Mechanizing Bisimulation Theorems for Relation-Changing Logics in Coq

Raul Fervari[1,2], Francisco Trucco[1] & Beta Ziliani[1,2]

[1] **FAMAF-UNC, Argentina**
[2] **CONICET, Argentina**

2nd DaLí Workshop, Porto, Portugal (2019)

Motivation

Automated Theorem Proving vs. Interactive Theorem Proving

- Mathematical proofs are complex and tedious.
- Pen-and-paper proofs are prone to errors.
- Computational tools are helpful.
- Automated Theorem Proving:
  1. In: Express statements of a theorem in a formal language.
  2. Machine: Algorithmic manipulations for these statements.
  3. Out: A proof / a counterexample.
- Easy to use for humans, but too heavy for computers (combinatorial explosion).

Motivation

Interactive Theorem Proving

- Verification of the correctness of a proof.
- The user provides enough information to the tool, in order to check the proof.
- Tactics: special *commands* to guide the proof.
- Two important uses of ITP's:
  - Obtain certified proofs.
  - Refine hypothesis of a proof.
- Examples of ITP's:
  - HOl4, HOL light, Isabelle, Lean, Coq.

Motivation

Our contributions and goals

1. Formalize and verify proofs for relation-changing logics, using ITP.
2. Obtain certifications for a general family of logics.
3. Starting point for a general framework for proof verification in modal logics.

Motivation

Interactive Theorem Proving in Practice

Some big problems using ITP:

- Verification of cryptographic protolocs in *security*

  [Meadows, 1994]

- Four color problem in *graph theory*

  [Gonthier, 2008]

- Transcendence for e and π in *number theory*

  [Bernard et al., 2016]

- Kepler conjecture in *combinatorial geometry*

  [Hales et al., 2017]

Related work

Formalizing and verifying (modal) logics

- Natural deduction system for $S5$ and $S5^n$ in Coq

  [de Wind, PhD 2001]

- Formalization in Lean of tableaux methods for ML

  [Wu & Goré, ITP 2019]

- Equivalence between proof systems for ML in Coq

  [González-Huesca et al., LSFA 2019]

- Proof language for differential dynamic logic in KeYmaera X

  [Bohrer & Platzer, CoRR 2019]

- Others…

  [Xavier et al., ENTCS 2018; D'Abrera & Goré, AiML 2018 (short)]

The Coq proof assistant

Main components

Gallina

Coq's specification language
higher order type theory
dependently-typed functional language

Tactics

commands for proof steps
elementary steps
advanced algorithms
Ltac allows the def. of new tactics

The Vernacular

the language of Gallina's commands
allows defs. of functions
statements of theorems
machine-checking of proofs
extraction of certified programs

Relation-changing modal logics

Syntax

$$\text{FORM} ::= \bot \mid p \mid \varphi \to \psi \mid \Diamond\varphi, \mid \blacklozenge_i\varphi$$

Relation-changing modal logics

Syntax

$$\text{FORM} ::= \bot \mid p \mid \varphi \to \psi \mid \Diamond\varphi, \mid \blacklozenge_i\varphi$$

Models

A model M is a triple $\mathsf{M} = \langle W, R, V \rangle$, where:

- W is a non-empty set of *points* or *states*;
- $R \subseteq W \times W$ is the *accessibility relation*;
- $V : \text{PROP} \mapsto 2^W$ is the *valuation*.

Let $w \in W$ we call M, w a *pointed model*.

Relation-changing modal logics

Model update functions

Given a set W, a model update function for W is a function

$$f_W : W \times 2^{W^2} \to 2^{W \times 2^{W^2}},$$

that takes $w \in W$ and $R \subseteq W^2$ and returns a set of possible updates

$$\{(w_1, R_1), \ldots, (w_n, R_n) \mid w_i \in W,\ R_i \subseteq W^2\}$$

Relation-changing modal logics

Model update functions

Given a set W, a model update function for W is a function

$$f_W : W \times 2^{W^2} \to 2^{W \times 2^{W^2}},$$

that takes $w \in W$ and $R \subseteq W^2$ and returns a set of possible updates

$$\{(w_1, R_1), \ldots, (w_n, R_n) \mid w_i \in W,\ R_i \subseteq W^2\}$$

Let $\mathscr{C}$ be a class of models, a family of model update functions f is defined as

$$f = \{f_W \mid \langle W, R, V\rangle \in \mathscr{C}\}.$$

Relation-changing modal logics

Semantics

Let $\mathrm{M} = \langle W, R, V \rangle$ be a model, $w \in W$.

$$
\begin{array}{lll}
\mathrm{M}, w \models \bot & & \text{never} \\
\mathrm{M}, w \models p & \text{iff} & w \in V(p) \\
\mathrm{M}, w \models \varphi \to \psi & \text{iff} & \mathrm{M}, w \not\models \varphi \text{ or } \mathrm{M}, w \models \psi \\
\mathrm{M}, w \models \Diamond \varphi & \text{iff} & \text{for some } v \in W \text{ s.t. } (w, v) \in R,\ \mathrm{M}, v \models \varphi
\end{array}
$$

Relation-changing modal logics

Semantics

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$.

$$
\begin{array}{lll}
\mathsf{M}, w \models \bot & & \text{never} \\
\mathsf{M}, w \models p & \text{iff} & w \in V(p) \\
\mathsf{M}, w \models \varphi \to \psi & \text{iff} & \mathsf{M}, w \not\models \varphi \text{ or } \mathsf{M}, w \models \psi \\
\mathsf{M}, w \models \Diamond \varphi & \text{iff} & \text{for some } v \in W \text{ s.t. } (w, v) \in R,\ \mathsf{M}, v \models \varphi \\
\mathsf{M}, w \models \blacklozenge_f \varphi & \text{iff} & \text{for some } (v, R') \in f_W(w, R),\ \langle W, R', V \rangle, v \models \varphi.
\end{array}
$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

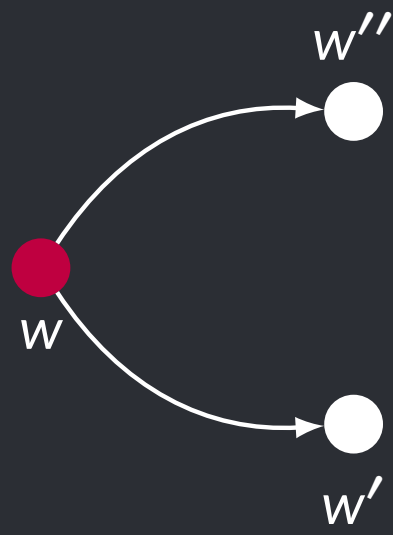
$$f^{\mathrm{sb}}_{W}(w, R) = \{(v, R \setminus (w, v)) \mid (w, v) \in R\}$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

$$f^{\mathsf{sb}}_{W}(w, R) = \{(v, R \setminus (w, v)) \mid (w, v) \in R\}$$



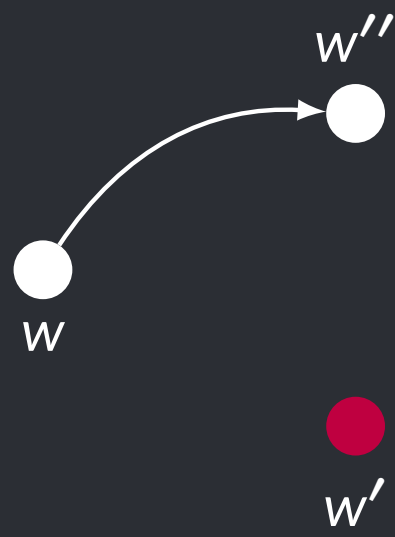
$$\langle W, R, V \rangle, w \models \blacklozenge_{f^{\mathsf{sb}}} \varphi$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

$$f^{\mathsf{sb}}_{W}(w, R) = \{(v, R \setminus (w, v)) \mid (w, v) \in R\}$$



$$\langle W, R \setminus (w, w'), V \rangle, w' \models \varphi$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

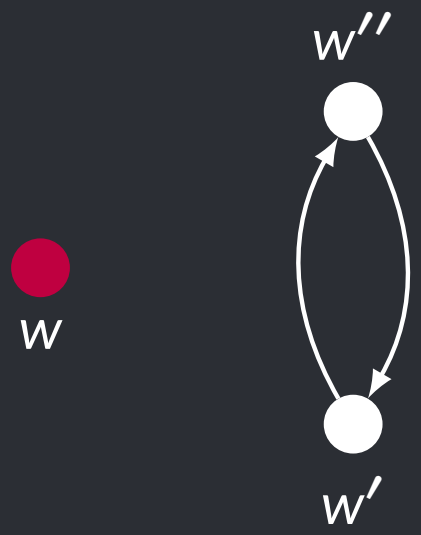
$$f^{\mathrm{br}}_{w}(w, R) = \{(v, R \cup (w, v)) \mid (w, v) \notin R\}$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

$$f^{\mathrm{br}}_{w}(w, R) = \{(v, R \cup (w, v)) \mid (w, v) \notin R\}$$



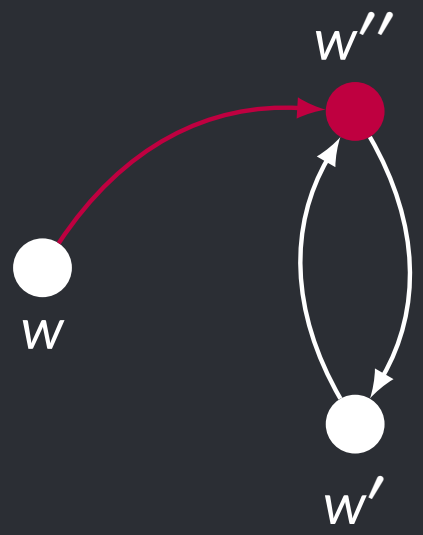
$$\langle W, R, V \rangle, w \models \blacklozenge_{f^{\mathrm{br}}} \varphi$$

Relation-changing modal logics

Examples

Let $\mathsf{M} = \langle W, R, V \rangle$ be a model, $w \in W$. Consider the model update function:

$$f^{\mathrm{br}}_{w}(w, R) = \{(v, R \cup (w, v)) \mid (w, v) \notin R\}$$



$$\langle W, R \cup (w, w''), V \rangle, w'' \models \varphi$$

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\Diamond_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\Diamond_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

(atomic harmony) for all $p \in \mathrm{PROP}$, $w \in V(p)$ iff $w' \in V'(p)$;

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\blacklozenge_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

(atomic harmony) for all $p \in \mathrm{PROP}$, $w \in V(p)$ iff $w' \in V'(p)$;

(zig) if $(w, v) \in S$, there is $v' \in W'$ s.t. $(w', v') \in S'$ and $(v, S)Z(v', S')$;

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\Diamond_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

(atomic harmony) for all $p \in \mathrm{PROP}$, $w \in V(p)$ iff $w' \in V'(p)$;

(zig) if $(w, v) \in S$, there is $v' \in W'$ s.t. $(w', v') \in S'$ and $(v, S)Z(v', S')$;

(zag) if $(w', v') \in S'$, there is $v \in W$ s.t. $(w, v) \in S$ and $(v, S)Z(v', S')$;

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\blacklozenge_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

(atomic harmony) for all $p \in \mathrm{PROP}$, $w \in V(p)$ iff $w' \in V'(p)$;

(zig) if $(w, v) \in S$, there is $v' \in W'$ s.t. $(w', v') \in S'$ and $(v, S)Z(v', S')$;

(zag) if $(w', v') \in S'$, there is $v \in W$ s.t. $(w, v) \in S$ and $(v, S)Z(v', S')$;

(f-zig) if $(v, T) \in f_W(w, S)$, there is $(v', T') \in f_{W'}(w', S')$ s.t. $(v, T)Z(v', T')$;

Relation-changing modal logics

Bisimulations

Definition (Bisimulations)

Let $\mathsf{M} = \langle W, R, V \rangle$, $\mathsf{M}' = \langle W', R', V' \rangle$, and f a family of model update functions. $Z \subseteq (W \times 2^{W^2}) \times (W' \times 2^{W'^2})$ is an $\mathsf{ML}(\blacklozenge_f)$-bisimulation if it satisfies the following conditions. If $(w, S)Z(w', S')$ then

(atomic harmony) for all $p \in \mathrm{PROP}$, $w \in V(p)$ iff $w' \in V'(p)$;

(zig) if $(w, v) \in S$, there is $v' \in W'$ s.t. $(w', v') \in S'$ and $(v, S)Z(v', S')$;

(zag) if $(w', v') \in S'$, there is $v \in W$ s.t. $(w, v) \in S$ and $(v, S)Z(v', S')$;

(f-zig) if $(v, T) \in f_W(w, S)$, there is $(v', T') \in f_{W'}(w', S')$ s.t. $(v, T)Z(v', T')$;

(f-zag) if $(v', T') \in f_{W'}(w', S')$, there is $(v, T) \in f_W(w, S)$ s.t. $(v, T)Z(v', T')$.

$\mathsf{M}, w \leftrightarrows_{\mathsf{ML}(\blacklozenge_f)} \mathsf{M}', w'$ if there is an $\mathsf{ML}(\blacklozenge_f)$-bisimulation Z s.t. $(w, R)Z(w', R')$.

Mechanization of Relation-Changing Logics

Propositional symbols

```
Inductive prop : Set := p : nat → prop.
```

- `prop` is a new type with a type constructor `p`.
- Given a natural number `n`, it constructs a `p n` in `prop`.

Mechanization of Relation-Changing Logics

Syntax

$$\boxed{\text{FORM} ::= \bot \mid p \mid \varphi \rightarrow \psi \mid \Diamond\varphi, \mid \blacklozenge_i \varphi}$$

Corresponds in Coq with:

```
Inductive form: Type :=
  | Bottom : form
  | Atom   : prop → form
  | If     : form → form → form
  | Diam   : form → form                (* Notation <m>phi *)
  | DynDiam: Dyn → form → form.         (* Notation <o> d phi *)
```

Mechanization of Relation-Changing Logics

Model update functions (muf)

$$\boxed{f_W : W \times 2^{W^2} \to 2^{W \times 2^{W^2}},}$$

i.e., for some (w, R),

$$\boxed{f_W(w, R) = \{(w_1, R_1), \ldots, (w_n, R_n) \mid w_i \in W,\ R_i \subseteq W^2\}}$$

Mechanization of Relation-Changing Logics

Model update functions (muf)

$$\boxed{f_W : W \times 2^{W^2} \to 2^{W \times 2^{W^2}},}$$

i.e., for some (w, R),

$$\boxed{f_W(w, R) = \{(w_1, R_1), \ldots, (w_n, R_n) \mid w_i \in W,\ R_i \subseteq W^2\}}$$

Corresponds in Coq with:

```
Definition point (W: Set) : Type := (W * Relation W).

Definition muf : Type := forall (W : Set),
  (point W) → (point W → Prop).
```

Invariance Theorem

A general result for RCML

Theorem (Invariance)

Let f be a family of model update functions, then $\mathsf{M}, w \leftrightarrows_{\mathsf{ML}(\blacklozenge_f)} \mathsf{M}', w'$ *implies* $\mathsf{M}, w \equiv_{\mathsf{ML}(\blacklozenge_f)} \mathsf{M}', w'$.

Invariance Theorem

A general result for RCML

Theorem (Invariance)

Let f be a family of model update functions, then $\mathsf{M}, w \leftrightarrows_{\mathsf{ML}(\blacklozenge_f)} \mathsf{M}', w'$ *implies* $\mathsf{M}, w \equiv_{\mathsf{ML}(\blacklozenge_f)} \mathsf{M}', w'$.

```
Theorem InvarianceUnderBisimulation :
  forall (p: point W) (p': point W'),
    bisimulable_at_points p p' → equivalent_at_points p p'.
```

Summing up

+ Coq formalization of relation-changing logics.
+ Mechanization of the invariance under bisimulation theorem.
+ First unified framework.

Summing up

+ Coq formalization of relation-changing logics.
+ Mechanization of the invariance under bisimulation theorem.
+ First unified framework.
? Use the framework for particular logics (DEL, Separation Logic).

Summing up

+ Coq formalization of relation-changing logics.
+ Mechanization of the invariance under bisimulation theorem.
+ First unified framework.
? Use the framework for particular logics (DEL, Separation Logic).
? Mechanization of other results (standard translations, completeness).

Summing up

+ Coq formalization of relation-changing logics.
+ Mechanization of the invariance under bisimulation theorem.
+ First unified framework.
? Use the framework for particular logics (DEL, Separation Logic).
? Mechanization of other results (standard translations, completeness).
? Implementation of specific tactics for our logics.