An ontology for consistent partial model checking

Michael Huth, Computing, Imperial College London.

Acknowledgments: Glenn Bruns and Gordon Plotkin.
Collaborators: Patrice Godefroid, Rahda Jagadeesan, Shekhar Pradhan, and David Schmidt.

Objectives and outline of talk

1. present reference ontology for reasoning about partially given models;
2. present material ontology for modal transition systems;
3. demonstrate that the mixed power-domain is of great use in such ontologies; and
4. sketch how modal transition systems determine a zero-dimensional Polish space of labeled transition systems, à la Flagg & Kopperman.

Checking total models

- $\mathcal{T} =$ class of total models T;
- $\mathcal{L} =$ logic with $\neg$ and $\wedge$;
- $\models \; \subseteq \mathcal{T} \times \mathcal{L}$ satisfaction relation,
  - has usual semantics for $\neg$ and $\wedge$; and
  - all $T \in \mathcal{T}$ are consistent: no $\phi \in \mathcal{L}$ with $T \models \phi \wedge \neg\phi$.

Examples:

- labeled transition systems (LTSs) with Hennessy-Milner logic;
- models of typed first-order logic with transitive closure;
- matroids and higher-order logic; etc.

Partial models

- $\mathcal{P} =$ class of partial models P;
- $\mathtt{up}\colon \mathcal{T} \to \mathcal{P}$ and $\mathtt{down}\colon \mathcal{P} \to \mathcal{T}$ with $\mathrm{id}_{\mathcal{T}} = \mathtt{down} \circ \mathtt{up}$;
- $\mathtt{impl} \subseteq \mathcal{P} \times \mathtt{up}(\mathcal{T})$ where
  - $\mathtt{impl} \cap \mathtt{up}(\mathcal{T}) \times \mathtt{up}(\mathcal{T})$ equivalence relation such that
  - $(\mathtt{up}(T), \mathtt{up}(T')) \in \mathtt{impl}$ iff T and T' satisfy the same formulas in $\mathcal{L}$.
- $(P, \mathtt{up}(T)) \in \mathtt{impl}$ means "T is an implementation of P."

Examples:

- modal transition systems; total models are LTSs; `impl`?
- Alloy programs; total models are standard models of first-order logic with transitive closure;
- partial matroids and higher-order logic; etc.

Checking partial models

- assertion checks: $P \models^{\mathrm{a}}_{t} \phi$ (**a**ssertion/**t**otal) iff $\forall T \in \mathcal{T}\colon (P, \mathtt{up}(T)) \in \mathtt{impl} \;\Rightarrow\; T \models \phi$;
- consistency checks: $P \models^{\mathrm{c}}_{t} \phi$ (**c**onsistency/**t**otal) iff $\exists T \in \mathcal{T}\colon (P, \mathtt{up}(T)) \in \mathtt{impl} \;\wedge\; T \models \phi$;
- refinement order: $P \sqsubseteq_t P'$ iff $\forall \phi \in \mathcal{L}\colon P \models^{\mathrm{a}}_{t} \phi \;\Rightarrow\; P' \models^{\mathrm{a}}_{t} \phi$;
- $P \sqsubseteq_t P'$ means "P' refines P" and "P abstracts P'."

Examples: $\models^{\mathrm{a}}_{t}$ and $\models^{\mathrm{c}}_{t}$ are the basis of

- Generalized Model Checking (Bruns & Godefroid 2000),
- the Focus Operation in program analysis (Ball et al. 2000),
- Semantic Minimization of propositional logic (Reps et al. 2002), etc.

Modal transition systems

- Labeled transition systems (LTSs)
  $(M, i) = (\Sigma, R \subseteq \Sigma \times \texttt{Act} \times \Sigma, i \in \Sigma)$ — $\mathcal{T}$;
- Modal transition systems (MTSs) $(M, i) = (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i)$ with $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$ — $\mathcal{P}$;
- HML for $\alpha \in \texttt{Act}$ — $\mathcal{L}$

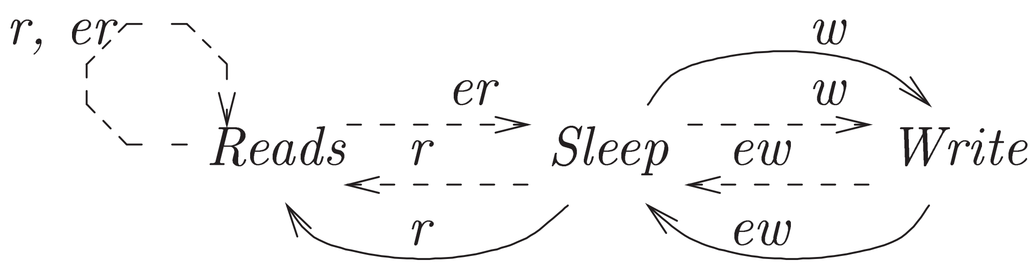
$$\phi ::= \texttt{tt} \mid \neg\phi \mid \phi \wedge \phi \mid (\exists\alpha)\phi$$

- $\texttt{up}(\Sigma, R, i) = (\Sigma, R, R, i)$, $\texttt{down}(\Sigma, R, R, i) = (\Sigma, R, i)$;
- $(\Sigma, R, i) \models (\exists\alpha)\phi$ iff $\exists(i, \alpha, i') \in R\colon (\Sigma, R, i') \models \phi$; rest as usual.

Next: an example.
Then: what is ?

An example

Consider the modal transition system



where dashed lines specify R^{c} and solid lines depict R^{a}.

- $(M, i) \models^{\mathrm{a}} \neg(\exists w)(\exists r)\mathtt{tt}$ holds at all i, because $(M, i) \models^{\mathrm{c}} (\exists w)(\exists r)\mathtt{tt}$ doesn't — there is no sequence of two R^{c}-transitions labeled by w and then r.

- $(M, \mathit{Sleep}) \models^{\mathrm{c}} (\exists r)(\exists r)(\exists er)(\exists w)\mathtt{tt}$ holds, because we can find (at Sleep) a sequence of four R^{c}-transitions labeled by these actions in that order. (Its assertion check, however, holds at no state.)

ementations for modal transition systems

- Define $\models^{\mathrm{m}}$, $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$:
  - $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i) \models^{\mathrm{m}} (\exists \alpha)\phi$ iff $\exists (i, \alpha, i') \in R^{\mathrm{m}} \colon (\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i') \models^{\mathrm{m}} \phi$;
  - $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i) \models^{\mathrm{m}} \neg\phi$ iff not $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i) \models^{\neg\mathrm{m}} \phi$, where $\neg\mathrm{a} = \mathrm{c}$ and $\neg\mathrm{c} = \mathrm{a}$; rest as usual;
- Define $(M, i) \sqsubseteq (N, j)$ iff $\forall \phi \in \mathcal{L} \colon (N, j) \models^{\mathrm{a}} \phi \;\Rightarrow\; (M, i) \models^{\mathrm{a}} \phi$;
- $\sqsubseteq$ has co-inductive characterization (Larsen 1989);
- $\mathtt{impl} \stackrel{\mathrm{def}}{=} \{((M, i), (N, j)) \mid (N, j) \sqsubseteq (M, i),\ (N, j) \in \mathtt{up}(\mathcal{T})\}$.

A domain of modal transition systems (HJS'03)

- additional assumption of **finite branching**:
  $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}, s \in \Sigma, \alpha \in \mathtt{Act} \;\Rightarrow\; \{s' \in \Sigma \mid (s, \alpha, s') \in R^{\mathrm{m}}\}$ finite;

- mixed power-domain (Heckmann 1990; Gunter 1992) M_D contains those (L, U), where L is Scott-closed and U Scott-compact upper in D, and $L = {\downarrow}(L \cap U)\}$ — ordered by $(L, U) \leq (L', U')$ iff $L \subseteq L'$ and $U' \subseteq U$;

- $\mathcal{U}$ SFP domain, initial solution of domain equation

$$D = \textstyle\prod_{\alpha \in \mathtt{Act}} \mathsf{M}_{\mathcal{U}}$$

- Element $d = ((d^{\mathrm{a}}_\alpha, d^{\mathrm{c}}_\alpha))_{\alpha \in \mathtt{Act}} \in \mathcal{U}$ as MTS $(\mathcal{U}, d)$: $(d, \alpha, d') \in R^{\mathrm{m}}$ iff $d' \in d^{\mathrm{m}}_\alpha$.

Example: $\perp_{\mathcal{U}}$ is $((\{\}, \mathcal{U}))_{\alpha \in \mathtt{Act}}$; $\mathsf{M}_{\{*\}}$ are the "flat booleans."

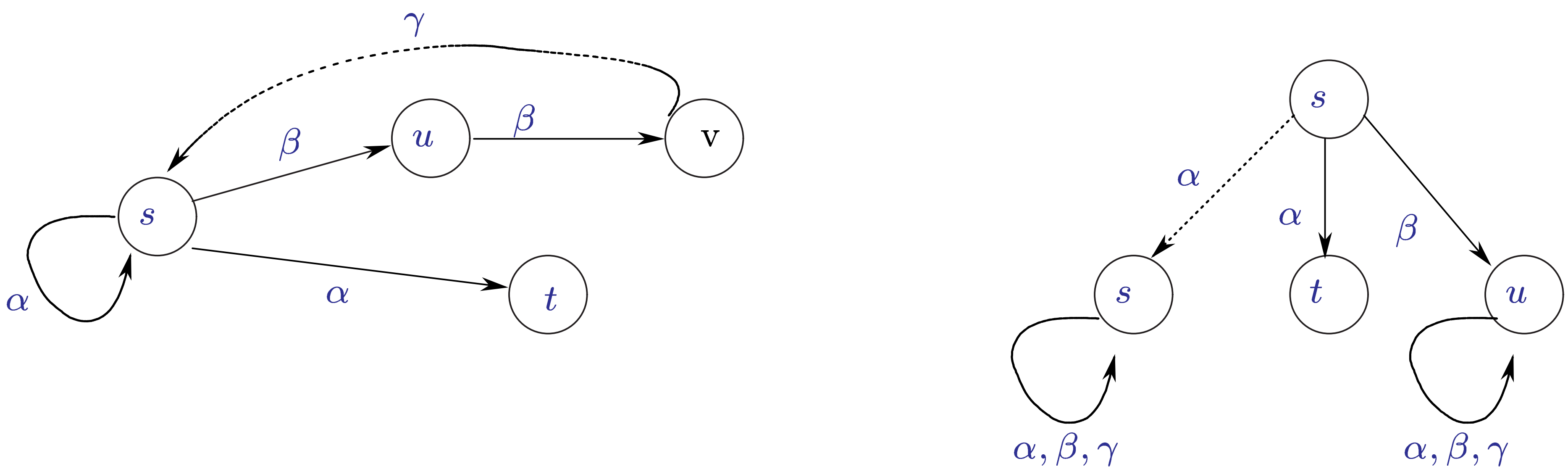
Universality of domain (HJS'03)

- **Properties as open/closed sets:** For all $\phi \in \mathcal{L}$,
  - the set $\llbracket \phi \rrbracket^{\mathrm{a}} \stackrel{\mathrm{def}}{=} \{d \in \mathcal{U} \mid (\mathcal{U}, d) \models^{\mathrm{a}} \phi\}$ is Scott-open in $\mathcal{U}$ and every compact element in $\mathcal{U}$ is of that form;
  - the set $\llbracket \phi \rrbracket^{\mathrm{c}} \stackrel{\mathrm{def}}{=} \{d \in \mathcal{U} \mid (\mathcal{U}, d) \models^{\mathrm{c}} \phi\}$ is Scott-closed in $\mathcal{U}$; uses Hofmann-Mislove Theorem;
- **Internal full abstraction:** the order $\leq_{\mathcal{U}}$ on $\mathcal{U}$ equals $\sqsubseteq^{-1} \cap \mathcal{U} \times \mathcal{U}$;
- **Universality:** there is a map $\langle\!| \ |\!\rangle : MTS \to \mathcal{U}$ such that $((M, i), (\mathcal{U}, \langle\!| (M, i) |\!\rangle)) \in \ \sqsubseteq \cap \sqsubseteq^{-1}$ for all MTSs (M, i).

Example: A system with one state and no transitions is embedded as $(\{\}, \{\})_{\alpha \in \mathtt{Act}}$.

Approximative embeddings

We define $\langle\!| \ (M, i) \ |\!\rangle$ as the directed supremum of $\langle\!| \ (M[n], i) \ |\!\rangle$ in $\mathcal{U}$.



To the left: an MTS (M, s). To the right: its finite approximation $(M[1], s)$, where s is unfolded once. (R^{c}-transitions that shadow R^{a}-transitions are omitted.)

Consistency of mix condition (HJS'03)

- In $\mathcal{U}$, we don't have $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$ since $L = \downarrow(L \cap U)$ does not imply $L \subseteq U$.
- In $\mathcal{U}$, we do have: $\forall(d, \alpha, d') \in R^{\mathrm{a}}\ \exists d'' \in \mathcal{U}\colon (d, \alpha, d'') \in R^{\mathrm{a}} \cap R^{\mathrm{c}}$ and $d'' \sqsubseteq d'$.
- Models $(\Sigma, R^{\mathrm{a}}, R^{\mathrm{c}}, i)$ with that property are consistent and are equivalent with respect to $\sqsubseteq$ to their saturation $(\Sigma, R^{\mathrm{a}} \cap R^{\mathrm{c}}, R^{\mathrm{c}})$;
- the saturation $(\Sigma, R^{\mathrm{a}} \cap R^{\mathrm{c}}, R^{\mathrm{c}})$ is a modal transition system;
- thus, elements of $\mathcal{U}$ generalize modal transition systems — without any sacrifices —
  - in that finite branching is replaced with **compactness**; and
  - the discrete consistency condition $L \subseteq U$ is replaced with the **ordered** consistency condition $L = \downarrow(L \cap U)$.

Maximal points

- Define $[(M,i)] \stackrel{\text{def}}{=} \{(N,j) \mid ((N,j),(M,i)) \in \sqsubseteq \cap \sqsubseteq^{-1}\}$, the equivalence class of (M,i) induced by $\sqsubseteq$;
- $\mathcal{U}$ universal $\Rightarrow$ $\mathcal{U}$ determines a choice function f, where each $[(M,i)]$ contains an element $f([(M,i)]) \in \mathcal{U}$;
- Since our reasoning will equate equivalent models, we identify elements of d with their equivalence class $[(\mathcal{U},d)]$; thus, $\mathcal{U}$ is a "quotient space;"
- for $d \sqsubseteq_t d' \stackrel{\text{def}}{=} \forall \phi \in \mathcal{L}\colon (\mathcal{U},d) \models^{\mathrm{a}}_t \phi \Rightarrow (\mathcal{U},d') \models^{\mathrm{a}}_t \phi$, we have
  - $d \leq e$ in $\mathcal{U} \Rightarrow d \sqsubseteq_t e$; converse?
  - can show: $d \sqsubseteq_t e$ iff $\uparrow e \cap \max(\mathcal{U}) \subseteq \uparrow d \cap \max(\mathcal{U})$.

LTS as maximal point space

- can show: $\max(\mathcal{U}) = \{d \in \mathcal{U} \mid \forall \phi \in \mathcal{L} \colon d \models^{c} \phi \;\Leftrightarrow\; d \models^{a} \phi\}$;
- all labeled transition systems get embedded into $\max(\mathcal{U})$; every $d \in \max(\mathcal{U})$ corresponds to a "topological" LTS;
- $\max(\mathcal{U})$ is a complete separable ultrametric space, aka a zero-dimensional Polish space, since $\mathcal{U}$ is SFP domain this follows from (Flagg & Kopperman 1997); to see zero-dimensionality explicitly:
  - $d \models^{a} \phi$ iff $d \models^{c} \phi$ on $\max(\mathcal{U})$;
  - $\{\llbracket \phi \rrbracket^{a} \mid \phi \in \mathcal{L}\}$ forms sub-basis of Scott-topology; and
  - all $\llbracket \phi \rrbracket^{c}$ are Scott-closed;
- $\max(\mathcal{U})$ compact? would then be a Stone space.

Conjectures (some of them bold)

- The map $\mu : \mathcal{U} \to [0, \infty)$ with $\mu(d) = 1/ \mid \{\phi \in \mathcal{L} \mid (\mathcal{U}, d) \models^{\mathrm{a}} \phi \text{ or } (\mathcal{U}, d) \models^{\mathrm{a}} \neg\phi\} \mid$ is a Lebesque measurement whose kernel is $\max(\mathcal{U})$;

- $\max(\mathcal{U})$ is **not** a Stone space in the topology induced by the Scott-topology of $\mathcal{U}$;

- the construction of a computational space for MTSs is generic in the reference ontology; and

- this generic construction gives rise to all computational spaces.

Conclusions

(This page is intentionally left blank.)