Topological analysis of refinement

Michael Huth\textsuperscript{1}

\textsuperscript{1}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.
Modal transition system of ’pub behavior’

Modal transition system $M = (\Sigma; R^a, R^c \subseteq \Sigma \times \text{Act} \times \Sigma)$

- $\Sigma = \{\text{Drinks}, \text{Talks}, \text{Waits}\}$ state space
- $R^a$ solid lines and $\Sigma \times \text{Act} \times \Sigma \setminus R^c$ (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 \cite{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
BobDrinks refines Drinks, 
TomTalks refines Talks ...

\[Q = \{ \text{(Drinks, BobDrinks)}, \text{(Drinks, TomDrinks)}, \text{(Waits, Waits)}, \text{(Talks, BobTalks)}, \text{(Talks, TomTalks)} \}\]
some other 3-valued models used in practice:

- partial Kripke structures \((\text{Bruns & Godefroid'99})\)
  \[
  M = (\Sigma; R \subseteq \Sigma \times \Sigma; L^a, L^c : AP \rightarrow \mathcal{P}(\Sigma))
  \]
  2-valued transitions, 3-valued state propositions \(L^a(q) \subseteq L^c(q)\)

- Kripke modal transition systems \((\text{hjs'01})\)
  \[
  M = (\Sigma; R^a, R^c \subseteq \Sigma \times \text{Act} \times \Sigma; L^a, L^c : AP \rightarrow \mathcal{P}(\Sigma))
  \]
  3-valued transitions \(R^a \subseteq R^c\)
  state propositions \(L^a(q) \subseteq L^c(q)\)

- \((\text{Jagadeesan & Godefroid'03})\):
  - all such formalisms inter-translate in PTIME and LOGSPACE
  - translations preserve and reflect refinement and model checks
  - \(\sim\) our domain model captures them all
Semantics of Hennessy-Milner logic

\[ \phi ::= \text{tt} \mid \neg \phi \mid \langle \alpha \rangle \phi \mid \phi \land \phi \quad (\alpha \in \text{Act}) \]

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

- \[ s \models^m \text{tt} \]
- \[ s \models^m \neg \phi \text{ iff not } s \models^m \neg \phi \text{ where } \neg a = c \text{ and } \neg c = a \]
- \[ s \models^m \langle \alpha \rangle \phi \text{ iff (for some } (s, \alpha, s') \in R^m, s' \models^m \phi) \]
- \[ s \models^m \phi_1 \land \phi_2 \text{ iff } (s \models^m \phi_1 \text{ and } s \models^m \phi_2) \]
- \[ \neg s \models^m \phi_1 \lor \phi_2 \text{ iff } (s \models^m \phi_1 \text{ or } s \models^m \phi_2) \text{ for } \phi_1 \lor \phi_2 = \neg(\neg \phi_1 \land \neg \phi_2) \]
- \[ \neg s \models^m [\alpha] \phi \text{ iff (for all } (s, \alpha, s') \in R^{-m}, s' \models^m \phi) \text{ for } [\alpha] = \neg \langle \alpha \rangle \neg \]
Example check

- **Talks** $\models^c \langle \text{drinks} \rangle tt$ as $(\text{Talks}, \text{drinks}, \text{Drinks}) \in R^c$
  - $\sim$ **Talks** $\not\models^a \neg \langle \text{drinks} \rangle tt$
- **Talks** $\not\models^a \langle \text{drinks} \rangle tt$ as there is no $(\text{Talks}, \text{drinks}, x) \in R^a$
  - $\sim$ **Talks** $\not\models^a \langle \text{drinks} \rangle tt \lor \neg \langle \text{drinks} \rangle tt$ (tautology)
Example check continued

- **Waits** $\not\models ^a [\text{newPint}] [\text{talks}] (\langle \text{drinks} \rangle \text{tt} \lor \neg \langle \text{drinks} \rangle \text{tt})$ as
  - (Waits, newPint, Drinks)(Drinks, talks, Talks) is $R^c$-path
  - Talks $\not\models ^a \langle \text{drinks} \rangle \text{tt} \lor \neg \langle \text{drinks} \rangle \text{tt}$

- **intuition:** $M$ "is" labelled transition system iff $M$ passes all tests $[\delta_1][\delta_2] \ldots [\delta_n](\langle \alpha \rangle \phi_k \lor \neg \langle \alpha \rangle \phi_k)$ for suitable $\phi_k$
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 (Scott’72)

set of those \([r,s]\) with 
\[0 \leq r \leq s \leq 1\]
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 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 $c : \mathbb{D} \times \mathbb{D} \to \mathbb{I}$
Domain model \textit{(hjs'04)}

- Initial, \(\omega\)-algebraic bifinite, solution \(\mathbb{D}\) of \(D = \prod_{\alpha \in \text{Act}} \mathcal{M}[D]\)
  where
  - \((L, U) \in \mathcal{M}[D]\) mixed powerdomain \textit{(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:
  - \(\bot_{\mathbb{D}} = (\{\}, \mathbb{D})_{\alpha \in \text{Act}} \in \mathbb{D}\) models universal stub
  - \((\{\}, \{\})_{\alpha \in \text{Act}} \in \text{max}(\mathbb{D})\) models deadlock
$\mathcal{D}$ as modal transition system $\mathcal{D}$ (hjs'04)

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

- modal transition system $\mathcal{D} = (\mathcal{D}; R^a, R^c)$ where
  - $R^a = \{(d, \alpha, d') | d' \in d^a_\alpha\}$
  - $R^c = \{(d, \alpha, d') | d' \in d^c_\alpha\}$
  - $d^a_\alpha$ ($d^c_\alpha$) set of $R^a_\alpha$-successors ($R^c_\alpha$-successors) of $d$

- minor detail: $R^a \nsubseteq R^c$ but $\mathcal{D}$ refinement-equivalent to modal transition system $(\mathcal{D}, R^a \cap R^c, R^c)$, $\mathcal{D}$ always denotes latter
Universality of $\mathcal{D}$ (hjs'04)

“For any image-finite modal transition system $M$ with initial state $i$ there is $\langle M, i \rangle \in \mathcal{D}$ 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
   $$p ::= 0 \mid \bot \mid \alpha_{tt}.p \mid \alpha_{\bot}.p \mid p + p \ (\alpha \in \text{Act})$$
3. Realize $(M, i)$ as “refinement limit” of truncations.
4. Embed truncation $p$ into $\mathcal{D}$ through denotational semantics of process algebra terms.
5. Use continuity/compactness argument in $\mathcal{D}$.
Denotational semantics of process algebra terms

\[
\begin{align*}
\{ 0 \} &= ((\emptyset, \emptyset))_{\alpha \in \text{Act}} \\
\{ \perp \} &= \perp_D \\
(\{ \alpha_{\top}.p \}^a_{\alpha}, \{ \alpha_{\top}.p \}^c_{\alpha}) &= (\down\{ p \}, \up\{ p \}) \\
(\{ \alpha_{\bot}.p \}^a_{\alpha}, \{ \alpha_{\bot}.p \}^c_{\alpha}) &= (\emptyset, \up\{ p \}) \\
(\{ \alpha_{v}.p \}^a_{\beta}, \{ \alpha_{v}.p \}^c_{\beta}) &= (\emptyset, \emptyset), \alpha \neq \beta, \; v \in \{ \top, \bot \} \\
\{ p + q \}^m_{\gamma} &= \{ p \}^m_{\gamma} \cup \{ q \}^m_{\gamma}, \; \gamma \in \text{Act}, \; m \in \{ a, c \}
\end{align*}
\]

- Interprets 0 as deadlock, \( \perp \) as universal stub, + as mix union of (Heckmann'90), prefixes as expected (plus saturations with \( \down \) and \( \up \)).
Example truncation

Truncation of depth one for TomDrinks; universal stub & deadlock as leaves.
Full abstraction of $\mathbb{D}$ \emph{(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 $(\mathcal{D}, d)$"

\textit{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 $(\mathcal{D}, d)$:"

   \begin{enumerate}
   \item $\mathcal{K}(\mathbb{D})$ order-generates $\mathbb{D}$ so $d \not\leq e$ implies $k \leq d$ and $k \not\leq e$ for some $k \in \mathcal{K}(\mathbb{D})$
   \item for each $k \in \mathcal{K}(\mathbb{D})$ there is $\phi_k$ so that for all $f \in \mathbb{D}$: $k \leq f$ iff $f \models^a \phi_k$
   \item thus $d \models^a \phi_k$ and $e \not\models^a \phi_k$ implies $e$ does not refine $d$ in $\mathcal{D}$. \hfill $\Box$
   \end{enumerate}
Three topologies

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

set of maximal elements of \( \mathbb{D} \)

1. Scott-topology:

\[ \sigma_{\mathbb{D}} = \{\uparrow k \mid k \in K(\mathbb{D})\} \]

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

2. Lawson-topology:

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

\( \lambda_{\mathbb{D}} \) compact Hausdorff

3. Lawson-condition (Lawson’97) crucial: topology

\[ \tau_X = \{U \cap \text{max}(\mathbb{D}) \mid U \in \sigma_{\mathbb{D}}\} \]

equals \{V \cap \text{max}(\mathbb{D}) \mid V \in \lambda_{\mathbb{D}}\} on \( X \) as \( \mathbb{D} \) bifinite
(\(X, \tau_X\)) Stone space

- (\(X, \tau_X\)) Stone space iff \(\tau_X\) is
  - compact: for all \(U \subseteq \tau_X\) with \(X \subseteq \bigcup U\) there is finite \(F \subseteq U\) with \(X \subseteq \bigcup F\) &
  - Hausdorff: for all \(x \neq x'\) in \(X\) there are \(O, O' \in \tau_X\) with \(x \in O\), \(x' \in O'\), and \(O \cap O' = \emptyset\) &
  - zero-dimensional: every \(U \in \tau_X\) union of sets that are \(\tau_X\)-open (in \(\tau_X\)) and \(\tau_X\)-closed (complement in \(\tau_X\))

- Lawson condition \(\Rightarrow \tau_X\) zero-dimensional & Hausdorff
- as \(\lambda_D\) compact, suffices to show \(\max(\mathbb{D})\) is \(\lambda_D\)-closed
Complete set of tests for maximality

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

$$\psi^\Delta_k, \alpha = [\delta_1][\delta_2] \ldots [\delta_n](\langle \alpha \rangle \phi_k \lor \neg \langle \alpha \rangle \phi_k)$$

where $(D, d)|=^a \phi_k$ iff $k \leq d$ — full abstraction in (hjs’04)

▶ for $m \in \{a, c\}$ set $\ll \phi \rr^m = \{ d \in D | (D, d)|=^m \phi \}$

▶ pass all tests:

$$C = \bigcap \{ \ll \psi^\Delta_k, \alpha \rr^a | \Delta \in \text{Act}^*, \alpha \in \text{Act}, k \in \text{K}(D) \}$$

▶ Plan: show

▶ each $\ll \phi \rr^a$ is $\lambda_D$-closed
▶ $C = \text{max}(D)$
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. \(\text{max}(\mathbb{D}) \subseteq C\): as \(C\) is \(\lambda_{\mathbb{D}}\)-closed, suffices to show embeddings of labelled transition systems are in \(C\) and dense in \(\text{max}(\mathbb{D})\)

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

\[\sim (X, \tau_{X})\] Stone space.
max(\mathcal{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(\mathcal{D})

2. any \((\mathcal{D}, d)\) with \(d \in \text{max}(\mathcal{D})\) refinement-equivalent to a labelled transition system as \(d^a_{\alpha} \cap d^c_{\alpha} = d^c_{\alpha} \subseteq \text{max}(\mathcal{D})\) for all \(\alpha \in \text{Act}\)

3. \(\mathcal{X} = \prod_{\alpha \in \text{Act}} \text{Compact} [\mathcal{X}, \tau_\mathcal{X}]\) where \(x_\alpha\) is \(\tau_\mathcal{X}\)-compact set of \(\alpha\)-successors for \(x = (x_\alpha)_{\alpha \in \text{Act}} \in \mathcal{X}\)
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 $s$

- $(X, \tau_X)$ Stone space & $\uparrow M, s \downarrow \cap \max(D)$ $\lambda_D$-closed $\Rightarrow$ there is image-finite labelled transition system $(L, l)$ such that
  - $l$ refines $s$ and
  - $l$ satisfies all formulas of $\Gamma$

- for $s = \bot_D$: familiar compactness theorem for Hennessy-Milner logic & labelled transition systems
Two familiar metrics

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

\[
d_{\mathbb{D}}(d, e) = \inf\{2^{-n} \mid \forall i \leq n: k_i \leq d \iff k_i \leq e\}
\]
\[
d_{\mathbb{X}}(x, y) = \inf\{2^{-n} \mid \forall i \leq n: k_i \leq x \iff k_i \leq y\}
\]

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

\[
c_1(d, e) = \inf \{ d_x(x, y) \mid x \in \uparrow d \cap \max(D), \ y \in \uparrow e \cap \max(D) \} \\
c_2(d, e) = \sup \{ d_x(x, y) \mid x \in \uparrow d \cap \max(D), \ y \in \uparrow e \cap \max(D) \}
\]

- intuition:
  - \(c_1(d, e)\) optimistic measure of consistency
  - \(c_2(d, e)\) pessimistic measure of consistency
  - monotone abstraction \((d, e) \mapsto [c_1(d, e), c_2(d, e)]: D \times D \to I\)

- \((X, \tau_X)\) Stone space, so
  - \(c_1(d, e) = 0\) iff \((D, d)\) and \((D, e)\) have common refinement
Example of common refinement

\[ c_1(d,e) = 0 \]
\[ c_2(d,e) = d_D(x,z) \]

y is common refinement

Huth

Topological analysis of 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:

$$\text{Does } \mathcal{I}[N, t] \subseteq \mathcal{I}[M, s] \text{ imply that } (N, t) \text{ refines } (M, s)?$$
Soundness & incompleteness in pictures

{ (|L,l|) | (L,l) in I[M,s] }  { (|L,l|) | (L,l) in I[N,t] }

soundness: (N,t) refines (M,s) and so I[N,t] in I[M,s]

putative incompleteness: (N,t) doesn’t refine (M,s) but I[N,t] in I[M,s]

Huth

Topological analysis of refinement
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

\[p ::= 0 | ⊥ | α_{tt}.p | α_⊥.p | p + p \ (α ∈ \text{Act})\]

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 “\([N, t]| \cap \max(D) \subseteq [M, s]| \cap \max(D)\) implies \(\mathcal{I}[N, t] \subseteq \mathcal{I}[M, s]\)” for all \((M, s)\) and \((N, t)\)

3. show “\([e \cap \max(D)] \subseteq [d \cap \max(D)]\) implies \(d \leq e\)” for all \(d, e ∈ D\): use item 1, compactness argument, and fact that \(\{d ∈ D \mid [d \cap \max(D)] \subseteq [k]\} ∈ σ_D\) for \(k ∈ K(D)\) by Hoffman-Mislove Theorem
New logical characterization

- $V(M, s, \phi)$ holds iff all $(L, l) \in I[M, s]$ 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

same set of maximal elements

set of those d for which d |/=^a phi holds contained in V_phi

V_phi = set of those d satisfying V(D,d,phi)
Scott open by Hofman–Mislove Theorem
Completeness & loss of precision for tests

- Refinement complete for implementations:
  \[ \forall k \in K(D): V_{\phi_k} = \| \phi_k \|^a \]
- Open questions:
  - For which additional \( \phi \) is \( V_{\phi} = \| \phi \|^a \)?
  - For which \( \phi \) is \( V_{\phi} \lambda_D \)-closed (and therefore of the form \( \| \psi \|^a \))?  
  - Wadge reducibility (Wadge'83) and Borel hierarchy for \( \| \phi \|^a \)
  and \( V_{\phi} \) in \( \varphi \)-space (Selivanov'04) \( D \) for modal mu-calculus?
Conclusions

This page is intentionally left blank.