subseteq [x]_{\mathtt{S}}$. We have the following Galois insertion

$$\langle \mathtt{M}_0(\mathtt{C}), \sqsubseteq_{\mathtt{m}} \rangle \underset{\alpha_{\mathtt{r}}}{\overset{\gamma_{\mathtt{r}}}{\leftrightarrows}} \langle \mathit{Rel}(\mathtt{C}), \preccurlyeq \rangle$$

where the abstraction function $\alpha_{\mathtt{r}}\colon \mathtt{M}_0(\mathtt{C}) \to \mathit{Rel}(\mathtt{C})$ is

$$\alpha_{\mathtt{r}}(\delta) \stackrel{\text{def}}{=} \{(x, y) \in \mathtt{C} \times \mathtt{C} \mid \delta(x, y) = 0\}$$

and the concretization function $\gamma_{\mathtt{r}} : \mathit{Rel}(\mathtt{C}) \to \mathtt{M}_0(\mathtt{C})$ is

$$\gamma_{\mathtt{r}}(\mathtt{R}) \stackrel{\text{def}}{=} \lambda(x, y).\ \begin{cases} 0 & x\,\mathtt{R}\,y \\ \infty & \text{otherwise} \end{cases}$$

Thus, the domain $\langle \mathit{Rel}(\mathtt{C}), \preccurlyeq \rangle$ is an abstraction of $\langle \mathtt{M}_0(\mathtt{C}), \sqsubseteq_{\mathtt{m}} \rangle$. Let $\rho_{\mathtt{r}} \stackrel{\text{def}}{=} \gamma_{\mathtt{r}} \circ \alpha_{\mathtt{r}}$, we have that $\rho_{\mathtt{r}}$ is a uco on $\mathtt{M}_0(\mathtt{C})$.

**Theorem 2.** *$\rho_{\mathtt{r}} \in \mathit{Uco}(\mathtt{M}_0(\mathtt{C}))$.*

Note that $\rho_{\mathtt{r}}$ is not an isomorphism since a 0-pseudo-metric $\delta$ may also assign non-zero distances between elements. However, through the abstraction, these distances are stretched to $\infty$ in $\rho_{\mathtt{r}}(\delta)$. More generally, $\rho_{\mathtt{r}}$ abstracts 0-pseudo-metrics into pseudo-metrics, ignoring all non-zero distances between elements.

Let $\mathtt{M}_{\mathtt{r}}(\mathtt{C}) \stackrel{\text{def}}{=} \rho_{\mathtt{r}}(\mathtt{M}_0(\mathtt{C})) = \rho_{\mathtt{r}} \circ \rho_0(\mathtt{M}(\mathtt{C}))$ and let $\delta_\infty \in \mathtt{M}_{\mathtt{r}}(\mathtt{C})$ be defined as:

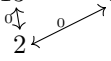
$$\delta_\infty \stackrel{\text{def}}{=} \lambda(x, y).\ \begin{cases} 0 & x = y \\ \infty & \text{otherwise} \end{cases}$$

**Proposition 3.** *$\langle \mathtt{M}_{\mathtt{r}}(\mathtt{C}), \sqsubseteq_{\mathtt{m}}, \sqcup_{\mathtt{m}}, \sqcap_{\mathtt{m}}, \delta_\top, \delta_\infty \rangle$ is a complete lattice.*

Note that $\delta_\top = \gamma_{\mathtt{r}}(\top)$, where $\top \in \mathit{Rel}(\mathtt{C})$ is such that $\forall x, y \in \mathtt{C}\colon x \top y$, and $\delta_\infty = \gamma_{\mathtt{r}}(\mathtt{id})$, where $\mathtt{id} \in \mathit{Rel}(\mathtt{C})$ is such that $x\,\mathtt{id}\,y \stackrel{\text{def}}{\Leftrightarrow} x = y$. Thus, $\mathtt{M}_{\mathtt{r}}(\mathtt{C}) \subset \mathtt{M}_0(\mathtt{C}) \subset \mathtt{M}(\mathtt{C})$ is the complete sub-lattice of $\mathtt{M}(\mathtt{C})$ *uniquely identifying equivalence relations.*

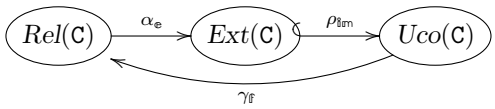
*Example 8.* Let us consider $\delta_t$ of Ex. 7. Its abstraction $\delta_r \stackrel{\text{def}}{=} \rho_{\mathtt{r}}(\delta_t)$ is such that $\delta_r = \delta_t$ except for $\delta_r(12, 14) = \delta_r(12, 34) = \infty$.

$\delta_r :$ $1 \overset{0}{\longleftrightarrow} 3$ $\quad 13 \overset{0}{\longleftrightarrow} 12$ $\quad 34 \overset{0}{\longleftrightarrow} 234$ $\quad \equiv$ $\boxed{1\ \ 3}$ $\boxed{2\ \ 12\ \ 13}$ $\boxed{34\ \ 234}$




In the depiction above on the right, we show an equivalent representation of $\delta_r$ where different elements inside the same box are assigned with a distance of zero, while all other distances between elements in different boxes or between the other, not depicted, elements of $\mathtt{C}$ are $\infty$. ◁

### 3.4 From Equivalence Relations to Upper Closure Operators




The next step in the abstraction process is to move from equivalence relations towards (extensive) functions and afterward to upper closure operators.

Let $\mathit{Fun}(\mathtt{C})$ be the set of total functions on $\mathtt{C}$ ordered point-wise, i.e., $f \mathrel{\dot{\leq}_\mathtt{c}} g \stackrel{\text{def}}{\Leftrightarrow} \forall x \in \mathtt{C} \,.\, f(x) \leq_\mathtt{c} g(x)$.

**Proposition 4.** *$\langle \mathit{Fun}(\mathtt{C}), \mathrel{\dot{\leq}_\mathtt{c}}, \dot{\vee}_\mathtt{c}, \dot{\wedge}_\mathtt{c}, \lambda x.\top_\mathtt{c}, \lambda x.\bot_\mathtt{c} \rangle$ is a complete lattice.*

Given an equivalence relation $\mathtt{R} \in \mathit{Rel}(\mathtt{C})$ we can construct a total function $f\colon \mathtt{C} \to \mathtt{C}$ that maps each element in $\mathtt{C}$ to a representative element of its equivalence class under $\mathtt{R}$. Various choices are possible for this representative element, but since our ultimate goal is to characterize ucos, which in particular are extensive functions, we define $f$ such that each equivalence class is mapped to its least upper bound, thus ensuring that $f$ is extensive.

Formally, let $\mathit{Ext}(\mathtt{C}) \stackrel{\text{def}}{=} \{f : \mathtt{C} \to \mathtt{C} \mid \forall x \in \mathtt{C} \,.\, x \leq_\mathtt{c} f(x)\} \subset \mathit{Fun}(\mathtt{C})$ be the set of all extensive functions on $\mathtt{C}$. Clearly $\mathit{Ext}(\mathtt{C})$ forms a complete sub-lattice of $\mathit{Fun}(\mathtt{C})$. Note that $\lambda x.\bot_\mathtt{c}$ is the smallest function with respect to the point-wise order in $\mathit{Fun}(\mathtt{C})$ but, not being extensive, it cannot be the smallest function in $\mathit{Ext}(\mathtt{C})$, where the bottom element is the identity function $\iota$.

**Proposition 5.** *$\langle \mathit{Ext}(\mathtt{C}), \mathrel{\dot{\leq}_\mathtt{c}}, \dot{\vee}_\mathtt{c}, \dot{\wedge}_\mathtt{c}, \lambda x.\top_\mathtt{c}, \iota \rangle$ is a complete lattice.*

We define the following function $\alpha_{\mathtt{e}}\colon \mathit{Rel}(\mathtt{C}) \to \mathit{Ext}(\mathtt{C})$ as

$$\alpha_{\mathtt{e}}(\mathtt{R}) \stackrel{\text{def}}{=} \lambda x \in \mathtt{C}.\ \bigvee([x]_\mathtt{R})$$

Note that $\alpha_{\mathtt{e}}$ is not surjective since an extensive function could lead the elements to be greater than the least upper bound.

*Example 9.* Suppose $\mathtt{C} = \wp(\{1,2,3,4\})$ and consider $\delta_r$ of Ex. 8. Let $\mathtt{R}$ the corresponding equivalence relation depicted in Ex. 8. Its abstraction $f \stackrel{\text{def}}{=} \alpha_{\mathtt{e}}(\mathtt{R})$ is the identity function except for $f(1) = f(3) = 13$, $f(2) = f(12) = f(13) = 123 = f(123)$, $f(34) = f(234) = 234$. Hence, $f$ collapses the image of 123 with the one of 2, 12, and 13, since, for instance, $f(12) = \bigvee([12]_\mathtt{R}) = \bigvee\{2, 12, 13\} = 123$. ◁

From the domain of extensive function $\mathit{Ext}(\mathtt{C})$, we can use the construction in [15] to further enforce monotonicity and idempotence thus characterizing the complete sub-lattice of ucos on $\mathtt{C}$, i.e., $\langle \mathit{Uco}(\mathtt{C}), \mathrel{\dot{\leq}_\mathtt{c}}, \dot{\vee}_\mathtt{c}, \dot{\wedge}_\mathtt{c}, \lambda x.\top_\mathtt{c}, \iota \rangle$, where the point-wise order $\mathrel{\dot{\leq}_\mathtt{c}}$ reflects the relative precision between ucos.

Let $\mathit{Mon}(\mathtt{C}) \stackrel{\text{def}}{=} \{f \in \mathit{Ext}(\mathtt{C}) \mid \forall x, y \in \mathtt{C} \,.\, x \leq_\mathtt{c} y \Rightarrow f(x) \leq_\mathtt{c} f(y)\}$ be the set of monotone extensive functions. To enforce monotonicity, we leverage the operator $\mathbb{M} : \mathit{Ext}(\mathtt{C}) \to \mathit{Mon}(\mathtt{C})$ [15] defined as

$$\mathbb{M}(f) \stackrel{\text{def}}{=} \lambda x. \bigvee \{f(y) \mid y \leq_\mathtt{c} x\}$$

which, given an extensive function $f \in \mathit{Ext}(\mathtt{C})$, yields the least monotone extensive function greater than $f$. This means that $\mathbb{M} \in \mathit{Uco}(\mathit{Ext}(\mathtt{C}))$, identifying the sub-lattice of monotone and extensive functions [15].

To enforce idempotence, we leverage $\mathbb{I} : \mathit{Mon}(\mathtt{C}) \to \mathit{Uco}(\mathtt{C})$ [15] defined as

$$\mathbb{I}(f) \stackrel{\text{def}}{=} \mathit{lfp}_f^{\dot{\leq}_\mathtt{C}} \ (\lambda g.g \circ g)$$

which, given a monotone and extensive function $f \in \mathit{Mon}(\mathtt{C})$, yields the smallest idempotent function greater than $f$. Thus, $\mathbb{I} \in \mathit{Uco}(\mathit{Mon}(\mathtt{C}))$ and, by defining $\rho_{\mathbb{I}\mathbb{M}} \stackrel{\text{def}}{=} \mathbb{I} \circ \mathbb{M} \in \mathit{Uco}(\mathit{Ext}(\mathtt{C}))$, we have $\mathit{Uco}(\mathtt{C}) = \rho_{\mathbb{I}\mathbb{M}}(\mathit{Ext}(\mathtt{C}))$.

We now define the following Galois insertion

$$\langle \mathit{Rel}(\mathtt{C}), \preccurlyeq \rangle \underset{\alpha_\mathbb{f}}{\overset{\gamma_\mathbb{f}}{\leftrightarrows}} \langle \mathit{Uco}(\mathtt{C}), \dot{\leq}_\mathtt{C} \rangle$$

where the abstraction $\alpha_\mathbb{f} \colon \mathit{Rel}(\mathtt{C}) \to \mathit{Uco}(\mathtt{C})$ is

$$\alpha_\mathbb{f}(\mathtt{R}) \stackrel{\text{def}}{=} \rho_{\mathbb{I}\mathbb{m}} \circ \alpha_\Subset(\mathtt{R})$$

and the concretization $\gamma_\mathbb{f} \colon \mathit{Uco}(\mathtt{C}) \to \mathit{Rel}(\mathtt{C})$ is

$$\gamma_\mathbb{f}(\rho) \stackrel{\text{def}}{=} \{(x, y) \in \mathtt{C} \times \mathtt{C} \mid \rho(x) = \rho(y)\}$$

We have that $\rho_\mathbb{f} \stackrel{\text{def}}{=} \gamma_\mathbb{f} \circ \alpha_\mathbb{f}$ defines a uco on $\mathit{Rel}(\mathtt{C})$.

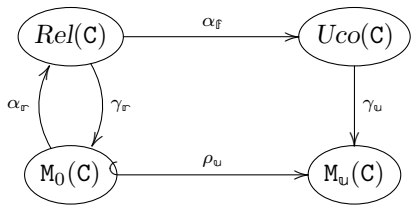
**Theorem 3.** $\rho_\mathbb{f} \in \mathit{Uco}(\mathit{Rel}(\mathtt{C}))$.

*Example 10.* Consider $\mathtt{C} = \wp(\{1, 2, 3, 4\})$ and $f$ of Ex. 9. Then $f_m \stackrel{\text{def}}{=} \mathbb{M}(f)$ is such that $f_m = f$ except for $f_m(14) = 134$, $f_m(23) = 123$, and $f_m(24) = f_m(124) = f_m(134) = f_m(1234) = 1234 = f_m(34) = f_m(234)$ (since $f_m(3)$ adds 1 and 3, while $f_m(34)$ adds 2 and 4). Finally, $\rho = \mathbb{I}(f_m)$ is such that $\rho = f_m$ except for $\rho(1) = \rho(3) = 123$ (since $f_m(1) = f_m(3) = 13$ and $f_m(13) = 123 = f_m(123)$) and $\rho(14) = 1234$ (since $f_m(14) = 134$ and $f_m(134) = 1234 = f_m(1234)$). The corresponding equivalence relation $\mathtt{R}_\rho \stackrel{\text{def}}{=} \gamma_\mathbb{f}(\rho)$ is

$$\mathtt{R}_\rho : \boxed{1 \quad 2 \quad 3 \quad 12 \quad 13 \quad 23 \quad 123} \qquad \boxed{14 \quad 24 \quad 34 \quad 124 \quad 134 \quad 234 \quad 1234}$$

representing a uco over $\mathtt{C} = \wp(\{1, 2, 3, 4\})$ with fix points $\{\varnothing, 4, 123, 1234\}$. ◁

### 3.5 Upper Closure Operators as Pre-Metrics: The Domain $\mathtt{M}_\mathbb{u}(\mathtt{C})$



The last step consists of identifying the pre-metrics that can be uniquely associated with a uco. We define the following Galois insertion

$$\langle \mathtt{M}_0(\mathtt{C}), \sqsubseteq_{\mathtt{m}} \rangle \underset{\alpha_{\mathtt{u}}}{\overset{\gamma_{\mathtt{u}}}{\leftrightarrows}} \langle \mathit{Uco}(\mathtt{C}), \dot{\leq}_{\mathtt{C}} \rangle$$

where the abstraction $\alpha_{\mathtt{u}} \colon \mathtt{M}_0(\mathtt{C}) \to \mathit{Uco}(\mathtt{C})$ is

$$\alpha_{\mathtt{u}} \overset{\text{def}}{=} \alpha_{\mathbb{f}} \circ \alpha_{\mathbb{r}}$$

and the concretization $\gamma_{\mathtt{u}} \colon \mathit{Uco}(\mathtt{C}) \to \mathtt{M}_0(\mathtt{C})$ is

$$\gamma_{\mathtt{u}}(\rho) \overset{\text{def}}{=} \gamma_{\mathbb{r}} \circ \gamma_{\mathbb{f}} = \lambda(x, y). \begin{cases} 0 & \rho(x) = \rho(y) \\ \infty & \text{otherwise} \end{cases}$$

We have that $\rho_{\mathtt{u}} \overset{\text{def}}{=} \gamma_{\mathtt{u}} \circ \alpha_{\mathtt{u}}$ defines a uco on $\mathtt{M}_0(\mathtt{C})$ forcing all the properties described in the previous sections on the collections of elements with 0-distance and forgetting (setting to $\infty$) all the other distances.

**Theorem 4.** *$\rho_{\mathtt{u}} \in \mathit{Uco}(\mathtt{M}_0(\mathtt{C}))$.*

Let $\mathtt{M}_{\mathtt{u}}(\mathtt{C}) \overset{\text{def}}{=} \rho_{\mathtt{u}}(\mathtt{M}_0(\mathtt{C})) = \rho_{\mathtt{u}} \circ \rho_0(\mathtt{M}(\mathtt{C}))$.

**Proposition 6.** *$\langle \mathtt{M}_{\mathtt{u}}(\mathtt{C}), \sqsubseteq_{\mathtt{m}}, \sqcup_{\mathtt{m}}, \sqcap_{\mathtt{m}}, \delta_{\top}, \delta_{\infty} \rangle$ is a complete lattice.*

We finally have the following increasing chain between pre-metric domains:

$$\mathtt{M}_{\mathtt{u}}(\mathtt{C}) \subset \mathtt{M}_{\mathbb{r}}(\mathtt{C}) \subset \mathtt{M}_0(\mathtt{C}) \subset \mathtt{M}(\mathtt{C})$$

In particular, $\mathtt{M}_{\mathtt{u}}(\mathtt{C})$ is the sub-lattice of pre-metrics *uniquely identifying ucos* on the complete lattice $\mathtt{C}$.

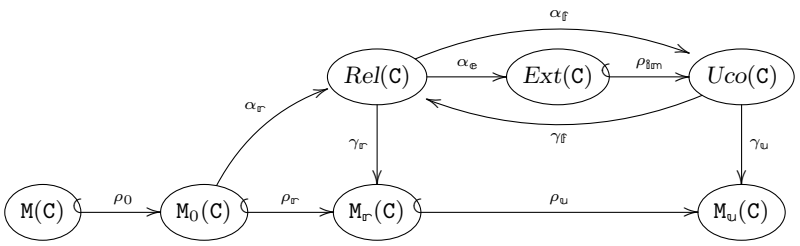



Fig. 2: From pre-metrics to ucos, and back.

Fig. 2 illustrates the full abstraction process from pre-metrics to ucos developed in this section. It shows that ucos can, in general, be viewed as specific instances of pre-metrics (via $\gamma_{\mathtt{u}}$). However, ucos are far from trivial: deriving one from a pre-metric requires that the distance satisfy specific and often stringent conditions. As a result, ucos obtained through abstraction ($\alpha_{\mathbb{f}}\alpha_{\mathbb{r}}\rho_{\mathtt{u}}$) retain a distinct identity, reflecting structural properties of the underlying domain $\mathtt{C}$.

## 4 Combining Distances (and Abstractions)

In this section, building on our view of ucos as abstractions of pre-metrics, we study a way to compose pre-metrics—akin to how compositions of ucos can be defined. Specifically, we define a combination of pre-metrics that enables a *layered abstraction*: a first pre-metric determines how to aggregate elements (at distance zero)—to select the domain of comparison—and a second pre-metric measures distances within this selected domain between the identified aggregations.

Let us consider $\delta_1, \delta_2 \in \mathtt{M}(\mathtt{C})$, and let $f[\delta_1]$ be a *selector map* $f[\delta_1] : \mathtt{C} \to \mathtt{C}$ associating with each element $z \in \mathtt{C}$ a unique element $f_z \in \mathtt{C}$ at distance of zero from $z$ with respect to $\delta_1$, i.e., such that if $f_z \stackrel{\text{def}}{=} f[\delta_1](z)$ then $\delta_1(f_z, z) = 0$. Then, we can *combine* $\delta_1$ and $\delta_2$, leveraging $f[\delta_1]$, as follows:

$$\delta_1 \triangleright_f \delta_2 \stackrel{\text{def}}{=} \lambda(x, y).\ \begin{cases} 0 & \delta_1(x, y) = 0 \\ \delta_2(f[\delta_1](x), f[\delta_1](y)) & \text{otherwise} \end{cases}$$

**Proposition 7.** *Let $\delta_1, \delta_2 \in \mathtt{M}(\mathtt{C})$. Then also $\delta_1 \triangleright_f \delta_2 \in \mathtt{M}(\mathtt{C})$.*

*Example 11.* Let $\Sigma$ be a chosen alphabet (finite set of characters) and let $\Sigma^*$ be the Kleene closure of $\Sigma$, i.e., the set of all strings of finite length over $\Sigma$. We consider the poset $\langle \wp(\Sigma^*), \subseteq \rangle$. Let us define $\delta_\Sigma \colon \wp(\Sigma^*) \times \wp(\Sigma^*) \to \mathbb{N}^\infty$ to compute the absolute difference between the number of string lengths between two sets of strings $W_1, W_2 \in \wp(\Sigma^*)$. Formally:

$$\delta_\Sigma(W_1, W_2) \stackrel{\text{def}}{=} \delta_{siz}(\{\text{length}(w_1) \mid w_1 \in W_1\}, \{\text{length}(w_2) \mid w_2 \in W_2\})$$

where $\delta_{siz}$ is the size distance of Ex. 3 and $\text{length}(w)$ is the number of characters composing the (finite) string $w$.

The composition $\delta_{siz} \triangleright_f \delta_\Sigma$, with $f[\delta_{siz}] = \iota$, computes the distance between the cardinality of string lengths only when the string sets have different cardinality. For instance, given $W_1 = \{a\}$ and $W_2 = \{bb\}$, then $\delta_{siz}(W_1, W_2) = 0$ and therefore $\delta_{siz} \triangleright_f \delta_\Sigma(W_1, W_2) = 0$. Instead, given $W_1$ and $W_3 = \{a, bb, cc\}$, we have $\delta_{siz} \triangleright_f \delta_\Sigma(W_1, W_2) = 2$ and thus $\delta_{siz} \triangleright_f \delta_\Sigma(W_1, W_3) = \delta_\Sigma(W_1, W_3) = 1$.

Vice versa, $\delta_\Sigma \triangleright_f \delta_{siz}$, with $f[\delta_\Sigma] = \iota$, computes the distance between the cardinality of the string sets only when the sets of their strings lengths have different lengths. For instance, $\delta_\Sigma(W_1, W_2) = 0$ and thus $\delta_\Sigma \triangleright_f \delta_{siz}(W_1, W_2) = 0$, while $\delta_\Sigma(W_1, W_3) = 1$ and therefore $\delta_\Sigma \triangleright_f \delta_{siz}(W_1, W_3) = \delta_{siz}(W_1, W_3) = 2$. ◁

At this point, we can use the operation $\triangleright_f$ for *combining* a distance $\delta_\rho \in \mathtt{M}_{\mathbb{U}}(\mathtt{C})$ characterizing a semantic abstraction $\rho \in \mathit{Uco}(\mathtt{C})$ (cf. Sec. 3.5), and another distance $\delta_{\mathtt{C}} \in \mathtt{M}(\mathtt{C})$ that we want to use for measuring the distances between abstract elements, i.e. elements in $\rho(\mathtt{C})$. As for selector function $f[\delta_\rho]$, we can exploit precisely the structure of the elements assigned with a distance of zero in $\delta_\rho$. Namely, we can take the least upper bound of the elements at distance zero, which by construction is at distance zero (cf. Sec. 3.4). Formally, let us define $\delta^\rho_{\mathtt{C}} \stackrel{\text{def}}{=} \delta_\rho \triangleright_f \delta_{\mathtt{C}}$ with $f[\delta_\rho] \stackrel{\text{def}}{=} \lambda x.\ \bigvee\{w \mid \delta_\rho(x, w) = 0\}$. Note that the definition of $f[\delta_\rho]$ satisfies the condition to be a selector function since, by construction of

$\delta_\rho \in \mathtt{M}_{\mathtt{u}}(\mathtt{C})$, we have that: $\forall x \in \mathtt{C}\,.\,\delta_\rho(f[\delta_\rho](x), x) = 0$. The combination distance $\delta_\rho \triangleright_f \delta_\mathtt{C}$ is the conjunction of a semantic approximation $\rho$ (cf. Def. 2) and a quantitative approximation $\delta_\mathtt{C}$ (cf. Def. 4):

**Proposition 8.** *Let $\delta_\rho \in \mathtt{M}_{\mathtt{u}}(\mathtt{C})$ characterize $\rho \in \mathit{Uco}(\mathtt{C})$ and let $\delta_\mathtt{C} \in \mathtt{M}(\mathtt{C})$. Let $f[\delta_\rho] = \lambda x.\ \bigvee\{w \mid \delta_\rho(x, w) = 0\}$ on $\mathtt{C}$, then*

$$\forall x, y \in \mathtt{C}\,.\,(\delta_\rho \triangleright_f \delta_\mathtt{C})(x, y) = \delta_\mathtt{C}(\rho(x), \rho(y))$$

We formally define this general notion of approximation below.

**Definition 6 (General Approximation).** *Let $\langle \mathtt{C}, \leq_\mathtt{c}\rangle$ be a poset and $\langle \mathtt{C}, \delta_\mathtt{C}\rangle$ be a pre-metric space, and let $\rho \in \mathit{Uco}(\mathtt{C})$. We define the general approximation as follows for any $x, y \in \mathtt{C}$:*

$$\delta^\rho_\mathtt{C}(x, y) \stackrel{\text{def}}{=} \delta_\mathtt{C}(\rho(x), \rho(y))$$

*An element $x \in \mathtt{C}$ is semantically approximated with $\rho$* and *quantitatively approximated by $\delta_\mathtt{C}$, up to $\varepsilon \in \mathbb{R}^\infty_{\geq 0}$, by any element in the set $\{y \in \mathtt{C} \mid \delta^\rho_\mathtt{C}(x, y) \leq \varepsilon\}$.*

That is, $\delta^\rho_\mathtt{C}(x, y)$ calculates the distance between the semantic approximations of $x$ and $y$ with $\rho$. Clearly, when considering the identity function $\iota \in \mathit{Uco}(\mathtt{C})$ as abstraction, it holds that $\delta_\iota \triangleright_f \delta_\mathtt{C} = \delta^\iota_\mathtt{C}(x, y) = \delta_\mathtt{C}(x, y)$ for any $x, y \in \mathtt{C}$.

*Example 12.* Continuing Ex. 2 and Ex. 5, the set $\{0, 1, 4\}$ can be semantically and quantitatively approximated by $\delta_{\mathsf{Int}} \triangleright_f \delta_{siz} = \delta^{\mathsf{Int}}_{siz}$ and $\varepsilon = 1$ in any set in

$$\{S \in \wp(\mathbb{Z}) \mid \delta^{\mathsf{Int}}_{siz}(\{0, 1, 4\}, S) \leq 1\} = \{S \in \wp(\mathbb{Z}) \mid \mathsf{Int}(S) = [-1, 4] \vee \mathsf{Int}(S) = [0, 5]\} \quad \triangleleft$$

In the following sections, we build on this general approximation framework a new confidentiality property—based on the notion of Abstract Non-Interference—that quantifies semantic variations in the output domain. This leads to a novel property we call *Partial Abstract Non-Interference*. We prove that it has a strong relation with Partial Completeness [5,7,8], a property modeling imprecision of an abstraction in the context of abstract interpretation, but it provides a novel *perspective* on precision, as it happens for the (not partial) corresponding notions.

## 5 (Partial) Completeness and Abstract Non-Interference

We briefly recall the notions of Completeness and Partial Completeness in abstract interpretation, as well as Abstract Non-Interference (ANI).

***Completeness.*** Given a monotone function $f\colon \mathtt{C} \to \mathtt{D}$ over posets $\langle \mathtt{C}, \leq_\mathtt{c}\rangle$ and $\langle \mathtt{D}, \leq_\mathtt{d}\rangle$, the abstractions $\eta \in \mathit{Uco}(\mathtt{C})$ and $\rho \in \mathit{Uco}(\mathtt{D})$ can be used to approximate computations, thus defining an abstract version $f^\sharp\colon \eta(\mathtt{C}) \to \rho(\mathtt{D})$ of $f$. An abstract function $f^\sharp$ is *sound* when $\rho \circ f \leq_\mathtt{d} f^\sharp \circ \eta$ [14]. A sound by construction approximation is $f^\alpha \stackrel{\text{def}}{=} \rho \circ f \circ \eta$, called the *best correct approximation* (bca) [14]

of $f$. Any $f^\sharp$ soundly approximating $f$ is, in fact, equal or less precise than the bca, formally: $\rho \circ f \leq_{\mathtt{D}} f^\alpha \leq_{\mathtt{D}} f^\sharp \circ \eta$ [14].

A sound abstract computation $f^\sharp \colon \eta(\mathtt{C}) \to \rho(\mathtt{D})$ performs a *precise* approximation of a (concrete) monotone function $f \colon \mathtt{C} \to \mathtt{D}$ whenever $\rho \circ f = f^\sharp \circ \eta$. It has been proved that for a precise abstract approximation to exist, the bca $f^\alpha$ must also be precise [13,26]. In particular, if $f^\sharp$ is a precise abstract approximation of $f$ then $f^\sharp = f^\alpha$ . *Completeness* [13,26] in abstract interpretation is a desirable property that ensures the existence of a precise abstract approximation of a (concrete) monotone function $f$. Formally[4]:

**Definition 7 (Completeness [13,26]).** *Let $\langle \mathtt{C}, \leq_{\mathtt{C}} \rangle$ and $\langle \mathtt{D}, \leq_{\mathtt{D}} \rangle$ be posets, and let $\eta \in Uco(\mathtt{C})$ and $\rho \in Uco(\mathtt{D})$ be the input and output abstractions, respectively. A monotone function $f \colon \mathtt{C} \to \mathtt{D}$ satisfies* Completeness *w.r.t. $\langle \eta, \rho \rangle$ when the following condition holds: $\forall x \in \mathtt{C} \,.\, \rho \circ f(x) = \rho \circ f \circ \eta(x)$.*

In other words, proving the Completeness of $f$ w.r.t. the input and output abstractions $\langle \eta, \rho \rangle$ means proving the bca $\rho \circ f \circ \eta$ is precise.

***Partial Completeness.*** In practice, Completeness is rarely satisfied. For this reason, Campion et al. [5,7,8] introduced a weaker notion of completeness, called *Partial Completeness*, by the use of pre-metrics *compatible* with the ordering of the underlying poset.

**Definition 8 (Order-Compatible Distance [8]).** *Let $\langle \mathtt{L}, \leq_{\mathtt{L}} \rangle$ be a poset. A distance $\delta : \mathtt{L} \times \mathtt{L} \to \mathbb{R}^\infty$ is said to be* compatible with the ordering $\leq_{\mathtt{L}}$ *or, in short,* $\leq_{\mathtt{L}}$-compatible*, if and only if it also satisfies the following property $\forall x, y, z \in \mathtt{L}$:*

$$x \leq_{\mathtt{L}} y \leq_{\mathtt{L}} z \;\Rightarrow\; \delta(x, y) \leq \delta(x, z) \wedge \delta(y, z) \leq \delta(x, z). \;\textit{(chains-order)}$$

*A poset $\langle \mathtt{L}, \leq_{\mathtt{L}} \rangle$ equipped with a $\leq_{\mathtt{L}}$-compatible distance $\delta$ is called a* distance compatible space *and is denoted by the triple $\langle \mathtt{L}, \leq_{\mathtt{L}}, \delta \rangle$.*

The purpose of the (*chains-order*) axiom is to give a meaning to distances between comparable elements. Notably, let $f_1^\sharp$ and $f_2^\sharp$ be sound abstract approximations of a concrete monotone function $f \colon \mathtt{C} \to \mathtt{D}$, i.e., $\rho \circ f \leq_{\mathtt{D}} f_1^\sharp \circ \eta$ and $\rho \circ f \leq_{\mathtt{D}} f_2^\sharp \circ \eta$. If $f_1^\sharp$ is more precise than $f_2^\sharp$, i.e., $f_1^\sharp \leq_{\mathtt{D}} f_2^\sharp$, we expect a decrease in the imprecision (distance) with respect to the concrete computation when using $f_1^\sharp$ rather than $f_2^\sharp$, i.e., $\forall x \in \mathtt{D} \colon \delta(\rho \circ f(x), f_1^\sharp \circ \eta(x)) \leq \delta(\rho \circ f(x), f_2^\sharp \circ \eta(x))$.

*Example 13.* The poset $\langle \wp(L), \subseteq \rangle$ and the size distance $\delta_{siz}$ from Ex. 3 form a pseudo-metric compatible space. ◁

For additional examples of order-compatible pre-metrics and their applications in domains used within the context of program analysis, we refer to [8].

[4] This definition of Completeness is also called Backward-Completeness [26].

Def. 8 is general enough to be instantiated with other definitions of distances used in the literature of abstract interpretation (see, e.g., [5,30,31,19,41]).

We can now recall the definition of $\varepsilon$-Partial Completeness, adapted here in the context of ucos and by leveraging Def. 6 for rewriting the condition.

**Definition 9 ($\varepsilon$-Partial Completeness [5,8]).** *Let $\langle \mathtt{C}, \leq_{\mathtt{C}} \rangle$ be a poset and $\langle \mathtt{D}, \leq_{\mathtt{D}}, \delta_{\mathtt{D}} \rangle$ be a pre-metric compatible space, let $\eta \in \mathit{Uco}(\mathtt{C})$ and $\rho \in \mathit{Uco}(\mathtt{D})$ be the input and output abstractions, respectively. Let $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$. A monotone function $f : \mathtt{C} \to \mathtt{D}$ satisfies* $\varepsilon$-Partial Completeness *w.r.t. $\langle \eta, \delta^{\rho}_{\mathtt{D}} \rangle$ if and only if the following condition holds: $\forall x \in \mathtt{C} \,.\, \delta^{\rho}_{\mathtt{D}}(f(x), f \circ \eta(x)) \leq \varepsilon$.*

The equality requirement of Def. 7 is relaxed by admitting a bounded imprecision, i.e. a bounded distance, between $\rho \circ f(x)$ and the bca $\rho \circ f \circ \eta(x)$ for all $x \in C$, which must not exceed $\varepsilon$. The imprecision to be measured and bounded is encoded in the pre-metric $\leq_{\mathtt{D}}$-compatible $\delta_{\mathtt{D}}$ defined on the output domain $\mathtt{D}$.

*Example 14.* We consider the pre-metric compatible space $\langle \wp(\mathbb{Z}), \subseteq, \delta_{siz} \rangle$ where $\delta_{siz}$ is the size distance defined in Ex. 3, the complete lattice $\langle \wp(\mathbb{Z}), \subseteq, \cup, \cap, \mathbb{Z}, \varnothing \rangle$, and the standard denotational collecting semantics over it $[\![\mathsf{Q}]\!] \colon \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$ of the following program $\mathsf{Q} \in \mathsf{Prog}$:

$$\textbf{while } x > 1 \textbf{ do } x := x - 2$$

Let us set $\rho = \eta = \mathsf{Int}$. Then $[\![\mathsf{Q}]\!]$ does not satisfy Completeness for $\langle \mathsf{Int}, \mathsf{Int} \rangle$ because for the input $\{2, 4\}$ we get:

$$\mathsf{Int}([\![\mathsf{Q}]\!]\{2,4\}) = [0,0] \subset [0,1] = \mathsf{Int}([\![\mathsf{Q}]\!]\{2,3,4\}) = \mathsf{Int}([\![\mathsf{Q}]\!]\mathsf{Int}(\{2,4\}))$$

However, if we allow an imprecision quantified by $\varepsilon = 1$, which for $\delta_{siz}$ corresponds to accepting one spurious element between the two results, we get:

$$\delta^{\mathsf{Int}}_{siz}([\![\mathsf{Q}]\!]\{2,4\}, [\![\mathsf{Q}]\!]\mathsf{Int}(\{2,4\})) = \delta_{siz}([0,0],[0,1]) \leq 1$$

In particular, it is easy to note that $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{Q}]\!]S, [\![\mathsf{Q}]\!]\mathsf{Int}(S)) \leq 1$, for all input sets $S \in \wp(\mathbb{Z})$, which implies that $[\![\mathsf{Q}]\!]$ satisfies 1-Partial Completeness w.r.t. $\langle \mathsf{Int}, \delta^{\mathsf{Int}}_{siz} \rangle$. ◁

It is worth noting that, if a function $f$ is proved to satisfy Completeness for abstractions $\langle \eta, \rho \rangle$, then $f$ is also 0-Partial Complete for $\langle \eta, \delta^{\rho}_{\mathtt{D}} \rangle$ with respect to any pre-metric order-compatible $\delta$ (thanks to the (*if-identity*) axiom). However, the converse does not hold if the (*iff-identity*) axiom is not satisfied by $\delta$, e.g., when $\delta$ is a pseudo-metric.

***Abstract Non-Interference.*** Non-Interference [27] is a confidentiality policy that safeguards sensitive input information from affecting observable computation results. This concept has been relaxed to encompass variations in properties that might influence computations [21,32,24,22,33]. Additionally, the distinction between secret/relevant and public/observable data can be interpreted as an abstraction of data. In particular, Non-Interference has been extended and refined

through abstract interpretation, yielding a confidentiality policy called Abstract Non-Interference [24]. Following [35], we will focus on the flavor of Abstract Non-Interference considering an input data property to protect, when assuming an abstract observation of computations (this notion is called narrow in [24]).

**Definition 10 (Abstract Non-Interference [24]).** *Let* $\langle \mathtt{C}, \leq_{\mathtt{C}} \rangle$ *and* $\langle \mathtt{D}, \leq_{\mathtt{D}} \rangle$ *be posets, and let* $\eta \in Uco(\mathtt{C})$ *and* $\rho \in Uco(\mathtt{D})$ *be abstractions. A function* $f : \mathtt{C} \to \mathtt{D}$ *satisfies* Abstract Non-Interference *(ANI for short) w.r.t.* $\langle \eta, \rho \rangle$ *when:*

$$\forall x, y \in \mathtt{C} \,.\, \eta(x) = \eta(y) \;\Rightarrow\; \rho \circ f(x) = \rho \circ f(y)$$

*Example 15.* Consider the complete lattice $\langle \wp(\mathbb{Z}), \subseteq, \cup, \cap, \mathbb{Z}, \varnothing \rangle$, the standard collecting semantics $[\![\mathsf{P}]\!] : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$, and the following program P:

$$\textbf{if } (x \bmod 2 = 0 \;\wedge\; x \neq 0) \textbf{ then } x := (x/2)^2 \textbf{ else } x := -x^2 + (1 - |x|)$$

where MOD is the modulo operation. Let $\mathsf{Par} \in Uco(\wp(\mathbb{Z}))$ be the parity abstraction over input values, and $\mathsf{Sign} \in Uco(\wp(\mathbb{Z}))$ the sign abstraction over output values (cf. Ex. 1). In this program, for any even value, we return a positive number; for 0, we return 1 (hence a positive value), while for odd numbers, we return a negative value. Formally, for all $N, M \in \wp(\mathbb{Z})$, if $\mathsf{Par}(N) = \mathsf{Par}(M)$ then we have $\mathsf{Sign}([\![P]\!]N) = \mathsf{Sign}([\![P]\!]M)$, thus $[\![\mathsf{P}]\!]$ satisfies ANI w.r.t. $\langle \mathsf{Par}, \mathsf{Sign} \rangle$. It should be clear that, if we consider as input abstractions any convex abstract domain other than Par (mixing in the same abstract value even and odd values) such as Sign or Int, then ANI w.r.t. Sign as output abstraction (e.g., $\langle \mathsf{Sign}, \mathsf{Sign} \rangle$ or $\langle \mathsf{Int}, \mathsf{Sign} \rangle$) does not hold anymore. ◁

Although Abstract Non-Interference and Completeness may initially appear to be distinct notions, they have been proved to be equivalent in [35]. This equivalence enables the reuse of verification mechanisms for ANI to verify Completeness. Conversely, domain transformers that induce Completeness (e.g., [26,3]) can also be repurposed to enforce ANI.

## 6 A *General Approximated* Confidentiality Property

Non-Interference [27] has been widely adopted to model various security properties, particularly confidentiality, which concerns the control of information flow within a computer system. Despite its widespread use in academic research, Non-Interference is rarely achievable in real-world systems for two main reasons: first, it is a very strong property that requires complete indistinguishability of data; second, practical systems often need to reveal some information to function—for example, a password checker necessarily leaks some information about the input when indicating whether access is granted. As a result, several weakened variants of Non-Interference have been proposed. Broadly, these relaxations fall into two categories, which correspond to the two types of approximation discussed in Sec. 4: *semantic* approximation and *quantitative* approximation.

Abstract Non-Interference (cf. Def. 10) adopts a semantic approach, replacing indistinguishability between *data* with indistinguishability between *properties of data*. This constitutes a semantic approximation, as it requires the abstraction of the program semantics to be indistinguishable whenever the inputs are indistinguishable with respect to a given abstract property. In language-based security, it means that if the observable output remains within the group of all acceptable outputs (modeled as an abstraction), the system is deemed secure.

Approximate Non-Interference [18] follows a quantitative approach, where *indistinguishability* between data is replaced by *similarity*. Originally introduced in the context of probabilistic process algebras, this notion requires that the observable behaviors of two agents differ by no more than a threshold $\varepsilon$, rather than being strictly identical as in standard Non-Interference [27].

Our idea is to *combine* the two approximation strategies (cf. Sec. 4)—semantic and quantitative—while keeping the two types of approximation explicitly distinct. This leads to a new notion called *Partial Abstract Non-Interference*, where *indistinguishability* between *data* is replaced by *similarity* between *properties of data*. In security, Partial ANI would offer a more refined modeling capability. Instead of requiring outputs to be indistinguishable under a coarse abstraction, it allow outputs to vary, as long as the variation remains within a specified quantitative bound. This enables a more nuanced treatment of security policies, especially when small, bounded differences in outputs are tolerable.

### 6.1 Partial Abstract Non-Interference

Partial Abstract Non-Interference is a novel relaxation of Non-Interference that combines both semantic and quantitative approximations. Specifically, it observes properties of data (as in ANI) rather than raw data, while allowing for a bounded distance between these observed properties.

**Definition 11 ($\varepsilon$-Partial Abstract Non-Interference).** *Let $\langle \mathtt{C}, \preceq_{\mathtt{C}} \rangle$ be the input domain and $\langle \mathtt{D}, \preceq_{\mathtt{D}} \rangle$ be the output one (posets), respectively. Let $\langle \mathtt{C}, \delta_{\mathtt{C}} \rangle$ and $\langle \mathtt{D}, \delta_{\mathtt{D}} \rangle$ be pre-metric spaces. Let $\eta \in \mathit{Uco}(\mathtt{C})$, $\rho \in \mathit{Uco}(\mathtt{D})$ be the abstractions of the input and output domains, respectively, and $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$. A function $f \colon \mathtt{C} \to \mathtt{D}$ satisfies* $\varepsilon$-Partial Abstract Non-Interference *($\varepsilon$-Partial ANI for short) w.r.t. $\langle \delta^{\eta}_{\mathtt{C}}, \delta^{\rho}_{\mathtt{D}} \rangle$ when the following implication holds:*

$$\forall x, y \in \mathtt{C} \,.\, \delta^{\eta}_{\mathtt{C}}(x, y) = 0 \;\Rightarrow\; \delta^{\rho}_{\mathtt{D}}(f(x), f(y)) \leq \varepsilon$$

Starting from inputs whose property distance is zero according to $\delta^{\eta}_{\mathtt{C}}$, i.e., $\delta^{\eta}_{\mathtt{C}}(x, y) = 0$, Partial ANI allows the function to produce different outputs, potentially with different properties under $\delta^{\rho}_{\mathtt{D}}$, as long as the variation remains bounded, specifically not exceeding a given threshold $\varepsilon$, i.e. $\delta^{\rho}_{\mathtt{D}}(f(x), f(y)) \leq \varepsilon$. It is important to note that the condition $\delta^{\eta}_{\mathtt{C}}(x, y) = 0$ does not imply $\eta(x) = \eta(y)$ (as required for ANI, cf. Def. 10) since $\delta_{\mathtt{C}}$ is a pre-metric and may therefore violate the (*iff-identity*) axiom. As a result, on the left-hand side of the implication, Partial ANI allows inputs to be mapped by $\eta$ to different abstract properties, while still being indistinguishable with respect to $\delta_{\mathtt{C}}$.

*Example 16.* Consider the program $\mathsf{R}$: **if** $x > 0$ **then** $x := x-1$ **else** $x := x+1$. and the standard collecting denotational semantics $[\![\mathsf{R}]\!]\colon \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$. Let us consider the counting distance $\delta_{siz}$, defined in Ex. 3 and the abstract domain of intervals $\mathsf{Int} \in \mathit{Uco}(\wp(\mathbb{Z}))$. In this program, if we start from an interval composed by positive values only (e.g. $[1, 8]$), then $[\![\mathsf{R}]\!]$ decreases all the values by one (i.e., $[0, 7]$). Something similar happens when all the elements in the interval are negative, e.g., $[-5, -2]$ returning $[-4, -1]$. The only case in which the dimension of an input interval changes is when the lower bound is non-positive (and thus increased by one) and the upper bound is positive (and thus decreased by one), e.g., $[-2, 5]$ becomes $[-1, 4]$. This means that starting from two sets $S_1, S_2 \in \wp(\mathbb{Z})$ whose interval abstraction has the same number of values (i.e., $\delta^{\mathsf{Int}}_{siz}(S_1, S_2) \leq 0$), e.g. $\delta^{\mathsf{Int}}_{siz}(\{-9, -2\}, \{1, 3, 5, 8\}) = 0$, we obtain as output two respective intervals with the same number of elements, e.g. $\delta^{\mathsf{Int}}_{siz}(\{-8, -1\}, \{0, 2, 4, 7\}) = \delta_{siz}([-8, -1], [0, 7]) = 0$, or, in the worst case, with a difference of two, i.e., $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}]\!]S_1, [\![\mathsf{R}]\!]S_2) \leq 2$. For instance, $\delta^{\mathsf{Int}}_{siz}(\{-5, 0, 2\}, \{1, 8\}) = 0$ in input, and $\delta^{\mathsf{Int}}_{siz}(\{-4, 1\}, \{0, 7\}) = 2$ in output. Hence, we can say that the collecting semantics of the program $\mathsf{R}$ satisfies 2-Partial ANI w.r.t. $\langle \delta^{\mathsf{Int}}_{siz}, \delta^{\mathsf{Int}}_{siz} \rangle$.

Conversely, consider this time the program $\mathsf{R}^*$ where $^*$ is the Kleene closure of regular commands [40] whose semantics is defined as follows: $\forall S \in \wp(\mathbb{Z})\ .\ [\![\mathsf{R}^*]\!]S \stackrel{\text{def}}{=} \bigcup\{[\![\mathsf{R}]\!]^n S \mid n \in \mathbb{N}\}$ and where $[\![\mathsf{R}]\!]^n$ is the composition of program $\mathsf{R}$ $n$ times. Then Partial ANI does not hold for any $\varepsilon$ (except for the trivial case $\varepsilon = \infty$). In particular, for any input whose interval abstraction has bounds of opposite sign, e.g., $[-2, 4]$, the result is precisely the same interval since the collecting semantics keeps the greater collection; if the lower bound is not negative, e.g., $[2, 6]$, then it is pushed to 0 in the output, i.e., $[0, 6]$; while if the upper bound is not positive, e.g., $[-4, -2]$, then this is pushed to 1, i.e., $[-4, 1]$. This means that for instance $\delta_{siz}([2, 6], [21, 25]) \leq 0$ but $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}^*]\!][2, 6], [\![\mathsf{R}^*]\!][21, 25]) = \delta_{siz}([0, 6], [0, 25]) = 19$, and this difference may increase without limit. ◁

By fixing the bound on the difference between output properties to $\varepsilon = 0$, Partial ANI reduces to the following slight generalization of ANI:

$$\forall x, y \in \mathsf{C}\ .\ \delta^{\eta}_{\mathsf{C}}(x, y) = 0 \ \Rightarrow\ \delta^{\rho}_{\mathsf{D}}(f(x), f(y)) \leq 0$$

This notion collapses to ANI (cf. Def. 10) when both $\delta_{\mathsf{C}}$ and $\delta_{\mathsf{D}}$ satisfy the (*iff-identity*) axiom, namely when both are quasisemi-metrics.

On the other hand, if we move into the field of process algebra, if we consider $\eta = \top$ (i.e., we do not have constraints on the input processes), $\delta_{\mathsf{C}}$ is any quasisemi-metric, and we consider as $\rho$ the observation of the processes, then Partial ANI (cf. Def. 11) collapses to Approximate Non-interference [18].

### 6.2 On the Relation with Partial Completeness

In the last decade, it has been proved that there is a strong relation between the property of Completeness in abstract interpretation and Abstract Non-Interference [35]. Specifically, we know that requiring Completeness of a function

w.r.t. an input and output abstractions, is equivalent to requiring that function inputs sharing the same property are mapped to outputs that also share the same property (i.e., ANI).

In this section, we study the relation between Partial Completeness (cf. Def. 9) and Partial ANI (cf. Def. 11). When generalizing ANI to Partial ANI by combining semantic and quantitative approximations, the equivalence between Completeness and ANI (proved in [35]) becomes an implication between $\varepsilon$-Partial ANI and $\varepsilon$-Partial Completeness. Vice versa, when we are considering a quasisemi-metric space and a pseudo-metric space for the input and output domains, respectively, there is an implication between $\varepsilon$-Partial Completeness and $2\varepsilon$-Partial ANI. These statements are proved in the following two theorems:

**Theorem 5 ($\varepsilon$-Partial ANI $\Rightarrow$ $\varepsilon$-Partial Completeness).** *Let $\langle \mathtt{C}, \preceq_{\mathtt{C}} \rangle$ be a poset equipped with a pre-metric (not necessarily order-compatible) $\delta_{\mathtt{C}}$, and $\langle \mathtt{D}, \preceq_{\mathtt{D}}, \delta_{\mathtt{D}} \rangle$ be a pre-metric compatible space. Let $\eta \in Uco(\mathtt{C})$, $\rho \in Uco(\mathtt{D})$ be abstractions and $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$. If a monotone function $f : \mathtt{C} \to \mathtt{D}$ satisfies $\varepsilon$-Partial ANI w.r.t. $\langle \delta^{\eta}_{\mathtt{C}}, \delta^{\rho}_{\mathtt{D}} \rangle$ then $f$ satisfies $\varepsilon$-Partial Completeness w.r.t. $\langle \eta, \delta^{\rho}_{\mathtt{D}} \rangle$, namely:*

$$[\forall x, y \in \mathtt{C}\,.\, \delta^{\eta}_{\mathtt{C}}(x, y) \leq 0 \Rightarrow \delta^{\rho}_{\mathtt{D}}(f(y), f(x)) \leq \varepsilon] \Rightarrow [\forall x \in \mathtt{C}\,.\, \delta^{\rho}_{\mathtt{D}}(f(x), f \circ \eta(x)) \leq \varepsilon]$$

*Example 17.* Consider again the pre-metric compatible space $\langle \wp(\mathbb{Z}), \subseteq, \delta_{siz} \rangle$ and the abstraction $\mathsf{Int} \in Uco(\wp(\mathbb{Z}))$. From Ex. 16, we know that $[\![\mathsf{R}]\!]$ satisfies 2-Partial ANI w.r.t. $\langle \delta^{\mathsf{Int}}_{siz}, \delta^{\mathsf{Int}}_{siz} \rangle$, i.e., $\delta^{\mathsf{Int}}_{siz}(X, Y) \leq 0 \Rightarrow \delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}]\!]X, [\![\mathsf{R}]\!]Y) \leq 2$ for any $X, Y \in \wp(\mathbb{Z})$. Thus, by Thm. 5, it satisfies 2-Partial Completeness w.r.t. $\langle \mathsf{Int}, \delta^{\mathsf{Int}}_{siz} \rangle$, i.e., $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}]\!]X, [\![\mathsf{R}]\!]\mathsf{Int}(X)) \leq 2$ for any $X \in \wp(\mathbb{Z})$. In fact, the bound 2 for Partial Completeness is not tight as $[\![\mathsf{R}]\!]$ also satisfies 1-Partial Completeness w.r.t. $\langle \mathsf{Int}, \delta^{\mathsf{Int}}_{siz} \rangle$. Indeed, given $X = \{-1, 1\}$, we have $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}]\!]\{-1, 1\}, [\![\mathsf{R}]\!]\mathsf{Int}(\{-1, 1\})) = \delta_{siz}([0, 0], [0, 1])) \leq 1$, while for any $Y \in \wp(\mathbb{Z}) \setminus \{-1, 1\}$ we have $\delta^{\mathsf{Int}}_{siz}([\![\mathsf{R}]\!]Y, [\![\mathsf{R}]\!]\mathsf{Int}(Y)) \leq 0$. ◁

**Theorem 6 ($\varepsilon$-Partial Completeness $\Rightarrow$ $2\varepsilon$-Partial ANI).** *Let $\langle \mathtt{C}, \preceq_{\mathtt{C}} \rangle$ be a poset equipped with a quasisemi-metric (not necessarily order-compatible) $\delta_{\mathtt{C}}$, and $\langle \mathtt{D}, \preceq_{\mathtt{D}}, \delta_{\mathtt{D}} \rangle$ be a pseudo-metric compatible space. Let $\eta \in Uco(\mathtt{C})$, $\rho \in Uco(\mathtt{D})$ be the input and output abstractions, respectively, and $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$. If a monotone function $f : \mathtt{C} \to \mathtt{D}$ satisfies $\varepsilon$-Partial Completeness w.r.t. $\langle \eta, \delta^{\rho}_{\mathtt{D}} \rangle$ then $f$ satisfies $2\varepsilon$-Partial ANI w.r.t. $\langle \delta^{\eta}_{\mathtt{C}}, \delta^{\rho}_{\mathtt{D}} \rangle$, namely:*

$$[\forall x \in \mathtt{C}\,.\, \delta^{\rho}_{\mathtt{D}}(f(x), f \circ \eta(x)) \leq \varepsilon] \Rightarrow [\forall x, y \in \mathtt{C}\,.\, \delta^{\eta}_{\mathtt{C}}(x, y) \leq 0 \Rightarrow \delta^{\rho}_{\mathtt{D}}(f(y), f(x)) \leq 2\varepsilon]$$

Thm. 5 shows that having a proof of $\varepsilon$-Partial ANI of $f$ w.r.t. $\langle \delta^{\eta}_{\mathtt{C}}, \delta^{\rho}_{\mathtt{D}} \rangle$, implies that $f$ is partial complete w.r.t. $\langle \eta, \delta^{\rho}_{\mathtt{D}} \rangle$ with the same bound of imprecision $\varepsilon$. In other words, if $f$ maps distinct inputs but having a zero distance according to $\delta_{\mathtt{C}}$, to corresponding outputs that differ by an $\varepsilon$ amount according to $\delta_{\mathtt{D}}$ (i.e., $f$ satisfies $\varepsilon$-Partial ANI), then there exists a sound abstract approximation of $f$ over $\langle \eta, \rho \rangle$, namely $\rho \circ f \circ \eta$, capable of producing a results with an imprecision, measured by $\delta_{\mathtt{D}}$, not greater than the bound $\varepsilon$.

On the other hand, the use of $\delta^{\eta}_{\mathtt{C}}$ and $\delta^{\rho}_{\mathtt{D}}$ in the definitions of Partial ANI (cf. Def. 11) and Partial Completeness (cf. Def 9) amplifies the bound on the

output error by a constant factor in Thm. 6. This is because Partial ANI bounds the distance between $\rho \circ f(x)$ and $\rho \circ f(y)$, for all $x, y \in \mathtt{C}$ that have distance smaller or equal than zero through the abstraction $\eta$, but Partial Completeness only guarantees a bound on the distance between $\rho \circ f(x)$ and $\rho \circ f(y)$, for all $x \in C$ with $y = \eta(x)$. We thus bound the output error for Partial ANI by adding up the distance between $\rho \circ f(x)$ and $\rho \circ f \circ \eta(x) = \rho \circ f \circ \eta(y)$, and between $\rho \circ f \circ \eta(x) = \rho \circ f \circ \eta(y)$ and $\rho \circ f(y)$.

Note also that Thm. 6 imposes stronger requirements than Thm. 5 on $\delta_{\mathtt{C}}$ and $\delta_{\mathtt{D}}$. Its applicability is more limited and strongly depends on which imprecision we are interested to measure, i.e. the type of distances used over the input and output domains, as shown by the following example.

*Example 18.* Consider again the pre-metric compatible space $\langle \wp(\mathbb{Z}), \subseteq, \delta_{siz} \rangle$ and the abstraction $\mathsf{Int} \in \mathit{Uco}(\wp(\mathbb{Z}))$. The collecting semantics $[\![\mathsf{R}]\!]$ from Ex. 16 satisfies 1-Partial Completeness w.r.t. $\langle \mathsf{Int}, \delta_{siz}^{\mathsf{Int}} \rangle$ (cf. Ex. 17). However, we cannot apply Thm. 6 to derive that $[\![\mathsf{R}]\!]$ also satisfies 2-Partial ANI w.r.t. $\langle \delta_{siz}^{\mathsf{Int}}, \delta_{siz}^{\mathsf{Int}} \rangle$ because $\delta_{siz}$ is not a quasisemi-metric (it does not satisfy the (*iff-identity*) axiom). ◁

The relation between 0-Partial ANI and Completeness (cf. Def. 7) is a straightforward corollary of Thm. 5 and Thm. 6.

**Corollary 1 (0-Partial ANI ⇔ Completeness).** *Let $\langle \mathtt{C}, \preceq_{\mathtt{C}} \rangle$ be a poset that is equipped with a (not necessarily order-compatible) pre-metric $\delta_{\mathtt{C}}$, and let $\langle \mathtt{D}, \preceq_{\mathtt{D}}, \delta_{\mathtt{D}} \rangle$ be a quasisemi-metric order-compatible space. Let $\eta \in \mathit{Uco}(\mathtt{C})$, $\rho \in \mathit{Uco}(\mathtt{D})$ be abstractions, and $\varepsilon \in \mathbb{R}^{\infty}_{\geq 0}$. A monotone function $f : \mathtt{C} \to \mathtt{D}$ satisfies 0-Partial ANI w.r.t. $\langle \delta_{\mathtt{C}}^{\eta}, \delta_{\mathtt{D}}^{\rho} \rangle$ if and only if $f$ satisfies Completeness w.r.t. $\langle \eta, \rho \rangle$, namely:*

$$[\forall x, y \in \mathtt{C} \,.\, \delta_{\mathtt{C}}^{\eta}(x, y) \leq 0 \;\Rightarrow\; \delta_{\mathtt{D}}^{\rho}(f(y), f(x)) \leq 0] \;\Leftrightarrow\; [\forall x \in \mathtt{C} \,.\, \rho f(x) = \rho \circ f \circ \eta(x)]$$

## 7 Related Work

The approach we propose, transitioning from pre-metrics to ucos, involves proving a non-trivial abstraction relation between equivalence relations and ucos. This is not the first work in this direction; indeed, in the literature [29], it has been shown that equivalence relations on a domain $\mathtt{C}$ correspond to ucos on $\wp(\mathtt{C})$ (and more generally, the most concrete uco associated with an equivalence relation $\mathtt{R}$, has $\mathtt{R}$ as its kernel). In the present work, we needed to associate any equivalence relation on $\mathtt{C}$ with a uco defined directly on $\mathtt{C}$, rather than on $\wp(\mathtt{C})$. This shift in the domain where the uco is formalized introduces a significant difference and makes the correspondence notably less straightforward. Indeed, defining a uco on $\wp(\mathtt{C})$ can be done straightforwardly by mapping each $x \in \mathtt{C}$ to its equivalence class (a subset of $\mathtt{C}$) as shown in [29]. In contrast, our approach requires defining a uco directly on $\mathtt{C}$, which means selecting a representative element within $\mathtt{C}$ for each equivalence class. This selection is nontrivial, as there is no canonical or optimal choice that naturally leads to a well-defined uco.

Another strongly related work is [15], where the authors define the function transformers making any total function in $\mathit{Fun}(\mathtt{C})$ a uco. In particular, they define the monotonicity transformer $\mathbb{M}$ and an extensivity transformer, let us call it $\mathbb{E}$, on generic total functions $\mathit{Fun}(\mathtt{C})$, showing also that $\mathbb{M} \circ \mathbb{E} = \mathbb{E} \circ \mathbb{M}$. In our work, we start from $\mathit{Rel}(\mathtt{C})$ (instead of $\mathit{Fun}(\mathtt{C})$), and we observed that it was possible to move from $\mathit{Rel}(\mathtt{C})$ to $\mathit{Ext}(\mathtt{C})$ directly, avoiding so far the application of $\mathbb{E}$ and applying $\mathbb{M}$ to extensive functions, thanks to the commutativity between the two transformers [15]. Finally, $\mathbb{I}$ is applied precisely to monotone and extensive functions, as it happens in [15], inhering so far all the results.

When considering the general approximation based on the combination of pre-metrics and abstractions, we can identify related ideas in other existing works. Partial Completeness (discussed in Sec. 5 and 6.2) is such an example. More recently, a similar idea has been explored in the context of Deep Neural Networks (a multi-layered machine learning model) robustness, where resistance to adversarial attacks is modeled by combining a distance over inputs with an abstraction of the outputs [25].

We also have a correspondence between ANI and Input Data (Non-)Usage [42] when $f$ is deterministic, i.e., Input Data (Non-)Usage is an instance of ANI [36].

Although Partial ANI is a novel notion, Thm. 6 (and Cor. 1) ensures that verification mechanisms developed for Partial Completeness can be reused to verify Partial ANI. For example, in [5], the authors introduced a proof system for deriving triples of the form $[\mathit{Pre}]P[\mathit{Post}, \varepsilon]$, meaning that the distance $\delta^{\rho}_{\mathtt{D}}(\llbracket P \rrbracket(\mathit{Pre}), \mathit{Post}) \leq \varepsilon$ holds. In light of Thm. 6, a proof of $[\mathit{Pre}]P[\llbracket P \rrbracket\rho(\mathit{Pre}), \varepsilon]$, that is, $\llbracket P \rrbracket$ satisfies $\varepsilon$-Partial Completeness w.r.t. $\langle \iota, \delta^{\rho}_{\mathtt{D}} \rangle$, implies that $\llbracket P \rrbracket$ also satisfies $2\varepsilon$-Partial ANI with respect to $\langle \delta^{\iota}_{\mathtt{C}}, \delta^{\rho}_{\mathtt{D}} \rangle$, assuming $\delta^{\iota}_{\mathtt{C}}$ is a quasi-metric. A similar reasoning applies to the proof system proposed in [23] to derive Completeness, which, under the premises of Cor. 1, also yield a proof of 0-Partial ANI. Moreover, existing (and potentially future) domain transformer techniques developed to enforce Completeness (e.g., [26,2]) and Partial Completeness can similarly be adapted to enforce Partial ANI.

## 8 Conclusion

We established a formal relation between quantitative approximations, formalized by pre-metrics, and semantic approximations, captured by upper closure operators, through a chain of Galois connections. This result shows that, under certain structural conditions on a pre-metric, a corresponding semantic abstraction can be derived via Galois connections. Conversely, abstractions defined via ucos can be interpreted as specific instances of pre-metrics, highlighting a bidirectional connection between the two frameworks. We then formalized a composition of pre-metrics that first selects the domain of comparison and then measures distances within this selected domain, thereby enabling a form of layered abstraction. Such a composition, when involving a distance characterizing a semantic abstraction and a distance characterizing a quantitative abstraction, defines a new form of approximation, called general approximation, combining

semantic and quantitative approaches while keeping the two types of approximations distinct. This general approximation captures the idea of allowing an approximate observation of data through abstraction, while also tolerating a certain error in the observation, quantified by a distance between abstractions. We believe that this is a promising approach to approximation, already used in some way in the literature, as we have seen in Sec. 7. In particular, we exploit this approach for defining a new partial form of ANI, where we accept an error in the observed output properties. We showed that this notion is strongly connected to the well-established property of Partial Completeness in abstract interpretation, mirroring the relation between the standard versions of ANI and Completeness.

As future work, we plan to formalize a deductive system specialized for proving Partial ANI of programs. Other deductive systems for the verification of Completeness [23] (and its local version [3]), Partial Completeness [5] and ANI [35] have already been formalized in the literature. As already discussed in Sec. 6, a verification mechanism for Partial ANI could build upon the framework developed for Partial Completeness and ANI [21], particularly in light of Thm. 6. This connection is promising, even though the approach in [5] focuses on a local variant of the property. Moreover, this future direction could inspire the development of an abstract interpretation-based static analyzer for verifying the Partial ANI property of programs. The challenge here lies in the fact that Partial ANI is a hyperproperty [12], and thus the standard abstract interpretation-based overapproximations of sets of traces cannot be directly applied.

The proposed Partial ANI notion is a *global* property, in the sense that it is universally quantified over all inputs. As a future work, we plan to formalize its *local* version, namely requiring Partial ANI over a strict subset of the input domain, and study its relation with other local properties in the context of abstract interpretation [1,3,6,34]. Dropping the universal quantification may invalidate the correlation already established between the global counterparts.

We formalized abstractions as ucos, which have been proven to be equivalent to Galois insertions [16]. In the future, we would like to consider weaker abstraction notions able to formalize properties that do not necessarily admit a best abstraction, such as the domain of convex polyhedra [28] or formal languages [4]. In this direction, the notion of weak closures defined in [35] could be considered.

Finally, in the literature there are numerous quantitative program properties under various formalisms (e.g. Quantitative Data Usage [38,37], Approximated Non-Interference [18], etc.) and other could be obtained by applying the general approximation mechanism of Sec. 4 (e.g. a quantitative general version of program monotonicity [6] or program continuity [9,11]). It could be interesting to build a taxonomy of quantitative program properties, in which the quantification mechanisms are expressed within a unified formalism, such as the combination of pre-metrics and abstractions presented in Sec. 4, and to study the assumptions under which one property implies another.

**Acknowledgements** This work was partially supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded

by the European Union - NextGenerationEU; by PRIN2022PNRR "RAP-ARA" (PE6) - codice MUR: P2022HXNSC; by the SAIF project, funded by the "France 2030" government investment plan managed by the French National Research Agency, under the reference ANR-23-PEIA-0006.

## References

1. Bruni, R., Giacobazzi, R., Gori, R., Ranzato, F.: A logic for locally complete abstract interpretations. In: 36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021. pp. 1–13. IEEE (2021). https://doi.org/10.1109/LICS52264.2021.9470608
2. Bruni, R., Giacobazzi, R., Gori, R., Ranzato, F.: Abstract interpretation repair. In: Jhala, R., Dillig, I. (eds.) PLDI '22: 43rd ACM SIGPLAN International Conference on Programming Language Design and Implementation. pp. 426–441. ACM (2022). https://doi.org/10.1145/3519939.3523453
3. Bruni, R., Giacobazzi, R., Gori, R., Ranzato, F.: A correctness and incorrectness program logic. J. ACM **70**(2), 15:1–15:45 (2023). https://doi.org/10.1145/3582267
4. Campion, M., Dalla Preda, M., Giacobazzi, R.: Abstract interpretation of indexed grammars. In: Chang, B.E. (ed.) 26th Static Analysis Symposium (SAS 2019). Lecture Notes in Computer Science, vol. 11822, pp. 121–139. Springer (2019). https://doi.org/10.1007/978-3-030-32304-2_7
5. Campion, M., Dalla Preda, M., Giacobazzi, R.: Partial (in)completeness in abstract interpretation: limiting the imprecision in program analysis. Proc. ACM Program. Lang. **6**(POPL), 1–31 (2022). https://doi.org/10.1145/3498721
6. Campion, M., Dalla Preda, M., Giacobazzi, R., Urban, C.: Monotonicity and the precision of program analysis. Proc. ACM Program. Lang. **8**(POPL), 1629–1662 (2024). https://doi.org/10.1145/3632897
7. Campion, M., Preda, M.D., Giacobazzi, R.: On the properties of partial completeness in abstract interpretation. In: Lago, U.D., Gorla, D. (eds.) Proceedings of the 23rd Italian Conference on Theoretical Computer Science, ICTCS 2022, Rome, Italy, September 7-9, 2022. CEUR Workshop Proceedings, vol. 3284, pp. 79–85. CEUR-WS.org (2022), https://ceur-ws.org/Vol-3284/8665.pdf
8. Campion, M., Urban, C., Preda, M.D., Giacobazzi, R.: A formal framework to measure the incompleteness of abstract interpretations. In: Hermenegildo, M.V., Morales, J.F. (eds.) Static Analysis - 30th International Symposium, SAS 2023. Lecture Notes in Computer Science, vol. 14284, pp. 114–138. Springer (2023). https://doi.org/10.1007/978-3-031-44245-2_7
9. Chaudhuri, S., Gulwani, S., Lublinerman, R.: Continuity Analysis of Programs. In: Proceedings of the 37th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. p. 57–70. POPL '10, Association for Computing Machinery (2010). https://doi.org/10.1145/1706299.1706308
10. Chaudhuri, S., Gulwani, S., Lublinerman, R.: Continuity and Robustness of Programs **55**(8), 107–115 (2012). https://doi.org/10.1145/2240236.2240262
11. Chaudhuri, S., Gulwani, S., Lublinerman, R., NavidPour, S.: Proving Programs Robust. In: Gyimóthy, T., Zeller, A. (eds.) SIGSOFT/FSE'11 19th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE-19). pp. 102–112. ACM (2011). https://doi.org/10.1145/2025113.2025131
12. Clarkson, M.R., Schneider, F.B.: Hyperproperties. J. Comput. Secur. **18**(6), 1157–1210 (2010). https://doi.org/10.3233/JCS-2009-0393

13. Cousot, P.: Principles of Abstract Interpretation. The MIT Press, Cambridge, Mass. (2021)
14. Cousot, P., Cousot, R.: Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: Graham, R.M., Harrison, M.A., Sethi, R. (eds.) Conference Record of the Fourth ACM Symposium on Principles of Programming Languages, Los Angeles, California, USA, January 1977. pp. 238–252. ACM (1977). https://doi.org/10.1145/512950.512973
15. Cousot, P., Cousot, R.: A constructive characterization of the lattices of all retractions, preclosure, quasi-closure and closure operators on a complete lattice. Portugaliae mathematica **38**(1-2), 185–198 (1979), http://eudml.org/doc/115380
16. Cousot, P., Cousot, R.: Systematic design of program analysis frameworks. In: Aho, A.V., Zilles, S.N., Rosen, B.K. (eds.) Conference Record of the Sixth Annual ACM Symposium on Principles of Programming Languages. pp. 269–282. ACM Press (1979). https://doi.org/10.1145/567752.567778
17. Deza, M.M., Laurent, M.: Geometry of cuts and metrics, Algorithms and combinatorics, vol. 15. Springer (1997). https://doi.org/10.1007/978-3-642-04295-9
18. Di Pierro, A., Hankin, C., Wiklicky, H.: Approximate non-interference. J. Comput. Secur. **12**(1), 37–82 (2004). https://doi.org/10.3233/JCS-2004-12103
19. Di Pierro, A., Wiklicky, H.: Measuring the precision of abstract interpretations. In: Lau, K. (ed.) 10th Logic Based Program Synthesis and Transformation (LOPSTR'00). LNCS, vol. 2042, pp. 147–164. Springer (2000)
20. Dwork, C., McSherry, F., Nissim, K., Smith, A.D.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006. LNCS, vol. 3876, pp. 265–284. Springer (2006). https://doi.org/10.1007/11681878_14
21. Giacobazzi, R., Mastroeni, I.: Proving abstract non-interference. In: J. Marcinkowski, A.T. (ed.) Annual Conf. of the European Association for Computer Science Logic (CSL '04). vol. 3210, pp. 280–294. Springer-Verlag (2004)
22. Giacobazzi, R., Mastroeni, I.: Adjoining classified and unclassified information by abstract interpretation. Journal of Computer Security **18**(5), 751 – 797 (2010)
23. Giacobazzi, R., Logozzo, F., Ranzato, F.: Analyzing program analyses. In: Rajamani, S.K., Walker, D. (eds.) Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015. pp. 261–273. ACM (2015). https://doi.org/10.1145/2676726.2676987
24. Giacobazzi, R., Mastroeni, I.: Abstract non-interference: A unifying framework for weakening information-flow. ACM Trans. Priv. Secur. **21**(2), 9:1–9:31 (2018). https://doi.org/10.1145/3175660
25. Giacobazzi, R., Mastroeni, I., Perantoni, E.: Adversities in abstract interpretation - accommodating robustness by abstract interpretation. ACM Trans. Program. Lang. Syst. **46**(2), 5 (2024). https://doi.org/10.1145/3649309
26. Giacobazzi, R., Ranzato, F., Scozzari, F.: Making abstract interpretations complete. J. ACM **47**(2), 361–416 (2000). https://doi.org/10.1145/333979.333989
27. Goguen, J.A., Meseguer, J.: Security policies and security models. In: 1982 IEEE Symposium on Security and Privacy, Oakland, CA, USA, April 26-28, 1982. pp. 11–20. IEEE Computer Society (1982). https://doi.org/10.1109/SP.1982.10014
28. Grünbaum, B., Klee, V., Perles, M.A., Shephard, G.C.: Convex polytopes, vol. 16. Springer (1967)
29. Hunt, S., Mastroeni, I.: The PER model of abstract non-interference. In: Hankin, C., Siveroni, I. (eds.) Static Analysis, 12th International Symposium, SAS 2005, London, UK, September 7-9, 2005, Proceedings. Lec-

ture Notes in Computer Science, vol. 3672, pp. 171–185. Springer (2005). https://doi.org/10.1007/11547662_13
30. Liew, D., Cogumbreiro, T., Lange, J.: Sound and partially-complete static analysis of data-races in GPU programs. Proc. ACM Program. Lang. **8**(OOPSLA2), 2434–2461 (2024). https://doi.org/10.1145/3689797
31. Logozzo, F.: Towards a quantitative estimation of abstract interpretations. In: Workshop on Quantitative Analysis of Software. Microsoft (June 2009), https://www.microsoft.com/en-us/research/publication/towards-a-quantitative-estimation-of-abstract-interpretations/
32. Mastroeni, I.: On the role of abstract non-interference in language-based security. In: Yi, K. (ed.) 3rd Asian Symp. on Programming Languages and Systems (APLAS '05). Lecture Notes in Computer Science, vol. 3780, pp. 418–433. Springer
33. Mastroeni, I.: Abstract interpretation-based approaches to security - a survey on abstract non-interference and its challenging applications. Electronic Proceedings in Theoretical Computer Science **129**, 41–65 (Sep 2013). https://doi.org/10.4204/eptcs.129.4, http://dx.doi.org/10.4204/EPTCS.129.4
34. Mastroeni, I.: Abstract local completeness - A local form of abstract non-interference. In: Krishna, S., Sankaranarayanan, S., Trivedi, A. (eds.) 26th Verification, Model Checking, and Abstract Interpretation (VMCAI 2025). Lecture Notes in Computer Science, vol. 15530, pp. 3–25. Springer (2025). https://doi.org/10.1007/978-3-031-82703-7_1
35. Mastroeni, I., Pasqua, M.: Domain precision in galois connection-less abstract interpretation. In: Hermenegildo, M.V., Morales, J.F. (eds.) Static Analysis - 30th International Symposium, SAS 2023, Cascais, Portugal, October 22-24, 2023, Proceedings. Lecture Notes in Computer Science, vol. 14284, pp. 434–459. Springer (2023). https://doi.org/10.1007/978-3-031-44245-2_19
36. Mazzucato, D.: Static Analysis by Abstract Interpretation of Quantitative Program Properties. (Analyse Statique par Interprétation Abstraite de Propriétés Quantitatives de Programmes). Ph.D. thesis, École Normale Supérieure, Paris, France (2024), https://tel.archives-ouvertes.fr/tel-04886659
37. Mazzucato, D., Campion, M., Urban, C.: Quantitative input usage static analysis. In: Benz, N., Gopinath, D., Shi, N. (eds.) NASA Formal Methods - 16th International Symposium, NFM 2024, Moffett Field, CA, USA, June 4-6, 2024, Proceedings. Lecture Notes in Computer Science, vol. 14627, pp. 79–98. Springer (2024). https://doi.org/10.1007/978-3-031-60698-4_5
38. Mazzucato, D., Campion, M., Urban, C.: Quantitative static timing analysis. In: Giacobazzi, R., Gorla, A. (eds.) Static Analysis - 31st International Symposium, SAS 2024, Pasadena, CA, USA, October 20-22, 2024, Proceedings. Lecture Notes in Computer Science, vol. 14995, pp. 268–299. Springer (2024). https://doi.org/10.1007/978-3-031-74776-2_11
39. Miné, A.: The octagon abstract domain. In: Burd, E., Aiken, P., Koschke, R. (eds.) Proc. of the 8th Working Conf. on Reverse Engineering, WCRE'01. p. 310. IEEE Computer Society (2001). https://doi.org/10.1109/WCRE.2001.957836
40. O'Hearn, P.W.: Incorrectness logic. Proc. ACM Program. Lang. **4**(POPL), 10:1–10:32 (2020). https://doi.org/10.1145/3371078
41. Sotin, P.: Quantifying the Precision of Numerical Abstract Domains. Research report (Feb 2010), https://inria.hal.science/inria-00457324
42. Urban, C., Müller, P.: An abstract interpretation framework for input data usage. In: Ahmed, A. (ed.) 27th European Symposium on Programming, ESOP 2018. Lecture Notes in Computer Science, vol. 10801, pp. 683–710. Springer (2018). https://doi.org/10.1007/978-3-319-89884-1_24