Minimal Models Modulo Subset-Simulation for Modal Logics

Fabio Papacchini   Renate A. Schmidt

The University of Manchester

{papacchf,schmidt}@cs.man.ac.uk

Motivation and Aim

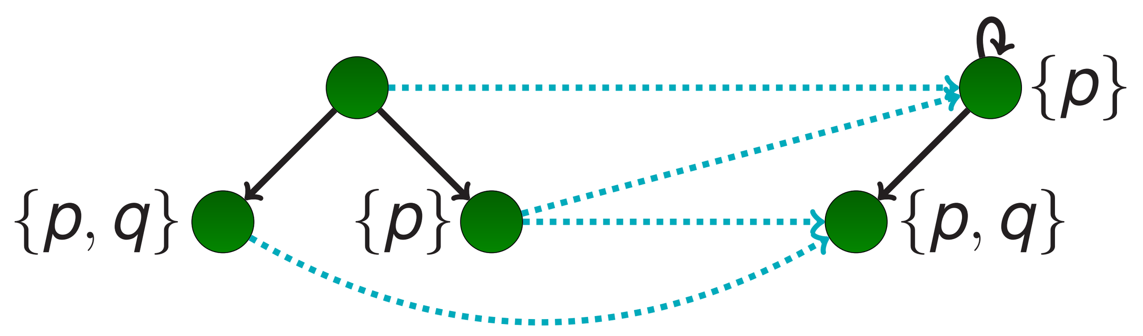
(Minimal) model generation is useful for several tasks such as hardware and software verification, fault analysis, and commonsense reasoning.

We aim to design a semantic and generic minimality criterion suitable for a big variety of modal logics. We also give a basic tableau calculus for computing the minimal models.

Subset-Simulation

Let $M = (W, R, V)$ and $M' = (W', R, V')$ be two models. A *subset-simulation* is a binary relation $S_\subseteq \subseteq W \times W'$ s.t. for any two worlds $u \in W$ and $u' \in W'$, $uS_\subseteq u'$ if

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



Minimal Models Modulo Subset-Simulation

Subset-simulation is a preorder over models.

$\Rightarrow$ Minimal models $=$ minimal elements of the preorder.

Simulation is used to reduce the number of minimal models.

Properties of the minimality criterion:

- applied to the graph representation of models (i.e., it is semantic),
- finite unravelled models are preferred over infinite unravelled models (not domain minimal),
- minimisation of the content of worlds,
- suitable for many modal logics.

Tableau Calculus

Input: a modal formula in negated normal form.

Branch selection strategy: the left most branch with the least number of worlds.

$$(\alpha)\ \frac{u : (\phi_1 \wedge \ldots \wedge \phi_n) \vee \Phi^+_\alpha}{\begin{array}{c} u : \phi_1 \vee \Phi^+_\alpha \\ \vdots \\ u : \phi_n \vee \Phi^+_\alpha \end{array}} \qquad (\Box)\ \frac{(u, v) : R \quad u : \Box\phi}{v : \phi}$$

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

where $\mathcal{A}$ is of the form $\Diamond\phi$, $\Box\phi$, or p_i, and $neg(\Phi^+) = \neg p_1 \wedge \ldots \wedge \neg p_n$ where p_i is a disjunct of Φ^+.

$$(\Diamond)\ \frac{u : \Diamond\phi}{\begin{array}{c} (u, u_1) : R \\ u_1 : \phi \end{array} \,\Big|\, \ldots \,\Big|\, \begin{array}{c} (u, u_n) : R \\ u_n : \phi \end{array} \,\Big|\, \begin{array}{c} (u, v) : R \\ v : \phi \end{array}}$$

where v is a fresh world.

$$(SBR)\ \frac{u : p_1, \ldots, u : p_n \quad u : \neg p_1 \vee \ldots \vee \neg p_n \vee \Phi^+_\alpha}{u : \Phi^+_\alpha}$$

Table: Rules of the tableau calculus

- Φ^+_α is a disjunction where no disjunct is a negated propositional variable,
- Φ^+ is a disjunction where no disjunct is a conjunction or a negated propositional variable.

Features of the calculus:

- lazy clausification ((α) rule) to reduce the number of inferences,
- complement splitting ((β) rule) to close “non-minimal” branches as soon as possible,
- exhaustive expansion of diamond formulae for minimal model completeness,
- selection-based resolution to reduce the number of inferences and to close branches.

The calculus is **refutationally sound and complete**.

The calculus is **minimal model complete**.

Subset-simulation test

- If the partial model of an open branch does not subset-simulates an already extracted model, but it is subset-simulated by it, then close the branch,
- compare newly extracted models with already extracted models and close branches accordingly.

The subset-simulation test guarantees **minimal model soundness**.

The calculus can be easily generalised to cover more expressive logics.

Termination depends on the logic under consideration.