

On the complexity of
semantic self-
minimization

AVoCS 2007

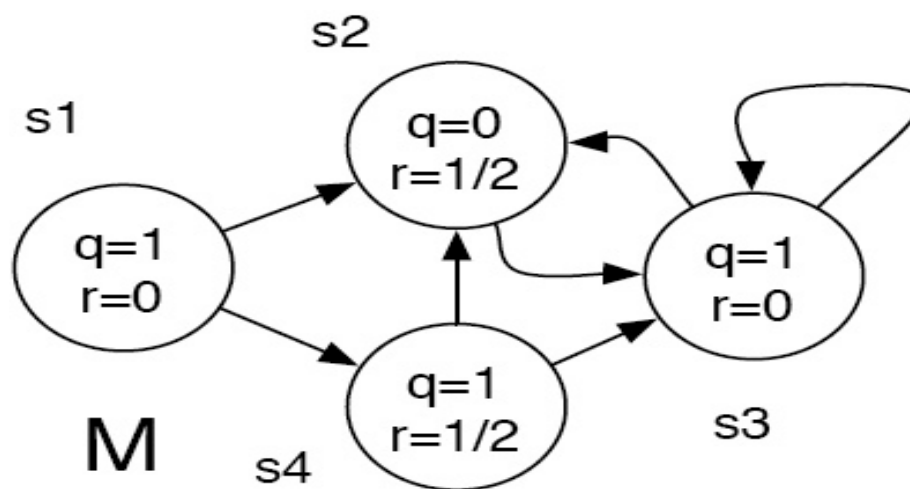
*Adam Antonik &
Michael Huth*

imperial.ac.uk/quads



Partial Kripke structures

- Often need aggressive abstraction of model prior to model checking
- Partial state spaces facilitate this, as Kripke structures with *3-valued* labeling [Bruns & Godefroid 1999]



Abstraction-based model checking

- Partial Kripke structures have abstraction & refinement notion
- System = Kripke structure
- Abstraction = *Partial* Kripke structure, refined by System
- Verification Problem: “*Do all Kripke structure refinements of Abstraction satisfy formula of mu-calculus?*”
 - If so, System will satisfy it, too.
 - If not, we may be no wiser.

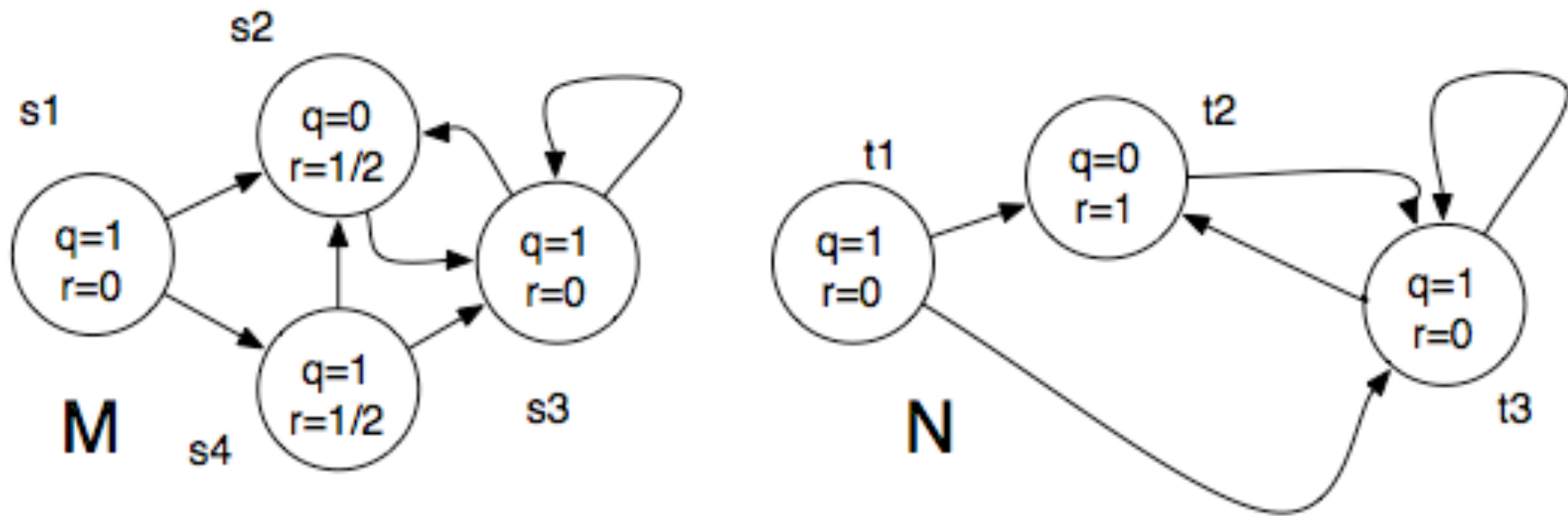
Complexity, Soundness & Incompleteness

- Verification Problem: “*Do all Kripke structure refinements of Abstraction satisfy formula of mu-calculus?*”
- This is EXPTIME-complete in formula, quadratic in model [Bruns & Godefroid 2000]
- Approximate version of Verification Problem linear in formula/model [Bruns & Godefroid 1999]
- If approximate version verifies abstraction, system also verified (*soundness*)
- If approximate version doesn't verify abstraction, system may still satisfy considered formula: *under-approximation* (incompleteness)

Refinement = Abstraction⁻¹

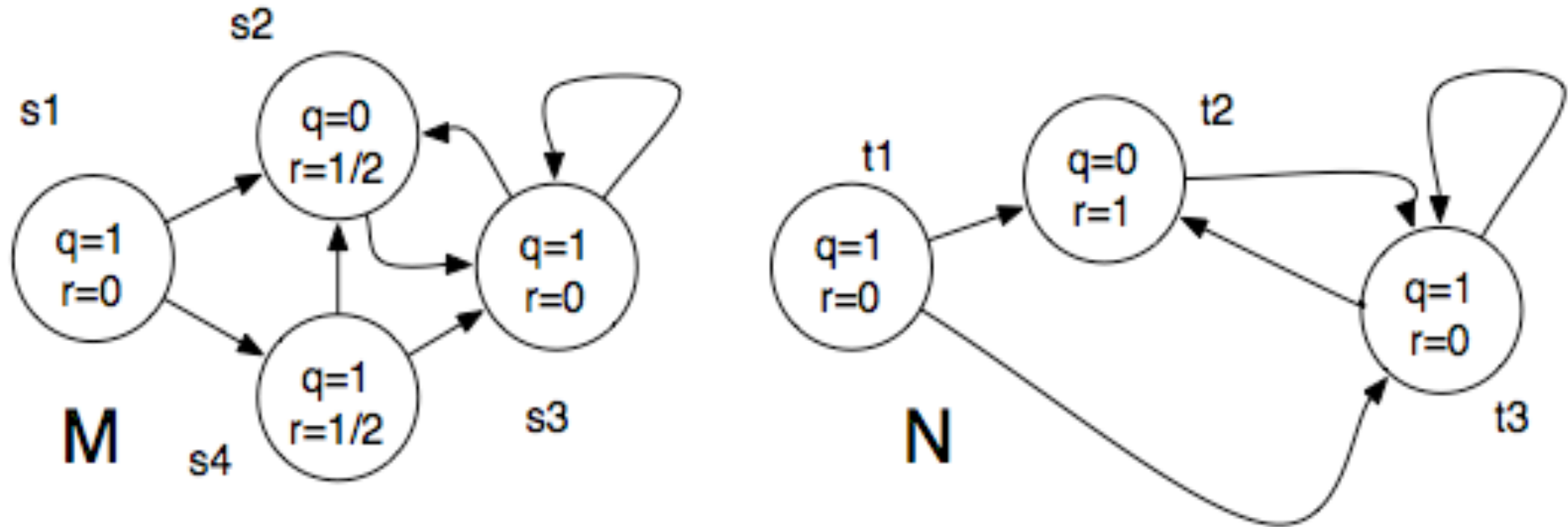
A binary relation $\preceq \subseteq S_M \times S_N$ is a refinement iff $s \preceq t$ implies

- (a) $L(s, q) \leq_i L(t, q)$ for all $q \in \mathbb{AP}$,
- (b) for all $(s, s') \in R_M$ there is $(t, t') \in R_N$ with $s' \preceq t'$, and
- (c) for all $(t, t') \in R_N$ there is $(s, s') \in R_M$ with $s' \preceq t'$.



$$1/2 \leq_i 0 \text{ and } 1/2 \leq_i 1$$

Example



*Pointed Kripke structure (N, t_1)
 refines pointed model (M, s_1)*

Formal Verification Problem

(M,s) pointed model: M with initial state s

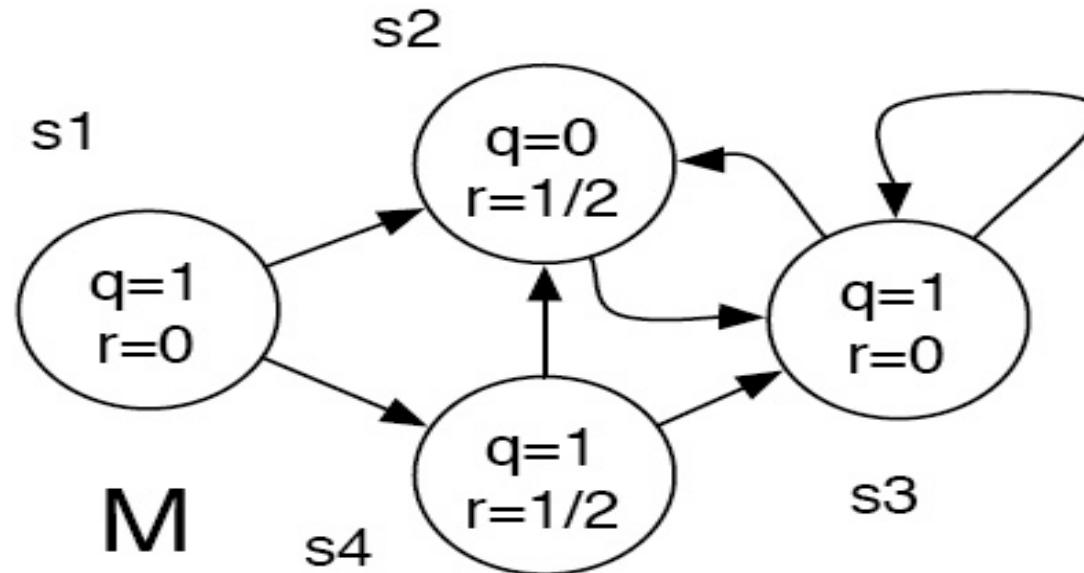
$$\text{VAL}(M, s, \phi)$$

holds iff all pointed Kripke structures that refine (M,s) satisfy ϕ

$$\text{SAT}(M, s, \phi)$$

holds iff some pointed Kripke structure refines (M,s) and satisfies ϕ

Example

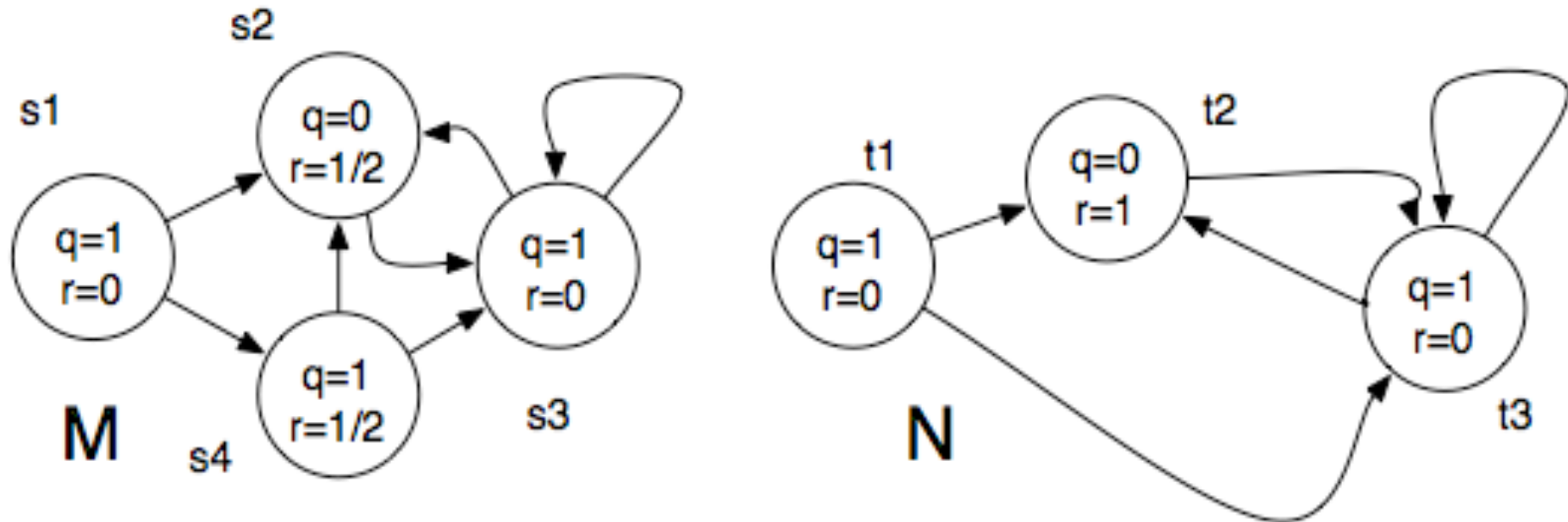


$\text{VAL}(M, s_1, \text{AF}(q \wedge \neg r))$

$\text{VAL}(M, s_1, \text{AF EG } \neg r)$

Both judgments hold

Counterexample



$$\text{VAL}(M, s_1, \text{AF AG } \neg r)$$

Doesn't hold: (N, t1) is counterexample

Approximate versions of judgments

- Use semantics similar to labeling algorithm
- Compositionally evaluate sub-formulas
- Do this *in pessimistic and in optimistic mode* for $\phi ::= q \mid Z \mid \phi \wedge \phi \mid \neg\phi \mid \text{EX } \phi \mid \mu Z.\phi$
- Pessimistic mode: under-approximates
$$\text{VAL}(M, s, \phi)$$
- Optimistic mode: over-approximates
$$\text{SAT}(M, s, \phi)$$

Optimistic (o) and pessimistic (p) approximative semantics for mu-calculus

Partial Kripke structure $M = (S, R, L)$

$$\models q \Vdash_{\rho}^o = \{s \mid L(s, q) \neq 0\}$$

$$\models q \Vdash_{\rho}^p = \{s \mid L(s, q) = 1\}$$

$$\models Z \Vdash_{\rho}^o = \rho(Z)$$

$$\models Z \Vdash_{\rho}^p = \rho(Z)$$

$$\models \phi \wedge \psi \Vdash_{\rho}^o = \models \phi \Vdash_{\rho}^o \cap \models \psi \Vdash_{\rho}^o$$

$$\models \phi \wedge \psi \Vdash_{\rho}^p = \models \phi \Vdash_{\rho}^p \cap \models \psi \Vdash_{\rho}^p$$

$$\models \neg \phi \Vdash_{\rho}^o = S \setminus \models \phi \Vdash_{\rho}^p$$

$$\models \neg \phi \Vdash_{\rho}^p = S \setminus \models \phi \Vdash_{\rho}^o$$

$$\models \text{EX } \phi \Vdash_{\rho}^o = \text{pre}(\models \phi \Vdash_{\rho}^o)$$

$$\models \text{EX } \phi \Vdash_{\rho}^p = \text{pre}(\models \phi \Vdash_{\rho}^p)$$

$$\models \mu Z. \phi \Vdash_{\rho}^o = \text{lfp } F_{\phi, \rho}^o$$

$$\models \mu Z. \phi \Vdash_{\rho}^p = \text{lfp } F_{\phi, \rho}^p$$

Formal soundness of approximation

For sentence ϕ and for $m \in \{o, p\}$ set

$$(M, s) \models^m \phi \quad \stackrel{\text{def}}{=} \quad s \in \llbracket \phi \rrbracket_\rho^m \text{ for some } \rho$$

Soundness as two, co-dependent,
implications:

$$(M, s) \models^p \phi \text{ implies } \text{VAL}(M, s, \phi)$$

$$\text{SAT}(M, s, \phi) \text{ implies } (M, s) \models^o \phi$$

Incompleteness of approximation

- If $L(s,q) = 1/2$, then the tautology $q \vee \neg q$ holds at state s , but the pessimistic semantics won't verify this.
- But pessimistic semantics is complete for many practically relevant property patterns [Antonik & Huth 2006], e.g.

$$\neg E[\neg q U r] \wedge E[\neg r U (q \wedge \neg r \wedge EX (E[\neg s U (r \wedge \neg s)])))]$$

“precedence chain: 2 stimuli, 1 response; globally, q and s precede r ”

patterns.project.cis.ksu.edu

Semantic self-minimization

- Sentence ϕ *pessimistically self-minimizing*:

Iff for all pointed models (M, s)

$$(M, s) \models^p \phi \Leftrightarrow \text{VAL}(M, s, \phi)$$

- Sentence ϕ *optimistically self-minimizing*:

Iff for all pointed models (M, s)

$$(M, s) \models^o \phi \Leftrightarrow \text{SAT}(M, s, \phi)$$

Decision Problems

- OSM = set of optimistically self-minimizing sentences
- PSM = set of pessimistically self-minimizing sentences
- VAL = set of valid sentences
- UNSAT = set of unsatisfiable sentences

Logics

Decision problems considered for three logics (i.e. for their sets of sentences):

- Propositional modal mu-calculus
- Propositional modal logic (no fixed points)
- Propositional logic (no fixed points, no modal operators)

Use generic variable for logics when convenient:

$$\mathcal{L} \in \{MC, PML, PL\}$$

Partition

- Logic partitioned into six sets:

I VAL

II UNSAT

III $OSM \setminus (VAL \cup PSM)$

IV $PSM \setminus (UNSAT \cup OSM)$

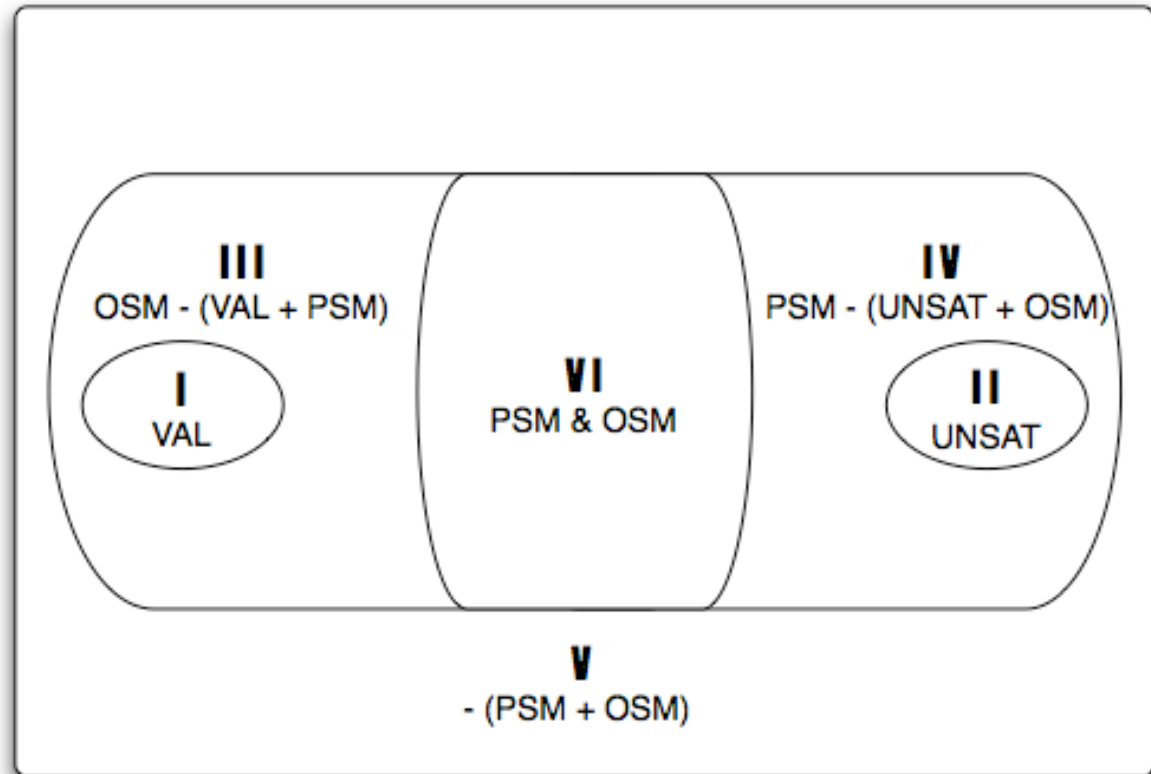
V $\mathcal{L} \setminus (PSM \cup OSM)$

VI $PSM \cap OSM$

Partition in a picture

Negation maps pairs of sets into each other:

- OSM and PSM
- I and II
- III and IV
- V and itself
- VI and itself



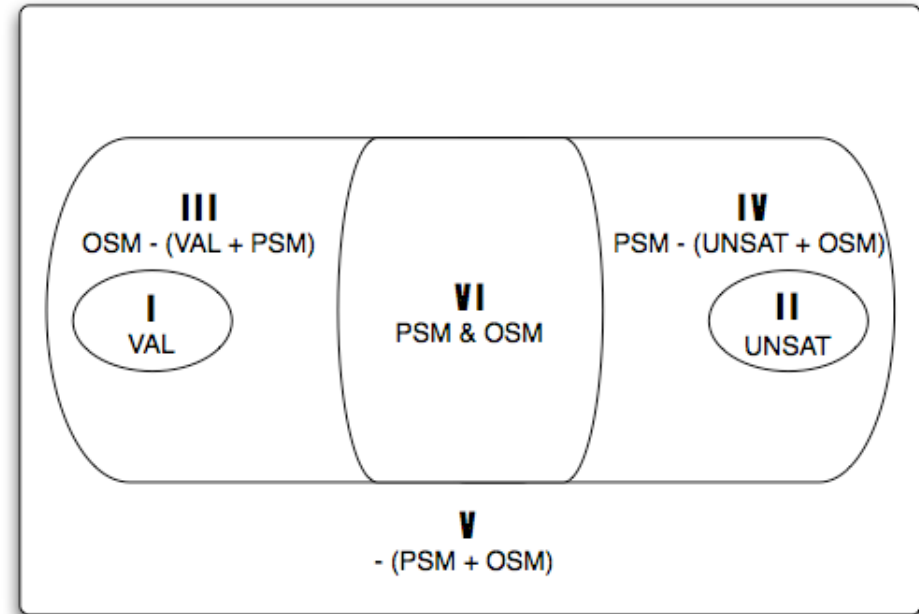
Also, VAL in OSM and disjoint from PSM.

Dually, UNSAT in PSM and disjoint from OSM.

Sets I and II

Deciding membership
in sets I and II has
- of course -
same complexity as
deciding validity of logic:

- EXPTIME-complete for mu-calculus
- PSPACE-complete for modal logic
- coNP-complete for propositional logic



Set OSM, hardness result

- Sentence in OSM iff its negation is in PSM
- So OSM and PSM have same complexity
- Deciding OSM at least as hard as deciding validity of logic:

$$E(\phi) = \phi \vee (x \wedge \neg x)$$

where x atomic proposition not occurring in ϕ

- This is desired reduction to VAL:

ϕ is valid iff $E(\phi)$ is in OSM

Hardness proof (for illustration)

- Let ϕ be valid, so $E(\phi)$ valid and so in OSM
- Let $E(\phi)$ be is OSM. Proof by contradiction: ϕ not valid, so ϕ false at some pointed Kripke structure (K,t) . Extend labeling L of K with $L(s,x) = 1/2$ for all states s , so K now partial Kripke structure. We get

$$(K, t) \models^o E(\phi)$$

for this extended K , but no refining Kripke structure of extended (K,t) satisfies $E(\phi)$ as this is semantically equivalent to ϕ on Kripke structures

Set OSM, upper bound for mu-calculus

- For mu-calculus, OSM in 2EXPTIME
- From ϕ construct two alternating tree automata - exponential blowup in worst case - and then do language inclusion check for these automata - exponential in size of these automata [Godefroid & Huth 2005]:

$$\mathcal{L}(A_{\models^o}^3) \subseteq \mathcal{L}(A_{\phi}^3)$$

- This language inclusion checks “*completeness half*” of

$$(M, s) \models^o \phi \Leftrightarrow \text{SAT}(M, s, \phi)$$

for all pointed models (M, s)

Set OSM, upper bound for modal logic

- For modal logic, OSM in EXPSPACE
- From ϕ construct two two alternating tree automata as before, and again check

$$\mathcal{L}(A_{\models \phi}^3) \subseteq \mathcal{L}(A_{\phi}^3)$$

- Both automata cannot distinguish trees at depths greater than size of ϕ (so called “*shallow model property*” of modal logic)
- So the above check is in PSPACE in the size of the automata

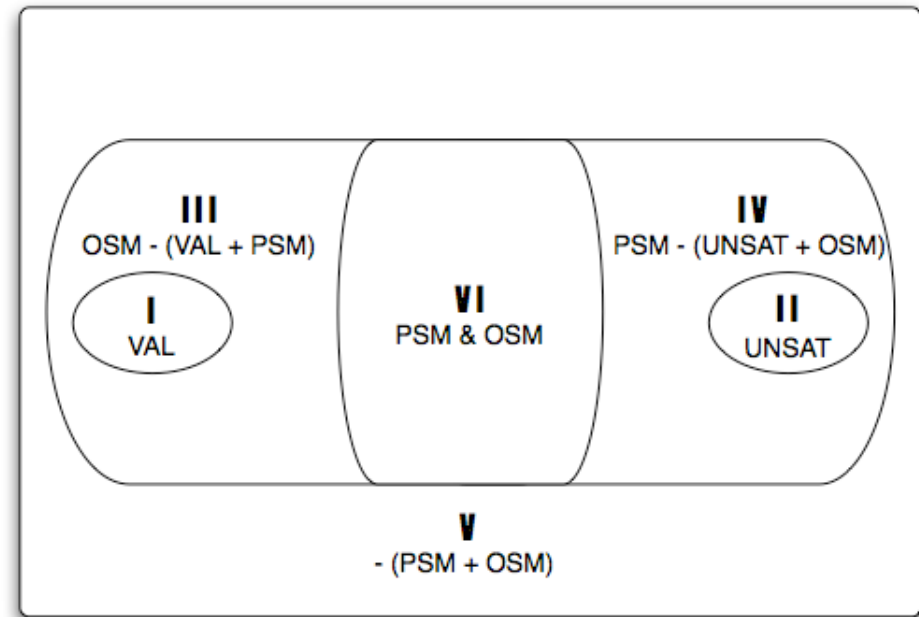
Set OSM, exact bound for propositional logic

- Already showed OSM is coNP-hard
- Show PL - OSM in NP:

```
boolean NotInOSM(phi) {
  **choose** model M such that M(x) = 1/2 for some x in AP(phi);
  if (M |=o phi) {
    for (all x in AP(phi) with M(x) = 1/2) {
      if (!(M[x --> 0] |=o phi) && !(M[x --> 1] |=o phi)) {
        ACCEPT;
      }
    }
  }
  REJECT;
}
```

Set III

Deciding set III at least as hard as deciding OSM, and so at least as hard as deciding VAL:



$$F(\phi) = (\phi \vee x) \wedge (y \wedge (z \vee \neg z))$$

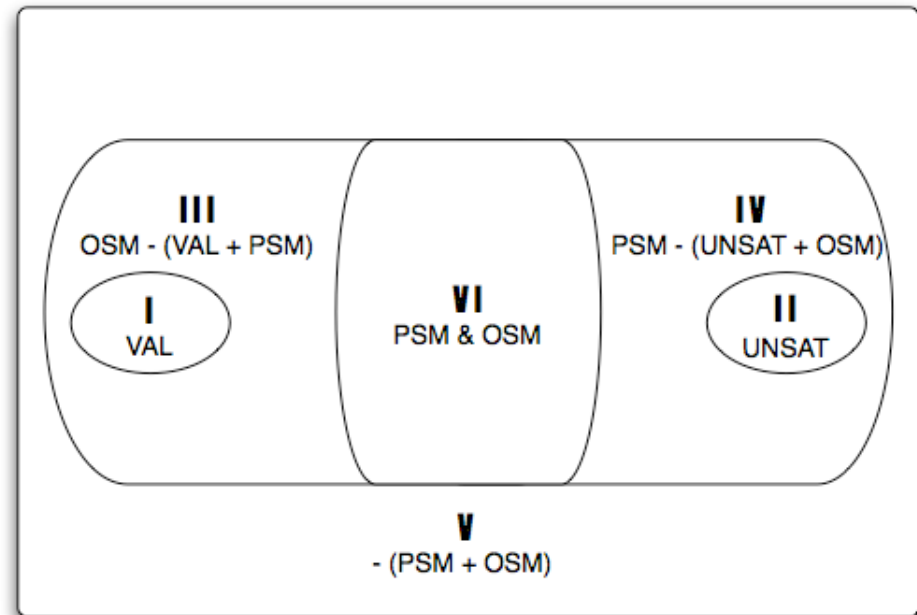
where x,y,z atomic propositions not occurring in ϕ

F is desired reduction:

$$F(\phi) \in \mathbf{III} \iff \phi \in \mathbf{OSM}$$

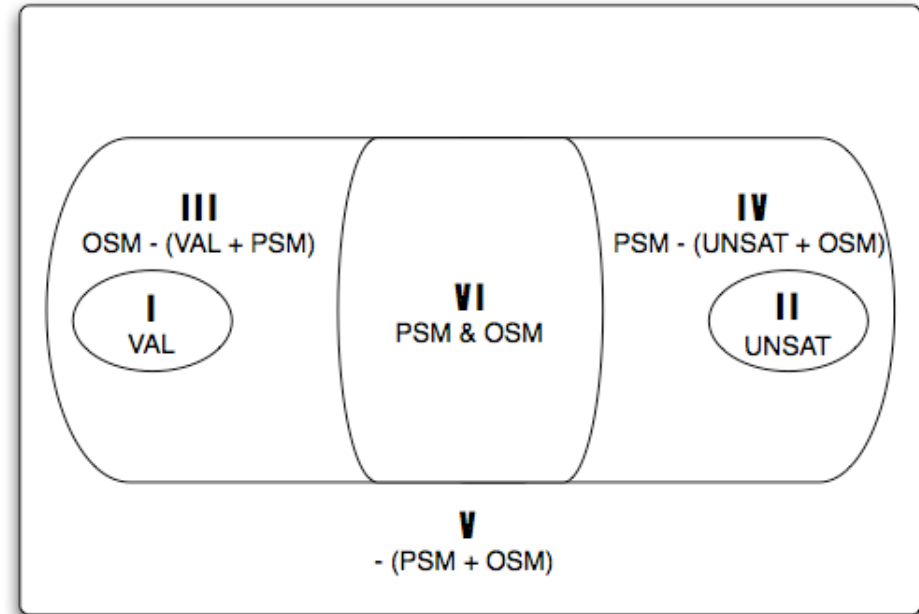
Set III, upper bound

- Mu-calculus: set III in $2EXPTIME$
- Modal logic: set III in $EXSPACE$
- Propositional logic: set III in DP (as intersection of language in NP with language in coNP) and coNP-hard
Don't know whether set III is DP-complete.



Set V

Deciding set V at least as hard as deciding *satisfiability* of the logic:



$$G(\phi) = (\phi \wedge (x \vee \neg x) \wedge y) \vee (z \wedge \neg z)$$

where x,y,z atomic propositions not occurring in ϕ

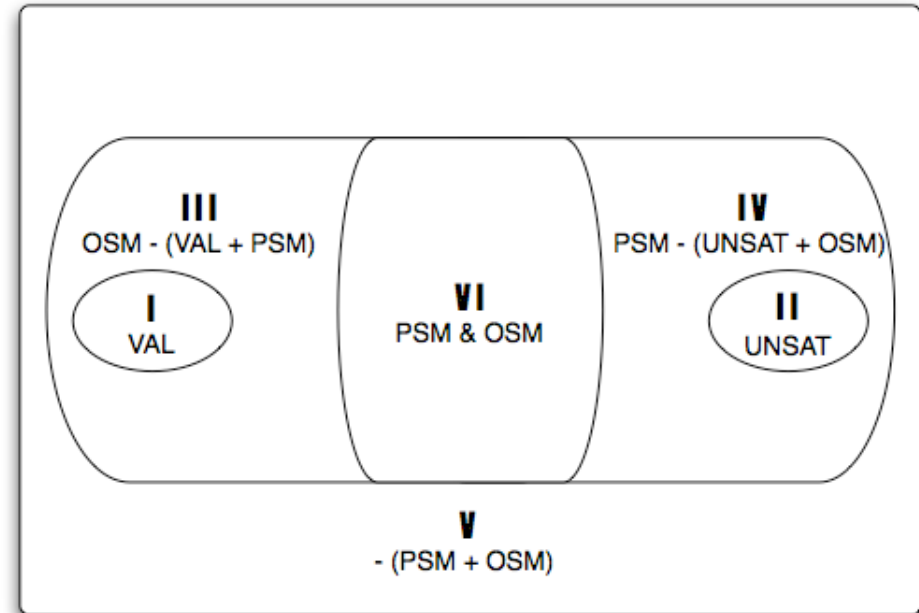
G is desired reduction:

$$\phi \text{ satisfiable} \iff G(\phi) \in \mathbf{V}$$

As upper bounds, we again get 2EXPTIME, EXPSPACE, and NP(-complete) - respectively

Set VI

- Formulas in set VI complete for optimistic and pessimistic approximate semantics

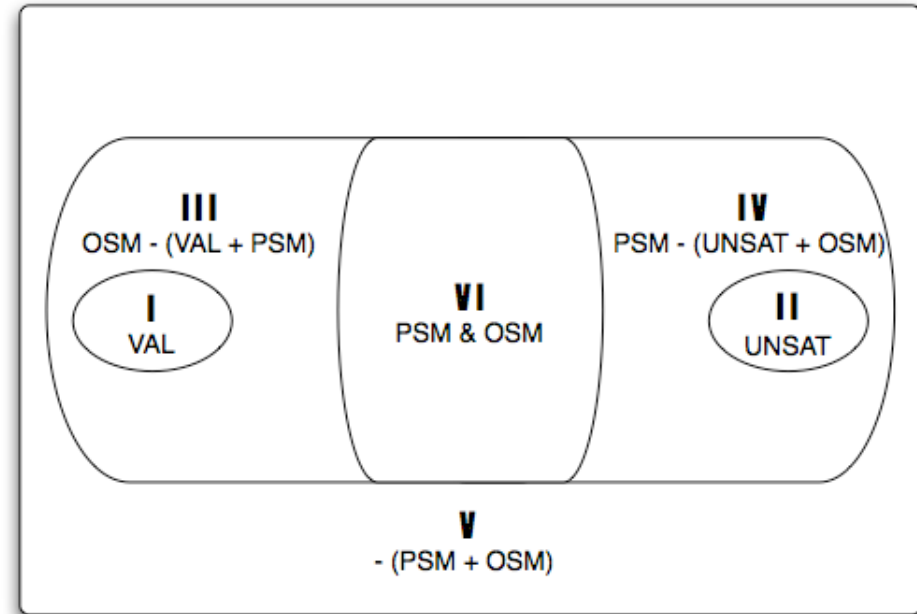


- From our results we immediately get upper bounds $2EPXTIME$, $EXPSPACE$ and $coNP$ for μ -calculus, modal logic, and propositional logic (respectively):

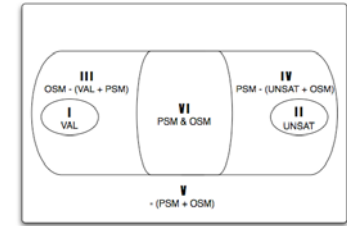
$$(\phi \in PSM \cap OSM) \Leftrightarrow (\phi \in OSM \ \& \ \neg\phi \in OSM)$$

“Experimental” data

- Used Perl script to randomly generate “all” formulas of propositional logic for sizes 1 to 5
- Size = number of occurrences of logical connectives in formula
- Brute-force decision of membership: in OSM (~75%), in set VI (~50%), and in NP-complete set V (~2.45%)
- Less formulas seem to be in set VI as number of logical operators in formula increases

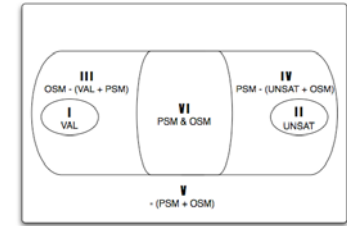


Summary of results for mu-calculus



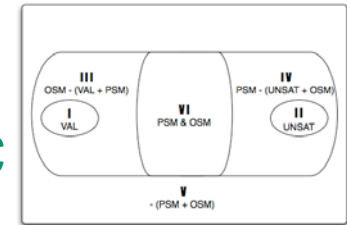
2EXPTIME, EXPTIME-hard	EXPTIME-complete	2EXPTIME
OSM	VAL	PSM \cap OSM
PSM	UNSAT	
OSM \setminus (VAL \cup PSM)		
PSM \setminus (UNSAT \cup OSM)		
$MC \setminus$ (PSM \cup OSM)		

Summary of results for modal logic



EXPSPACE, PSPACE-hard	PSPACE-complete	EXPSPACE
OSM	VAL	PSM \cap OSM
PSM	UNSAT	
$OSM \setminus (VAL \cup PSM)$		
$PSM \setminus (UNSAT \cup OSM)$		
$PML \setminus (PSM \cup OSM)$		

Summary of results for propositional logic

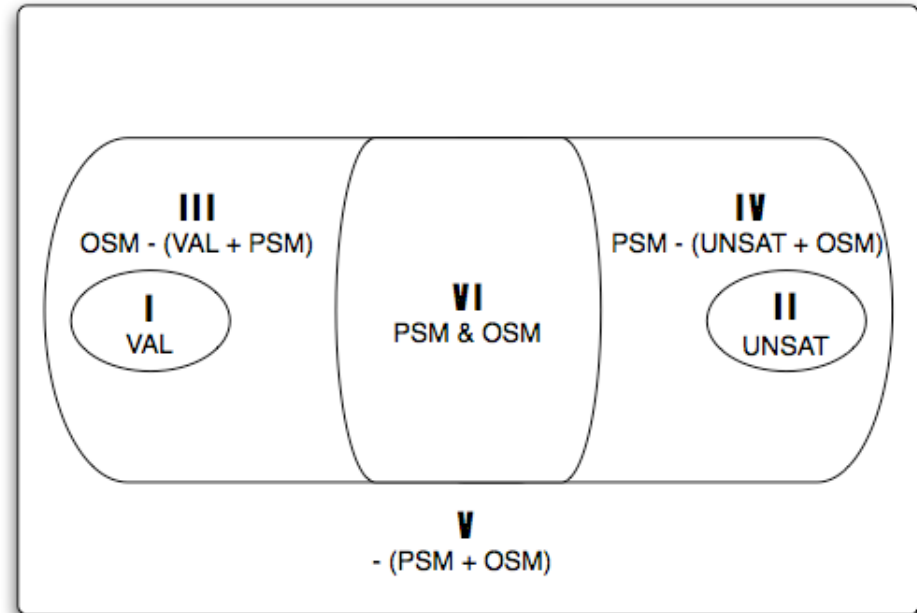


DP, coNP-hard	NP-complete	coNP-complete	coNP
$OSM \setminus (VAL \cup PSM)$	$\mathcal{P}\mathcal{L} \setminus (PSM \cup OSM)$	VAL	$PSM \cap OSM$
$PSM \setminus (UNSAT \cup OSM)$		UNSAT	
		OSM	
		PSM	

Conclusions

- Studied complexity of deciding whether a formula loses precision in an approximate semantics for 3-valued models.
- For mu-calculus and modal logic, we showed that the complexity of validity is a lower bound for this, our upper bounds show an exponential gap.
- For propositional logic, this gap disappears.
- For propositional logic, deciding whether a formula loses precision for optimistic and pessimistic approximation matches complexity of satisfiability.

Future work



- Narrow currently exponential complexity gap for OSM, for mu-calculus and modal logic.
- Attempt hardness proofs for sets VI. Study Turing reductions.
- Study precision of patterns outside of LTL&CTL and ACTL.
- Study self-minimization for linear-time temporal logics.

Related work (not already discussed)

- [Larsen & Thomsen 1989] studied partial models of labeled transition systems and their refinement
- [Van Frassen 1966] defined and studied supervaluational meaning as precise version of approximate 3-valued semantics
- [Blamey 1980] proved that propositional logic formulas always have (in our terminology) semantically equivalent formulas that are self-minimizing
- [Reps et al. 2002] used BBDs and prime-implicants to implement semantic minimizations of propositional logic more efficiently

References to all related work are in the paper.

Thank you.

