Why Propositional Quantification Makes Modal Logics on Trees Robustly Hard?

Stéphane Demri
– LSV, CNRS, ENS Paris-Saclay –

Joint work with

Bartosz Bednarczyk
– U. of Dresden & U. of Wroclaw –

I3S, June 2019
Realm of (modal) logics updating models

- Logics of public announcements [Plaza, ISMIS’89]
- Sabotage modal logics [van Benthem, 2002]
- Separation logics [Reynolds, LiCS’02]
- Logic with separating modalities LSM [Courtauld & Galmiche & Pym, TCS 2016]
- Propositional team logic [Hannula et al., ToCL 2018]
- Logics with reactive Kripke semantics [Gabbay, Book 2013]
Overview

1. Second-order modal logics

2. Tree semantics

3. Fragments of quantified CTL under the tree semantics
   - Bounding the branching degree
   - Computational complexity with EX only
   - Harvest of TOWER-hard logics on tree-like models
Second-order modal logics
Modal logics in a nutshell

- Formulae: \( \phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \lozenge \phi \mid \Box \phi. \)

- Kripke-style structures \( \mathcal{M} = (W, R, V) \):
  - \( W \): non-empty set of worlds.
  - \( R \subseteq W \times W \): accessibility relation.
  - \( V : \text{PROP} \rightarrow \mathcal{P}(W) \): valuation.

\[
\begin{array}{c}
\vcenter{\hbox{\begin{tikzpicture}
  \node (w) at (0,0) [label=left:w] {w};
  \node (p) at (1,0) [label=left:p] {p};
  \node (q) at (2,0) [label=left:q] {q};
  \node (w') at (1,1) [label=left:w'] {w'};\end{tikzpicture}}}
\quad \vcenter{\hbox{\begin{tikzpicture}
  \node (p) at (0,0) [label=left:p] {p};
  \node (q) at (1,0) [label=left:q] {q};
  \node (p') at (0,1) [label=left:p'] {p'};\end{tikzpicture}}}
\end{array}
\]

- Satisfaction relation:
  - \( \mathcal{M}, w \models p \iff w \in V(p) \).
  - \( \mathcal{M}, w \models \lozenge \phi \iff \text{there is } w' \text{ s.t. } (w, w') \in R \text{ and } \mathcal{M}, w' \models \phi. \)
  - \( \mathcal{M}, w \models \Box \phi \iff \text{for all } w' \text{ s.t. } (w, w') \in R, \mathcal{M}, w' \models \phi. \)
Ubiquity of modal logics

• Satisfiability problem: given a formula \( \phi \), are there \( M, w \) such that \( M, w \models \phi \)?

• Plethora of modal logics depending on the frame conditions:
  • Modal logic S5: \( R \) is an equivalence relation (or \( R = W \times W \)).
  • Modal logic K: \( R \) is arbitrary (or \( (W, R) \) is a finite tree).
  • Modal logic S4: \( R \) is reflexive and transitive.

• Epistemic/temporal logics can be viewed as modal logics with
  • specific frame conditions (e.g., \( (W, R) \) is a tree),
  • multiple modalities (e.g., \( \Diamond \) and \( \Diamond^* \) associated to \( R^* \)),
  • modalities of arity \( > 1 \) (e.g., the until operator \( U \)).

\( \phi U \psi, \phi \quad \phi \quad \phi \quad \phi \quad \psi \)

• Computation Tree Logic CTL for model-checking:
  • Models are usually total Kripke-style structures.
  • Modalities are \( EX \) (\( \approx \Diamond \)), \( EF \) (\( \approx \Diamond^* \)), \( E(U\cdot) \) and \( A(U\cdot) \).
A natural need for model updates

- At the bottom line: changing the pointed model with $\Diamond$.

- Saboting the model with $\Diamond$.

- Removing worlds with the public announcement $[\phi]$.

See e.g., [van Benthem, 2005; Löding & Rohde, FST&TCS’03]

See e.g., [Plaza, ISMIS’89]
Propositional quantification in modal logics
– or, the modal way from SAT to QBF –

• Changing valuations with $\exists p$.

\[
\begin{align*}
\models & \exists p \Box p \\
\end{align*}
\]

See e.g., [Fine, Theoria 1970]

\begin{itemize}
  \item QK formulae: $\phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \Diamond \phi \mid \Box \phi \mid \exists p \phi$. \\
  \item $\mathcal{M}, w \models \exists p \phi$ iff there is a $p$-variant $\mathcal{M}'$ s.t. $\mathcal{M}', w \models \phi$. \\
  \item Variants second-order modal logics QS4, QS5, etc.
\end{itemize}

See e.g. [Kripke, JSL 1959; Fine, PhD 1969; Kaplan, JSL 1970]
**Fine’s results** [Fine, PhD thesis ’69, Theoria 1970]

- For any modal logic \( \mathcal{L} \) between \( K \) and \( S4 \), the satisfiability problem for \( Q\mathcal{L} \) is undecidable.

- \( QS5 \) has the exponential-size model property, the satisfiability problem is decidable and every formula is logically equivalent to a formula in graded modal logic \( GS5 \).

- Hilbert-style axiomatisation for \( QS5 \) and variants.

- ... and also
  - Reduction from second-order predicate logic to \( QS4.2 \) or for logics weaker than \( S4.2 \). [Kaminski & Tiomkin, NDJFL 1996]
  - Second-order quantification and two \( S5 \)-modalities lead to undecidability. [Antonelli & Thomason, JSL 2002]

\( S4.2 \) is characterised by reflexive, transitive and convergent modal frames.
Our original motivation: relationships with separation logics

- Separation logics for deductive verification use separating conjunction $\ast$ for properties on disjoint parts of the memory. [Reynolds, LiCS’02]

- Memory state $(s, h)$:
  
  \[
  \text{store } s : \text{PVAR} \rightarrow \text{Val} \quad \text{heap } h : \text{Loc} \rightarrow_{\text{fin}} \text{Val}
  \]

- Disjoint heaps when $\text{dom}(h_1) \cap \text{dom}(h_2) = \emptyset$ and disjoint union $h_1 \uplus h_2$.

- $(s, h) \models \phi_1 \ast \phi_2$ iff there are $h_1, h_2$ such that $h = h_1 \uplus h_2$, $(s, h_1) \models \phi_1$ and $(s, h_2) \models \phi_2$. 

Second-order modal logics
Separating conjunction as propositional quantification

\[
\models \phi_1 \neq \phi_2
\]

\[
\models \phi_1^p \neq \phi_2^p
\]

Second-order quantification is used in many contexts, see e.g.

- To design algorithms for ATL with strategy contexts.
  [Laroussinie & Markey, IC 2015]

- Relationships with epistemic reasoning.
  [Belardinelli & van der Hoek, AAAI’16]

- Enriching the modal $\mu$-calculus for control synthesis.
  [Riedweg & Pinchinat, MFCS’03]

- $\downarrow_x$ in hybrid modal logic is already a form of propositional quantification.
  [Areces & Blackburn & Marx, JSL 2001]
QCTL under the tree semantics
Tree unfolding preserves quantifier-free modal formulae

Tree semantics
QCTL: Quantified CTL

\[ \phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \text{EX}\phi \mid \exists p \phi \quad (\Diamond \approx \text{EX}) \]

\[ \mid E(\phi U \psi) \mid A(\phi U \psi) \]

- Models are total Kripke structures \( M = (W, R, V) \).

- \( M, w \models \exists p \phi \) iff there is \( M' \) s.t. \( M \approx_{AP \backslash \{p\}} M' \) & \( M', w \models \phi \).
Tree semantics [Laroussinie & Markey, LMCS 2014]

- Satisfiability problem for QCTL\(^t\) (tree semantics):
  
  **input:** a QCTL formula \(\phi\).

  **output:** 1 iff there is a finite total Kripke structure whose tree unfolding satisfies \(\phi\).

- \(\text{SAT}(\text{QCTL}^t)\) is \text{TOWER}-complete.

  \text{TOWER:} class of problems of time complexity bounded by a tower of exponentials, whose height is an elementary function of the input

  [Schmitz, TOCT 2016].

---

Tree semantics [Laroussinie & Markey, LMCS 2014]

- Satisfiability problem for QCTL\(^t\) (tree semantics):

  **input:** a QCTL formula \(\phi\).

  **output:** 1 iff there is a finite total Kripke structure whose tree unfolding satisfies \(\phi\).

- SAT(QCTL\(^t\)) is TOWER-complete.

  \text{TOWER:} class of problems of time complexity bounded by a tower of exponentials, whose height is an elementary function of the input

  [Schmitz, TOCT 2016].

Our investigation

- What is the complexity of \( \text{SAT}(\text{QCTL}^t_X) \), where \( \text{QCTL}^t_X \) is \( \text{QCTL}^t \) restricted to \( \text{EX} \)?
  (known \( \text{TOWER} \)-hardness proof for \( \text{SAT}(\text{QCTL}^t) \) uses \( \text{U} \))

- An elementary upper bound may lead to a similar bound for some modal separation logic [Demri & Fervari, AiML'18].

- Similar question for \( \text{SAT}(\text{QCTL}^{ft}_X) \) where \( \text{QCTL}^{ft}_X \) is the variant of \( \text{QCTL}^t_X \) on finite trees.

- Similar questions with \( \text{EF} \) or \( \text{EXEF} \).

- Second-order extension of modal logics characterised by classes of trees, including results for K, KD, D4, K4, S4, GL.
Nominals and local nominals

- Nominals from hybrid (modal) logics: propositional variables that hold true in a unique world.
  
  [Areces & Blackburn & Marx, JSL 2001]

- \( Q\phi \): there is a unique world satisfying \( \phi \) [Fine, PhD 1969].
  
  See also [Garson, 1984; Kaminski & Tiomkin, NDFL 1996].

- A toolkit for introducing local nominals \( x \).
  - \( \text{nom}(x, k) \): there is exactly one descendant at depth \( k \) satisfying \( x \).
    
    \[
    \text{nom}(x, k) \overset{\text{def}}{=} \text{EX}^k x \land \neg \exists p \left( \text{EX}^k(x \land p) \land \text{EX}^k(x \land \neg p) \right).
    \]

  - \( \@_x^k \phi \overset{\text{def}}{=} \text{EX}^k(x \land \phi) \): this unique descendant satisfies \( \phi \).

  - \( \text{diff-nom}(x_1, \ldots, x_\alpha, k) \): \( \alpha \) distinct descendants at depth \( k \).
    
    \[
    \text{diff-nom}(x_1, \ldots, x_\alpha, k) \overset{\text{def}}{=} \bigwedge_{i \in [1, \alpha]} \text{nom}(x_i, k) \land \bigwedge_{i < j \in [1, \alpha]} \neg \@_x^k x_j.
    \]
Local nominals are helpful!

- Simulation of first-order quantification on a given set of nodes of bounded depth.

- At most $2^n$ children ($\Diamond_{\leq 2^n} \top$ in graded modal logics):

  $$\exists p_0, \ldots, p_{n-1} \forall x, y \; \text{diff-nom}(x, y, 1) \rightarrow$$

  $$\neg \left( \bigwedge_{i \in [0, n-1]} @^1_x p_i \leftrightarrow @^1_y p_i \right).$$

[David & Laroussinie & Markey, CONCUR’16]
Bounding the branching degree
Bounding the branching degree

- $\text{QCTL}^t_{\leq N}$: variant of QCTL$^t_X$ with $N$-bounded tree models.

- A formula $\phi$ of modal depth $k$ can only reach the nodes of depth at most $k$ from the root.

- $\text{SAT}(\text{QCTL}^t_{\leq N})$ is in EXPSPACE:
  1. Guess a finite tree $\mathcal{T}$ with at most $N$ children per node and of depth $k$.
  2. Check whether $\mathcal{T}, \varepsilon \models \phi$, using a polynomial-space algorithm running on exponential-size inputs.
  3. Invoke Savitch’s Theorem for getting rid of the non-determinism and get EXPSPACE.
Alternating multi-tiling problem

- $\text{AExp}_{\text{POL}}$: class of problems decidable with an exponential-time ATM and a polynomial number of alternations. ($\text{Nexptime} \subseteq \text{AExp}_{\text{POL}} \subseteq \text{ExpSpace}$)

- The algorithm can be refined to obtain $\text{AExp}_{\text{POL}}$.

- $\text{AExp}_{\text{POL}}$-complete alternating multi-tiling problem.

[Bozzelli et al., GANDALF’17; Molinari, PhD 2019]

for all $w_1 \in T_0^{2^n}$, there is $w_2 \in T_0^{2^n}$ such that $\cdots$ for all $w_{n-1} \in T_0^{2^n}$, there is $w_n \in T_0^{2^n}$ such that there is a solution $(\tau_1, \ldots, \tau_n)$?
Idea of the reduction

• The grid $[0, 2^n - 1]^2$ is encoded by a binary tree of depth $2n$.

• Horizontal and vertical constraints encoded thanks to local nominals (at depth $2n$) and standard arithmetical reasoning on $n$-bit numbers.

• Quantifications on the first rows naturally expressed by propositional quantifications.

• For all $N \geq 2$, $\text{SAT}(\text{QCTL}_{X, \leq N}^t)$ is $\text{AEXP}_{\text{POL}}$-complete.

• $\text{SAT}(\text{QCTL}_{X, \leq 1}^t)$ is $\text{PSPACE}$-complete (easy).
Tower-hardness of $\text{SAT}(\text{QCTL}^t_X)$
How to prove Tower-hardness

• Uniform elementary reduction from $k$-\textsc{NExpTime}-complete tiling problems $\text{Tiling}_k$.

• $t(0, n) = n$ and $t(k + 1, n) = 2^{t(k, n)}$.

• $\text{Tiling}_k$:
  
  \textbf{input:}  
  \begin{itemize}
    \item $(\mathcal{T}, \mathcal{H}, \mathcal{V})$ (tile types, horizontal and vertical matching relations),
    \item $c = t_0, t_1, \ldots, t_{n-1} \in \mathcal{T}^n$: initial condition.
  \end{itemize}

  \textbf{output:} 1 iff the grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$ can be tiled (with usual constraints)?
High-level description of the reduction from $\text{Tiling}_k$

- Grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$ as a tree model:
  - The root $\varepsilon$ has $t(k + 1, n)$ children.
  - $t(k, n)$ children of $\varepsilon$ are distinguished and receive a number in $[0, t(k, n) - 1]$.
  - Each child of $\varepsilon$ has exactly $t(k, n)$ children and each child has a number in $[0, t(k, n) - 1]$.

Encoding of the grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$
Enforcing $t(k, n)$ children

- The most difficult and substantial part of the proof.

- Any node is of type 0.

- Node $v$ of type $k > 0$:
  - every child is of type $k - 1$.
  - $v$ has $t(k, n)$ children numbered from 0 to $t(k, n) - 1$.

- A number for a node of type 0 is encoded by $p_{n-1}, \ldots, p_0$.

- A number for a node of type $k > 0$
  - is encoded by the truth value $val$ on its children,
  - it belongs to $[0, t(k + 1, n) - 1]$.
Enforcing $t(k, n)$ children

Type $k$

$\text{val} = \top, \text{nb} = 0$

$\text{nb} = t(k+1, n) - 1$

Type $(k-1)$

$\text{val} = \top, \text{nb} = t(k, n) - 1$

Type $(k-2)$

$\text{val} = \bot, \text{nb} = 0$

$\text{val} = \bot, \text{nb} = t(k-1, n) - 1$

Type 0

$\text{nb} = 1$

$p_{n-1} = \ldots = p_1 = \bot, p_0 = \top$
Specifications for a node of type $k > 0$

- Every child is of type $k - 1$.
- There is a child with number equal to zero.
- Distinct children have distinct numbers in $[0, t(k, n) - 1]$.
- If a child has number $m < t(k, n) - 1$, then there is a sibling with number equal to $m + 1$.

\[
\text{type}(k) \overset{\text{def}}{=} \text{AX}(\text{type}(k - 1)) \land \text{EX}(\text{first}(k - 1)) \land \text{uniq}(k) \land \text{compl}(k).
\]

- $\text{SAT}(\text{QCTL}_X^t)$ is Tower-complete \cite{Bednarczyk & Demri, LiCS’19} (many developments are omitted here)
Other Tower-hard logics on tree-like models
Other fragments of quantified CTL

- **QCTL** formulae: \( \phi ::= p \mid \neg \phi \mid \phi \land \phi \mid EF \phi \mid \exists p \phi. \)

\[
\bigwedge_{0 \leq i \leq k} AG(l_i \rightarrow \neg \exists p (p \land EF(l_i \land \neg p))) \quad \text{(no stuttering)}
\]

\[
t(i, \exists p \psi) \overset{\text{def}}{=} \exists p t(i, \psi) \quad t(i, \text{EX} \psi) \overset{\text{def}}{=} EF(l_{i-1} \land t(i - 1, \psi)).
\]
Hardness results

- Given $\phi$ of modal depth $k$, $\phi$ is satisfiable for $\text{QCTL}^t_X$ iff $t(k, \phi) \land \text{shape}(k)$ is satisfiable for $\text{QCTL}^t_F$.

- $\text{SAT}(\text{QCTL}^t_F)$ and $\text{SAT}(\text{QCTL}^t_{XF})$ are Tower-hard.

- Tower-hardness holds also for $\text{SAT}(\text{QCTL}^f_{XF})$ and $\text{SAT}(\text{QCTL}^f_{XF})$ with the finite tree semantics.

- Latest news: $\text{SAT}(\text{QCTL}^t_F)$ restricted to formulae of temporal depth two is already Tower-hard. [Mansutti, to be sub.]
Characterisation for standard modal logics

• Pick a modal logic $\mathcal{L}$ characterised by a class of tree-like frames $\mathcal{C}$ and extend it with propositional quantification.

• Examples of class $\mathcal{C}$ for standard modal logics
  • $\text{K}$: finite trees. ($\Box \approx \text{EX}$)
  • $\text{GL}$ (after Gödel & Löb): structures $(W, R^+, V)$ such that $(W, R)$ is a finite tree. ($\Box \approx \text{EXEF}$)
  • $\text{S4}$: structures $(W, R^*, V)$ s.t. $(W, R)$ is a finite-branching tree for which all the maximal branches are infinite. ($\Box \approx \text{EF}$)
  • etc.

• Over the appropriate classes of trees, these modal logics with propositional quantification are TOWER-complete.

• E.g., for GL, it corresponds exactly to $\text{QCTL}^{ft}_{\text{XF}}$. 
Concluding remarks

- \( \text{SAT}(\text{QCTL}^t_X) \) is Tower-hard, as well as second-order K on finite trees.

- As by-products, \( \text{SAT}(\text{QCTL}^t_{XF}) \) and \( \text{SAT}(\text{QCTL}^t_F) \) are Tower-hard too!

- Moreover, Tower-hardness for
  - second-order S4 on finite-branching trees for which all maximal branches are infinite (\( \approx \text{QCTL}^t_F \)),
  - second-order GL under the finite transitive tree semantics.

- Future direction:
  - Expressive power of fragments.
  - Interesting fragments with elementary complexity.
  - Fragments preserving Tower-hardness.
  See e.g. recent Mansutti’s results restricting temp. depth.