

# Semantic Minimizations for Temporal Logics

Michael Huth<sup>1</sup>

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

Semantics and its Applications Workshop  
19-20 December 2005, Tel Aviv, Israel  
**Joint work with Patrice Godefroid**

- 1 Propositional logic
- 2 Temporal logics
- 3 References & Acknowledgments

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a main method”

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a `main` method”
- **behavior:** “an audio plug-in may be present in a browser”

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a `main` method”
- **behavior:** “an audio plug-in may be present in a browser”
- **interface:** “requires `balance >= 0`”

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a main method”
- **behavior:** “an audio plug-in may be present in a browser”
- **interface:** “requires balance  $\geq 0$ ”
- **topology:** “node may have no neighbor in broadcast range”

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a main method”
- **behavior:** “an audio plug-in may be present in a browser”
- **interface:** “requires balance  $\geq 0$ ”
- **topology:** “node may have no neighbor in broadcast range”
- **shape analysis:** “pointer  $x$  may point to cell  $c$  in the heap”

# Applications of under-specification or abstraction

- **state:** “a .NET component may have a main method”
- **behavior:** “an audio plug-in may be present in a browser”
- **interface:** “requires balance  $\geq 0$ ”
- **topology:** “node may have no neighbor in broadcast range”
- **shape analysis:** “pointer  $x$  may point to cell  $c$  in the heap”
- **space-time:** “packets will get through in ad-hoc network”

# Under-specifying propositional models

- models, total functions from atomic propositions to 0, 1/2, 1:  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  refines model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  **refines** model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$
- e.g.  $[p \mapsto 1, q \mapsto 0]$  refines  $[p \mapsto 1/2, q \mapsto 0]$  but  
 $[p \mapsto 1, q \mapsto 1]$  does not refine  $[p \mapsto 1/2, q \mapsto 0]$

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  **refines** model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$
- e.g.  $[p \mapsto 1, q \mapsto 0]$  refines  $[p \mapsto 1/2, q \mapsto 0]$  but  
 $[p \mapsto 1, q \mapsto 1]$  does not refine  $[p \mapsto 1/2, q \mapsto 0]$
- **propositional logic**  $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi$

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  **refines** model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$
- e.g.  $[p \mapsto 1, q \mapsto 0]$  refines  $[p \mapsto 1/2, q \mapsto 0]$  but  
 $[p \mapsto 1, q \mapsto 1]$  does not refine  $[p \mapsto 1/2, q \mapsto 0]$
- propositional logic  $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi$
- **model  $M$  2-valued iff  $M^{-1}(1/2) = \{\}$**

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  **refines** model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$
- e.g.  $[p \mapsto 1, q \mapsto 0]$  refines  $[p \mapsto 1/2, q \mapsto 0]$  but  
 $[p \mapsto 1, q \mapsto 1]$  does not refine  $[p \mapsto 1/2, q \mapsto 0]$
- propositional logic  $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi$
- model  $M$  **2-valued** iff  $M^{-1}(1/2) = \{\}$
- **thorough semantics**:  $M \models^{th} \phi$  iff all 2-valued refinements of  $M$  satisfy  $\phi$  in standard semantics

# Under-specifying propositional models

- models, total functions from atomic propositions to  $0, 1/2, 1$ :  
 $M: \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- e.g.  $[p \mapsto 1/2, q \mapsto 0]$
- model  $M'$  **refines** model  $M$  iff  
 $\forall p \in \text{AtomProp}: M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$
- e.g.  $[p \mapsto 1, q \mapsto 0]$  refines  $[p \mapsto 1/2, q \mapsto 0]$  but  
 $[p \mapsto 1, q \mapsto 1]$  does not refine  $[p \mapsto 1/2, q \mapsto 0]$
- propositional logic  $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi$
- model  $M$  **2-valued** iff  $M^{-1}(1/2) = \{\}$
- **thorough** semantics:  $M \models^{th} \phi$  iff all 2-valued refinements of  $M$  satisfy  $\phi$  in standard semantics
- e.g.  $[p \mapsto 1/2, q \mapsto 0] \models^{th} \neg q$  but  $[p \mapsto 1/2, q \mapsto 0] \not\models^{th} p$

# Galois adjunction

- 3-valued model  $M$  determines set of 2-valued models through refinement

# Galois adjunction

- 3-valued model  $M$  determines set of 2-valued models through refinement
- such sets  $\mathcal{C}$  determine 3-valued model through “independent attribute analysis”

$$\alpha(\mathcal{C})(p) = \begin{cases} 1 & \text{if } N(p) = 1 \text{ for all } N \in \mathcal{C}, \\ 0 & \text{if } N(p) = 0 \text{ for all } N \in \mathcal{C}, \text{ and} \\ 1/2 & \text{otherwise} \end{cases}$$

$$\gamma(M) = \{N \mid N \text{ 2-valued \& } N \text{ refines } M\}$$

$$\mathcal{C} \subseteq \gamma(\alpha(\mathcal{C})) \quad \alpha(\gamma(L)) = L$$

# Galois adjunction

- 3-valued model  $M$  determines set of 2-valued models through refinement
- such sets  $\mathcal{C}$  determine 3-valued model through “**independent attribute analysis**”

$$\alpha(\mathcal{C})(p) = \begin{cases} 1 & \text{if } N(p) = 1 \text{ for all } N \in \mathcal{C}, \\ 0 & \text{if } N(p) = 0 \text{ for all } N \in \mathcal{C}, \text{ and} \\ 1/2 & \text{otherwise} \end{cases}$$

$$\gamma(M) = \{N \mid N \text{ 2-valued \& } N \text{ refines } M\}$$

$$\mathcal{C} \subseteq \gamma(\alpha(\mathcal{C})) \quad \alpha(\gamma(L)) = L$$

- $M \models^{th} \phi$  and  $M \models^{th} \neg\phi$  record consensus of  $\gamma(M)$  on  $\phi$

# Thorough semantics as validity problem

- each model  $M$  has formula  $\phi_M$  of propositional logic with

$$\forall \phi: (M \models^{th} \phi) \Leftrightarrow (\phi_M \rightarrow \phi \text{ is valid}).$$

# Thorough semantics as validity problem

- each model  $M$  has formula  $\phi_M$  of propositional logic with

$$\forall \phi: (M \models^{th} \phi) \Leftrightarrow (\phi_M \rightarrow \phi \text{ is valid}).$$

- e.g.  $[p \mapsto 1/2, q \mapsto 1, r \mapsto 0] \models^{th} \phi$  iff  $q \wedge \neg r \rightarrow \phi$  is valid

# Thorough semantics as validity problem

- each model  $M$  has formula  $\phi_M$  of propositional logic with

$$\forall \phi: (M \models^{th} \phi) \Leftrightarrow (\phi_M \rightarrow \phi \text{ is valid}).$$

- e.g.  $[p \mapsto 1/2, q \mapsto 1, r \mapsto 0] \models^{th} \phi$  iff  $q \wedge \neg r \rightarrow \phi$  is valid
- $\phi_M$  records all obligations that refinements of  $M$  have to meet

# Thorough semantics as validity problem

- each model  $M$  has formula  $\phi_M$  of propositional logic with

$$\forall\phi: (M \models^{th} \phi) \Leftrightarrow (\phi_M \rightarrow \phi \text{ is valid}).$$

- e.g.  $[p \mapsto 1/2, q \mapsto 1, r \mapsto 0] \models^{th} \phi$  iff  $q \wedge \neg r \rightarrow \phi$  is valid
- $\phi_M$  records all obligations that refinements of  $M$  have to meet
- **validity of  $\phi_M \rightarrow \phi$  captures “all refinements of  $M$  satisfy  $\phi$ ”**

# Thorough semantics as validity problem

- each model  $M$  has formula  $\phi_M$  of propositional logic with

$$\forall \phi: (M \models^{th} \phi) \Leftrightarrow (\phi_M \rightarrow \phi \text{ is valid}).$$

- e.g.  $[p \mapsto 1/2, q \mapsto 1, r \mapsto 0] \models^{th} \phi$  iff  $q \wedge \neg r \rightarrow \phi$  is valid
- $\phi_M$  records all obligations that refinements of  $M$  have to meet
- validity of  $\phi_M \rightarrow \phi$  captures “all refinements of  $M$  satisfy  $\phi$ ”
- e.g.  $q \wedge \neg r \rightarrow (p \rightarrow q \rightarrow r)$  is not valid and  
 $[p \mapsto 1, q \mapsto 1, r \mapsto 0]$  is a refinement of  
 $[p \mapsto 1/2, q \mapsto 1, r \mapsto 0]$  that does not satisfy  $p \rightarrow q \rightarrow r$

# Under-approximating thorough semantics

- seek efficient judgment  $M \models \phi$  that under-approximates  $M \models^{th} \phi$

# Under-approximating thorough semantics

- seek efficient judgment  $M \models \phi$  that **under-approximates**  $M \models^{th} \phi$
- **define  $M \models \phi$  assuming that all formulas are in negation normal form**

# Under-approximating thorough semantics

- seek efficient judgment  $M \models \phi$  that **under-approximates**  $M \models^{th} \phi$
- define  $M \models \phi$  assuming that all formulas are in negation normal form
- e.g. convert  $\neg(p \rightarrow q \rightarrow r)$  into  $p \wedge q \wedge \neg r$  first

$$M \models p \quad \text{iff} \quad M(p) = 1 \quad // \textit{pessimistic}$$

$$M \models \neg p \quad \text{iff} \quad M(p) = 0 \quad // \textit{pessimistic}$$

$$M \models \phi \vee \psi \quad \text{iff} \quad M \models \phi \text{ or } M \models \psi$$

$$M \models \phi \wedge \psi \quad \text{iff} \quad M \models \phi \text{ and } M \models \psi$$

# Under-approximating thorough semantics

- seek efficient judgment  $M \models \phi$  that **under-approximates**  $M \models^{th} \phi$
- define  $M \models \phi$  assuming that all formulas are in negation normal form
- e.g. convert  $\neg(p \rightarrow q \rightarrow r)$  into  $p \wedge q \wedge \neg r$  first

$$M \models p \quad \text{iff} \quad M(p) = 1 \quad // \textit{pessimistic}$$

$$M \models \neg p \quad \text{iff} \quad M(p) = 0 \quad // \textit{pessimistic}$$

$$M \models \phi \vee \psi \quad \text{iff} \quad M \models \phi \text{ or } M \models \psi$$

$$M \models \phi \wedge \psi \quad \text{iff} \quad M \models \phi \text{ and } M \models \psi$$

- loss of precision for  $\vee$  as  $\models$  is compositional, e.g.  
 $[p \mapsto 1/2] \not\models p \vee \neg p$  whereas  $[p \mapsto 1/2] \models^{th} p \vee \neg p$

# Under-approximating thorough semantics

- seek efficient judgment  $M \models \phi$  that **under-approximates**  $M \models^{th} \phi$
- define  $M \models \phi$  assuming that all formulas are in negation normal form
- e.g. convert  $\neg(p \rightarrow q \rightarrow r)$  into  $p \wedge q \wedge \neg r$  first

$$M \models p \quad \text{iff} \quad M(p) = 1 \quad // \textit{pessimistic}$$

$$M \models \neg p \quad \text{iff} \quad M(p) = 0 \quad // \textit{pessimistic}$$

$$M \models \phi \vee \psi \quad \text{iff} \quad M \models \phi \text{ or } M \models \psi$$

$$M \models \phi \wedge \psi \quad \text{iff} \quad M \models \phi \text{ and } M \models \psi$$

- loss of precision for  $\vee$  as  $\models$  is compositional, e.g.  $[p \mapsto 1/2] \not\models p \vee \neg p$  whereas  $[p \mapsto 1/2] \models^{th} p \vee \neg p$
- **Under-approximation as soundness: for all  $M$  and  $\phi$ ,  $M \models \phi$  implies  $M \models^{th} \phi$**

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?
- **Ill defined question. Is  $M$  fixed? Is  $\phi$  fixed?**

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?
- Ill defined question. Is  $M$  fixed? Is  $\phi$  fixed?
- For each  $\phi$ , is there a  $\phi'$  in the same logic such that

$$\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi') ? \quad (1)$$

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?
- Ill defined question. Is  $M$  fixed? Is  $\phi$  fixed?
- For each  $\phi$ , is there a  $\phi'$  in the same logic such that

$$\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi') ? \quad (1)$$

- Let's call any  $\phi'$  in (1) a semantic minimization [Reps et al. 2002] of  $\phi$ .

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?
- Ill defined question. Is  $M$  fixed? Is  $\phi$  fixed?
- For each  $\phi$ , is there a  $\phi'$  **in the same logic** such that

$$\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi') ? \quad (1)$$

- Let's call any  $\phi'$  in (1) a **semantic minimization** [Reps et al. 2002] of  $\phi$ .
- **In our terminology: "Every  $\phi$  of propositional logic has a semantic minimization in propositional logic."** [Blamey 1980]

# Semantic minimization

- For each  $M$ , can reduce  $M \models^{th} \phi$  to validity check  $\phi_M \rightarrow \phi$ .
- Can we reduce  $M \models^{th} \phi$  to a model check?
- Ill defined question. Is  $M$  fixed? Is  $\phi$  fixed?
- For each  $\phi$ , is there a  $\phi'$  in the same logic such that

$$\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi') ? \quad (1)$$

- Let's call any  $\phi'$  in (1) a **semantic minimization** [Reps et al. 2002] of  $\phi$ .
- In our terminology: "Every  $\phi$  of propositional logic has a semantic minimization in propositional logic." [Blamey 1980]
- **Proof uses mutually recursive CNFs. Establishes that  $\models$  is functionally complete for functions  $\{0, 1/2, 1\}^n \rightarrow \{0, 1/2, 1\}$  that are monotone in information ordering  $1/2 < 0, 1$**

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , uniformly for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- **Can we state patterns  $\phi$  for which  $\phi'$  is provably short?**

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- Can we state patterns  $\phi$  for which  $\phi'$  is provably short?
- **In particular, are there interesting and abundantly many patterns  $\phi$  for which “ $\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi)$ ” holds? Call such  $\phi$  pessimistically self-minimizing**

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- Can we state patterns  $\phi$  for which  $\phi'$  is provably short?
- In particular, are there interesting and abundantly many patterns  $\phi$  for which “ $\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi)$ ” holds?  
Call such  $\phi$  pessimistically self-minimizing
- **examples of pessimistically self-minimizing  $\phi$ :**

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- Can we state patterns  $\phi$  for which  $\phi'$  is provably short?
- In particular, are there interesting and abundantly many patterns  $\phi$  for which “ $\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi)$ ” holds?  
Call such  $\phi$  pessimistically self-minimizing
- examples of **pessimistically self-minimizing**  $\phi$ :
  - all “monotone”  $\phi$ , no atoms in mixed polarity

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- Can we state patterns  $\phi$  for which  $\phi'$  is provably short?
- In particular, are there interesting and abundantly many patterns  $\phi$  for which “ $\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi)$ ” holds?  
Call such  $\phi$  pessimistically self-minimizing
- examples of **pessimistically self-minimizing**  $\phi$ :
  - all “monotone”  $\phi$ , no atoms in mixed polarity
  - **non-monotone**  $(p \rightarrow q) \wedge (q \rightarrow p)$

# Self-minimizing patterns

- Reducing  $M \models^{th} \phi$  to  $M \models \phi'$ , **uniformly** for all  $M$ , may throw the baby out with the bath water:  
computing  $\phi \mapsto \phi'$  is coNP-hard for propositional logic
- Of course one can hope that  $\phi'$  will stay manageable, e.g. through the use of BDDs and prime implicant algorithms [Reps et al. 2002]
- Can we state patterns  $\phi$  for which  $\phi'$  is provably short?
- In particular, are there interesting and abundantly many patterns  $\phi$  for which “ $\forall M: (M \models^{th} \phi) \Leftrightarrow (M \models \phi)$ ” holds?  
Call such  $\phi$  pessimistically self-minimizing
- examples of **pessimistically self-minimizing**  $\phi$ :
  - all “monotone”  $\phi$ , no atoms in mixed polarity
  - non-monotone  $(p \rightarrow q) \wedge (q \rightarrow p)$
- **$p \vee \neg p$  not pessimistically self-minimizing**

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings
- For which temporal logics do Blamey's results on semantic minimizations extend?

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings
- For which temporal logics do Blamey's results on semantic minimizations extend?
- What proof constructs replace that of mutually recursive CNFs?

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings
- For which temporal logics do Blamey's results on semantic minimizations extend?
- What proof constructs replace that of mutually recursive CNFs?
- **What is the complexity of computing such semantic minimizations?**

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings
- For which temporal logics do Blamey's results on semantic minimizations extend?
- What proof constructs replace that of mutually recursive CNFs?
- What is the complexity of computing such semantic minimizations?
- **Are there interesting temporal patterns of self-minimization?**

# Research agenda

- Models, refinement, thorough & compositional semantics for temporal logics exist in extant literature
- Semantic minimization and self-minimization are defined similarly in those temporal settings
- For which temporal logics do Blamey's results on semantic minimizations extend?
- What proof constructs replace that of mutually recursive CNFs?
- What is the complexity of computing such semantic minimizations?
- Are there interesting temporal patterns of self-minimization?
- This talk sheds some light on only some of these questions.

# Partial Kripke structures

- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:

# Partial Kripke structures

- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:
  - state set  $S$ ,

# Partial Kripke structures

- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:
  - state set  $S$ ,
  - transition relation  $R \subseteq S \times S$ ,

# Partial Kripke structures

- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:
  - state set  $S$ ,
  - transition relation  $R \subseteq S \times S$ ,
  - **propositional labeling**  $L: S \times \text{AtomProp} \rightarrow \{0, 1/2, 1\}$

# Partial Kripke structures

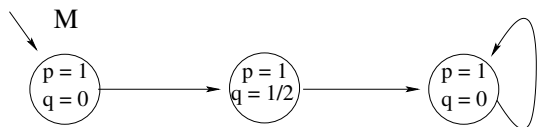
- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:
  - state set  $S$ ,
  - transition relation  $R \subseteq S \times S$ ,
  - propositional labeling  $L: S \times \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- for each state  $s$ ,  $L(s, \cdot)$  is 3-valued model of propositional logic

# Partial Kripke structures

- partial Kripke structures [Bruns & Godefroid 1999] are 3-valued models for propositional logic “extended over time” [Abramsky 1993]:
  - state set  $S$ ,
  - transition relation  $R \subseteq S \times S$ ,
  - propositional labeling  $L: S \times \text{AtomProp} \rightarrow \{0, 1/2, 1\}$
- for each state  $s$ ,  $L(s, \cdot)$  is 3-valued model of propositional logic
- **refinement, thorough & compositional semantics also extended over time**

# Example of partial Kripke structure

```
void someArithmetic() {
  x,y = 1,0;
  x,y = 2*f(x),f(y);
  x,y = x+1,0; }
```



- $f: \text{int} \rightarrow \text{int}$  **unknown function**
- model  $M$  above obtained by **predicate abstraction** with respect to  $p = \text{"x is odd"}$  and  $q = \text{"y is odd"}$
- $M \not\models EG\neg q \vee EF(\neg p \wedge q)$  but  $M \models^{th} EG\neg q \vee EF(\neg p \wedge q)$ , note the **mixed polarity** for  $q$

# Refinement

- information ordering

# Refinement

- information ordering
  - $1/2 \leq_l 0$

# Refinement

- information ordering
  - $1/2 \leq_l 0$
  - $1/2 \leq_l 1$

# Refinement

- information ordering
  - $1/2 \leq_I 0$
  - $1/2 \leq_I 1$
  - 0 and 1 maximal with respect to  $\leq_I$

# Refinement

- information ordering
  - $1/2 \leq_I 0$
  - $1/2 \leq_I 1$
  - 0 and 1 maximal with respect to  $\leq_I$
- For models  $M_i = (S_i, R_i, L_i)$  with  $i = 1, 2$  the *completeness preorder* [Bruns & Godefroid 1999] is the greatest relation  $\preceq \subseteq S_1 \times S_2$  such that  $s_1 \preceq s_2$  implies

# Refinement

- information ordering
  - $1/2 \leq_I 0$
  - $1/2 \leq_I 1$
  - 0 and 1 maximal with respect to  $\leq_I$
- For models  $M_i = (S_i, R_i, L_i)$  with  $i = 1, 2$  the *completeness preorder* [Bruns & Godefroid 1999] is the greatest relation  $\preceq \subseteq S_1 \times S_2$  such that  $s_1 \preceq s_2$  implies
  - ①  $\forall q \in \text{AtomProp}: L_1(s_1, q) \leq_I L_2(s_2, q),$

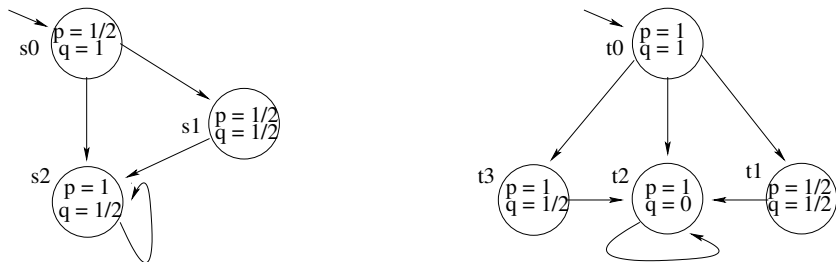
# Refinement

- information ordering
  - $1/2 \leq_I 0$
  - $1/2 \leq_I 1$
  - 0 and 1 maximal with respect to  $\leq_I$
- For models  $M_i = (S_i, R_i, L_i)$  with  $i = 1, 2$  the *completeness preorder* [Bruns & Godefroid 1999] is the greatest relation  $\preceq \subseteq S_1 \times S_2$  such that  $s_1 \preceq s_2$  implies
  - 1  $\forall q \in \text{AtomProp}: L_1(s_1, q) \leq_I L_2(s_2, q)$ ,
  - 2  $\forall (s_1, s'_1) \in R_1 \exists (s_2, s'_2) \in R_2: s'_1 \preceq s'_2$ , and

# Refinement

- information ordering
  - $1/2 \leq_I 0$
  - $1/2 \leq_I 1$
  - 0 and 1 maximal with respect to  $\leq_I$
- For models  $M_i = (S_i, R_i, L_i)$  with  $i = 1, 2$  the *completeness preorder* [Bruns & Godefroid 1999] is the greatest relation  $\preceq \subseteq S_1 \times S_2$  such that  $s_1 \preceq s_2$  implies
  - 1  $\forall q \in \text{AtomProp}: L_1(s_1, q) \leq_I L_2(s_2, q)$ ,
  - 2  $\forall (s_1, s'_1) \in R_1 \exists (s_2, s'_2) \in R_2: s'_1 \preceq s'_2$ , and
  - 3  $\forall (s_2, s'_2) \in R_2 \exists (s_1, s'_1) \in R_1: s'_1 \preceq s'_2$ .

# Example of refinement



- $t_0$  refines  $s_0$ ,  $t_1$  refines  $s_1$ , and  $t_2$  and  $t_3$  refine  $s_2$

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$
- $M \models^{th} \phi$  iff for all  $N \in \gamma(M)$ ,  
 $N$  satisfies  $\phi$  in standard semantics

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$
- $M \models^{th} \phi$  iff for all  $N \in \gamma(M)$ ,  
 $N$  satisfies  $\phi$  in standard semantics
- $\alpha(\mathcal{C})$  no longer a single model

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$
- $M \models^{th} \phi$  iff for all  $N \in \gamma(M)$ ,  
 $N$  satisfies  $\phi$  in standard semantics
- $\alpha(\mathcal{C})$  no longer a single model
- Galois adjunction (not an insertion) between

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$
- $M \models^{th} \phi$  iff for all  $N \in \gamma(M)$ ,  
 $N$  satisfies  $\phi$  in standard semantics
- $\alpha(\mathcal{C})$  **no longer a single model**
- Galois adjunction (not an insertion) between
  - **compact sets of Kripke structures and**

# Thorough semantics

- Kripke structures are those partial Kripke structures whose labeling function  $L$  satisfies  $L^{-1}(1/2) = \{\}$
- $\gamma(M) = \{N \mid N \text{ Kripke structure \& } N \text{ refines } M\}$
- $M \models^{th} \phi$  iff for all  $N \in \gamma(M)$ ,  
 $N$  satisfies  $\phi$  in standard semantics
- $\alpha(\mathcal{C})$  **no longer a single model**
- Galois adjunction (not an insertion) between
  - compact sets of Kripke structures and
  - **bounded Scott-closed sets of partial Kripke structures in a fully abstract domain model for refinement**

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

- again convert  $\phi$  into negation normal form first

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

- again convert  $\phi$  into negation normal form first
- $M \models \phi$  already defined for propositional operators

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

- again convert  $\phi$  into negation normal form first
- $M \models \phi$  already defined for propositional operators
- extend that definition to remaining operators, modalities and fixed points, in the “usual” manner

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

- again convert  $\phi$  into negation normal form first
- $M \models \phi$  already defined for propositional operators
- extend that definition to remaining operators, modalities and fixed points, in the “usual” manner
- soundness ( $M \models \phi$  implies  $M \models^{th} \phi$ ) and incompleteness ( $M \models^{th} \phi$  does not imply  $M \models \phi$ ) inherited from propositional setting

# Compositional semantics for modal mu-calculus

- modal mu-calculus

$$\phi ::= p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi \mid \mu Z.\phi \mid \nu Z.\phi$$

all free  $Z$  in  $\mu Z.\phi$  or  $\nu Z.\phi$  under even scope of negations

- again convert  $\phi$  into negation normal form first
- $M \models \phi$  already defined for propositional operators
- extend that definition to remaining operators, modalities and fixed points, in the “usual” manner
- soundness ( $M \models \phi$  implies  $M \models^{th} \phi$ ) and incompleteness ( $M \models^{th} \phi$  does not imply  $M \models \phi$ ) inherited from propositional setting
- $M \models^{th} \phi$  reduces to validity check  $\phi_M \rightarrow \phi$  where  $\phi_M$  expressible in modal mu-calculus without any  $\mu Z.\psi$ , if finite-state

# Self-minimization for temporal logics

- $\phi$  is pessimistically self-minimizing (ps) iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$

# Self-minimization for temporal logics

- $\phi$  is **pessimistically self-minimizing (ps)** iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$
- $\phi$  is **optimistically self-minimizing (os)** iff  $\neg\phi$  is pessimistically self-minimizing

# Self-minimization for temporal logics

- $\phi$  is **pessimistically self-minimizing (ps)** iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$
- $\phi$  is **optimistically self-minimizing (os)** iff  $\neg\phi$  is pessimistically self-minimizing
- **deciding pessimistic self-minimization reduces to language inclusion check of alternating parity tree automata, EXPTIME-hard**

# Self-minimization for temporal logics

- $\phi$  is **pessimistically self-minimizing (ps)** iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$
- $\phi$  is **optimistically self-minimizing (os)** iff  $\neg\phi$  is pessimistically self-minimizing
- deciding pessimistic self-minimization reduces to language inclusion check of alternating parity tree automata,  
**EXPTIME-hard**
- **identify patterns of self-minimization by “efficient grammar”**

# Self-minimization for temporal logics

- $\phi$  is **pessimistically self-minimizing (ps)** iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$
- $\phi$  is **optimistically self-minimizing (os)** iff  $\neg\phi$  is pessimistically self-minimizing
- deciding pessimistic self-minimization reduces to language inclusion check of alternating parity tree automata,  
**EXPTIME-hard**
- identify patterns of self-minimization by “efficient grammar”
- **write  $\phi\#\psi$  to state that  $\phi$  and  $\psi$  share no  $p \in \text{AtomProp}$**

# Self-minimization for temporal logics

- $\phi$  is **pessimistically self-minimizing (ps)** iff for all  $M$ ,  
 $(M \models \phi) \Leftrightarrow (M \models^{th} \phi)$
- $\phi$  is **optimistically self-minimizing (os)** iff  $\neg\phi$  is pessimistically self-minimizing
- deciding pessimistic self-minimization reduces to language inclusion check of alternating parity tree automata,  
**EXPTIME-hard**
- identify patterns of self-minimization by “efficient grammar”
- write  $\phi\#\psi$  to state that  $\phi$  and  $\psi$  share no  $p \in \text{AtomProp}$
- write  $\phi\exists$  ( $\phi\forall$ ) if the negation normal form of  $\phi$  is known to be an existential (resp., universal) one

# Patterns of temporal self-minimization

$$\begin{aligned}
 \text{ps} & ::= \mathcal{M} \mid \mathcal{R} \mid \neg \text{os} \mid \text{ps} \wedge \text{ps} \mid \text{ps}_{\forall\#} \vee \text{ps}_{\forall\#} \\
 & \quad \text{EXps} \mid \text{AXps} \mid \text{EGps} \mid \text{AGps} \\
 & \quad \text{AFps}_{\forall} \mid \text{A}[\text{ps}_{\forall\#} \text{Ups}_{\forall\#}] \\
 \text{os} & ::= \mathcal{M} \mid \mathcal{R} \mid \neg \text{ps} \mid \text{os} \vee \text{os} \mid \text{os}_{\exists\#} \wedge \text{os}_{\exists\#} \\
 & \quad \text{EXos} \mid \text{AXos} \mid \text{EFos} \mid \text{AFos} \\
 & \quad \text{EGos}_{\exists} \mid \text{E}[\text{os}_{\exists} \text{Uos}] \mid \text{ref}(\text{OS})
 \end{aligned}$$

- $\mathcal{M}$  ranges over “monotone”  $\phi$
- $\mathcal{R}$  ranges over all  $\phi_M$
- $\text{ref}(\mathcal{O})$  is defined as  $(\bigwedge_{O \in \mathcal{O}} \text{EXO}) \wedge (\text{AX} \vee \mathcal{O})$
- various proof techniques,  
e.g. **multiple-model checking** for  $\mathcal{R}$  in  $\text{os}$

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)

$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi$

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)

$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid EX\phi \mid AX\phi$

- every  $\phi$  of PML has semantic minimization in PML

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)  
 $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \text{EX}\phi \mid \text{AX}\phi$
- every  $\phi$  of PML has semantic minimization in PML
- proof defines non-deterministic tree automata  $A_\phi^3$  from non-deterministic tree automata  $A_\phi$  with transition function  $\rho$  through  $\rho_\phi^3(s, a^3, k) = \bigcup_{a \in \gamma(a^3)} \rho(s, a, k)$

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)  
 $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \text{EX}\phi \mid \text{AX}\phi$
- every  $\phi$  of PML has semantic minimization in PML
- proof defines **non-deterministic tree automata**  $A_\phi^3$  from non-deterministic tree automata  $A_\phi$  with transition function  $\rho$  through  $\rho_\phi^3(s, a^3, k) = \bigcup_{a \in \gamma(a^3)} \rho(s, a, k)$
- $a^3$  is 3-valued model of propositional logic,  $k$  arity of successor set,  $A_\phi$  accepts 2-valued trees satisfying  $\phi$

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)  
 $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \text{EX}\phi \mid \text{AX}\phi$
- every  $\phi$  of PML has semantic minimization in PML
- proof defines **non-deterministic tree automata**  $A_\phi^3$  from non-deterministic tree automata  $A_\phi$  with transition function  $\rho$  through  $\rho_\phi^3(s, a^3, k) = \bigcup_{a \in \gamma(a^3)} \rho(s, a, k)$
- $a^3$  is 3-valued model of propositional logic,  $k$  arity of successor set,  $A_\phi$  accepts 2-valued trees satisfying  $\phi$
- **then convert  $A_\phi^3$  into formula of PML**

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)
 
$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \text{EX}\phi \mid \text{AX}\phi$$
- every  $\phi$  of PML has semantic minimization in PML
- proof defines **non-deterministic tree automata**  $A_\phi^3$  from non-deterministic tree automata  $A_\phi$  with transition function  $\rho$  through  $\rho_\phi^3(s, a^3, k) = \bigcup_{a \in \gamma(a^3)} \rho(s, a, k)$
- $a^3$  is 3-valued model of propositional logic,  $k$  arity of successor set,  $A_\phi$  accepts 2-valued trees satisfying  $\phi$
- then convert  $A_\phi^3$  into formula of PML
- e.g. semantic minimization of  $\neg(\text{EX}q_1 \wedge \text{AX}(\neg q_1 \vee q_2))$  computes to  $\neg(\text{EX}(q_1 \wedge q_2) \wedge \text{AX}(\neg q_1 \vee q_2))$

# Semantic minimizations for propositional modal logic

- propositional modal logic (PML)  
 $\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \text{EX}\phi \mid \text{AX}\phi$
- every  $\phi$  of PML has semantic minimization in PML
- proof defines **non-deterministic tree automata**  $A_\phi^3$  from non-deterministic tree automata  $A_\phi$  with transition function  $\rho$  through  $\rho_\phi^3(s, a^3, k) = \bigcup_{a \in \gamma(a^3)} \rho(s, a, k)$
- $a^3$  is 3-valued model of propositional logic,  $k$  arity of successor set,  $A_\phi$  accepts 2-valued trees satisfying  $\phi$
- then convert  $A_\phi^3$  into formula of PML
- e.g. semantic minimization of  $\neg(\text{EX}q_1 \wedge \text{AX}(\neg q_1 \vee q_2))$  computes to  $\neg(\text{EX}(q_1 \wedge q_2) \wedge \text{AX}(\neg q_1 \vee q_2))$
- **consequence:  $M \models^{th} \phi$  for PML in ALOGTIME in size of model  $M$**

# Semantic minimizations for modal mu-calculus

- every  $\phi$  of modal mu-calculus has semantic minimization in the modal mu-calculus

# Semantic minimizations for modal mu-calculus

- every  $\phi$  of modal mu-calculus has semantic minimization in the modal mu-calculus
- proof as for PML but for non-deterministic parity tree automata

# Semantic minimizations for modal mu-calculus

- every  $\phi$  of modal mu-calculus has semantic minimization in the modal mu-calculus
- proof as for PML but for non-deterministic **parity** tree automata
- e.g. for CTL formula  $\phi = \neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  this proof constructs the formula  $\neg \mu Z_1.(q_1 \rightarrow q_2) \vee [\mu Z_2.AXZ_1 \wedge EX(q_1 \wedge (q_2 \vee Z_2))]$  of the modal mu-calculus

# Semantic minimizations for modal mu-calculus

- every  $\phi$  of modal mu-calculus has semantic minimization in the modal mu-calculus
- proof as for PML but for non-deterministic **parity** tree automata
- e.g. for CTL formula  $\phi = \neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  this proof constructs the formula  $\neg \mu Z_1.(q_1 \rightarrow q_2) \vee [\mu Z_2.AXZ_1 \wedge EX(q_1 \wedge (q_2 \vee Z_2))]$  of the modal mu-calculus
- **this existence result does not seem to have consequences on complexity of  $M \models^{th} \phi$  for modal mu-calculus**

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

- so existence of semantic minimization for CTL formula  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  in CTL\* would imply  $NLOGSPACE = PTIME$

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

- so existence of semantic minimization for CTL formula  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  in CTL\* would imply  $NLOGSPACE = PTIME$
- can do better than such a “reduction”:

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

- so existence of semantic minimization for CTL formula  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  in CTL\* would imply NLOGSPACE = PTIME
- can do better than such a “reduction”:
  - semantic minimization for  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  exists in modal mu-calculus:
 
$$\phi' = \neg \mu Z_1. (q_1 \rightarrow q_2) \vee [\mu Z_2. AXZ_1 \wedge EX(q_1 \wedge (q_2 \vee Z_2))]$$

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

- so existence of semantic minimization for CTL formula  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  in CTL\* would imply NLOGSPACE = PTIME
- can do better than such a “reduction”:
  - semantic minimization for  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  exists in modal mu-calculus:
 
$$\phi' = \neg \mu Z_1. (q_1 \rightarrow q_2) \vee [\mu Z_2. AXZ_1 \wedge EX(q_1 \wedge (q_2 \vee Z_2))]$$
  - can prove that  $\phi'$  is not expressible in CTL\*

# Semantic minimizations for CTL and CTL\*

- for each instance  $C$  of the MONOTONE\_CIRCUIT\_VALUE decision problem, we have partial Kripke structure  $M_C$  with

$$(M_C \models^{th} \neg A[(EXq_1)U(q_1 \rightarrow q_2)]) \Leftrightarrow (\text{value of } C \text{ is } 0)$$

- so existence of semantic minimization for CTL formula  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  in CTL\* would imply NLOGSPACE = PTIME
- can do better than such a “reduction”:
  - semantic minimization for  $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$  exists in modal mu-calculus:
 
$$\phi' = \neg \mu Z_1. (q_1 \rightarrow q_2) \vee [\mu Z_2. AXZ_1 \wedge EX(q_1 \wedge (q_2 \vee Z_2))]$$
  - can prove that  $\phi'$  is not expressible in CTL\*
- so not all formulas of CTL or CTL\* have semantic minimizations in CTL\*

## Some references

- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS 2005, pages 158–167.

## Some references

- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS 2005, pages 158–167.
- M. Huth, R. Jagadeesan, and D. Schmidt *A domain equation for refinement of partial systems*. *Mathematical Structures in Computer Science* 14(4):469–505.

## Some references

- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS 2005, pages 158–167.
- M. Huth, R. Jagadeesan, and D. Schmidt *A domain equation for refinement of partial systems*. Mathematical Structures in Computer Science 14(4):469–505.
- M. Huth *Labelled Transition Systems as a Stone Space*. Logical Methods in Computer Science 1(1:1)1-28.

## Some references

- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS 2005, pages 158–167.
- M. Huth, R. Jagadeesan, and D. Schmidt *A domain equation for refinement of partial systems*. Mathematical Structures in Computer Science 14(4):469–505.
- M. Huth *Labelled Transition Systems as a Stone Space*. Logical Methods in Computer Science 1(1:1)1-28.
- M. Huth *Refinement is Complete for Implementations*. *Formal Aspects of Computing* 17(2):113–137, 2005.

## Some references

- P. Godefroid & M. Huth *Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics*. Proc. of LICS 2005, pages 158–167.
- M. Huth, R. Jagadeesan, and D. Schmidt *A domain equation for refinement of partial systems*. Mathematical Structures in Computer Science 14(4):469–505.
- M. Huth *Labelled Transition Systems as a Stone Space*. Logical Methods in Computer Science 1(1:1)1-28.
- M. Huth *Refinement is Complete for Implementations*. *Formal Aspects of Computing* 17(2):113–137, 2005.
- Detailed references to related and originating work (e.g. by *Kim Larsen*) can be found in these papers.

# Acknowledgments

- Patrice Godefroid (for being co-author of this work)

# Acknowledgments

- Patrice Godefroid (for being co-author of this work)
- Radha Jagadeesan & David Schmidt (for their comments)

# Acknowledgments

- Patrice Godefroid (for being co-author of this work)
- Radha Jagadeesan & David Schmidt (for their comments)
- UK Engineering and Physical Sciences Research Council (for its generous support of this work)

# Acknowledgments

- Patrice Godefroid (for being co-author of this work)
- Radha Jagadeesan & David Schmidt (for their comments)
- UK Engineering and Physical Sciences Research Council (for its generous support of this work)
- Samson, Alex, and Mooly (for having invited me to this workshop)