

Free Lunch in the Borel Hierarchy for Partial Spaces?

Michael Huth¹

¹Department of Computing
Imperial College London

Schloß Dagstuhl Seminar on *Computational Structures for Modelling
Space, Time and Causality*

22 August 2007, Schloß Dagstuhl, Germany

Based on joint work with *Adam Antonik, Patrice Godefroid, Radha
Jagadeesan, and David Schmidt*

Acknowledgment: *Victor Selivanov*

1 Reflective space of partial systems

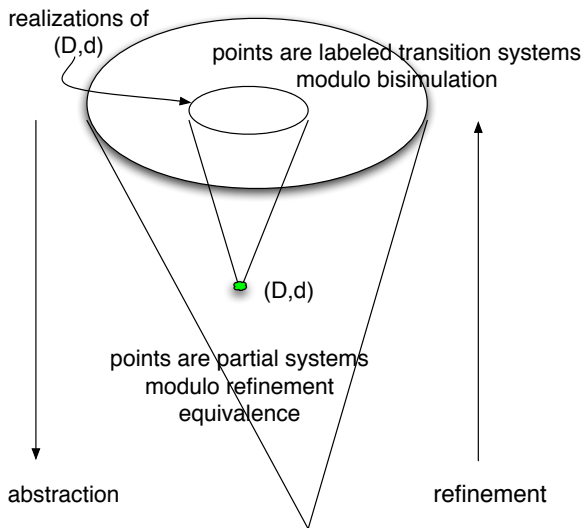
2 Model checking partial systems

3 Wrapping it up

Solving a domain equation

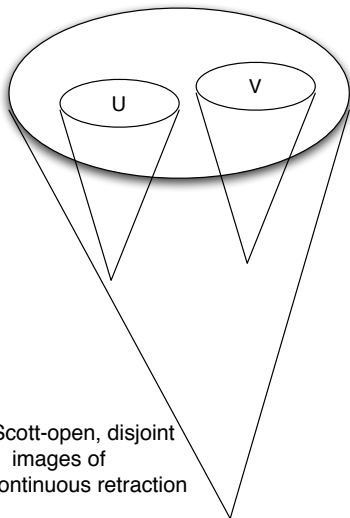
- (\mathcal{D}, \leq) initial solution of $D = \prod_{\alpha \in Act} M[D]$
- Act finite set of actions
- mixed power domain
 $M[D] = \{(L, U) \mid L = \Downarrow L, U = \Uparrow U \text{ both Lawson-closed, } \Downarrow(L \cap U) = L\}$
- $(L, U) \leq (L', U')$ iff $L \subseteq L'$ and $U' \leq U$
- $d = (d_\alpha^L, d_\alpha^U)_{\alpha \in Act}$ state of partial system
 - $d_\alpha^L \subseteq \mathcal{D}$ set of states definitely reachable from d under action α
 - $\mathcal{D} \setminus d_\alpha^U$ set of states definitely not reachable from d under action α

Partial system and its realizations



- model \mathcal{D} fully abstract: $d \leq d'$ iff partial system (\mathcal{D}, d) co-inductively refined by partial system (\mathcal{D}, d')
- model \mathcal{D} universal: all partial systems embed into \mathcal{D} , embedding preserves and reflects refinement
- model \mathcal{D} appropriate: maximal points space for labeled transition systems up to bisimulation
 - Lawson- and Scott-topology induce same topology on $\max(\mathcal{D})$
 - elements of $\max(\mathcal{D})$ all labeled transition systems up to bisimulation
 - topology on $\max(\mathcal{D})$ natural one, based on testing

Reflective space \mathcal{D} (Selivanov)



U, V Scott-open, disjoint
images of
Scott-continuous retraction

- model \mathcal{D} is reflective space:
 - there are disjoint Scott-open sets U and V in \mathcal{D} that are images of Scott-continuous retractions
- so Borel hierarchy of \mathcal{D} strict (Selivanov)
- so Borel hierarchy of $\max(\mathcal{D})$ strict, as subspace of \mathcal{D} (Selivanov)
- model checking:
 - which $d \in \mathcal{D}$ satisfy given property ϕ ?
 - understand complexity of set of all $d \in \mathcal{D}$ that satisfy ϕ

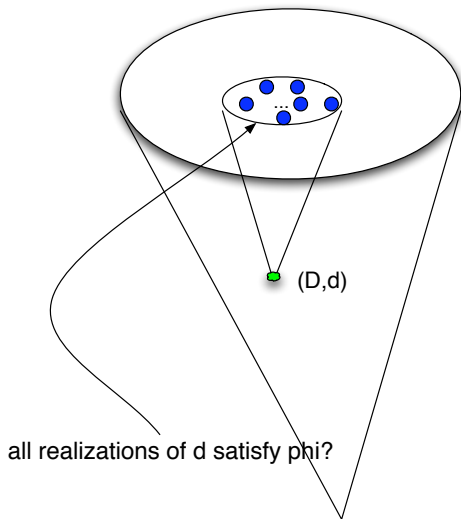
Approximation semantics for Hennessy-Milner logic

$$\phi ::= \mathbf{tt} \mid \neg\phi \mid \phi \wedge \phi \mid \langle\alpha\rangle\phi \quad (\text{HML})$$

for $m \in \{v, s\}$ with $\neg v = s$ and $\neg s = v$ we set

- $\llbracket \mathbf{tt} \rrbracket^m = \mathcal{D}$
- $\llbracket \neg\phi \rrbracket^m = \mathcal{D} \setminus \llbracket \phi \rrbracket^{\neg m}$
- $\llbracket \phi_1 \wedge \phi_2 \rrbracket^m = \llbracket \phi_1 \rrbracket^m \cap \llbracket \phi_2 \rrbracket^m$
- $\llbracket \langle\alpha\rangle\phi \rrbracket^v = \{d \in \mathcal{D} \mid d_\alpha^L \cap \llbracket \phi \rrbracket^v \neq \emptyset\}$
- $\llbracket \langle\alpha\rangle\phi \rrbracket^s = \{d \in \mathcal{D} \mid d_\alpha^U \cap \llbracket \phi \rrbracket^v \neq \emptyset\}$

Note that $\llbracket \neg\langle\alpha\rangle\neg\phi \rrbracket^v = \{d \in \mathcal{D} \mid d_\alpha^U \subseteq \llbracket \phi \rrbracket^v\}$.



$$V_\phi = \{d \in \mathcal{D} \mid \max(\mathcal{D}) \cap \uparrow d \subseteq \llbracket \phi \rrbracket^v\}$$

- $d \in V_\phi$ iff all realizations of d satisfy ϕ , noting that

$$\llbracket \phi \rrbracket^v \cap \max(\mathcal{D}) = \llbracket \phi \rrbracket^s \cap \max(\mathcal{D})$$

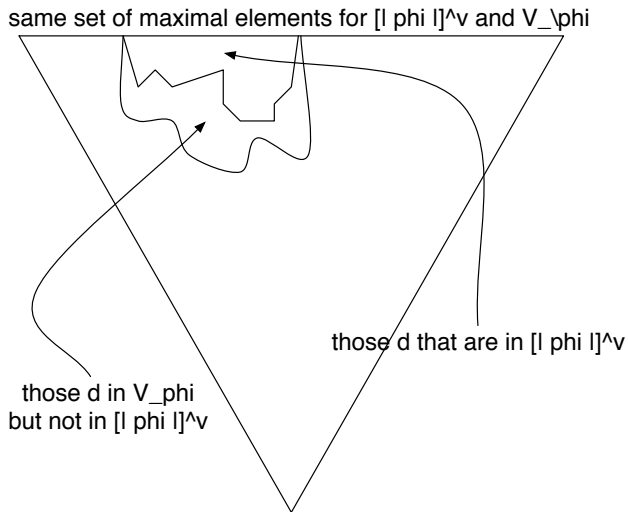
is usual semantics of HML for labeled transition systems

- approximation is sound

$$\llbracket \phi \rrbracket^v \subseteq V_\phi$$

generally incomplete

Approximative vs. precise semantics: picture



Consider all d for which (\mathcal{D}, d) is “finite-state”:

- “ $d \in \llbracket \phi \rrbracket^v?$ ” efficiently computable:
 - linear complexity for propositional logic and HML
 - in $\text{NP} \cap \text{coNP}$ for modal mu-calculus
- “ $d \in V_\phi?$ ” generally expensive
 - coNP-complete for propositional logic
 - PSPACE-complete for HML
 - EXPTIME-complete for modal mu-calculus

Expressiveness of approximation

$$\forall \phi \in \text{HML} \exists \phi^\vee \in \text{HML}: V_\phi = \llbracket \phi^\vee \rrbracket^\vee \quad (\text{SM})$$

- in particular, all V_ϕ are Scott-compact, Scott-open in \mathcal{D}
- (SM) also holds if HML is replaced with the modal mu-calculus — HML extended with least and greatest fixed points
- for CTL formula, written in state-based form,

$$\eta = \neg A[\text{EX}q_1 U(q_1 \rightarrow q_2)]$$

$V_\eta \neq \llbracket \psi \rrbracket^\vee$ for all CTL* formulas ψ

- worst-case: length of ϕ^\vee exponential in length of ϕ
- so checking “ $d \in \llbracket \phi^\vee \rrbracket^\vee$?” not necessarily cheaper than checking “ $d \in V_\phi$?”

Empirical precision of approximation

All patterns from patterns.projects.cis.ksu.edu, given in state-based form,

- either satisfy auspicious $\phi = \phi^\vee$, e.g.:
 - “Absence of P, After Q Until R”:
 $AG(Q \wedge \neg R \rightarrow A[PWR])$
 - “Precedence Chain: Two Stimuli, One Response, Globally”:
 $\neg E[\neg SUP] \wedge E[\neg PU(S \wedge \neg P \wedge EX(E[\neg TU(P \wedge \neg T)]))]$
- or ϕ^\vee is linear expansion of ϕ , e.g.:
 - “Absence of P before R”:
 $A[\neg P \vee AG(\neg R)WR]^\vee = A[\neg P \vee AX(AG(\neg R))WR]$.

So linear checks of these patterns always possible.

Precision for propositional logic

- propositional logic

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \quad (\text{PL})$$

over set of propositions $(p \in)AP$, expressible in HML if $AP \subseteq Act$ and $p \in AP$ encoded as $\langle p \rangle \tau\tau$

- semantics $\llbracket \phi \rrbracket^m$ therefore derived for PL
- Consider decision problems for PL:

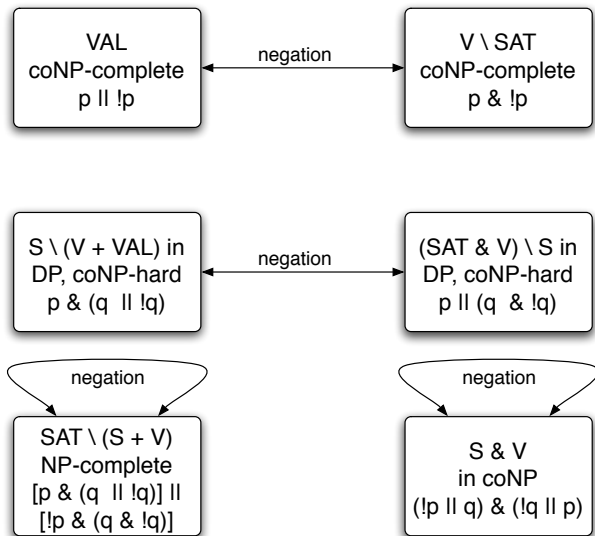
$$VAL = \{\phi \in \text{PL} \mid \phi \text{ valid}\}$$

$$SAT = \{\phi \in \text{PL} \mid \phi \text{ satisfiable}\}$$

$$V = \{\phi \in \text{PL} \mid V_\phi = \llbracket \phi \rrbracket^v\}$$

$$S = \{\phi \in \text{PL} \mid \neg\phi \in V\}$$

Partition of PL and its complexity



- Domain-theoretic model for partial systems enables study of tradeoff between precision of model checks and their computational complexity.
- Semantic transformations $\phi \mapsto \phi^v$ exist that obtain precise check for ϕ by running cheap check on ϕ^v .
- Worst case: ϕ^v exponential in ϕ so transformation not viable.
- Empirical case: patterns of ϕ that people seem to check in practice have ϕ^v as linear blow-up of ϕ only.
- Still need to understand complexity of deciding whether transformation can be the identity: “ $\phi = \phi^v$?”:
 - presented partial results on propositional logic
 - have made progress for HML and the modal mu-calculus.¹

¹Not reported here.

- A. Antonik & M. Huth *Efficient Patterns for Model Checking Partial State Spaces in $CTL \cap LTL$* . ENTCS 158:41–57, 2006.
- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS'05, pages 158–167, 2005.
- M. Huth, R. Jagadeesan, and D. Schmidt *A domain equation for refinement of partial systems*. Mathematical Structures in Computer Science 14(4):469–505, 2004.
- M. Huth *Labelled Transition Systems as a Stone Space*. Logical Methods in Computer Science 1(1:1)1-28, 2005.
- M. Huth *Refinement is Complete for Implementations*. Formal Aspects of Computing 17(2):113–137, 2005.