refinement is complete for implementations

Michael Huth
Department of Computing
Imperial College London

acknowledgments: Radha Jagadeesan and David Schmidt

outline

0 motivation

1 modal transition systems & refinement

2 domain model for refinement

3 completeness of refinement for implementations

4 conclusions

0 motivation

unify related strands of work:

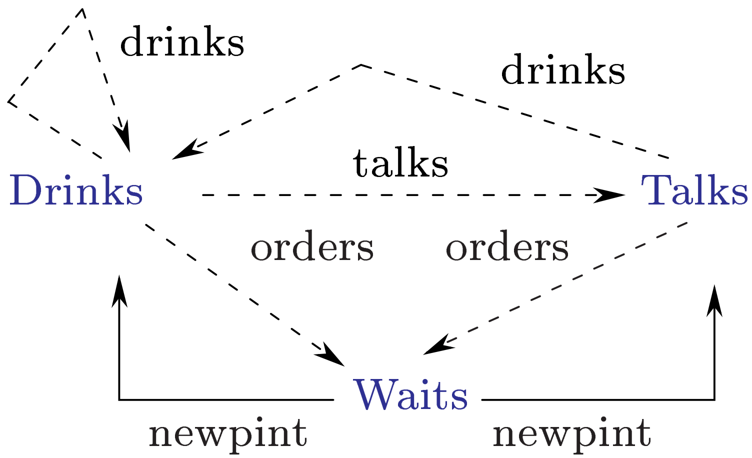
- metric semantics of processes (de Bakker & Zucker'82)
- under-specification & refinement (Larsen & Thomsen'88)
- domain theory for transition systems (Abramsky'91)
- classical spaces as maximal-points spaces (Lawson'97)

do this for finite set of events Act

exploit unification to determine structure of refinement:
refinement as *inverse containment of implementations*

1 modal transition systems & refinement

modal transition system of 'pub behavior'



modal transition system $M = (\Sigma; R^a, R^c \subseteq \Sigma \times Act \times \Sigma)$

- $\Sigma = \{\text{Drinks}, \text{Talks}, \text{Waits}\}$ state space
- R^a solid lines and $\Sigma \times Act \times \Sigma \setminus R^c$ (*contractual guarantees*)
- $R^c \setminus R^a$ dashed lines (*contractual possibilities*)
- consistency condition on transition relations: $R^a \subseteq R^c$

refinement

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

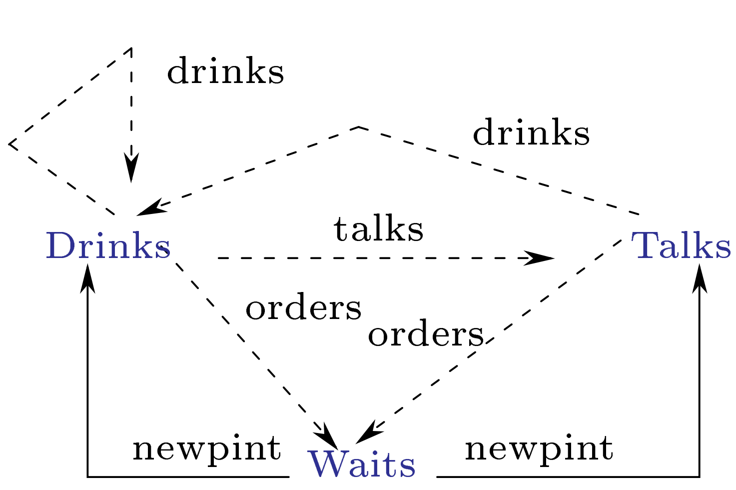
1. if $(s, \alpha, s') \in R^a$, there is $(t, \alpha, t') \in R^a$ with $(s', t') \in Q$
2. if $(t, \alpha, t') \in R^c$, there is $(s, \alpha, s') \in R^c$ with $(s', t') \in Q$

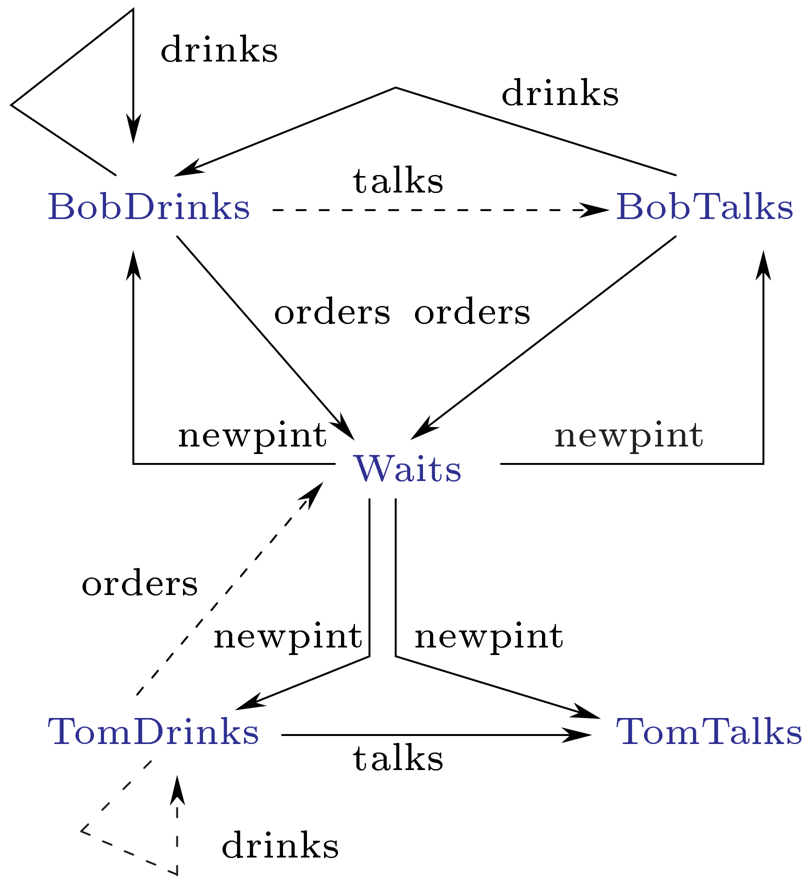
t *refines, is abstracted by,* s iff (there is such a Q with $(s, t) \in Q$)
refinement-equivalence is mutual refinement

intuition:

- solid lines have to be implemented or happen
- only dashed and solid lines may be implemented or may happen
- all of the above *co-inductively*
- implementations are refinements with $R^c = R^a$:
  labelled transition systems

refinement example





BobDrinks refines Drinks,

TomTalks refines Talks ...

$$Q = \{(\text{Drinks}, \text{BobDrinks}), (\text{Drinks}, \text{TomDrinks}), (\text{Waits}, \text{Waits}),\\ (\text{Talks}, \text{BobTalks}), (\text{Talks}, \text{TomTalks})\}$$

expressiveness of formalism

some other 3-valued models used in practice:

- partial Kripke structures (Bruns & Godefroid'99)
  $M = (\Sigma; R \subseteq \Sigma \times \Sigma; L^a, L^c \colon AP \to \mathcal{P}(\Sigma))$
  2-valued transitions, 3-valued state propositions $L^a(q) \subseteq L^c(q)$
- Kripke modal transition systems (hjs'01)
  $M = (\Sigma; R^a, R^c \subseteq \Sigma \times Act \times \Sigma; L^a, L^c \colon AP \to \mathcal{P}(\Sigma))$
  3-valued transitions $R^a \subseteq R^c$
  state propositions $L^a(q) \subseteq L^c(q)$

(Jagadeesan & Godefroid'03):

- all such formalisms inter-translate in PTIME and LOGSPACE
- translations preserve and reflect refinement and model checks

$\Rightarrow$ our domain model captures them all

semantics of Hennessy-Milner logic

$$\phi ::= tt \mid \neg\phi \mid \langle\alpha\rangle\phi \mid \phi \wedge \phi \qquad (\alpha \in Act)$$

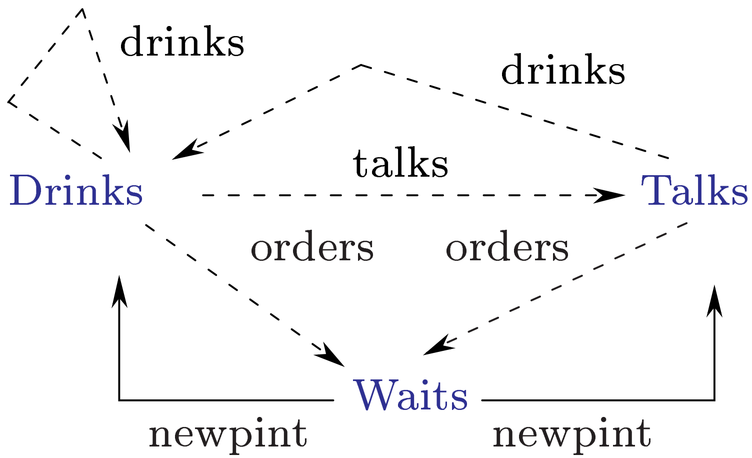
judgments $s \models^m \phi$ for $m \in \{a, c\} \equiv \{$is **a**sserted, may be **c**onsistent$\}$

- $s \models^m tt$
- $s \models^m \neg\phi$ 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



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

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

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

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

logical characterization of refinement

the following are equivalent — due to (Larsen'89):

- t refines s
- for all ϕ, $s \models^a \phi$ implies $t \models^a \phi$
- for all ϕ, $t \models^c \phi$ implies $s \models^c \phi$

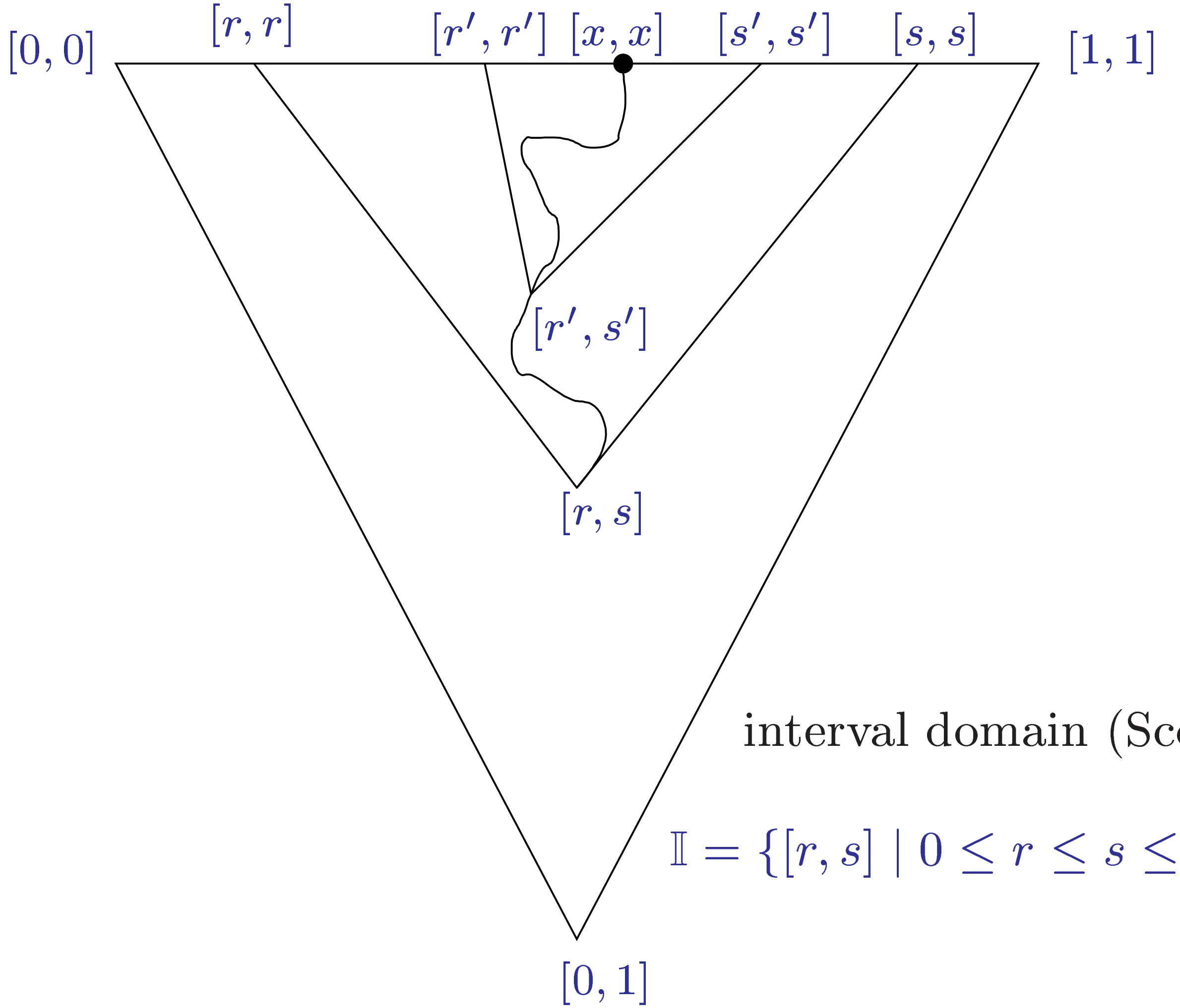
generalizes result for bisimulation:

for labelled transition systems, refinement is bisimulation &
$\models^a$ equals $\models^c$ and is familiar semantics

$\Rightarrow$ judgments $s \models^a \phi$ sound under refinement
$\Rightarrow$ judgments $t \models^c \phi$ sound under abstraction

2 domain model for refinement (hjs'04)

approximating real numbers



interval domain (Scott'72)

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

interval domain as metaphor

- intervals $[r, s]$ as partial reals: any $x \in [r, s]$ possible
- $\max(\mathbb{I}) \equiv [0, 1]$
- Scott-topology on $\mathbb{I}$ induces compact Euclidean topology on $\max(\mathbb{I})$
- intervals with rational endpoints densely approximate reals

objectives: seek domain $\mathbb{D}$ for modal transition systems & similar facts for labelled transition systems as $\max(\mathbb{D})$

domain model (hjs'04)

initial, ω-algebraic bifinite, solution $\mathbb{D}$ of $D = \prod_{\alpha \in Act} \mathcal{M}[D]$ where

- $(L, U) \in \mathcal{M}[D]$ mixed powerdomain (Heckmann'90, Gunter'92)
- $L = \downarrow L$, $U = \uparrow U$ Lawson-closed & $L = \downarrow(L \cap U)$ — ordered version of $R^a \subseteq R^c$ — 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 $U' \subseteq U$

example elements:

- $\perp_{\mathbb{D}} = (\{\}, \mathbb{D})_{\alpha \in Act} \in \mathbb{D}$ models universal stub
- $(\{\}, \{\})_{\alpha \in Act} \in \max(\mathbb{D})$ models deadlock

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

recursion $d = ((d^a_\alpha, d^c_\alpha))_{\alpha \in Act}$ derived 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 denotes latter

universality of $\mathcal{D}$ (hjs'04)

"for any image-finite modal transition system M with initial state i there is $\langle\!| M, i |\!\rangle \in \mathbb{D}$ such that (M, i) and $(\mathcal{D}, \langle\!| M, i |\!\rangle)$ are refinement-equivalent"

proof:

1. for each $n \geq 0$ unwind and truncate (M, i) as tree of depth $\leq n$
2. express truncations as denotations of terms in 3-valued process algebra $p ::= \ \mathbf{0} \ | \ \perp \ | \ \alpha_{tt}.p \ | \ \alpha_{\perp}.p \ | \ p + p \quad (\alpha \in Act)$
3. realize (M, i) as "refinement limit" of truncations
4. embed truncation p into $\mathbb{D}$ through denotational semantics of process algebra terms
5. use continuity/compactness argument in $\mathbb{D}$ $\blacksquare$

denotational semantics of process algebra terms

$$\{\!|\ \mathbf{0}\ |\!\} = ((\{\},\{\}))_{\alpha\in Act}$$

$$\{\!|\ \bot\ |\!\} = \bot_{\mathbb{D}}$$

$$(\{\!|\ \alpha_{tt}.p\ |\!\}^a_\alpha, \{\!|\ \alpha_{tt}.p\ |\!\}^c_\alpha) = (\Downarrow\{\!|\ p\ |\!\}, \Uparrow\{\!|\ p\ |\!\})$$

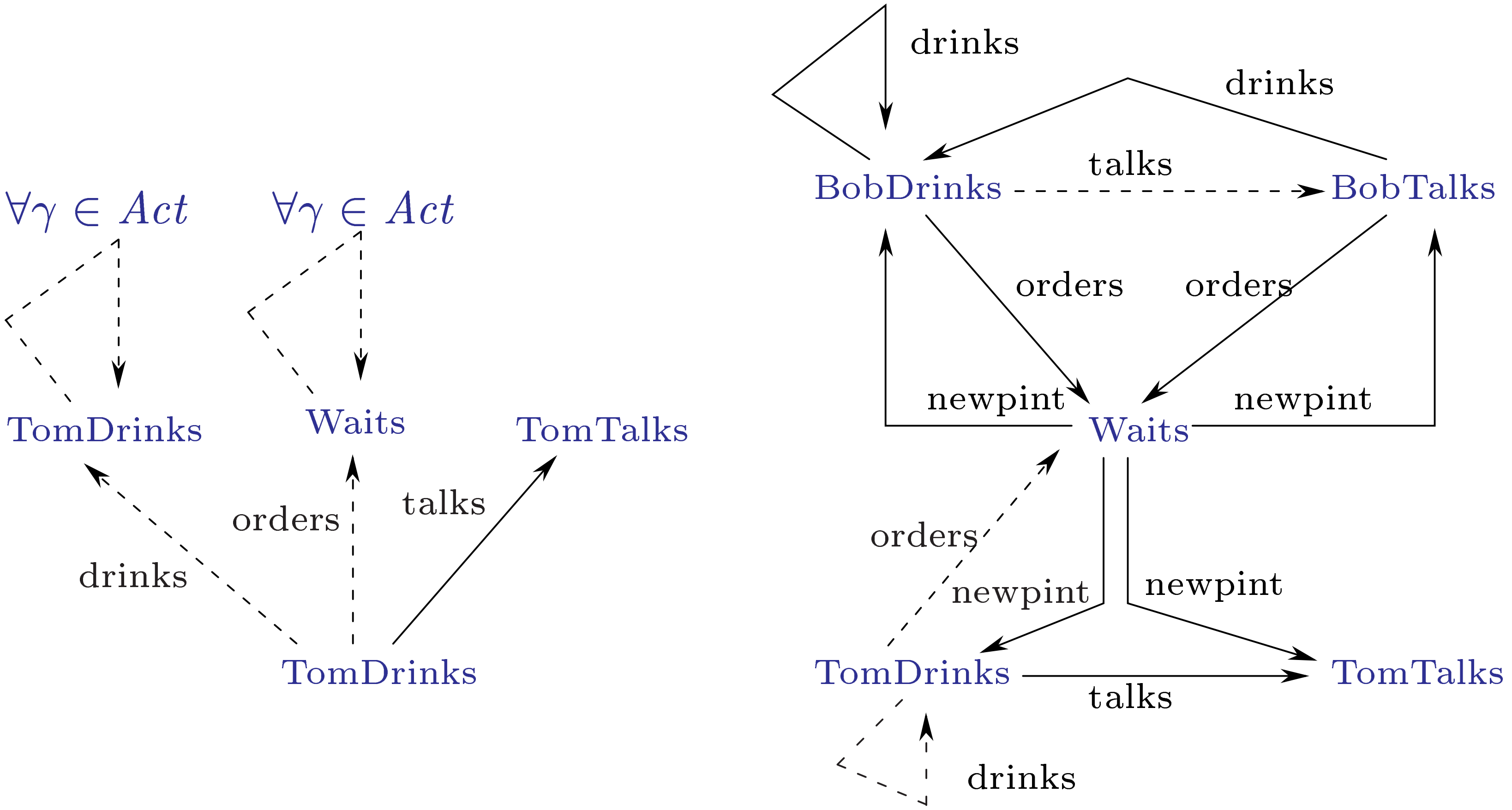
$$(\{\!|\ \alpha_{\bot}.p\ |\!\}^a_\alpha, \{\!|\ \alpha_{\bot}.p\ |\!\}^c_\alpha) = (\{\}, \Uparrow\{\!|\ p\ |\!\})$$

$$(\{\!|\ \alpha_{v}.p\ |\!\}^a_\beta, \{\!|\ \alpha_{v}.p\ |\!\}^c_\beta) = (\{\},\{\}),\ \alpha \neq \beta,\ v \in \{tt, \bot\}$$

$$\{\!|\ p+q\ |\!\}^m_\gamma = \{\!|\ p\ |\!\}^m_\gamma \cup \{\!|\ q\ |\!\}^m_\gamma,\ \gamma \in Act,\ m \in \{a, c\}$$

interprets $\mathbf{0}$ as deadlock, $\bot$ as universal stub, $+$ as mix union of (Heckmann'90), prefixes as expected plus saturations with $\Downarrow$ and $\Uparrow$

example truncation



truncation of depth one for TomDrinks; two kinds of leaves
(two-point abstract interpretation): universal stub & deadlock

full abstraction of $\mathbb{D}$ (hjs'04)

"the order on $\mathbb{D}$ is greatest refinement relation on $\mathcal{D}$: for all $d, e \in \mathbb{D}$: $d \leq e$ iff $(\mathcal{D}, e)$ refines $(\mathcal{D}, d)$"

proof:

1. show that $\leq$ is refinement, hardwired into definition of $\mathbb{D}$ and $\mathcal{D}$
2. use logical characterization of refinement to show "$d \not\leq e$ implies that $(\mathcal{D}, e)$ does not refine $(\mathcal{D}, d)$:"
   (a) $\mathbf{K}(\mathbb{D})$ order-generates $\mathbb{D}$ so $d \not\leq e$ implies $k \leq d$ and $k \not\leq e$ for some $k \in \mathbf{K}(\mathbb{D})$
   (b) for each $k \in \mathbf{K}(\mathbb{D})$ there is ϕ_k so that for all $f \in \mathbb{D}$: $k \leq f$ iff $f \models^a \phi_k$
   (c) thus $d \models^a \phi_k$ and $e \not\models^a \phi_k$ implies e does not refine d in $\mathcal{D}$ ∎

3 refinement is complete for implementations

soundness of refinement for implementations

- class of implementations $\mathcal{I}[M, s]$ of $(M, s) =$ all labelled transition systems (L, l) that refine (M, s)

- refinement transitive so

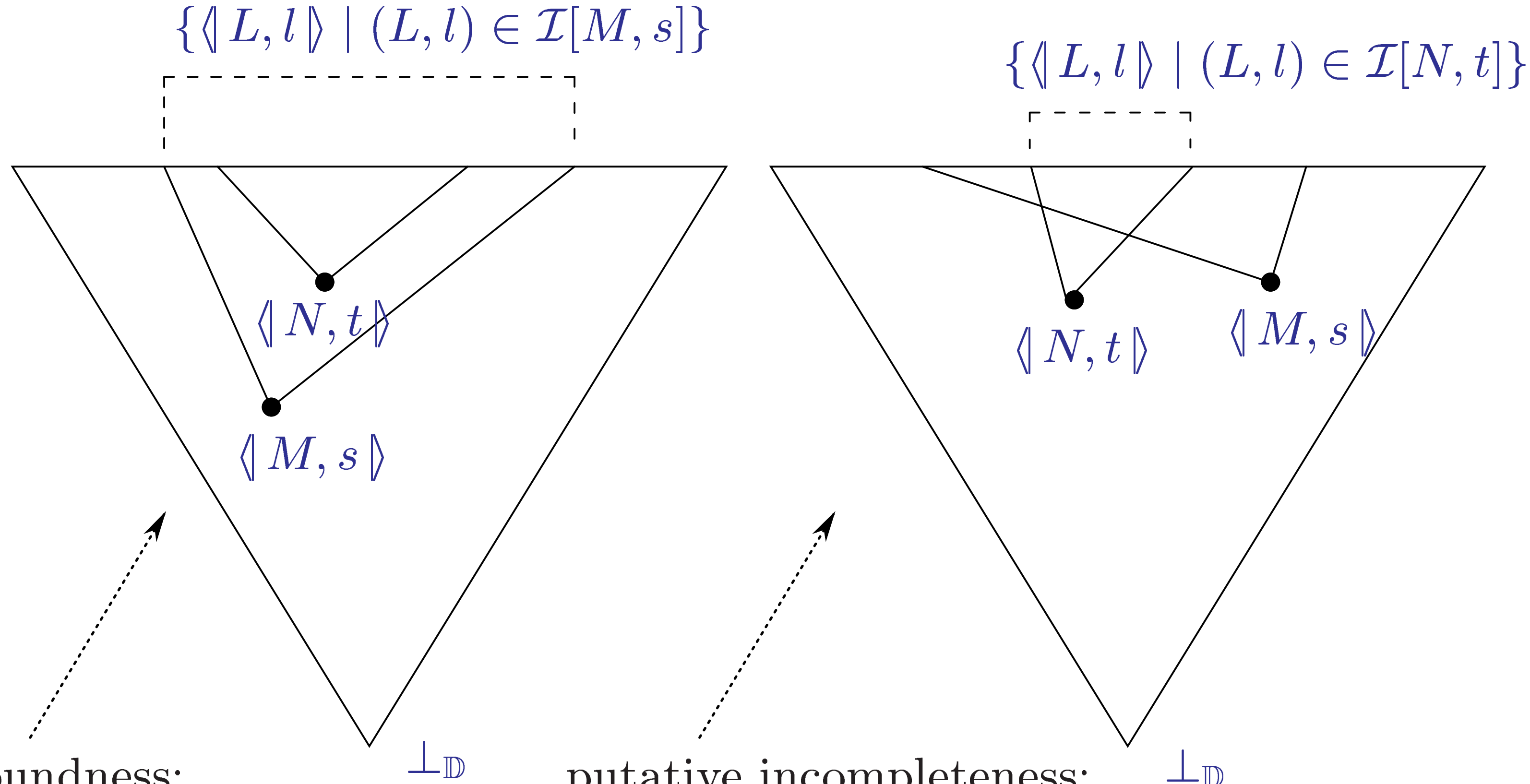
$$(N, t) \text{ refines } (M, s) \;\Rightarrow\; \mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$$

- implication captures *soundness:* step-wise refinement cannot introduce new implementations

- reverse containment of implementations *ought to be* refinement:

Does $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ imply that (N, t) refines (M, s)?

soundness & incompleteness in pictures



soundness:
(N, t) refines (M, s) and so
$\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$

putative incompleteness:
(N, t) doesn't refine (M, s)
but $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$

refinement is complete for implementations

" for all modal transition systems (M, s) and (N, t),
$\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ implies that (N, t) refines (M, s)"

proof:

1. prove this for s and t denotations of process algebra terms
   $p ::= \ \mathbf{0} \mid \perp \mid \alpha_{tt}.p \mid \alpha_{\perp}.p \mid p + p \quad (\alpha \in Act)$
   argument: use $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ to dynamically synthesize winning strategies in refinement game (adapted from Stirling'96) for s and t
2. show "$\Uparrow\!\llparenthesis N, t \rrparenthesis \cap \max(\mathbb{D}) \subseteq \Uparrow\!\llparenthesis M, s \rrparenthesis \cap \max(\mathbb{D})$ iff $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$" for all (M, s) and (N, t)
3. show "$\Uparrow e \cap \max(\mathbb{D}) \subseteq \Uparrow d \cap \max(\mathbb{D})$ implies $d \leq e$" for all $d, e \in \mathbb{D}$: use item 1, compactness argument, and fact that $\{d \in \mathbb{D} \mid \Uparrow d \cap \max(\mathbb{D}) \subseteq \Uparrow k\} \in \sigma_{\mathbb{D}}$ is Scott-open for all $k \in \mathbf{K}(\mathbb{D})$ by Hofman-Mislove Theorem ∎

new logical characterization

$V(M,s,\phi)$ holds iff all $(L,l) \in \mathcal{I}[M,s]$ satisfy ϕ

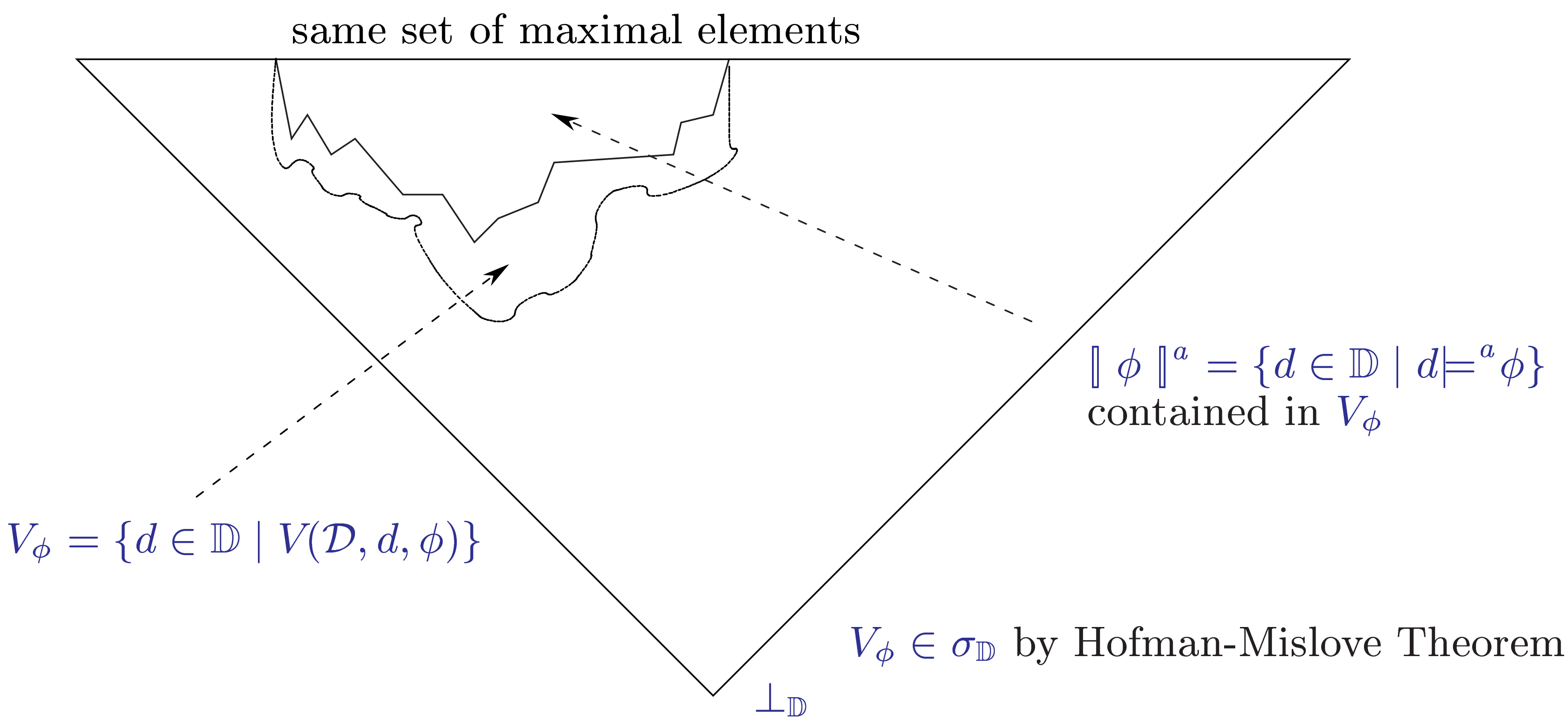
- soundness of $\models^a$: $(M,s) \models^a \phi \;\Rightarrow\; V(M,s,\phi)$
- soundness of $\models^c$: $(M,s) \not\models^c \phi \;\Rightarrow\; V(M,s,\neg\phi)$
- converse false: all $\langle\alpha\rangle tt \vee \neg\langle\alpha\rangle tt$ tautologies

new logical characterization of refinement:

(N,t) refines (M,s) iff (for all ϕ: $V(M,s,\phi)$ implies $V(N,t,\phi)$)

proof: "only if" immediate from $\mathcal{I}[N,t] \subseteq \mathcal{I}[M,s]$; "if:" proof by contradiction: if (N,t) does not refine (M,s), there is $(L,l) \in \mathcal{I}[N,t] \setminus \mathcal{I}[M,s]$ by completeness of refinement; by compactness, there is p with $\{\!|\, p \,|\!\} \leq \langle\!|\, M,s \,|\!\rangle$ and $\{\!|\, p \,|\!\} \not\leq \langle\!|\, L,l \,|\!\rangle$; the former means $V(M,s,\phi_{\{\!|p|\!\}})$, the latter rules out $V(N,t,\phi_{\{\!|p|\!\}})$. ■

loss of precision



completeness & loss of precision for tests

refinement is complete for implementations

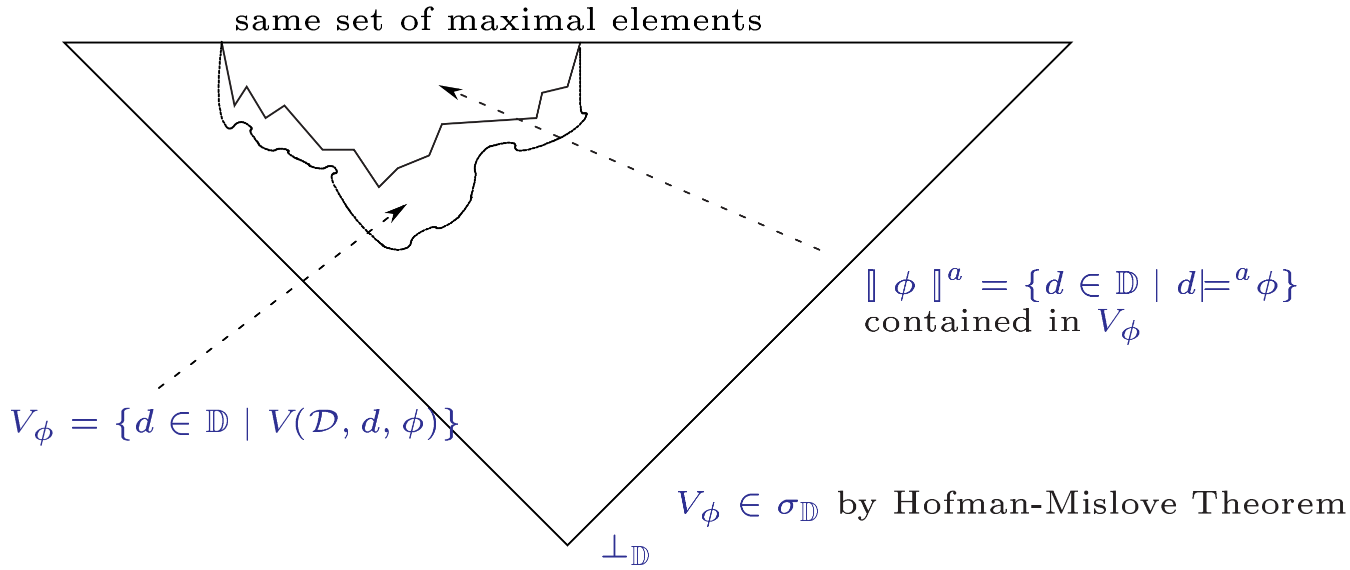
$\Leftrightarrow \quad \forall k \in \mathbf{K}(\mathbb{D})\colon V_{\phi_k} = \llbracket \phi_k \rrbracket^a$

proof: Use that $\mathbf{K}(\mathbb{D})$ equals set of all $\{\!\mid p \mid\!\}$.

1. For p with $V_{\phi_{\{\mid p \mid\}}} \neq \llbracket \phi_{\{\mid p \mid\}} \rrbracket^a$ there is (M, s) such that $V(M, s, \phi_{\{\mid p \mid\}})$ holds but $(M, s) \not\models^a \phi_{\{\mid p \mid\}}$. The former renders $\mathcal{I}[\mathcal{D}, \{\!\mid p \mid\!\}] \subseteq \mathcal{I}[M, s]$, the latter means $\{\!\mid p \mid\!\} \not\leq \langle\!\mid M, s \mid\!\rangle$ so refinement is incomplete.

2. Let $V_{\phi_{\{\mid p \mid\}}} = \llbracket \phi_{\{\mid p \mid\}} \rrbracket^a$ for all p. Proof by contradiction: Let $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ and (N, t) does not refine (M, s). By compactness, there is p with $\{\!\mid p \mid\!\} \leq \langle\!\mid M, s \mid\!\rangle$ and $\{\!\mid p \mid\!\} \not\leq \langle\!\mid N, t \mid\!\rangle$. The former and $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ ensure $\langle\!\mid N, t \mid\!\rangle \in V_{\phi_{\{\mid p \mid\}}}$ which equals $\llbracket \phi_{\{\mid p \mid\}} \rrbracket^a$ by assumption. So $(N, t) \models^a \phi_{\{\mid p \mid\}}$, i.e. $\{\!\mid p \mid\!\} \leq \langle\!\mid N, t \mid\!\rangle$. $\blacksquare$

open questions



- for which additional ϕ is $V_\phi = [\![\phi]\!]^a$?
  for such ϕ, validity checking *is* model checking

- for which ϕ is V_ϕ $\lambda_{\mathbb{D}}$-closed (and therefore of the form $[\![\psi]\!]^a$)?
  for such ϕ validity checking is *reducible* to model checking

4 conclusions

outline revisited:

0 motivation

1 modal transition systems and refinement

2 domain model for refinement

3 refinement as reverse containment of implementations