

# Topological analysis of refinement

Michael Huth<sup>1</sup>

<sup>1</sup>Department of Computing  
Imperial College London

Michaelmas 2004, Concepts of Space Seminar  
Acknowledgement: **Radha Jagadeesan and David Schmidt**

Modal transition systems and refinement

Domain model for refinement **(hjs'04)**

Compactness theorem for refinement

Consistency measure for refinement

Refinement is complete for implementations

# 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 all this for finite set of events *Act*.

# Exploit unification to determine structure of refinement

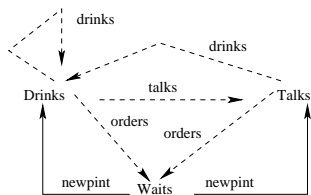
- ▶ Compactness theorem for temporal logic
- ▶ Consistency measure for under-specification
- ▶ Refinement as inverse containment of implementations
- ▶ Model checking multiple models collectively — not in this talk.



# Refinement

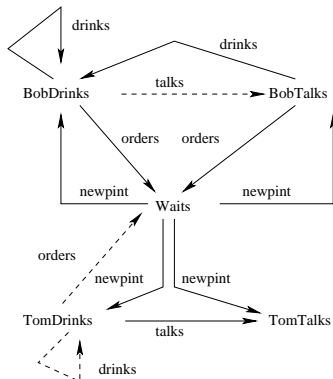
- ▶  $Q \subseteq \Sigma \times \Sigma$  is **refinement** (Larsen'89, Dams 96) iff  $(s, t) \in Q$  implies
  1. if  $(s, \alpha, s') \in R^a$ , there is  $(t, \alpha, t') \in R^a$  with  $(s', t') \in Q$
  2. if  $(t, \alpha, t') \in R^c$ , there is  $(s, \alpha, s') \in R^c$  with  $(s', t') \in Q$
- ▶  $t$  **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 ...



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

# Expressiveness of formalism

- ▶ some other 3-valued models used in practice:
  - ▶ partial Kripke structures (Bruns & Godefroid'99)
    - $M = (\Sigma; R \subseteq \Sigma \times \Sigma; L^a, L^c: AP \rightarrow \mathcal{P}(\Sigma))$
    - 2-valued transitions, 3-valued state propositions  $L^a(q) \subseteq L^c(q)$
  - ▶ Kripke modal transition systems (hjs'01)
    - $M = (\Sigma; R^a, R^c \subseteq \Sigma \times Act \times \Sigma; L^a, L^c: AP \rightarrow \mathcal{P}(\Sigma))$
    - 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
- ▶  $\rightsquigarrow$  our domain model captures them all

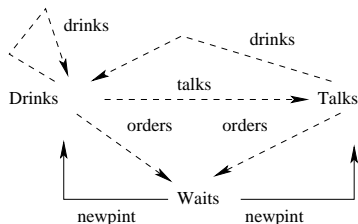
# Semantics of Hennessy-Milner logic

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

$s \models^m \phi$  for  $m \in \{a, c\} \equiv \{\text{is asserted, may be consistent}\}$

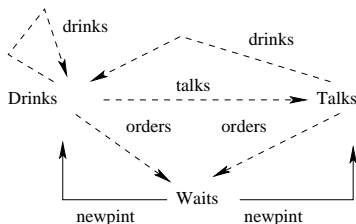
- ▶  $s \models^m tt$
- ▶  $s \models^m \neg\phi$  iff not  $s \models^{\neg m} \phi$       where  $\neg a = c$  and  $\neg c = a$
- ▶  $s \models^m \langle\alpha\rangle\phi$  iff (for some  $(s, \alpha, s') \in R^m$ ,  $s' \models^m \phi$ )
- ▶  $s \models^m \phi_1 \wedge \phi_2$  iff ( $s \models^m \phi_1$  and  $s \models^m \phi_2$ )
- ▶  $\sim s \models^m \phi_1 \vee \phi_2$  iff ( $s \models^m \phi_1$  or  $s \models^m \phi_2$ ) for  
 $\phi_1 \vee \phi_2 = \neg(\neg\phi_1 \wedge \neg\phi_2)$
- ▶  $\sim s \models^m [\alpha]\phi$  iff (for all  $(s, \alpha, s') \in R^{\neg m}$ ,  $s' \models^m \phi$ ) for  
 $[\alpha] = \neg\langle\alpha\rangle\neg$

# Example check



- ▶  $\text{Talks} \models^c \langle \text{drinks} \rangle tt$  as  $(\text{Talks}, \text{drinks}, \text{Drinks}) \in R^c$ 
  - ▶  $\leadsto \text{Talks} \not\models^a \neg \langle \text{drinks} \rangle tt$
- ▶  $\text{Talks} \not\models^a \langle \text{drinks} \rangle tt$  as there is no  $(\text{Talks}, \text{drinks}, x) \in R^a$ 
  - ▶  $\leadsto \text{Talks} \not\models^a \langle \text{drinks} \rangle tt \vee \neg \langle \text{drinks} \rangle tt$  (tautology)

# Example check continued

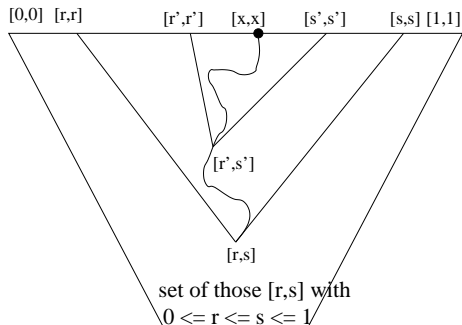


- ▶  $\text{Waits} \not\models^a [\text{newPint}][\text{talks}](\langle \text{drinks} \rangle tt \vee \neg \langle \text{drinks} \rangle tt)$  as
  - ▶  $(\text{Waits}, \text{newPint}, \text{Drinks})(\text{Drinks}, \text{talks}, \text{Talks})$  is  $R^c$ -path
  - ▶  $\text{Talks} \not\models^a \langle \text{drinks} \rangle tt \vee \neg \langle \text{drinks} \rangle tt$
- ▶ intuition:  $M$  “is” labelled transition system iff  $M$  passes all tests  $[\delta_1][\delta_2] \dots [\delta_n](\langle \alpha \rangle \phi_k \vee \neg \langle \alpha \rangle \phi_k)$  for suitable  $\phi_k$

# Logical characterization of refinement

- ▶ The following are equivalent — due to (Larsen'89):
  - ▶  $t$  refines  $s$
  - ▶ for all  $\phi$ ,  $s \models^a \phi$  implies  $t \models^a \phi$
  - ▶ for all  $\phi$ ,  $t \models^c \phi$  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
- ▶  $s \models^a \phi$  sound under refinement
- ▶  $t \models^c \phi$  sound under abstraction

# Approximating real numbers



# 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 Euclidean topology on  $\max(\mathbb{I})$
- ▶ intervals densely approximate reals
- ▶ *objectives*: seek
  - ▶ domain  $\mathbb{D}$  for modal transition systems & similar facts for labelled transition systems as  $\max(\mathbb{D})$
  - ▶ monotone consistency measure  $c: \mathbb{D} \times \mathbb{D} \rightarrow \mathbb{I}$

# Domain model (hjs'04)

- ▶ Initial,  $\omega$ -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  $d = ((d_\alpha^a, d_\alpha^c))_{\alpha \in Act}$  via  $\mathbb{D} = \prod_{\alpha \in Act} \mathcal{M}[\mathbb{D}]$
- ▶ modal transition system  $\mathcal{D} = (\mathbb{D}; \mathbb{R}^a, \mathbb{R}^c)$  where
- ▶  $\mathbb{R}^a = \{(d, \alpha, d') \mid d' \in d_\alpha^a\}$
- ▶  $\mathbb{R}^c = \{(d, \alpha, d') \mid d' \in d_\alpha^c\}$
- ▶  $d_\alpha^a$  ( $d_\alpha^c$ ) set of  $\mathbb{R}_\alpha^a$ -successors ( $\mathbb{R}_\alpha^c$ -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
 
$$p ::= \mathbf{0} \mid \perp \mid \alpha_{tt}.p \mid \alpha_{\perp}.p \mid p + p \quad (\alpha \in Act).$$
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  $\mathbb{D}$ .

# Denotational semantics of process algebra terms

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

$$\{\perp\} = \perp_{\mathbb{D}}$$

$$(\{\alpha_{tt} \cdot p\}_{\alpha}^a, \{\alpha_{tt} \cdot p\}_{\alpha}^c) = (\downarrow\{p\}, \uparrow\{p\})$$

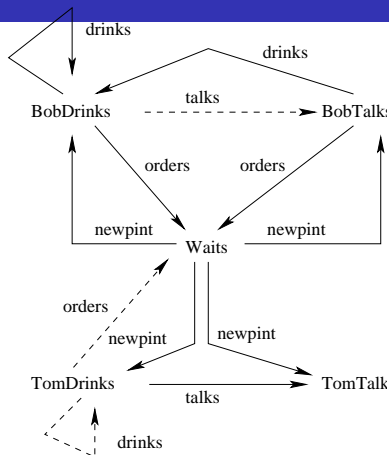
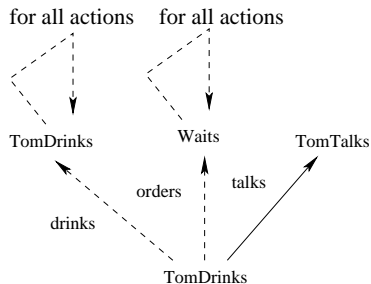
$$(\{\alpha_{\perp} \cdot p\}_{\alpha}^a, \{\alpha_{\perp} \cdot p\}_{\alpha}^c) = (\{\}, \uparrow\{p\})$$

$$(\{\alpha_v \cdot p\}_{\beta}^a, \{\alpha_v \cdot p\}_{\beta}^c) = (\{\}, \{\}), \alpha \neq \beta, v \in \{tt, \perp\}$$

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

- Interprets  $\mathbf{0}$  as deadlock,  $\perp$  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; universal stub & deadlock as leaves.

## 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  $(\mathcal{D}, d)$ :”
  - 2.1  $\mathbf{K}(\mathbb{D})$  order-generates  $\mathbb{D}$  so  $d \not\leq e$  implies  $k \leq d$  and  $k \not\leq e$  for some  $k \in \mathbf{K}(\mathbb{D})$
  - 2.2 for each  $k \in \mathbf{K}(\mathbb{D})$  there is  $\phi_k$  so that for all  $f \in \mathbb{D}$ :  $k \leq f$  iff  $f \models^a \phi_k$
  - 2.3 thus  $d \models^a \phi_k$  and  $e \not\models^a \phi_k$  implies  $e$  does not refine  $d$  in  $\mathcal{D}$ . □

## Three topologies

$$\mathbb{X} = \max(\mathbb{D}) = \{d \in \mathbb{D} \mid \forall e \in \mathbb{D}: d \leq e \Rightarrow d = e\}$$

set of maximal elements of  $\mathbb{D}$

1. Scott-topology:

$$\sigma_{\mathbb{D}} = \{\uparrow k \mid k \in \mathbf{K}(\mathbb{D})\}$$

$\sigma_{\mathbb{D}}$  is  $T_0$  &  $\mathbf{K}(\mathbb{D}) =$  set of embeddings of all truncated trees

2. Lawson-topology:

$$\lambda_{\mathbb{D}} = \{\uparrow k \setminus \uparrow l \mid k, l \in \mathbf{K}(\mathbb{D})\}$$

$\lambda_{\mathbb{D}}$  compact Hausdorff

3. 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  $\mathbb{X}$  as  $\mathbb{D}$  bifinite

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

- ▶  $(\mathbb{X}, \tau_{\mathbb{X}})$  **Stone space** iff  $\tau_{\mathbb{X}}$  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  $U \in \tau_{\mathbb{X}}$  union of sets that are  $\tau_{\mathbb{X}}$ -open (in  $\tau_{\mathbb{X}}$ ) and  $\tau_{\mathbb{X}}$ -closed (complement in  $\tau_{\mathbb{X}}$ )
- ▶ 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  $\Delta = \delta_1 \delta_2 \dots \delta_n \in Act^*$ ,  $\alpha \in Act$ ,  $k \in \mathbf{K}(\mathbb{D})$  define test

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

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

- ▶ for  $m \in \{a, c\}$  set  $\llbracket \phi \rrbracket^m = \{d \in \mathbb{D} \mid (\mathcal{D}, d) \models^m \phi\}$
- ▶ pass all tests:  
 $C = \bigcap \{ \llbracket \psi_k^{\Delta, \alpha} \rrbracket^a \mid \Delta \in Act^*, \alpha \in Act, k \in \mathbf{K}(\mathbb{D}) \}$
- ▶ *Plan:* show
  - ▶ each  $\llbracket \phi \rrbracket^a$  is  $\lambda_{\mathbb{D}}$ -closed
  - ▶  $C = \max(\mathbb{D})$

## $\max(\mathbb{D})$ is $\lambda_{\mathbb{D}}$ -closed

*Proof:*

1.  $\|\phi\|^a$  is  $\lambda_{\mathbb{D}}$ -closed: mutual structural induction on  $\phi$  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  $d \models^a \psi_k^{\Delta, \alpha}$

►  $\rightsquigarrow (\mathbb{X}, \tau_{\mathbb{X}})$  Stone space. □

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

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

# Compactness theorem for refinement

- ▶ given:
  - ▶ modal transition system  $M$  with initial state  $s$ ,  $\Gamma$  set of formulas of Hennessy-Milner logic
  - ▶ for all finite subsets  $\Pi$  of  $\Gamma$ ,  $\bigwedge \Pi$  satisfiable over labelled transition systems that refine  $s$
- ▶  $(\mathbb{X}, \tau_{\mathbb{X}})$  Stone space &  $\uparrow \langle M, s \rangle \cap \max(\mathbb{D})$   $\lambda_{\mathbb{D}}$ -closed  $\Rightarrow$  there is image-finite labelled transition system  $(L, l)$  such that
  - ▶  $l$  refines  $s$  and
  - ▶  $l$  satisfies all formulas of  $\Gamma$
- ▶ for  $s = \perp_{\mathbb{D}}$ : familiar compactness theorem for Hennessy-Milner logic & labelled transition systems

## Two familiar metrics

For  $k_0, k_1, \dots$  enumeration of  $\mathbf{K}(\mathbb{D})$ :

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

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

noteworthy points:

- ▶ enumeration in increasing modal depth of  $\phi_{k_n}$  for  $n \geq 0$
- ▶ in both metrics: the closer models are, the more effort (i.e. modal depth) needed to distinguish them by tests
- ▶  $d_{\mathbb{D}}$  induces  $\lambda_{\mathbb{D}}$ ,  $d_{\mathbb{X}}$  induces  $\tau_{\mathbb{X}}$

## Two consistency measures

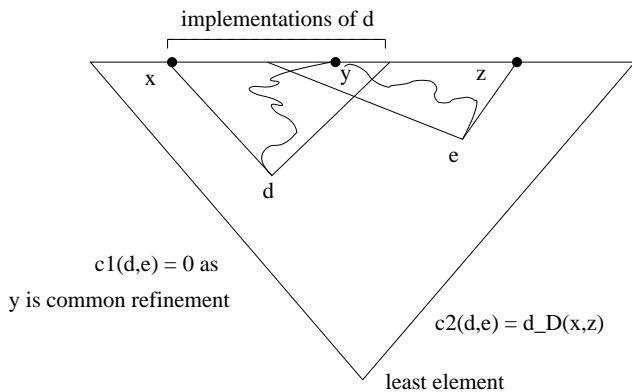
- ▶  $(M, s)$  and  $(N, t)$  **consistent** iff they have common refinement

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

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

- ▶ intuition:
  - ▶  $c_1(d, e)$  optimistic measure of consistency
  - ▶  $c_2(d, e)$  pessimistic measure of consistency
  - ▶ monotone abstraction  $(d, e) \mapsto [c_1(d, e), c_2(d, e)]: \mathbb{D} \times \mathbb{D} \rightarrow \mathbb{I}$
- ▶  $(\mathbb{X}, \tau_{\mathbb{X}})$  Stone space, so
  - $c_1(d, e) = 0$  iff  $((\mathcal{D}, d)$  and  $(\mathcal{D}, e)$  have common refinement)

# Example of common refinement



# Soundness of refinement for implementations

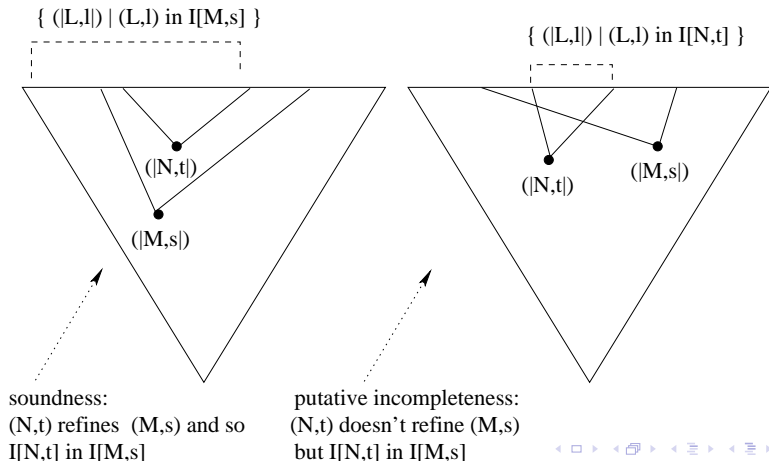
- ▶ class of implementations  $\mathcal{I}[M, s]$  of  $(M, s) =$  all labelled transition systems  $(L, l)$  that refine  $(M, s)$
- ▶ refinement transitive so

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

- ▶ 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



# Refinement 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  $(M, s)$ ”

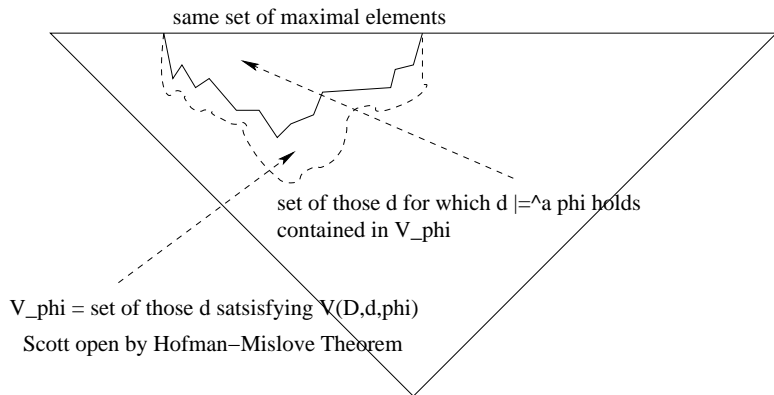
1. prove this for  $s$  and  $t$  denotations of process algebra terms  
 $p ::= \mathbf{0} \mid \perp \mid \alpha_{tt}.p \mid \alpha_{\perp}.p \mid p + p \quad (\alpha \in Act)$   
 argument: use  $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$  to dynamically synthesize winning strategies in refinement game, adapted from (Stirling'96), for  $s$  and  $t$
2. show “ $\uparrow\downarrow N, t \downarrow \cap \max(\mathbb{D}) \subseteq \uparrow\downarrow M, s \downarrow \cap \max(\mathbb{D})$  implies  $\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]$ ” 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  $\{d \in \mathbb{D} \mid \uparrow d \cap \max(\mathbb{D}) \subseteq \uparrow k\} \in \sigma_{\mathbb{D}}$  for  $k \in \mathbf{K}(\mathbb{D})$  by Hoffman-Mislove Theorem

## New logical characterization

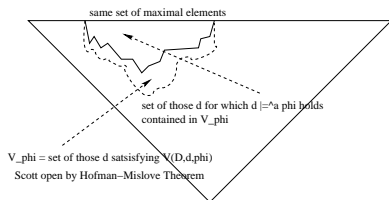
- ▶  $V(M, s, \phi)$  holds iff all  $(L, l) \in \mathcal{I}[M, s]$  satisfy  $\phi$ 
  - ▶ soundness of  $\models^a$ :  $(M, s) \models^a \phi \Rightarrow V(M, s, \phi)$
  - ▶ converse false: all  $\psi_k^{\Delta, \alpha}$  tautologies
- ▶ new logical characterization of refinement
  - ▶  $(N, t)$  refines  $(M, s)$  iff (for all  $\phi$ :  $V(M, s, \phi)$  implies  $V(N, t, \phi)$ )
- ▶ *Proof*:
  - ▶ “only if” by soundness of  $\models^a$  and  $\models^c$
  - ▶ “if:” completeness of refinement & soundness of  $\models^a$  and  $\models^c$



# Loss of precision



# Completeness & loss of precision for tests



- ▶ refinement complete for implementations

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

- ▶ open questions:

- ▶ for which additional  $\phi$  is  $V_\phi = \llbracket \phi \rrbracket^a$ ?
- ▶ for which  $\phi$  is  $V_\phi$   $\lambda_{\mathbb{D}}$ -closed (and therefore of the form  $\llbracket \psi \rrbracket^a$ )?
- ▶ Wadge reducibility (Wadge'83) and Borel hierarchy for  $\llbracket \phi \rrbracket^a$  and  $V_\phi$  in  $\varphi$ -space (Selivanov'04)  $\mathbb{D}$  for modal  $\mu$ -calculus?

# Conclusions

This page is intentionally left blank.