Terminating Minimal Model Generation Procedures for Propositional Modal Logics

Fabio Papacchini   Renate A. Schmidt

School of Computer Science
The University of Manchester

July 21, 2014

(Minimal) Model Generation

Useful for several tasks:

- hardware and software verification
- fault analysis
- commonsense reasoning
- query answering
- ...

Minimality criteria:

- domain minimality
- minimisation of a certain set of predicates
- minimal Herbrand models
- In this talk: models minimal modulo subset-simulation

Aims

- a new minimality criterion based on subset-simulation
- minimal model generation procedures for all sublogics of $\mathbf{S5}$
  - sound
  - refutationally complete
  - minimal model complete
  - minimal model sound
- blocking techniques for all the logics under consideration

Propositional Modal Logic

Syntax: $\phi ::= \bot \mid \top \mid p_i \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \Box\phi \mid \Diamond\phi$

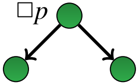
Kripke Semantics: An interpretation $\mathcal{I}$ is a tuple (W, R, V).

Propositional Modal Logic

Syntax: $\phi ::= \bot \mid \top \mid p_i \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \Box\phi \mid \Diamond\phi$

Kripke Semantics: An interpretation $\mathcal{I}$ is a tuple (W, R, V).

Box semantics



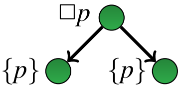
V assigns a set of propositional symbols to each element of W.

Propositional Modal Logic

Syntax: $\phi ::= \bot \mid \top \mid p_i \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \Box\phi \mid \Diamond\phi$

Kripke Semantics: An interpretation $\mathcal{I}$ is a tuple (W, R, V).

Box semantics



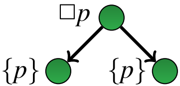
V assigns a set of propositional symbols to each element of W.

Propositional Modal Logic

Syntax: $\phi ::= \bot \mid \top \mid p_i \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \Box\phi \mid \Diamond\phi$

Kripke Semantics: An interpretation $\mathcal{I}$ is a tuple (W, R, V).

Box semantics



Diamond semantics

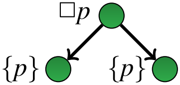
V assigns a set of propositional symbols to each element of W.

Propositional Modal Logic

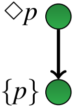
Syntax: $\phi ::= \bot \mid \top \mid p_i \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \Box\phi \mid \Diamond\phi$

Kripke Semantics: An interpretation $\mathcal{I}$ is a tuple (W, R, V).

Box semantics



Diamond semantics



V assigns a set of propositional symbols to each element of W.

Frame Properties

Fifteen possible logics:

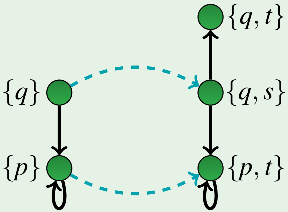
K, **KT**, **KB**, **KTB**, **KD**, **KDB**, **K4**, **K5**, **KT4**, **KD4**, **KD5**, **K45**, **KD45**, **KB4** and **KT5**$(=$ **S5**$)$

$\Box$	Axiom	Frame condition	First-order representation
K			
T	$\Box p \to p$	reflexivity	$\forall x R(x,x)$
B	$p \to \Box\Diamond p$	symmetry	$\forall x \forall y (R(x,y) \to R(y,x))$
D	$\Box p \to \Diamond p$	seriality	$\forall x \exists y R(x,y)$
4	$\Box p \to \Box\Box p$	transitivity	$\forall x \forall y \forall z (R(x,y) \wedge R(y,z) \to R(x,z))$
5	$\Diamond p \to \Box\Diamond p$	Euclideanness	$\forall x \forall y \forall z (R(x,y) \wedge R(x,z) \to R(y,z))$

Subset-Simulation $S_\subseteq$

Relation between nodes of two models $\mathcal{I} = (W, R, V)$ and $\mathcal{I}' = (W', R', V')$ s.t. for any two worlds $u \in W$ and $u' \in W'$, if uSu' then the following hold.

- $V(u) \subseteq V'(u')$, and
- if uRv, then there exists a $v' \in W'$ such that $u'R'v'$ and vSv'.



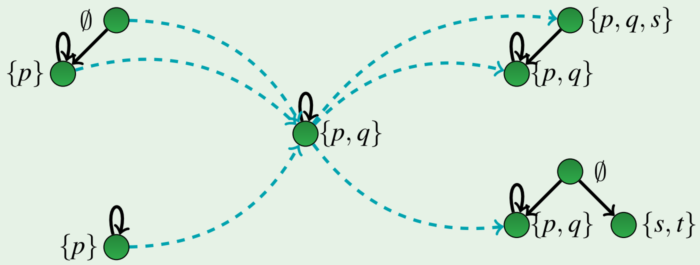
If for all $u \in W$ there is at least one $u' \in W'$ such that uSu', then we call $S_\subseteq$ a full subset-simulation from $\mathcal{I}$ to $\mathcal{I}'$ ($\mathcal{I} \leq_\subseteq \mathcal{I}'$).

Models Minimal Modulo Subset-Simulation

Subset-simulation is a preorder on models.

Definition

A model $\mathcal{I}$ of a modal formula φ is minimal modulo subset-simulation iff for any model $\mathcal{I}'$ of φ, if $\mathcal{I}' \leq_{\subseteq} \mathcal{I}$, then $\mathcal{I} \leq_{\subseteq} \mathcal{I}'$.

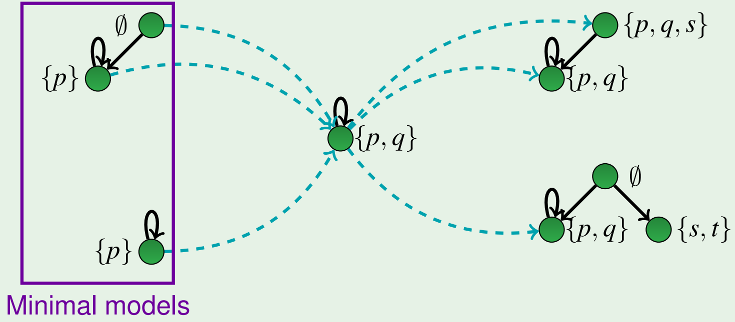


Models Minimal Modulo Subset-Simulation

Subset-simulation is a preorder on models.

Definition

A model $\mathcal{I}$ of a modal formula φ is minimal modulo subset-simulation iff for any model $\mathcal{I}'$ of φ, if $\mathcal{I}' \leq_{\subseteq} \mathcal{I}$, then $\mathcal{I} \leq_{\subseteq} \mathcal{I}'$.

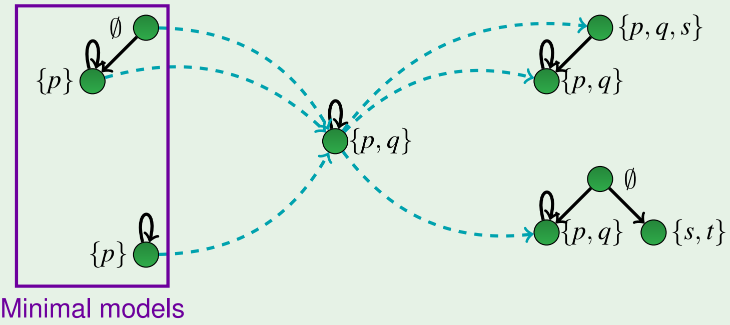


Models Minimal Modulo Subset-Simulation

Subset-simulation is a preorder on models.

Definition

A model $\mathcal{I}$ of a modal formula φ is minimal modulo subset-simulation iff for any model $\mathcal{I}'$ of φ, if $\mathcal{I}' \leq_{\subseteq} \mathcal{I}$, then $\mathcal{I} \leq_{\subseteq} \mathcal{I}'$.



Infinitely many minimal models can belong to a symmetry class.

Minimal Model Soundness and Completeness

Minimal Model Soundness

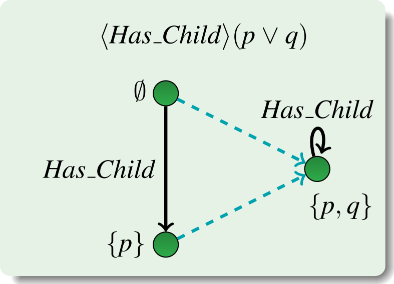
A procedure is minimal model sound if it generates only models minimal modulo subset-simulation.

Minimal Model Completeness

A procedure is minimal model complete if it generates at least one model minimal modulo subset-simulation per symmetry class.

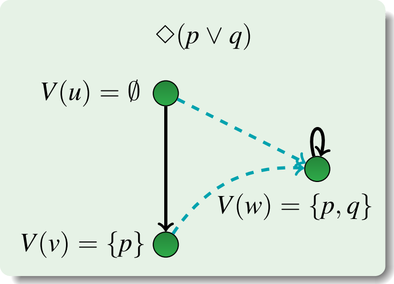
Properties of the Minimality Criterion

- loop free models are preferred
- syntax independent
- minimisation of the valuation function
- suitable for many non-classical logics



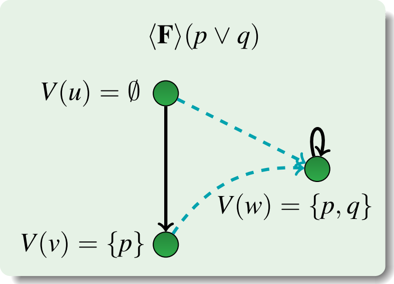
Properties of the Minimality Criterion

- loop free models are preferred
- syntax independent
- minimisation of the valuation function
- suitable for many non-classical logics



Properties of the Minimality Criterion

- loop free models are preferred
- syntax independent
- minimisation of the valuation function
- suitable for many non-classical logics



Procedures for Computing Minimal Models

Combination of tableaux calculi and a minimality test.

Procedures for Computing Minimal Models

Combination of tableaux calculi and a minimality test.

Tableaux calculi properties

- goal-oriented rules
- modularity
- termination
- minimal model completeness

Procedures for Computing Minimal Models

Combination of tableaux calculi and a minimality test.

Tableaux calculi properties

- goal-oriented rules
- modularity
- termination
- minimal model completeness

Subset-simulation test

- closes unwanted branches of a tableau
- logic independent
- ensures minimal model soundness

Tableau Calculus

Input: a modal formula in negation normal form.

Tableau Calculus

Input: a modal formula in negation normal form.

Selection-based resolution:

- closure rule
- removes negative information from disjunctions

$$(SBR)\ \frac{u : p_1 \ \ \ldots\ \ u : p_n \qquad u : \neg p_1 \vee \ldots \vee \neg p_n \vee \Phi_\alpha^+}{u : \Phi_\alpha^+}$$

Φ_α^+: a disjunction where no disjunct is of the form $\neg p_i$.

Tableau Calculus

Input: a modal formula in negation normal form.

Selection-based resolution:

- closure rule
- removes negative information from disjunctions

$$(SBR)\ \frac{u : p_1 \ \ \ldots \ \ u : p_n \qquad u : \neg p_1 \vee \ldots \vee \neg p_n \vee \Phi_\alpha^+}{u : \Phi_\alpha^+}$$

Lazy clausification:

- avoids preprocessing steps
- results in less inferences

$$(\alpha)\ \frac{u : (\phi_1 \wedge \ldots \wedge \phi_n) \vee \Phi_\alpha^+}{\begin{array}{c} u : \phi_1 \vee \Phi_\alpha^+ \\ \vdots \\ u : \phi_n \vee \Phi_\alpha^+ \end{array}}$$

Φ_α^+: a disjunction where no disjunct is of the form $\neg p_i$.

Tableau Calculus (cont'd)

Complement splitting:

- variation of the standard β rule
- detects trivially non-minimal models

$$(\beta)\ \frac{u : \mathcal{A} \vee \Phi^+}{\begin{array}{l|l} u : \mathcal{A} & u : \Phi^+ \\ u : neg(\Phi^+) & \end{array}}$$

$$\mathcal{A} ::= p \mid \Diamond\phi \mid \Box\phi$$
$$neg(\Phi^+) = \neg p_1 \wedge \ldots \wedge \neg p_n$$

Φ^+: a disjunction where no disjunct is of the form $\neg p_i$ or is a conjunction.

Tableau Calculus (cont'd)

Complement splitting:

- variation of the standard β rule
- detects trivially non-minimal models

$$(\beta)\ \frac{u : \mathcal{A} \vee \Phi^+}{\begin{array}{l|l} u : \mathcal{A} & u : \Phi^+ \\ u : neg(\Phi^+) & \end{array}}$$

$$\mathcal{A} ::= p \mid \Diamond\phi \mid \Box\phi$$
$$neg(\Phi^+) = \neg p_1 \wedge \ldots \wedge \neg p_n$$

Expansion of diamond and box formulae:

$$(\Diamond)\ \frac{u : \Diamond\phi}{\begin{array}{c}(u, v) : R \\ v : \phi\end{array}}$$

v is a fresh new world

$$(\Box)\ \frac{(u, v) : R \qquad u : \Box\phi}{v : \phi}$$

Φ^+: a disjunction where no disjunct is of the form $\neg p_i$ or is a conjunction.

Frame Properties Rules

$$(\mathbf{T})\ \frac{}{(u,u) : R} \qquad\qquad (\mathbf{B})\ \frac{(u,v) : R}{(v,u) : R}$$

$$(\mathbf{4})\ \frac{(u,v) : R \qquad (v,w) : R}{(u,w) : R} \qquad\qquad (\mathbf{5})\ \frac{(u,v) : R \qquad (u,w) : R}{(v,w) : R}$$

$$(\mathbf{D})\ \frac{}{u : \Diamond\top}$$

Properties of the Tableaux Calculi

- sound
- refutationally complete
- minimal model complete
- NOT minimal model sound

Minimal Model Completeness

A procedure is minimal model complete if it generates at least one model minimal modulo subset-simulation per symmetry class.

Minimal Model Soundness

A procedure is minimal model sound if it generates only models minimal modulo subset-simulation.

Subset-Simulation Test

Early closure of "non-minimal" branches

A partial model $\mathcal{I}$ subset-simulates an extracted model $\mathcal{I}'$ ($\mathcal{I}' \leq_{\subseteq} \mathcal{I}$).

- $\mathcal{I}$ not minimal or redundant $\Rightarrow$ close the current branch

Subset-Simulation Test

Early closure of “non-minimal” branches

A partial model $\mathcal{I}$ subset-simulates an extracted model $\mathcal{I}'$ ($\mathcal{I}' \leq_{\subseteq} \mathcal{I}$).

- $\mathcal{I}$ not minimal or redundant $\Rightarrow$ close the current branch

Backward closure of branches - minimal model refining

$\mathcal{I} =$ newly extracted model, $S =$ current set of minimal models.

- if there is an $\mathcal{I}' \in S$ s.t. $\mathcal{I}' \leq_{\subseteq} \mathcal{I}$, close the current branch
- close all the branches from which an $\mathcal{I}'$ s.t. $\mathcal{I} \leq_{\subseteq} \mathcal{I}'$ was extracted

Properties of the Procedures (so far)

- sound
- refutationally complete
- minimal model complete
- minimal model sound

Properties of the Procedures (so far)

- sound
- refutationally complete
- minimal model complete
- minimal model sound

They might not terminate!

Termination

A procedure terminates if the tableau calculus has strong termination.

Termination

$\mathbf{K}$, $\mathbf{KT}$, $\mathbf{KB}$ and $\mathbf{KTB}$: already terminating.

Main Problem

Finding blocking techniques that preserve minimal model completeness.

Termination

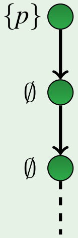
K, **KT**, **KB** and **KTB**: already terminating.

Main Problem

Finding blocking techniques that preserve minimal model completeness.

KD and **KDB**

- non-termination is caused by seriality
- infinite paths $u_1, \ldots, u_i$ where $V(u_j) = \emptyset$



Termination

K, **KT**, **KB** and **KTB**: already terminating.

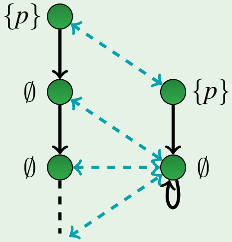
Main Problem

Finding blocking techniques that preserve minimal model completeness.

KD and **KDB**

- non-termination is caused by seriality
- infinite paths $u_1, \ldots, u_i$ where $V(u_j) = \emptyset$

  $\Rightarrow$ create a loop on u_1



Termination (cont'd)

K4, **KT4** and **KD4**

Known blocking techniques are

- subset blocking
- ancestor equality blocking
- anywhere equality blocking

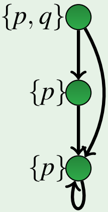
Termination (cont'd)

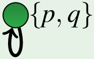
$\mathbf{K4}$, $\mathbf{KT4}$ and $\mathbf{KD4}$

Known blocking techniques are

- subset blocking
- ancestor equality blocking
- anywhere equality blocking

$p \wedge q \wedge \Box\Diamond p \wedge \Diamond p$





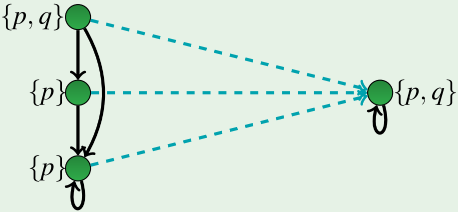
Termination (cont'd)

K4, **KT4** and **KD4**

Known blocking techniques are

- subset blocking
- ancestor equality blocking
- anywhere equality blocking

$p \wedge q \wedge \Box\Diamond p \wedge \Diamond p$



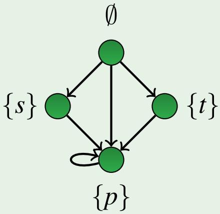
Termination (cont'd)

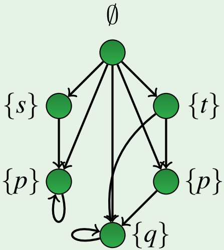
K4, **KT4** and **KD4**

Known blocking techniques are

- ~~subset blocking~~
- ancestor equality blocking
- anywhere equality blocking

$\Diamond s \wedge \Diamond t \wedge \Box\Diamond(p \vee q)$





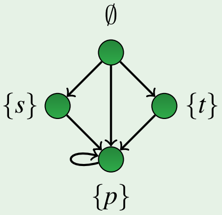
Termination (cont'd)

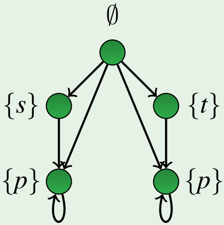
$\mathbf{K4}$, $\mathbf{KT4}$ and $\mathbf{KD4}$

Known blocking techniques are

- ~~subset blocking~~
- ancestor equality blocking
- ~~anywhere equality blocking~~

$$\Diamond s \wedge \Diamond t \wedge \Box\Diamond(p \vee q)$$





Termination (cont'd)

K5, **KD5**, **K45**, **KD45**, **KB4** and **KT5**: dynamic anywhere equality blocking.

For any two non-root worlds u and v

- Euclideanness $\Rightarrow$ R reflexive, symmetric, transitive
- $\mathcal{L}(u) = \mathcal{L}(v) \Rightarrow$ merging u and v preserves minimality

Termination (cont'd)

K5, **KD5**, **K45**, **KD45**, **KB4** and **KT5**: dynamic anywhere equality blocking.

For any two non-root worlds u and v

- Euclideanness $\Rightarrow$ R reflexive, symmetric, transitive
- $\mathcal{L}(u) = \mathcal{L}(v) \Rightarrow$ merging u and v preserves minimality

Theorem

All the normal modal logics between $\mathbf{K}$ and $\mathbf{KT5}$ have finitely many symmetry classes of models minimal modulo subset-simulation.

Conclusion and Further Work

- a new minimality criterion based on subset-simulation
- procedures for all the sublogics of **KT5**
  - sound
  - refutationally complete
  - minimal model complete
  - minimal model sound
  - terminating

Conclusion and Further Work

- a new minimality criterion based on subset-simulation
- procedures for all the sublogics of **KT5**
  - sound
  - refutationally complete
  - minimal model complete
  - minimal model sound
  - terminating
- generalisations to more expressive logics
  - multi-modal logics
  - universal modalities
  - inclusion axioms
  - converse relation
- generalisation to fragments of first-order logic
  - guarded fragment
  - guarded negation
- implementation