A Partial Metric Semantics of Higher-Order Types and Approximate Program Transformations

Guillaume Geoffroy, Paolo Pistone

DIAPASoN, Università di Bologna

26th January 2021

How to measure distances between programs?

Why measure distances between programs?

Why measure distances between programs?

Justify approximate transformations:

Why measure distances between programs?

Justify approximate transformations:

```
float Q_rsqrt( float number ) {
  int32_t i; float x2, y;
  const float threehalfs = 1.5F;

  x2 = number * 0.5F;
  y  = number;
  i  = * ( long * ) &y; // evil floating point
                        // bit-level hacking
  i  = 0x5f3759df - ( i >> 1 ) // WTF?
  y  = * ( float * ) &i;
  y  = y * ( threehalfs - ( x2 * y * y ) );
  return y;
}
```

Why measure distances between programs?

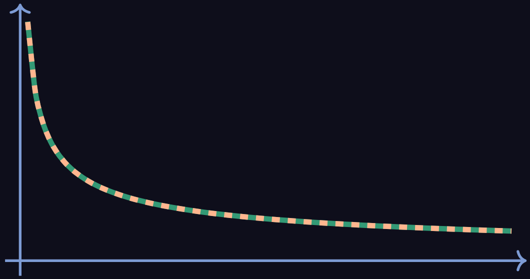
Justify approximate transformations:

```
float Q_rsqrt( float number ) {
  int32_t i; float x2, y;
  const float threehalfs = 1.5F;

  x2 = number * 0.5F;
  y  = number;
  i  = * ( long * ) &y; // evil floating point
                        // bit-level hacking
  i  = 0x5f3759df - ( i >> 1 ) // WTF?
  y  = * ( float * ) &i;
  y  = y * ( threehalfs - ( x2 * y * y ) );
  return y;
}
```

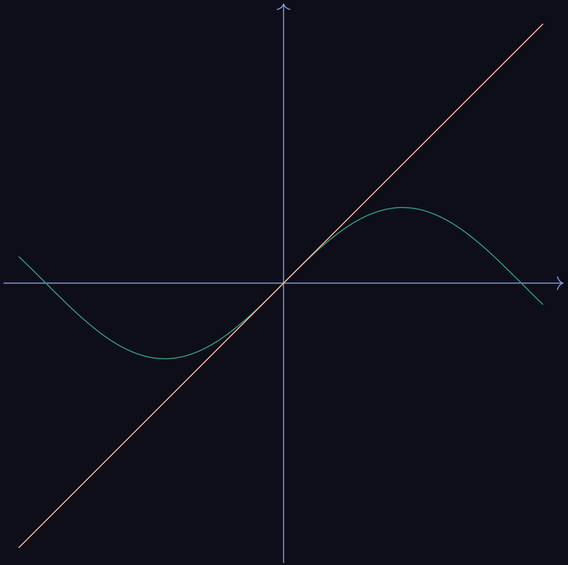
Why measure distances between programs?

Justify approximate transformations:

```
float Q_rsqrt( float number ) {
  int32_t i; float x2, y;
  const float threehalfs = 1.5F;

  x2 = number * 0.5F;
  y  = number;
  i  = * ( long * ) &y; // evil floating point
                        // bit-level hacking
  i  = 0x5f3759df - ( i >> 1 ) // WTF?
  y  = * ( float * ) &i;
  y  = y * ( threehalfs - ( x2 * y * y ) );
  return y;
}
```



A context-dependent transformation



$$|x| \leq 0.1 \rightsquigarrow \delta < 0.2\%$$

$$|x| \leq 0.2 \rightsquigarrow \delta < 0.7\%$$

$$|x| \leq 0.5 \rightsquigarrow \delta < 5\%$$

$$|x| \leq 1 \quad \rightsquigarrow \delta < 20\%$$

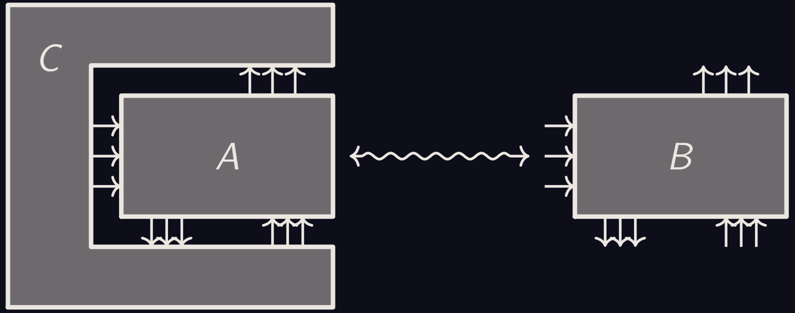
Approximate semantics

[Dal Lago, Gavazzo, Yoshimizu: Differential logical relations]

- Substitute part of a program with a close enough approximation of it,
- Whether this substitution is close enough depends on the context,
- Interaction with the context goes both ways.

Approximate semantics

[Dal Lago, Gavazzo, Yoshimizu: Differential logical relations]



Differential logical relations

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x, y) = |x - y|$,

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x, y) = |x - y|$,
- $d(\sin, \mathrm{id}) = \left(x \mapsto \left|\sin(x) - x\right|\right)$

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x, y) = |x - y|$,
- $d(\sin, \mathrm{id}) = (x, e) \mapsto \bigvee_{y \ st\ |x-y| \leq e} \max \left(\begin{array}{l} |\sin(x) - y|, \\ |\sin(y) - x| \end{array} \right)$,

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x,y) = |x - y|$,
- $d(\sin, \mathrm{id}) = (x, e) \mapsto \bigvee_{y \ st \ |x-y| \leq e} \max \begin{pmatrix} |\sin(x) - y|, \\ |\sin(y) - x| \end{pmatrix}$,
- $d(f, g) = (x, e) \mapsto \bigvee_{y \ st \ d(x,y) \leq e} \max \begin{pmatrix} d(f(x), g(y)), \\ d(f(y), g(x)) \end{pmatrix}$,

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x, y) = |x - y|$,
- $d(\sin, \mathrm{id}) = (x, e) \mapsto \bigvee_{y \text{ st } |x-y| \leq e} \max \begin{pmatrix} |\sin(x) - y|, \\ |\sin(y) - x| \end{pmatrix}$,
- $d(f, g) = (x, e) \mapsto \bigvee_{y \text{ st } d(x,y) \leq e} \max \begin{pmatrix} d(f(x), g(y)), \\ d(f(y), g(x)) \end{pmatrix}$,
- $d(\mathrm{id}, \mathrm{id}) = (x, e) \mapsto e$.

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x, y) = |x - y|$,
- $d(\sin, \mathrm{id}) = (x, e) \mapsto \bigvee_{y \ st \ |x-y| \leq e} \max \begin{pmatrix} |\sin(x) - y|, \\ |\sin(y) - x| \end{pmatrix}$,
- $d(f, g) = (x, e) \mapsto \bigvee_{y \ st \ d(x,y) \leq e} \max \begin{pmatrix} d(f(x), g(y)), \\ d(f(y), g(x)) \end{pmatrix}$,
- $d(\mathrm{id}, \mathrm{id}) = (x, e) \mapsto e$.

Distances between programs of type A measured in $(\llparenthesis A \rrparenthesis, \leq, \bigvee, +)$

Differential logical relations

How distances are defined:

- $x, y \in \mathbb{R} \rightsquigarrow d(x,y) = |x - y|$,
- $d(\sin, \mathrm{id}) = (x, e) \mapsto \bigvee_{y\ st\ |x-y| \leq e} \max \begin{pmatrix} |\sin(x) - y|, \\ |\sin(y) - x| \end{pmatrix}$,
- $d(f, g) = (x, e) \mapsto \bigvee_{y\ st\ d(x,y) \leq e} \max \begin{pmatrix} d(f(x), g(y)), \\ d(f(y), g(x)) \end{pmatrix}$,
- $d(\mathrm{id}, \mathrm{id}) = (x, e) \mapsto e$.

Distances between programs of type A measured in $((\!|A|\!), \leq, \bigvee, +)$
$\rightsquigarrow$ quantale.

Differential logical relations

Type A interpreted by

- A set $[A]$ of denotations,
- A quantale $((\!|A|\!), \leq, +)$ of distances,
- A "distance function" $d : [A] \times [A] \to (\!|A|\!)$

Differential logical relations

Type A interpreted by

- A set $[A]$ of denotations,
- A quantale $((\!|A|\!), \leq, +)$ of distances,
- A "distance function" $d : [A] \times [A] \to (\!|A|\!)$ with $d(x, x) \neq 0$ in general.

Differential logical relations

Type A interpreted by

- A set $[A]$ of denotations,
- A quantale $(\llparenthesis A \rrparenthesis, \leq, +)$ of distances,
- A "distance function" $d : [A] \times [A] \to \llparenthesis A \rrparenthesis$ with $d(x, x) \neq 0$ in general.

Triangular inequality of partial metric spaces:

$$d(x, z) + d(y, y) \leq d(x, y) + d(y, z)$$

Differential logical relations

Type A interpreted by

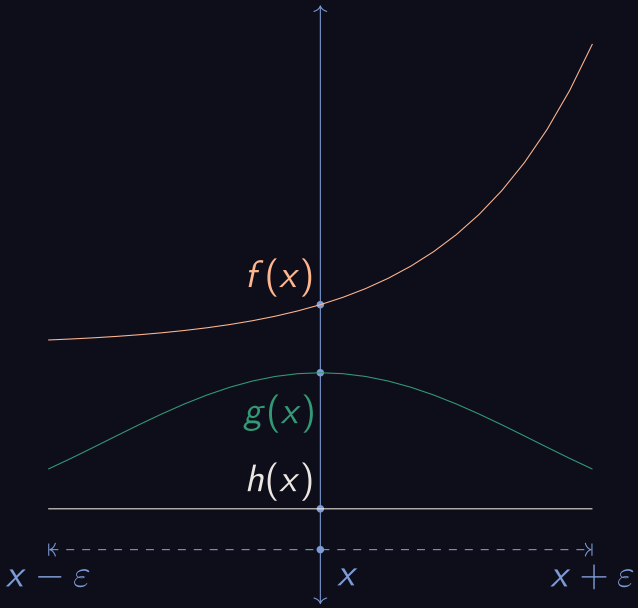
- A set $[A]$ of denotations,
- A quantale $(\llparenthesis A \rrparenthesis, \leq, +)$ of distances,
- A "distance function" $d : [A] \times [A] \to \llparenthesis A \rrparenthesis$ with $d(x, x) \neq 0$ in general.

Triangular inequality of partial metric spaces:

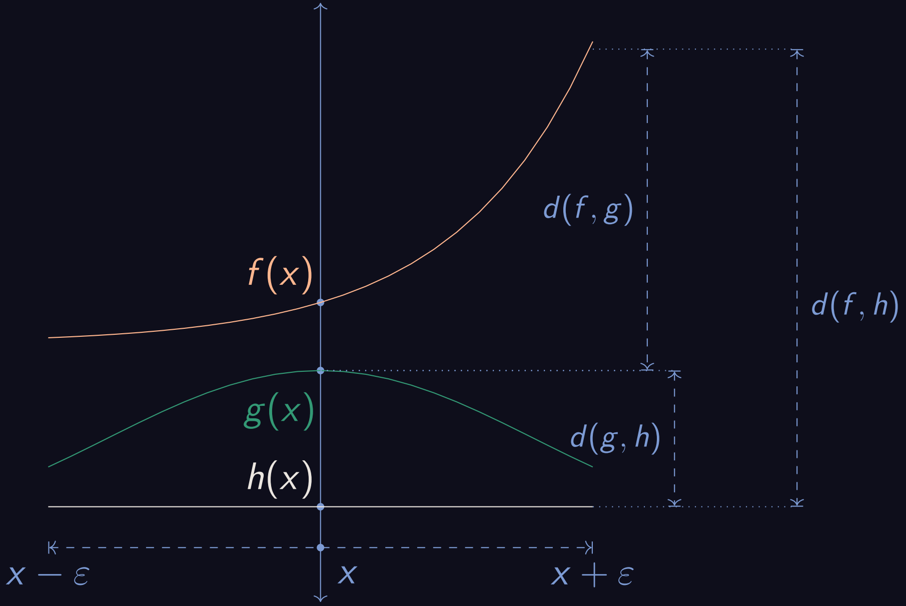
$$d(x, z) + d(y, y) \leq d(x, y) + d(y, z)$$

Not satisfied

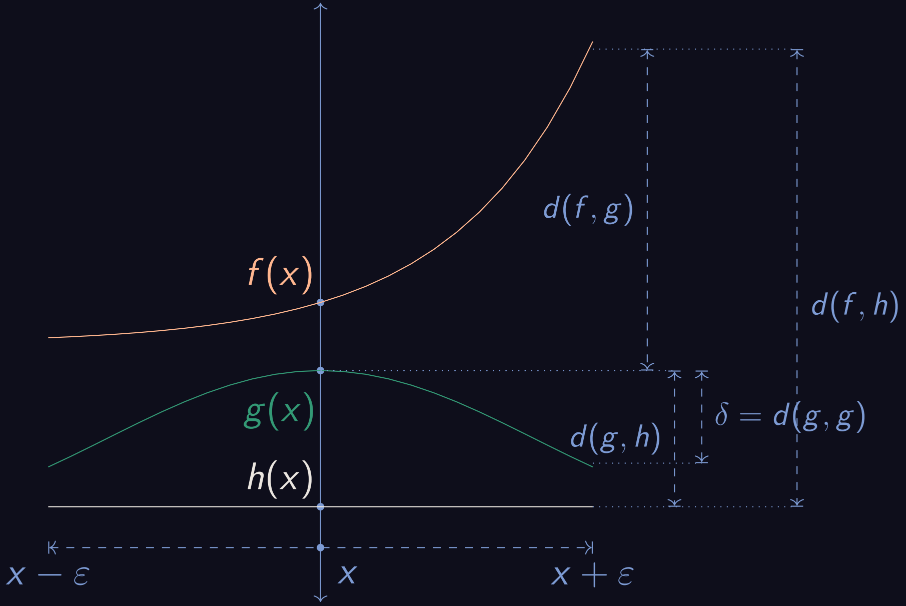
DLRs are not partial metric spaces



DLRs are not partial metric spaces



DLRs are not partial metric spaces



Object of this talk

Two ideas:

- By changing slightly how distances between functions are computed, we obtain partial metric spaces,
- Independently of distances, approximate semantics $\leftrightarrow$ cartesian lax-closed poset-enriched categories.

A change in point of view:

- Forget about reference points

Object of this talk

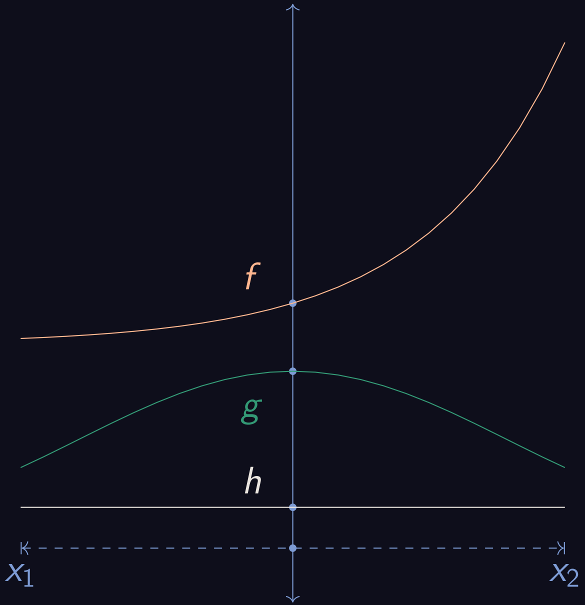
Two ideas:

- By changing slightly how distances between functions are computed, we obtain partial metric spaces,
- Independently of distances, approximate semantics $\leftrightarrow$ cartesian lax-closed poset-enriched categories.

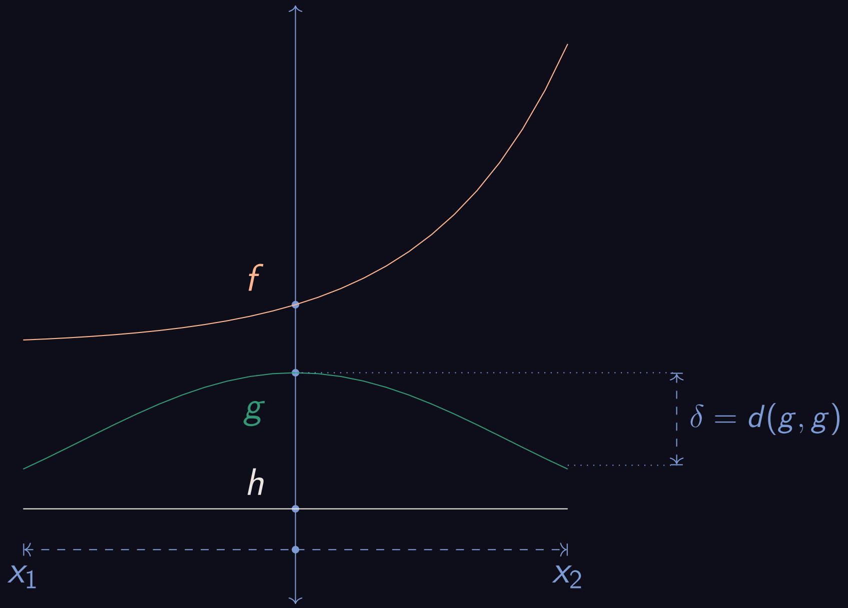
A change in point of view:

- Forget about reference points: $1 \pm 0.1 \rightsquigarrow [0.9, 1.1]$.

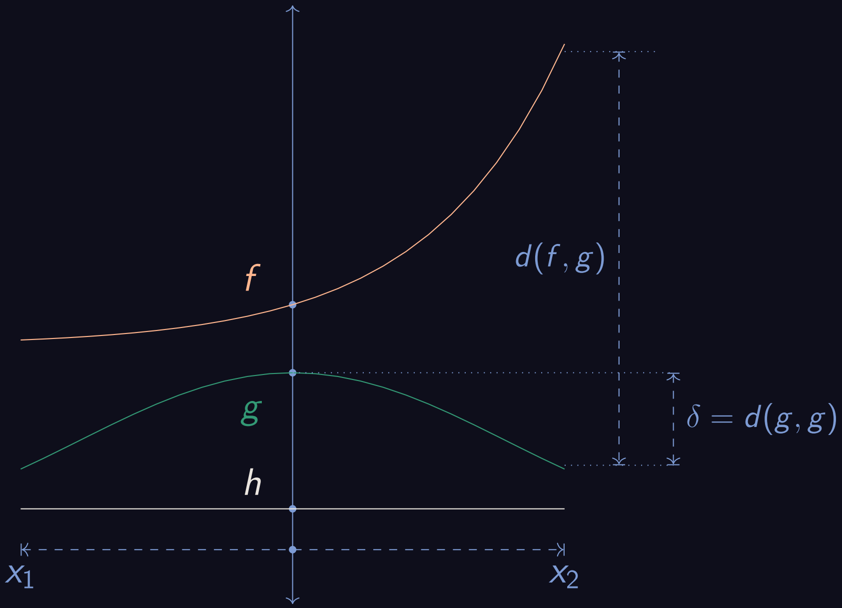
Removing the reference: balls ⇝ intervals



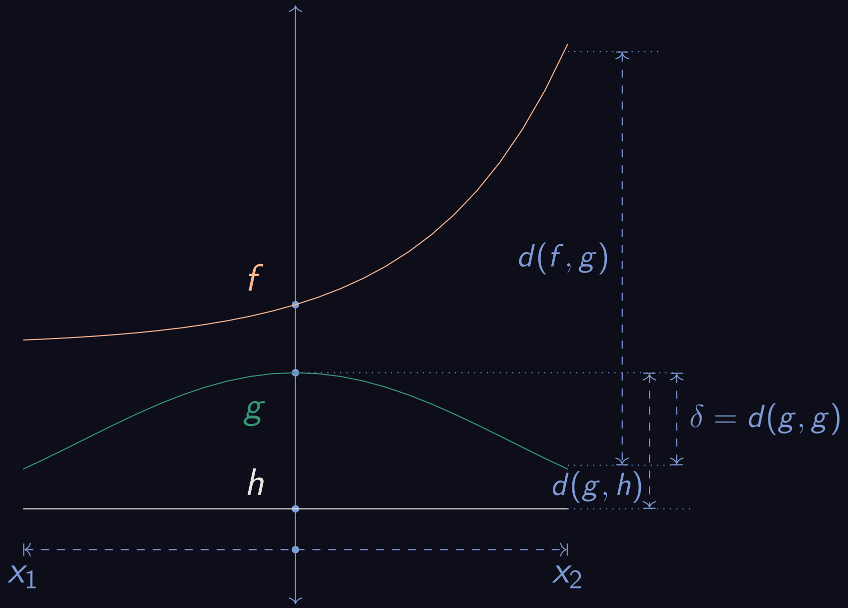
Removing the reference: balls $\rightsquigarrow$ intervals



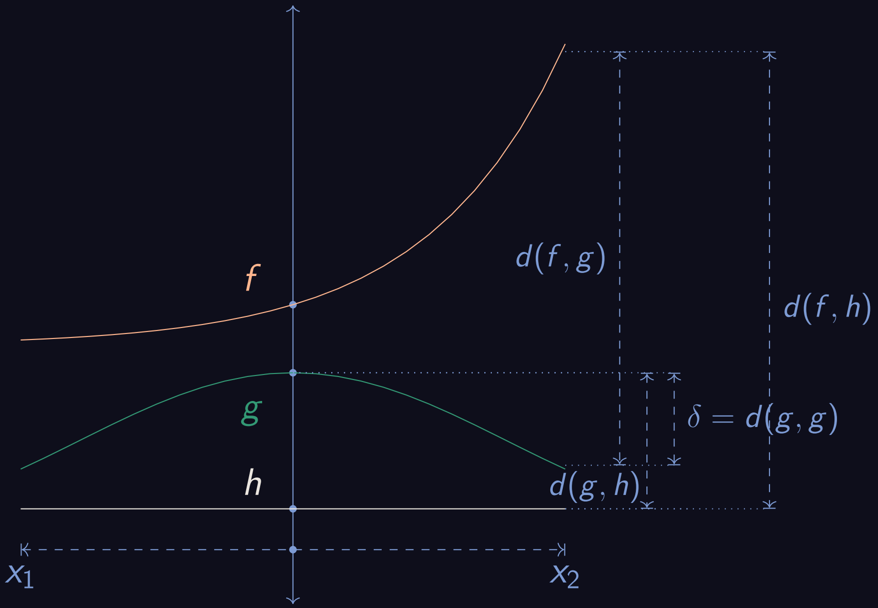
Removing the reference: balls $\rightsquigarrow$ intervals



Removing the reference: balls ⇝ intervals

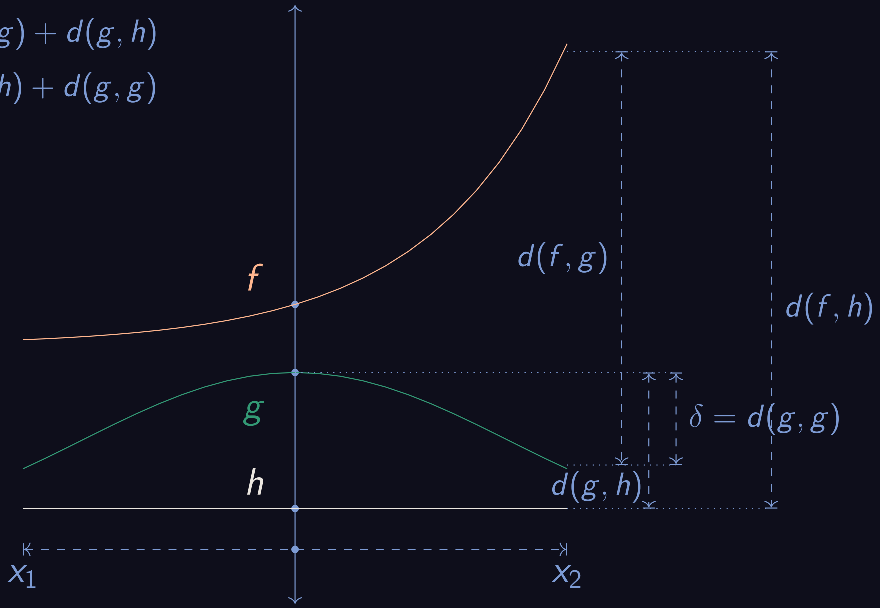


Removing the reference: balls ⇝ intervals



Removing the reference: balls ⇝ intervals

$$d(f,g) + d(g,h) \geq d(f,h) + d(g,g)$$



Diameter spaces

To each simple type A, asssociate

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*:
  - $[\text{Real}] = \mathbb{R}$,
  - $[A \times B] = [A] \times [B]$,
  - $[A \to B] = [A] \to [B]$,

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*:
  - $[\mathrm{Real}] = \mathbb{R}$,
  - $[A \times B] = [A] \times [B]$,
  - $[A \to B] = [A] \to [B]$,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*:
  - $[\![\mathrm{Real}]\!]$ = non-empty compact intervals $+ \mathbb{R}$,
  - $[\![A \times B]\!]$ = products of intervals,
  - $[\![A \to B]\!] = \{f \; st \; \forall x, f(x) \in \varphi(x)\}$ for all $\varphi \in [A] \to [\![B]\!]$,

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*:
  - $[\mathrm{Real}] = \mathbb{R}$,
  - $[A \times B] = [A] \times [B]$,
  - $[A \to B] = [A] \to [B]$,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*:
  - $[\![\mathrm{Real}]\!] =$ non-empty compact intervals $+ \mathbb{R}$,
  - $[\![A \times B]\!] =$ products of intervals,
  - $[\![A \to B]\!] = \{f \;\; st\; \forall x, f(x) \in \varphi(x)\}$ for all $\varphi \in [A] \to [\![B]\!]$,
- a quantale $(\![A]\!)$ of *distances*:
  - $(\![\mathrm{Real}]\!) = [0, +\infty]$,
  - $(\![A \times B]\!) = (\![A]\!) \times (\![B]\!)$,
  - $(\![A \to B]\!) = [\![A]\!] \to (\![B]\!)$,

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*:
  - $[\text{Real}] = \mathbb{R}$,
  - $[A \times B] = [A] \times [B]$,
  - $[A \to B] = [A] \to [B]$,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*:
  - $[\![\text{Real}]\!] =$ non-empty compact intervals $+ \mathbb{R}$,
  - $[\![A \times B]\!] =$ products of intervals,
  - $[\![A \to B]\!] = \{f \ st\ \forall x, f(x) \in \varphi(x)\}$ for all $\varphi \in [A] \to [\![B]\!]$,
- a quantale $(\!|A|\!)$ of *distances*:
  - $(\!|\text{Real}|\!) = [0, +\infty]$,
  - $(\!|A \times B|\!) = (\!|A|\!) \times (\!|B|\!)$,
  - $(\!|A \to B|\!) = [\![A]\!] \to (\!|B|\!)$,
- a *diameter function* $\delta_A : [\![A]\!] \to (\!|A|\!)$:

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*:
  - $[\![\text{Real}]\!] =$ non-empty compact intervals $+ \mathbb{R}$,
  - $[\![A \times B]\!] =$ products of intervals,
  - $[\![A \to B]\!] = \{f \;\; st \; \forall x, f(x) \in \varphi(x)\}$ for all $\varphi \in [A] \to [\![B]\!]$,
- a quantale $(\!|A|\!)$ of *distances*:
  - $(\!|\text{Real}|\!) = [0, +\infty]$,
  - $(\!|A \times B|\!) = (\!|A|\!) \times (\!|B|\!)$,
  - $(\!|A \to B|\!) = [\![A]\!] \to (\!|B|\!)$,
- a *diameter function* $\delta_A : [\![A]\!] \to (\!|A|\!)$:
  - $\delta_{\text{Real}} = [x_1, x_2] \mapsto x_2 - x_1$,
  - $\delta_{A \times B} = a \times b \mapsto (\delta_A(a), \delta_B(b))$,
  - $\delta_{A \to B} = F \mapsto (a \mapsto \delta_B(\{f(x);\; f \in F, x \in a\}))$.

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*,
- a quantale $(\!|A|\!)$ of *distances*,
- a *diameter function* $\delta_A : [\![A]\!] \to (\!|A|\!)$.

Diameter spaces

To each simple type A, asssociate

- a set $[A]$ of *denotations*,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*,
- a quantale $(\!|A|\!)$ of *distances*,
- a *diameter function* $\delta_A : [\![A]\!] \to (\!|A|\!)$.

Let $d(x, y) = \delta(\text{smallest interval containing } x \text{ and } y)$

Diameter spaces

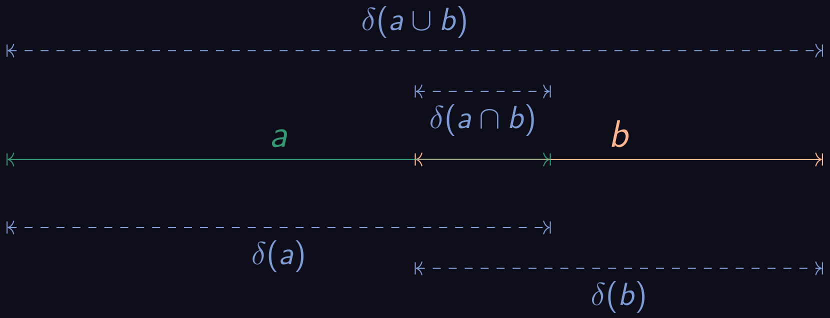
To each simple type A, asssociate

- a set $[A]$ of *denotations*,
- a set $[\![A]\!] \subseteq \mathcal{P}([A]) \setminus \{\emptyset\}$ of *intervals*,
- a quantale $(\!|A|\!)$ of *distances*,
- a *diameter function* $\delta_A : [\![A]\!] \to (\!|A|\!)$.

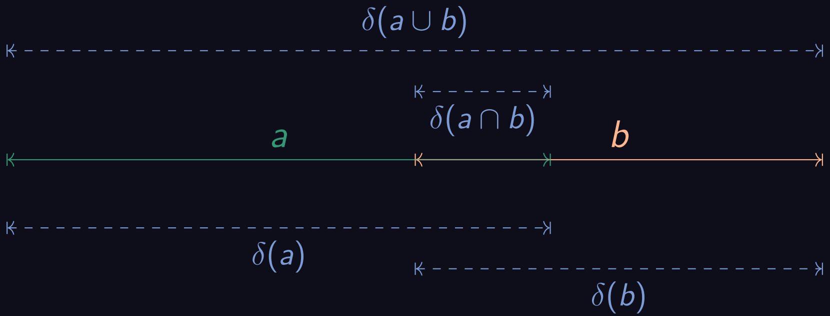
Let $d(x, y) = \delta(\text{smallest interval containing } x \text{ and } y)$:

Do we have $d(x, z) + d(y, y) \leq d(x, y) + d(y, z)$?

Sub-modularity

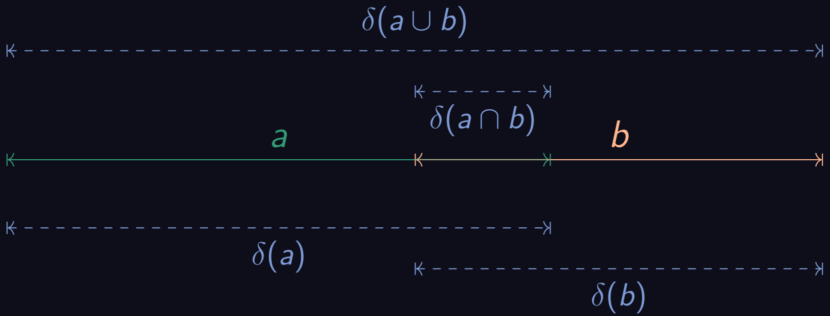


Sub-modularity



For all types A, if $a \wedge b \neq \emptyset$, $\delta_A(a \vee b) + \delta_A(a \wedge b) \leq \delta_A(a) + \delta_A(b)$

Sub-modularity



For all types A, if $a \wedge b \neq \emptyset$, $\delta_A(a \vee b) + \delta_A(a \wedge b) \leq \delta_A(a) + \delta_A(b)$

$\rightsquigarrow d(x, z) + d(y, y) \leq d(x, y) + d(y, z)$

Approximate specifications

Approximate specifications

Definition: An *approximate function* from A to B is an interval $f \subseteq [\![A \to B]\!]$.

Approximate specifications

Definition: An *approximate function* from A to B is an interval $f \subseteq [\![A \to B]\!]$.

Types and approximate functions do not form a category:
no associativity

Approximate specifications

Definition: An *approximate function* from A to B is a monotone map from $[\![A]\!]$ to $[\![B]\!]$.

Approximate specifications

Definition: An *approximate function* from A to B is a monotone map from $[\![A]\!]$ to $[\![B]\!]$.

Types and approximate functions do form a category

Approximate specifications

Definition: An *approximate function* from A to B is a monotone map from $[\![A]\!]$ to $[\![B]\!]$.

Types and approximate functions do form a category

$$[\![A]\!] \to [\![B]\!] \underset{\text{unpack}}{\overset{\text{pack}}{\rightleftarrows}} [\![A \to B]\!]$$

Approximate specifications

Definition: An *approximate function* from A to B is a monotone map from $[\![A]\!]$ to $[\![B]\!]$.

Types and approximate functions do form a category

$$[\![A]\!] \to [\![B]\!] \underset{\text{unpack}}{\overset{\text{pack}}{\rightleftarrows}} [\![A \to B]\!]$$

$$\text{unpack}(\text{pack}(f)) \leq f \qquad\qquad \text{pack}(\text{unpack}(g)) \geq g$$

Approximate specifications

Definition: An *approximate function* from A to B is a monotone map from $[\![A]\!]$ to $[\![B]\!]$.

Types and approximate functions do form a category

$$[\![A]\!] \to [\![B]\!] \underset{\text{unpack}}{\overset{\text{pack}}{\rightleftarrows}} [\![A \to B]\!]$$

$$\text{unpack}(\text{pack}(f)) \leq f \qquad \text{pack}(\text{unpack}(g)) \geq g$$

$\rightsquigarrow$ cartesian lax-closed category

Thank you!