beyond image-finiteness: labelled transition systems as a Stone space

Michael Huth
Department of Computing
Imperial College London

acknowledgments: Radha Jagadeesan, David Schmidt, and referees

outline

0 motivation

1 domain of modal transition systems

2 Stone space of labelled transition systems

3 compactness theorem & consistency measure

4 conclusions

0 motivation

unify related strands of work:

- metric semantics of processes (de Bakker & Zucker'82)
- under-specification & refinement (Larsen & Thomsen'88)
- domain theory for transition systems (Abramsky'91)
- classical spaces as maximal-points spaces (Lawson'97)

do this for finite set of events Act

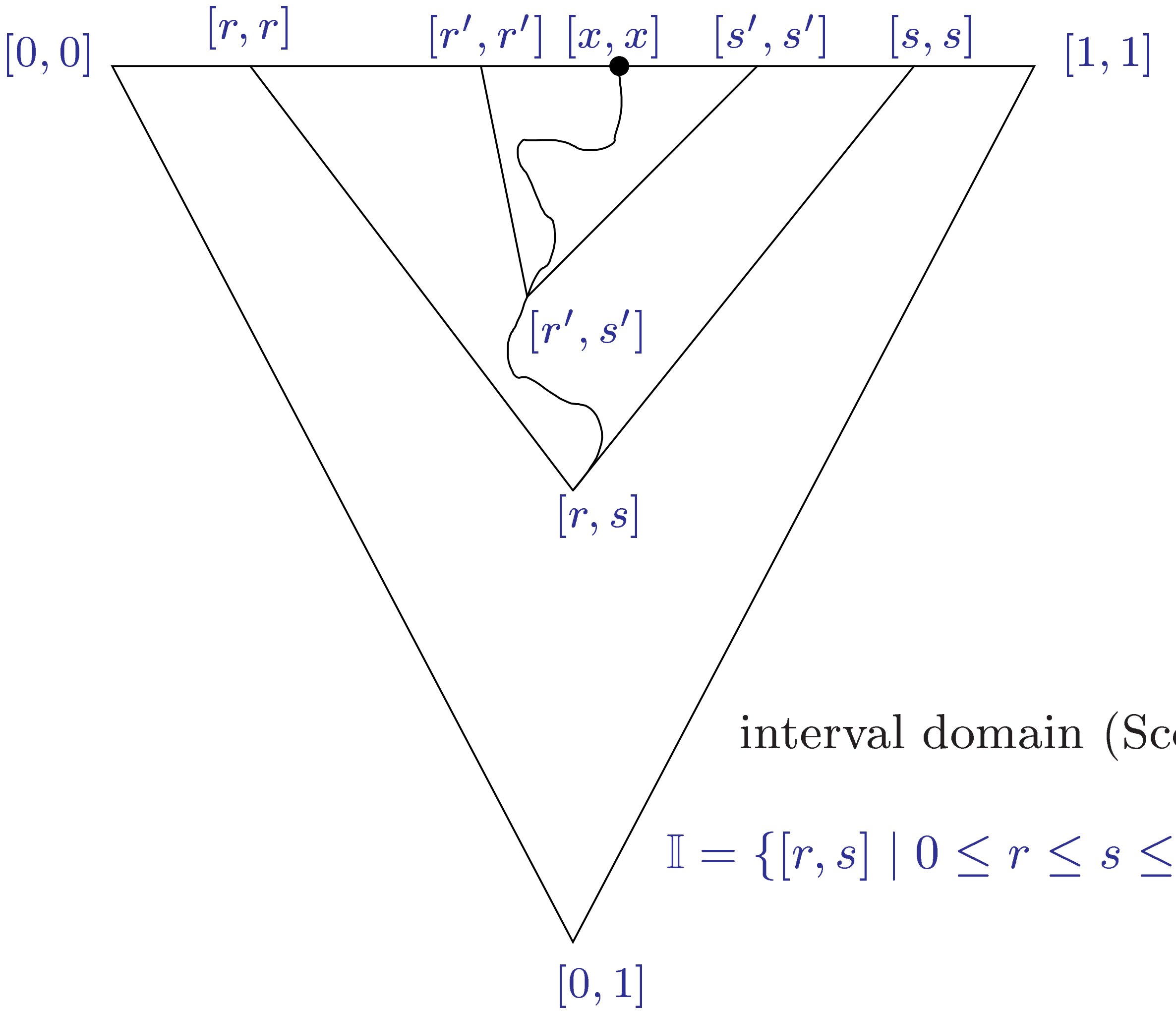
0' motivation cont'd

comprehend structure of refinement:

- compactness theorem for temporal logic
- consistency measure for under-specification
- refinement as inverse containment of implementations*
- model checking multiple models collectively*

* not in this talk or paper

1 domain of modal transition systems



interval domain (Scott'72)

$$\mathbb{I} = \{[r,s] \mid 0 \leq r \leq s \leq 1\}$$

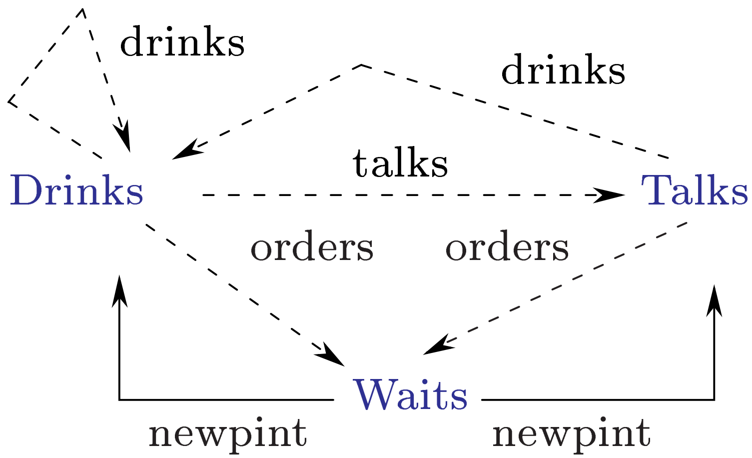
properties of interval domain

- intervals as partial reals
- $\max(\mathbb{I}) \equiv [0, 1]$
- Scott-topology on $\mathbb{I}$ induces Euclidean topology on $\max(\mathbb{I})$
- intervals densely approximate reals

objectives:

- seek domain $\mathbb{D}$ for modal transition systems and similar facts for labelled transition systems as $\max(\mathbb{D})$
- get monotone consistency measure $c\colon \mathbb{D} \times \mathbb{D} \to \mathbb{I}$

modal transition system of 'pub behavior'



modal transition system $M = (\Sigma, R^a, R^c)$

- $\Sigma = \{\text{Drinks}, \text{Talks}, \text{Waits}\}$ state space
- R^a solid lines (*contractual guarantees*)
- $R^c \setminus R^a$ dashed lines (*contractual possibilities*)

refinement

$Q \subseteq \Sigma \times \Sigma$ is *refinement* (Larsen'89, Dams 96) iff $(s, t) \in Q$ implies

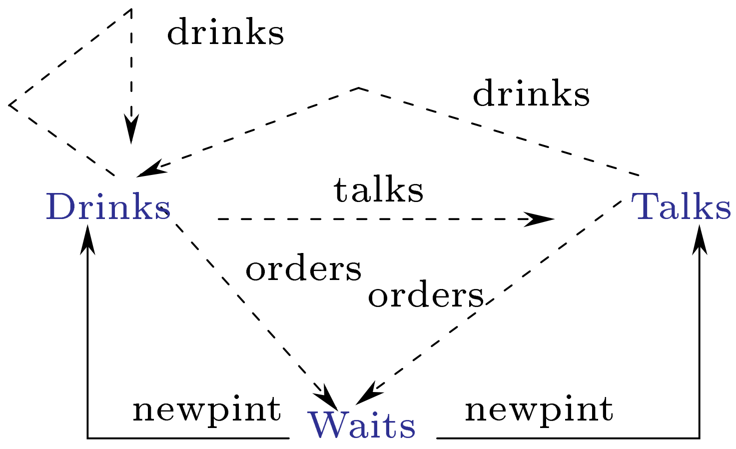
1. if $(s, \alpha, s') \in R^a$, there is $(t, \alpha, t') \in R^a$ with $(s', t') \in Q$
2. if $(t, \alpha, t') \in R^c$, there is $(s, \alpha, s') \in R^c$ with $(s', t') \in Q$

t *refines, is abstracted by,* s iff (there is such a Q with $(s, t) \in Q$)

intuition:

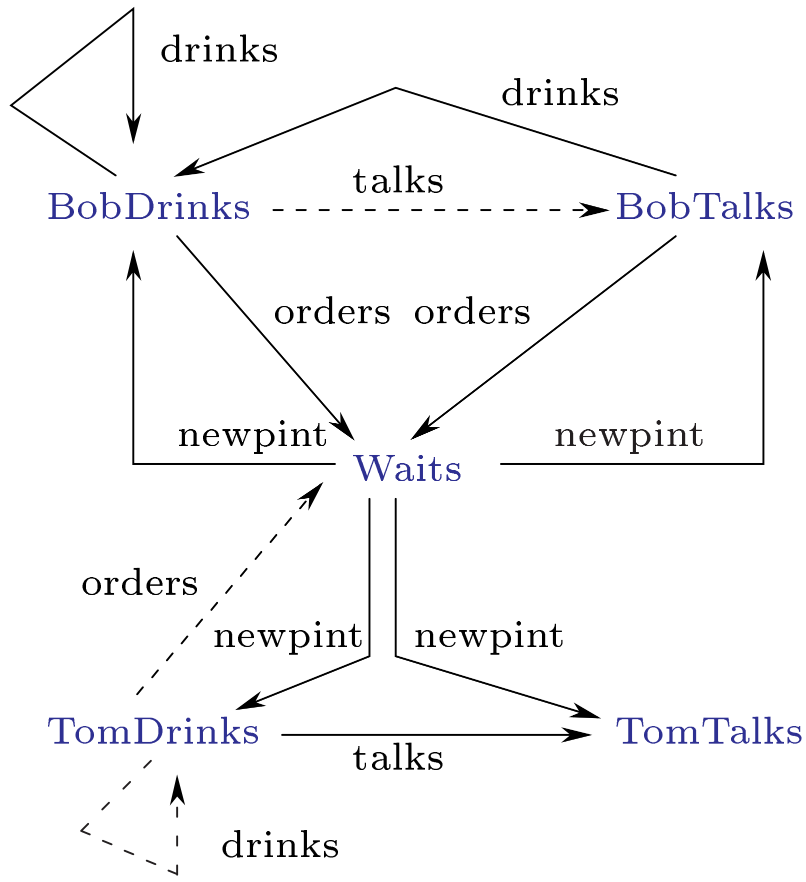
- solid lines have to be implemented or happen
- only dashed and solid lines may be implemented or may happen

refinement example



BobDrinks refines Drinks,

TomTalks refines Talks ...



semantics of Hennessy-Milner logic

$$\phi ::= \text{true} \;\mid\; \neg\phi \;\mid\; \langle\alpha\rangle\phi \;\mid\; \phi \wedge \phi \qquad (\alpha \in Act)$$

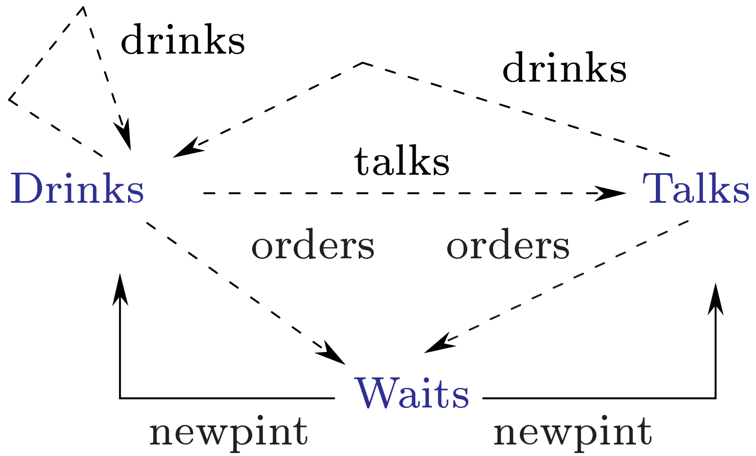
judgments $s \models^m \phi$ for $m \in \{a, c\} \equiv \{\text{is } \mathbf{a}\text{sserted}, \text{may be } \mathbf{c}\text{onsistent}\}$

- $s \models^m \text{true}$
- $s \models^m \neg\phi$ iff not $s \models^{\neg m} \phi$ where $\neg a = c$ and $\neg c = a$
- $s \models^m \langle\alpha\rangle\phi$ iff (for some $(s, \alpha, s') \in R^m$, $s' \models^m \phi$)
- $s \models^m \phi_1 \wedge \phi_2$ iff ($s \models^m \phi_1$ and $s \models^m \phi_2$)

implies

- $s \models^m \phi_1 \vee \phi_2$ iff ($s \models^m \phi_1$ or $s \models^m \phi_2$) for $\phi_1 \vee \phi_2 = \neg(\neg\phi_1 \wedge \neg\phi_2)$
- $s \models^m [\alpha]\phi$ iff (for all $(s, \alpha, s') \in R^{\neg m}\mathbf{!}$, $s' \models^m \phi$) for $[\alpha] = \neg\langle\alpha\rangle\neg$

example check



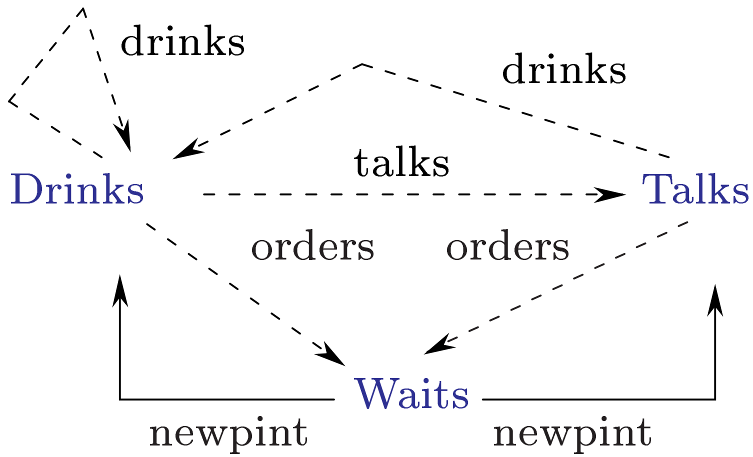
$\text{Talks} \models^c \langle \text{drinks} \rangle \text{true}$ as $(\text{Talks}, \text{drinks}, \text{Drinks}) \in R^c$

$\Rightarrow \qquad \text{Talks} \not\models^a \neg \langle \text{drinks} \rangle \text{true}$

$\text{Talks} \not\models^a \langle \text{drinks} \rangle \text{true}$ as there is no $(\text{Talks}, \text{drinks}, x) \in R^a$

$\Rightarrow \qquad \text{Talks} \not\models^a \langle \text{drinks} \rangle \text{true} \vee \neg \langle \text{drinks} \rangle \text{true}$ (tautology)

example check cont'd



$\text{Waits} \not\models^a [\text{newPint}][\text{talks}](\langle\text{drinks}\rangle\text{true} \vee \neg\langle\text{drinks}\rangle\text{true})$ as

- $(\text{Waits}, \text{newPint}, \text{Drinks})(\text{Drinks}, \text{talks}, \text{Talks})$ is R^c-path
- $\text{Talks} \not\models^a \langle\text{drinks}\rangle\text{true} \vee \neg\langle\text{drinks}\rangle\text{true}$

intuition: M "is" labelled transitions system iff M passes all checks $[\delta_1][\delta_2]\ldots[\delta_n](\langle\alpha\rangle\phi_k \vee \neg\langle\alpha\rangle\phi_k)$ for suitable ϕ_k

domain model (hjs'04)

- initial, ω-algebraic bifinite, solution $\mathbb{D}$ of

$$D = \prod_{\alpha \in Act} \mathcal{M}[D]$$

- $\mathcal{M}[D]$ mixed powerdomain of D (Heckmann'90, Gunter'92)
- elements (L, U): $L = \Downarrow L$, $U = \Uparrow U$ Lawson-closed; $L = \Downarrow(L \cap U)$
  where $\Downarrow X = \{d \in D \mid \exists x \in X : d \leq x\}$
  $\Uparrow X = \{d \in D \mid \exists x \in X : x \leq d\}$
- $(L, U) \leq (L', U')$ iff $L \subseteq L'$ and $U' \subseteq U$
- $\perp_{\mathbb{D}} = (\{\}, \mathbb{D})_{\alpha \in Act} \in \mathbb{D}$ models universal stub
- $(\{\}, \{\})_{\alpha \in Act} \in \max(\mathbb{D})$ models deadlock

$\mathbb{D}$ as modal transition system $\mathcal{D}$ (hjs'04)

recursion $d = ((d^a_\alpha, d^c_\alpha))_{\alpha \in Act}$ from $\mathbb{D} = \prod_{\alpha \in Act} \mathcal{M}[\mathbb{D}]$

modal transition system $\mathcal{D} = (\mathbb{D}, \mathbb{R}^a, \mathbb{R}^c)$ where

$$\mathbb{R}^a = \{(d, \alpha, d') \mid d' \in d^a_\alpha\}$$

$$\mathbb{R}^c = \{(d, \alpha, d') \mid d' \in d^c_\alpha\}$$

d^a_α (d^c_α) set of $\mathbb{R}^a_\alpha$-successors ($\mathbb{R}^c_\alpha$-successors) of d

minor detail: $\mathbb{R}^a \not\subseteq \mathbb{R}^c$ but $\mathcal{D}$ refinement-equivalent to *modal* transition system $(\mathbb{D}, \mathbb{R}^a \cap \mathbb{R}^c, \mathbb{R}^c)$, $\mathcal{D}$ always refers to the latter

universality and full abstraction (hjs'04)

- *universality:* exists $\langle\!| M, i |\!\rangle \in \mathbb{D}$ for any image-finite M with initial state i such that (M, i) and $(\mathcal{D}, \langle\!| M, i |\!\rangle)$ are refinement-equivalent
- *full abstraction:* for all $d, e \in \mathbb{D}$: $d \leq e$ iff $(\mathcal{D}, e)$ refines $(\mathcal{D}, d)$

proof of universality: unwind and truncate modal transition system (may-leaves and deadlock-leaves), do a continuity argument

proof of full abstraction: standard argument but for $\models^a$

2 Stone space of labelled transition systems

Scott-topology: $\sigma_{\mathbb{D}} = \{\Uparrow k \mid k \in \mathbf{K}(\mathbb{D})\}$ where $\mathbf{K}(\mathbb{D}) =$ embeddings of truncated modal transition systems

Lawson-topology: $\lambda_{\mathbb{D}} = \{\Uparrow k \setminus \Uparrow l \mid k, l \in \mathbf{K}(\mathbb{D})\}$

Lawson-condition (Lawson'97) crucial: topology $\tau_{\mathbb{X}} = \{U \cap \max(\mathbb{D}) \mid U \in \sigma_{\mathbb{D}}\}$ equals $\{V \cap \max(\mathbb{D}) \mid V \in \lambda_{\mathbb{D}}\}$ on $\mathbb{X} = \max(\mathbb{D})$ as $\mathbb{D}$ bifinite

two-step proof:

1. $(\mathbb{X}, \tau_{\mathbb{X}})$ Stone space
2. $\mathbb{X} = \max(\mathbb{D})$ "is" quotient space of all labelled transition systems under bisimulation

$(\mathbb{X}, \tau_{\mathbb{X}})$ as Stone space

step 1: $\tau_{\mathbb{X}}$ is

- *compact:* for all $\mathcal{U} \subseteq \tau_{\mathbb{X}}$ with $\mathbb{X} \subseteq \bigcup \mathcal{U}$ there is finite $\mathcal{F} \subseteq \mathcal{U}$ with $\mathbb{X} \subseteq \bigcup \mathcal{F}$
- *Hausdorff:* for all $x \neq x'$ in $\mathbb{X}$ there are $O, O' \in \tau_{\mathbb{X}}$ with $x \in O$, $x' \in O'$ and $O \cap O' = \{\}$
- *zero-dimensional:* every $U \in \tau_{\mathbb{X}}$ is union of sets that are $\tau_{\mathbb{X}}$-open *and* $\tau_{\mathbb{X}}$-closed

Lawson condition $\Rightarrow$ $\tau_{\mathbb{X}}$ zero-dimensional & Hausdorff

as $\lambda_{\mathbb{D}}$ compact, suffices to show $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed

complete set of tests for maximality

- for $\Delta = \delta_1\delta_2\ldots\delta_n \in Act^*$, $\alpha \in Act$, $k \in \mathbf{K}(\mathbb{D})$ define a test

$$\psi_k^{\Delta,\,\alpha} = [\delta_1][\delta_2]\ldots[\delta_n](\langle\alpha\rangle\phi_k \vee \neg\langle\alpha\rangle\phi_k)$$

  where $(\mathcal{D}, d)\models^a \phi_k$ iff $k \le d$ — full abstraction in (hjs'04)

- for $m \in \{a, c\}$ set $\| \phi \|^m = \{d \in \mathbb{D} \mid (\mathcal{D}, d)\models^m \phi\}$
- pass all tests: $C = \bigcap\{\| \psi_k^{\Delta,\,\alpha} \|^a \mid \Delta \in Act^*, \alpha \in Act, k \in \mathbf{K}(\mathbb{D})\}$

plan:

- show each $\| \phi \|^a$ is $\lambda_{\mathbb{D}}$-closed
- show $C = \max(\mathbb{D})$

proof sketch: $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$-closed

1. $\| \phi \|^a$ is $\lambda_{\mathbb{D}}$-closed: mutual structural induction on ϕ in

   "$\| \phi \|^c$ and $\| \phi \|^a$ are $\lambda_{\mathbb{D}}$-closed *and* $\lambda_{\mathbb{D}}$-open"

2. $\max(\mathbb{D}) \subseteq C$: as C is $\lambda_{\mathbb{D}}$-closed, suffices to show embeddings of labelled transition systems are in C and dense in $\max(\mathbb{D})$

3. $C \subseteq \max(\mathbb{D})$: exploit fine structure of $(\mathbb{D}, \leq)$ and that $d \in C$ passes all tests $d \models^a \psi_k^{\Delta, \alpha}$

$\Rightarrow$ $(\mathbb{X}, \tau_{\mathbb{X}})$ Stone space

$\max(\mathbb{D})$ as quotient space of bisimulation

1. $(M, i) \mapsto \langle\!|\, M, i \,|\!\rangle$ extends to non-image-finite case, labelled transition systems embedded into $\max(\mathbb{D})$
2. any $(\mathcal{D}, d)$ with $d \in \max(\mathbb{D})$ refinement-equivalent to a labelled transition system
3. $\mathbb{X} = \prod_{\alpha \in Act} Compact[\mathbb{X}, \tau_{\mathbb{X}}]$ where x_α is $\tau_{\mathbb{X}}$-compact set of α-successors for $x = (x_\alpha)_{\alpha \in Act} \in \mathbb{X}$

3 compactness theorem & consistency measure

given:

- modal transition system with initial state s, Γ set of formulas of Hennessy-Milner logic
- for all finite subsets Π of Γ, $\bigwedge \Pi$ satisfiable over labelled transition systems that refine s

$(\mathbb{X}, \tau_{\mathbb{X}})$ Stone space $\Rightarrow$ there is labelled transition system that refines s and satisfies all formulas of Γ

for $s = \perp_{\mathbb{D}}$: familiar compactness theorem

3' compactness theorem & consistency measure

two familiar metrics for $k_0, k_1, \ldots$ enumeration of $\mathbf{K}(\mathbb{D})$:

$$d_{\mathbb{D}}(d,e) = \mathit{inf}\{2^{-n} \mid \forall i \leq n\colon k_i \leq d \text{ iff } k_i \leq e\}$$
$$d_{\mathbb{X}}(x,y) = \mathit{inf}\{2^{-n} \mid \forall i \leq n\colon k_i \leq x \text{ iff } k_i \leq y\}$$

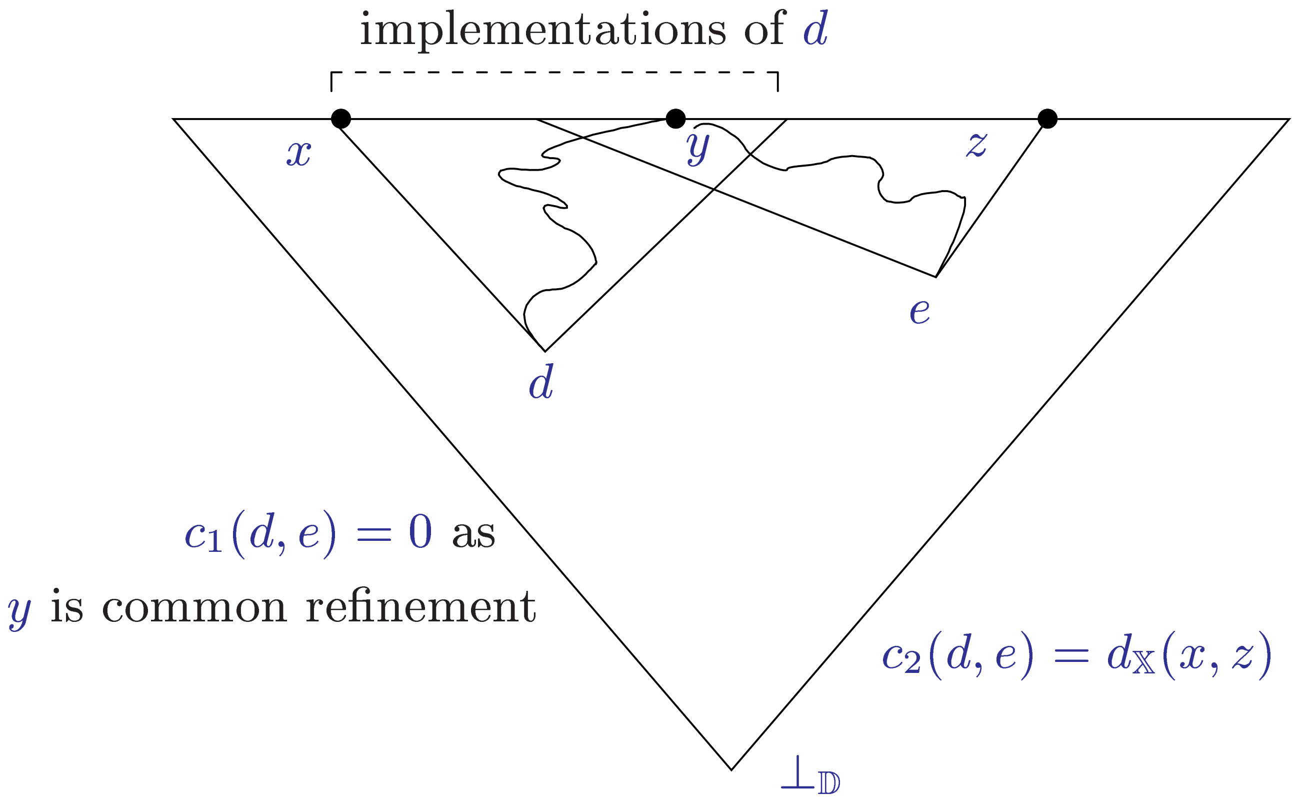
monotone map $(d,e) \mapsto [c_1(d,e), c_2(d,e)]\colon \mathbb{D} \times \mathbb{D} \to \mathbb{I}$

$$c_1(d,e) = \mathit{inf}\{d_{\mathbb{X}}(x,y) \mid x \in {\uparrow}d \cap \max(\mathbb{D}),\ y \in {\uparrow}e \cap \max(\mathbb{D})\}$$
$$c_2(d,e) = \mathit{sup}\{d_{\mathbb{X}}(x,y) \mid x \in {\uparrow}d \cap \max(\mathbb{D}),\ y \in {\uparrow}e \cap \max(\mathbb{D})\}$$

$(\mathbb{X}, \tau_{\mathbb{X}})$ Stone space $\Rightarrow$ $c_1(d,e) = 0$ iff ($(\mathcal{D}, d)$ and $(\mathcal{D}, e)$ have common refinement)

$\Rightarrow$ $c_1(d,e)$ sound an optimistic measure of degree of inconsistency

example of common refinement



4 conclusions

this page is intentionally left blank