Systematic Verification of the Modal Logic Cube in Isabelle/HOL

Christoph Benzmüller[1] Maximilian Claus[1] Nik Sultana[2]

[1]Dep. of Mathematics and Computer Science, Freie Universität Berlin, Germany

[2]Computer Lab, Cambridge University, UK

PxTP 2015, 02.08.15

Objective

- Proof object for expressive strength of different modal logics
- Two approaches:
  - Proof-theoretic (*$100 modal logic challenge* [Rabe, Pudlák, Sutcliffe, Shen])
  - Model-theoretic (here)
- Reason with and about modal logic by using an embedding in HOL
- Employ automated reasoners like *LEO-II* and *Satallax* via *Sledgehammer* as well as *Nitpick*

Quantified Modal Logic (QML) with Kripke Semantics

Language:

$$F ::= \mathcal{V} \mid \neg F \mid F \wedge F \mid F \vee F \mid (\forall \mathcal{V})F \mid (\exists \mathcal{V})F \mid \Box F \mid \Diamond F$$

Model: $\langle W, R, \models \rangle$

- Set of "possible worlds" W
- Accessibility relation $R \subseteq W \times W$
- $\models \subseteq W \times \mathcal{WFF}$ to check if a world satisfies some formula

$w \models \neg A$ iff $w \not\models A$

$w \models A \wedge B$ iff $w \models A$ and $w \models B$

$w \models A \vee B$ iff $w \models A$ or $w \models B$

$w \models (\forall v)A$ iff $w \models A[a \leftarrow B]$ for all $B \in \mathcal{WWF}$

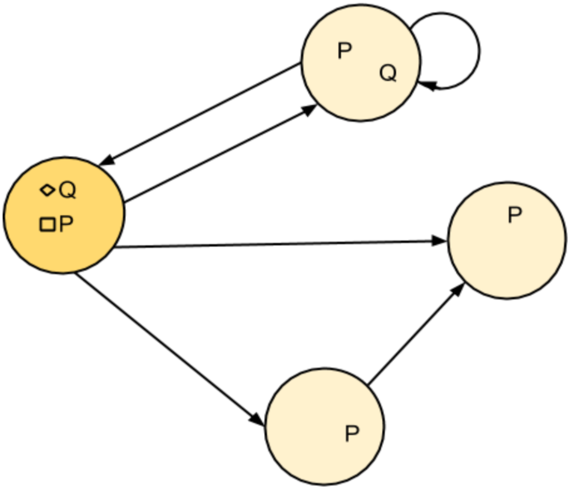
$w \models (\exists v)A$ iff there exists a $B \in \mathcal{WWF}$ such that $w \models A[a \leftarrow B]$

$w \models \Box A$ iff $u \models A$ for all u such that wRu

$w \models \Diamond A$ iff there exists a u such that wRu and $u \models A$

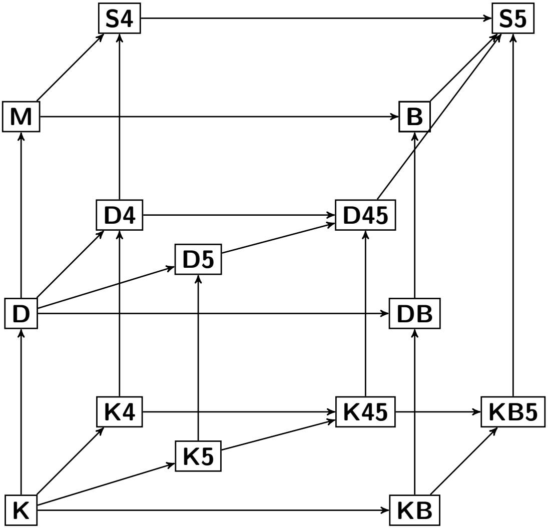
Validity: A valid in model $\langle W, R, \models \rangle$ iff $w \models A$ for all $w \in W$

Kripke Structure



$W = P, Q$

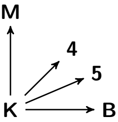
The Modal Logic Cube



S5 $\equiv$ **M5** $\equiv$ **MB5** $\equiv$ **M4B5** $\equiv$ **M45** $\equiv$ **M4B** $\equiv$ **D4B** $\equiv$ **D4B5** $\equiv$ **DB5**

KB5 $\equiv$ **K4B5** $\equiv$ **K4B**

M:	$\Box P \rightarrow P$
B:	$P \rightarrow \Box\Diamond P$
D:	$\Box P \rightarrow \Diamond P$
4:	$\Box P \rightarrow \Box\Box P$
5:	$\Diamond P \rightarrow \Box\Diamond P$



Embedding of QML in HOL

[Benzmüller, Paulson]

type_synonym $\sigma = (i \rightarrow bool)$

$\neg^m$	$:: \sigma \rightarrow \sigma$	$\neg^m \phi \equiv (\lambda w. \neg(\phi\, w))$
$\wedge^m$	$:: \sigma \rightarrow \sigma \rightarrow \sigma$	$\phi \wedge^m \psi \equiv (\lambda w. \phi\, w \wedge \psi\, w)$
$\vee^m$	$:: \sigma \rightarrow \sigma \rightarrow \sigma$	$\phi \vee^m \psi \equiv (\lambda w. \phi\, w \vee \psi\, w)$
$\rightarrow^m$	$:: \sigma \rightarrow \sigma \rightarrow \sigma$	$\phi \rightarrow^m \psi \equiv (\lambda w. \phi\, w \rightarrow \psi\, w)$
$\leftrightarrow^m$	$:: \sigma \rightarrow \sigma \rightarrow \sigma$	$\phi \leftrightarrow^m \psi \equiv (\lambda w. \phi\, w \leftrightarrow \psi\, w)$
$\forall^m$	$:: (a \rightarrow \sigma) \rightarrow \sigma$	$\forall^m \Psi \equiv (\lambda w. \forall x. \Psi\, x\, w)$
$\exists^m$	$:: (a \rightarrow \sigma) \rightarrow \sigma$	$\exists^m \Psi \equiv (\lambda w. \exists x. \Psi\, x\, w)$
$\Box$	$:: (i \rightarrow i \rightarrow bool) \rightarrow \sigma \rightarrow \sigma$	$\Box R \phi \equiv (\lambda w. \forall v. R\, w\, v \rightarrow \phi\, v)$
$\Diamond$	$:: (i \rightarrow i \rightarrow bool) \rightarrow \sigma \rightarrow \sigma$	$\Diamond R \phi \equiv (\lambda w. \exists v. R\, w\, v \wedge \phi\, v)$

$valid :: \sigma \rightarrow bool$ **where** $valid\ p \equiv \forall w. p\, w$

Correspondence Results

Sahlqvist formulae

Axioms

$$M \equiv \lambda R.valid(\forall^m(\lambda P.(\Box^R P) \rightarrow^m P))$$

$$B \equiv \lambda R.valid(\forall^m(\lambda P.P \rightarrow^m \Box^R \Diamond^R P))$$

$$D \equiv \lambda R.valid(\forall^m(\lambda P.(\Box^R P) \rightarrow^m \Diamond^R P))$$

$$4 \equiv \lambda R.valid(\forall^m(\lambda P.(\Box^R P) \rightarrow^m \Box^R \Box^R P))$$

$$5 \equiv \lambda R.valid(\forall^m(\lambda P.(\Diamond^R P) \rightarrow^m \Box^R \Diamond^R P))$$

Model Constraints

$$refl \equiv \lambda R.\forall S.R\ S\ S$$

$$sym \equiv \lambda R.\forall ST.(R\ S\ T \rightarrow R\ T\ S)$$

$$ser \equiv \lambda R.\forall S.\exists T.R\ S\ T$$

$$trans \equiv \lambda R.\forall STU.(R\ S\ T \wedge R\ T\ U \rightarrow R\ S\ U)$$

$$eucl \equiv \lambda R.\forall STU.(R\ S\ T \wedge R\ S\ U \rightarrow R\ T\ U)$$

Correspondence Results

Sahlqvist formulae

Axiom M corresponds to Reflexivity

theorem A1 : $(\forall R.(\mathit{refl}\ R) \leftrightarrow (M\ R))$ **by** (metis M-def refl-def)

Axiom B corresponds to Symmetry

lemma A2-a : $(\forall R.(\mathit{sym}\ R) \rightarrow (B\ R))$ **by** (metis B-def sym-def)

lemma A2-b : $(\forall R.(B\ R) \rightarrow (\mathit{sym}\ R))$ **by** (simp add:B-def sym-def, force)

theorem A2 : $(\forall R.(\mathit{sym}\ R) \leftrightarrow (B\ R))$ **by** (metis A2-a A2-b)

Axiom D corresponds to Seriality

theorem A3 : $(\forall R.(\mathit{ser}\ R) \leftrightarrow (D\ R))$ **by** (metis D-def ser-def)

Axiom 4 corresponds to Transitivity

theorem A4 : $(\forall R.(\mathit{trans}\ R) \leftrightarrow (IV\ R))$ **by** (metis IV-def trans-def)

Alternative Axiomatisations

M5 $\leftrightarrow$ MB5

theorem B1 : $\forall R.\ (\mathit{refl}\ R \wedge \mathit{eucl}\ R) \leftrightarrow (\mathit{refl}\ R \wedge \mathit{sym}\ R \wedge \mathit{eucl}\ R)$
  by (metis eucl-def refl-def sym-def)
theorem B1-alt : $\forall R.\ (M\ R \wedge V\ R) \leftrightarrow (M\ R \wedge B\ R \wedge V\ R)$
  by (metis A1 A2 A5 B1)

M5 $\leftrightarrow$ D4B

theorem B5 : $\forall R.\ (\mathit{refl}\ R \wedge \mathit{eucl}\ R) \leftrightarrow (\mathit{ser}\ R \wedge \mathit{trans}\ R \wedge \mathit{sym}\ R)$
  by (metis eucl-def refl-def ser-def sym-def trans-def)

KB5 $\leftrightarrow$ K4B

theorem B9 : $\forall R.\ (\mathit{sym}\ R \wedge \mathit{eucl}\ R) \leftrightarrow (\mathit{trans}\ R \wedge \mathit{sym}\ R)$
  by (metis eucl-def sym-def trans-def)

Inclusion Relations

Approach

Investigate relative strength of logics. Say $A > B$ iff logic A can prove more theorems than logic B.

- Model-theoretic view: $K4 > K$ says "Not every model is transitive"
- Showing $A' \geq A$ is easy if A' results from adding more axioms to A (every proof in A is also a valid proof in A')
- In general, it is difficult for the ATPs to derive proofs for strict relations $A > B$
- Use *Nitpick* to generate counter-examples and use their features as hints for the provers
  - Number of worlds
  - Complete description of the relation

Inclusion Relations

Example: K4 > K

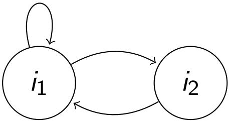
- **Step A**: In order to show K4 > K, conjecture K4 $\leq$ K:

$$\forall R.\ \mathit{trans}\ R$$

- Obtain counter model with *Nitpick*:

$$\begin{aligned} R = (\lambda x. -) \\ \quad i1 := (\lambda x. -)(i1 := \mathit{True}, i2 := \mathit{True}), \\ \quad i2 := (\lambda x. -)(i1 := \mathit{True}, i2 := \mathit{False})) \end{aligned}$$

- Diagram:



Inclusion Relations

Example: K4 > K (cont.)

- **Step B**: Give arity information to prover as a hint ($\#_2$ is a distinctiveness lemma):

$$\#_2\ i1\ i2 \rightarrow \forall R.\ \neg(\mathit{trans}\ R)$$

- **Step C**: In case this is not sufficient, supply the complete counter model (r constant):

$$\#_2\ i1\ i2 \wedge r\ i1\ i1 \wedge r\ i1\ i2 \wedge r\ i2\ i1 \wedge \neg r\ i2\ i2 \rightarrow \neg(\mathit{trans}\ r)$$

- **Step D**: Additionally, the counter models can be proven to be minimal in the number of worlds:

$$\#_1\ i1 \rightarrow (\forall R.\ \mathit{eucl}\ R)$$

Inclusion Relations

Results

- All but 4 problems can be solved by Satallax and LEO-II if they are supplied arity information
  - "ATP challenge problems"
- For 10 of these problems Metis integration fails
  - "Isabelle challenge problems"
- 5 of these can also be solved by CVC4 with Metis integration succeeding

- We can obtain Isar proofs for all problems solved by Satallax and LEO-II with Nik Sultana's proof translation tool

Discussion

- HOL-ATPs handle these sorts of proofs quite well (< 1 min of total computation time for whole cube), in contrast to popular FOL provers
- Potential for automation: Cooperation of ATPs with counter model finders like *Nitpick*
- Approach could be used for verifying axiomatisations within other non-classical logics (e.g. conditional logics)
- We could even automate the whole process!