Unifying Hyper and Epistemic Temporal Logics

Laura Bozzelli[1], Bastien Maubert[2], and Sophie Pinchinat[3]

[1] UPM, Madrid, Spain.
[2] LORIA - CNRS / Université de Lorraine, Nancy, France.
[3] IRISA, Université de Rennes 1, France.

Abstract. In the literature, two powerful temporal logic formalisms have been proposed for expressing information-flow security requirements, that in general, go beyond regular properties. One is classic, based on the knowledge modalities of epistemic logic. The other one, the so-called hyper logic, is more recent and subsumes many proposals from the literature. In an attempt to better understand how these logics compare with each other, we consider the logic KCTL^* (the extension of CTL^* with knowledge modalities and synchronous perfect recall semantics) and $\mathsf{HyperCTL}^*$. We first establish that KCTL^* and $\mathsf{HyperCTL}^*$ are expressively incomparable. Then, we introduce a natural linear past extension of $\mathsf{HyperCTL}^*$, called $\mathsf{HyperCTL}^*_{lp}$, that unifies KCTL^* and $\mathsf{HyperCTL}^*$. We show that the model-checking problem for $\mathsf{HyperCTL}^*_{lp}$ is decidable, and we provide its exact computational complexity in terms of a new measure of path quantifiers' alternation. For this, we settle open complexity issues for unrestricted quantified propositional temporal logic.

1 Introduction

Temporal logics provide a fundamental framework for the description of the dynamic behavior of reactive systems, and they usually support the successful model-checking approach to automatically verify complex finite-state systems.

Classic *regular* temporal logics, such as standard LTL [21] or the more expressive CTL^* [10], lack mechanisms to relate distinct paths or executions of a system. These mechanisms are required to formally express information-flow security properties which specify how information may propagate from inputs to outputs, such as non-interference [12] or opacity [5]. In the literature, two powerful temporal logic formalisms have been proposed for expressing such security requirements that, in general, go beyond regular properties.

One is classical and is based on the extension of temporal logic with the knowledge modalities of epistemic logic [11], which relate paths that are observationally equivalent for a given agent. A classic instance is KCTL^*, the extension of CTL^* with knowledge modalities under the synchronous perfect recall semantics (where an agent remembers the whole sequence of its observations, and observations are time-sensitive) [14, 24, 22, 8]. This logic and its linear-time

We acknowledge financial suppport from ERC project EPS 313360.

fragment, KLTL, have been used to specify secrecy policies that involve sets of execution traces sharing some similar information [1, 13, 3].

In the second, more recent, framework [7] one can express properties of sets of execution traces, known as *hyperproperties*; these are useful to formalize security policies, such as non-interference [12] and observational determinism [18]. The general hyper logical framework introduced in [7] is based on a second-order logic for which model-checking is undecidable. More recently, fragments of this logic have been introduced [6], namely the logics HyperCTL* and HyperLTL, for which model checking is decidable. These logics extend CTL* and LTL in a simple and natural way by allowing explicit and simultaneous quantification over multiple paths. In [6], an extension of the semantics of HyperCTL* and HyperLTL is also considered. In this setting, a formula can refer to propositions which extend the alphabet AP of the model K. Then, the path quantification ranges over all the traces on the augmented alphabet whose projections over AP correspond to the execution traces of K. Within this affected generalization, KLTL can be effectively expressed in HyperLTL [6]. The logic HyperCTL* also generalizes the temporal logic secLTL, introduced in [9]. Other logics for hyperproperties were introduced in [19] but no general approach to verifying such logics exists.

Contribution. Our first contribution in this paper is the comparison of the expressive power of hyper temporal logics and epistemic temporal logics. We establish by formal non-trivial arguments that HyperCTL* and KCTL* are expressively incomparable.

As a second contribution, we unify HyperCTL* and KCTL* by extending HyperCTL* with new logical features which provide very natural modeling facilities. The proposed extension is based on two important observations: first, HyperCTL* has no explicit mechanism to refer to the past which would be useful to relate histories of different executions (paths). This ability is partially supported in KCTL* by means of observational equivalences between path prefixes; however, such equivalences are not expressed in the logic itself but are given as separate input parameters in the model specification. On the other hand, it is well-known that temporal logics which combine both past and future temporal modalities make specifications easier to write and more natural. In particular, the *linear past* setting, where the history of the current situation increases with time and is never forgotten, especially suits the specification of dynamic behaviors. A relevant example is given by the logic CTL$^*_{lp}$, a well-known equi-expressive linear past extension of CTL* [15] obtained by adding past temporal modalities and where path quantification is 'memoryful': it ranges over paths that start at the root of the computation tree and visit the current node. The second observation is that HyperCTL* has no explicit mechanism to select, at a given non-initial instant, paths which do not visit the current node. This is clearly a strong limitation for expressing general information-flow requirements.

We remove the above two limitations of HyperCTL* by introducing both linear past modalities and the *general hyper quantifier*, where path quantification ranges over all the paths that start at the root of the computation tree. These new features yield a novel logic that we call HyperCTL$^*_{lp}$. In fact, as we for-

mally establish, the only addition of general path quantification to $\mathsf{HyperCTL}^*$ makes the resulting logic already more expressive than $\mathsf{HyperCTL}^*$. However, it remains open whether both linear past and general quantification are necessary to capture all the KCTL^* definable properties. Like for the logics KCTL^* and $\mathsf{HyperCTL}^*$, the finite-state model-checking problem for $\mathsf{HyperCTL}^*_{lp}$ is non-elementarily decidable, and we provide the exact complexity in terms of a variant of the standard alternation depth of path quantifiers. For this, we settle complexity issues for satisfiability of full Quantified Propositional Temporal Logic (QPTL) [23]. The optimal upper bounds for full QPTL are obtained by a sophisticated generalization of the standard automata-theoretic approach for QPTL in prenex normal form [23], which exploits a subclass of parity two-way alternating word automata. Our results also improve in a meaningful way the upper bounds provided in [6] for model-checking of $\mathsf{HyperCTL}^*$. An extended version of this paper with all the proofs can be found in [4].

2 Preliminaries

Let $\mathbb{N}$ be the set of natural numbers and for all $i, j \in \mathbb{N}$, let $[i, j] := \{h \in \mathbb{N} \mid i \leq h \leq j\}$. We fix a *finite* set AP of atomic propositions. A *trace* is a finite or infinite word over 2^{AP}. For a word w over some alphabet, $|w|$ is the length of w ($|w| = \infty$ if w is infinite), and for each $0 \leq i < |w|$, $w(i)$ is the i^{th} symbol of w. For a logic formalism $\mathcal{L}$ and an $\mathcal{L}$ formula φ, the size $|\varphi|$ of φ is the number of subformulas of φ.

Structures and tree structures. A *Kripke structure* (*over* AP) is a tuple $K = \langle S, s_0, E, V\rangle$, where S is a set of states, $s_0 \in S$ is the initial state, $E \subseteq S \times S$ is a transition relation such that for each $s \in S$, $(s, t) \in E$ for some $t \in S$, and $V : S \to 2^{\mathsf{AP}}$ is an AP*-valuation* assigning to each state s the set of propositions in AP which hold at s. A *path* $\pi = t_0, t_1, \ldots$ of K is an infinite word over S such that for all $i \geq 0$, $(t_i, t_{i+1}) \in E$. For each $i \geq 0$, $\pi[0, i]$ denotes the prefix of π leading to the i^{th} state and $\pi[i, \infty]$ the suffix of π from the i^{th} state. A finite path of K is a prefix of some path of K. An *initial path* of K is a path starting from the initial state. For a (finite) path $\pi = t_0, t_1, \ldots$, the *trace* $V(\pi)$ *of* π is $V(t_0), V(t_1), \ldots$. We say that $K = \langle S, s_0, E, V\rangle$ is a *tree structure* if S is a prefix-closed subset of $\mathbb{N}^*$, $s_0 = \varepsilon$ (the root of K), and $(\tau, \tau') \in E \Rightarrow \tau' = \tau \cdot i$ for some $i \in \mathbb{N}$. States of a tree structure are also called *nodes*. For a Kripke structure K, $Unw(K)$ is the tree structure obtained by unwinding K from the initial state. A *tree structure* is *regular* if it is the unwinding of some finite Kripke structure.

2.1 Temporal logics with knowledge modalities

We recall the *non-regular* extensions, denoted by KCTL^* and KLTL, of standard CTL^* and LTL obtained by adding the knowledge modalities of epistemic logic under the *synchronous* perfect recall semantics [14, 24, 22, 8]. Unlike the asynchronous setting, the synchronous setting can be considered time sensitive in the

sense that it can model an observer who knows that a transition has occurred even if the observation has not changed. We fix a finite set Agts of agents.

Formulas φ of KCTL^* over Agts and AP are defined as follows:

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathsf{X}\varphi \mid \varphi \mathsf{U} \varphi \mid \exists\varphi \mid \mathsf{K}_a\varphi$$

where $p \in \mathsf{AP}$, $a \in \mathsf{Agts}$, X and U are the "next" and "until" temporal modalities, $\exists$ is the CTL^* existential path quantifier, and K_a is the knowledge modality for agent a. We also use standard shorthands: $\forall\varphi := \neg\exists\neg\varphi$ ("universal path quantifier"), $\mathsf{F}\varphi := \top\mathsf{U}\varphi$ ("eventually") and its dual $\mathsf{G}\varphi := \neg\mathsf{F}\neg\varphi$ ("always"). A formula φ is a *sentence* if each temporal/knowledge modality is in the scope of a path quantifier. The logic KLTL is the LTL-like fragment of KCTL^* consisting of sentences of the form $\forall\varphi$, where φ does not contain any path quantifier.

The logic KCTL^* is interpreted over *extended* Kripke structures (K, Obs), i.e., Kripke structures K equipped with an *observation map* $Obs : \mathsf{Agts} \to 2^{\mathsf{AP}}$ associating to each agent $a \in \mathsf{Agts}$, the set $Obs(a)$ of propositions which are observable by agent a. For an agent a and a finite trace $w \in (2^{\mathsf{AP}})^*$, the a-observable part $Obs_a(w)$ of w is the trace of length $|w|$ such that $Obs_a(w)(i) = w(i) \cap Obs(a)$ for all $0 \leq i < |w|$. Two finite traces w and w' are *(synchronously) Obs_a-equivalent* if $Obs_a(w) = Obs_a(w')$ (note that $|w| = |w'|$). Intuitively, an agent a does not distinguish prefixes of paths whose traces are Obs_a-equivalent.

For a KCTL^* formula φ, an extended Kripke structure $\Lambda = (K, Obs)$, an *initial* path π of K, and a position i along π, the satisfaction relation $\pi, i \models_\Lambda \varphi$ for KCTL^* is defined as follows (we omit the clauses for the Boolean connectives):

$$\begin{array}{ll}
\pi, i \models_\Lambda p & \Leftrightarrow p \in V(\pi(i)) \\
\pi, i \models_\Lambda \mathsf{X}\varphi & \Leftrightarrow \pi, i+1 \models_\Lambda \varphi \\
\pi, i \models_\Lambda \varphi_1 \mathsf{U} \varphi_2 & \Leftrightarrow \text{for some } j \geq i : \pi, j \models_\Lambda \varphi_2 \text{ and } \pi, k \models_\Lambda \varphi_1 \text{ for all } i \leq k < j \\
\pi, i \models_\Lambda \exists\varphi & \Leftrightarrow \pi', i \models_\Lambda \varphi \text{ for some initial path } \pi' \text{ of } K \text{ s.t. } \pi'[0,i] = \pi[0,i] \\
\pi, i \models_\Lambda \mathsf{K}_a\varphi & \Leftrightarrow \text{for all initial paths } \pi' \text{ of } K \text{ such that} \\
 & \quad V(\pi[0,i]) \text{ and } V(\pi'[0,i]) \text{ are } Obs_a\text{-equivalent, } \pi', i \models_\Lambda \varphi
\end{array}$$

We say that (K, Obs) *satisfies* φ, denoted $(K, Obs) \models \varphi$, if there is an initial path π of K s.t. $\pi, 0 \models_{(K,Obs)} \varphi$. Note that if φ is a sentence, then the satisfaction relation $\pi, 0 \models_{(K,Obs)} \varphi$ is independent of π. One can easily show that KCTL^* is bisimulation invariant and, in particular, $(K, Obs) \models \varphi$ iff $(Unw(K), Obs) \models \varphi$.

Example 1. Let us consider the KLTL sentence $\varphi_p := \forall\mathsf{XF}\mathsf{K}_a\neg p$. For all observation maps Obs such that $Obs(a) = \emptyset$, $(K, Obs) \models \varphi_p$ means that there is some non-root level in the unwinding of K at which *no* node satisfies p. Property ϕ_p is a well-known non-regular context-free branching-time property (see e.g. [2]).

2.2 Hyper logics

In this section, we first recall the logics $\mathsf{HyperCTL}^*$ and $\mathsf{HyperLTL}$ [6] which are non-regular extensions of CTL^* and LTL with a restricted form of explicit first-order quantification over paths. Intuitively, path variables are used to express

linear-time properties simultaneously on multiple paths. Then, we introduce the novel logic $\mathsf{HyperCTL}^*_{lp}$, an extension of $\mathsf{HyperCTL}^*$ obtained by adding linear past and the general hyper path quantifier. In this logic, path quantification is 'memoryful', i.e., it ranges over paths that start at the root of the computation tree (the unwinding of the Kripke structure) and either visit the current node τ (*regular* path quantification), or visit a node τ' at the same level as τ (*non-regular* path quantification).

The logic HyperCTL* [6]. For a finite set VAR of *path variables*, the syntax of $\mathsf{HyperCTL}^*$ formulas φ over AP and VAR is defined as follows:

$$\varphi ::= \top \mid p[x] \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathsf{X}\varphi \mid \varphi \mathsf{U} \varphi \mid \exists x.\varphi$$

where $p \in \mathsf{AP}$, $x \in \mathsf{VAR}$, and $\exists x$ is the *hyper* existential path quantifier for variable x. Informally, formula $\exists x.\varphi$ requires that there is an initial path π such that φ holds when x is mapped to π, and $p[x]$ asserts that p holds at the current position of the path assigned to x. The hyper universal quantifier $\forall x$ is defined as: $\forall x.\varphi := \neg\exists x.\neg\varphi$. A $\mathsf{HyperCTL}^*$ formula φ is a *sentence* if each temporal modality occurs in the scope of a path quantifier and for each atomic formula $p[x]$, x is bound by a path quantifier. The logic $\mathsf{HyperLTL}$ is the fragment of $\mathsf{HyperCTL}^*$ consisting of formulas in prenex form, i.e., of the form $Q_1 x_1 \ldots . Q_n x_n . \varphi$, where $Q_1, \ldots, Q_n \in \{\exists, \forall\}$ and φ does not contain any path quantifier.

We give a semantics for $\mathsf{HyperCTL}^*$ that is equivalent to the one in [6] but more suitable for a linear-past generalization. $\mathsf{HyperCTL}^*$ formulas φ are interpreted over Kripke structures $K = \langle S, s_0, E, V\rangle$ equipped with a *path assignment* $\Pi : \mathsf{VAR} \to S^\omega$ associating to each variable $x \in \mathsf{VAR}$ an *initial path* of K, a variable $y \in \mathsf{VAR}$, and a position $i \geq 0$. Intuitively, $\Pi(y)$ is the current path and i is the current position along the paths in Π. The satisfaction relation $\Pi, y, i \models_K \varphi$ is defined as follows (we omit the clauses for the Boolean connectives):

$$\begin{aligned}
\Pi, y, i \models_K p[x] \quad &\Leftrightarrow p \in V(\Pi(x)(i)) \\
\Pi, y, i \models_K \mathsf{X}\varphi \quad &\Leftrightarrow \Pi, y, i+1 \models_K \varphi \\
\Pi, y, i \models_K \varphi_1 \mathsf{U} \varphi_2 \quad &\Leftrightarrow \text{for some } j \geq i : \Pi, y, j \models_K \varphi_2 \text{ and} \\
&\qquad \Pi, y, k \models_K \varphi_1 \text{ for all } i \leq k < j \\
\Pi, y, i \models_K \exists x.\varphi \quad &\Leftrightarrow \text{for some initial path } \pi \text{ of } K \text{ such that } \pi[0,i] = \Pi(y)[0,i], \\
&\qquad \Pi[x \leftarrow \pi], x, i \models \varphi
\end{aligned}$$

where $\Pi[x \leftarrow \pi](x) = \pi$ and $\Pi[x \leftarrow \pi](y) = \Pi(y)$ for all $y \neq x$. We say that K *satisfies* φ, written $K \models \varphi$, if there is a path assignment Π of K and $y \in \mathsf{VAR}$ such that $\Pi, y, 0 \models_K \varphi$. If φ is a *sentence*, then the satisfaction relation $\Pi, y, 0 \models_K \varphi$ is independent of y and Π.

Example 2. As an example of a formula expressing a non-regular requirement, we consider the $\mathsf{HyperLTL}$ sentence $\exists x.\exists y.\ p[x]\ \mathsf{U}\ \Big((p[x] \wedge \neg p[y]) \wedge \mathsf{XG}(p[x] \leftrightarrow p[y])\Big)$ which asserts that there are two distinct initial paths π and π' and $\ell > 0$ such that p always holds along the prefix $\pi[0,\ell]$, p does not hold at position ℓ of π', and the valuations of p along π and π' coincide for all positions $j > \ell$.

The novel logic $\mathsf{HyperCTL}^*_{lp}$. $\mathsf{HyperCTL}^*_{lp}$ formulas φ are defined as follows:

$$\varphi ::= \top \mid p[x] \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathsf{X}\varphi \mid \mathsf{X}^-\varphi \mid \varphi\mathsf{U}\varphi \mid \varphi\mathsf{U}^-\varphi \mid \exists x.\varphi \mid \exists^G x.\varphi$$

where X^- and U^- are the past-time counterparts of the temporal modalities X and U, respectively, and $\exists^G x$ is the *general* (hyper) existential quantifier for variable x. We also use some shorthands: $\forall^G x.\,\varphi := \neg\exists^G x.\,\neg\varphi$ ("general universal path quantifier"), $\mathsf{F}^-\varphi := \top\mathsf{U}^-\varphi$ ("sometime in the past") and its dual $\mathsf{G}^-\varphi := \neg\mathsf{F}^-\neg\varphi$ ("always in the past"). The notion of sentence is defined as for $\mathsf{HyperCTL}^*$. The semantics of the modalities X^-, U^-, and $\exists^G x$ is as follows.

$$\begin{array}{ll}
\Pi, y, i \models_K \mathsf{X}^-\varphi & \Leftrightarrow i > 0 \text{ and } \Pi, y, i-1 \models_K \varphi \\
\Pi, y, i \models_K \varphi_1\mathsf{U}^-\varphi_2 & \Leftrightarrow \text{for some } j \leq i : \Pi, y, j \models_K \varphi_2 \text{ and} \\
 & \qquad \Pi, y, k \models_K \varphi_1 \text{ for all } j < k \leq i \\
\Pi, y, i \models_K \exists^G x.\varphi & \Leftrightarrow \text{for some initial path } \pi \text{ of } K,\ \Pi[x \leftarrow \pi], x, i \models \varphi
\end{array}$$

Thus, general hyper quantification range over all the initial paths (not only the ones which visit the current node). The satisfaction relation $K \models \varphi$ is defined as for $\mathsf{HyperCTL}^*$. Note that while the one-variable fragment of $\mathsf{HyperCTL}^*$ corresponds to standard CTL^*, the $\exists^G$-free one-variable fragment of $\mathsf{HyperCTL}^*_{lp}$ corresponds to the well-known equi-expressive linear past memoryful extension CTL^*_{lp} of CTL^* [15]. The model-checking problem for $\mathsf{HyperCTL}^*_{lp}$ is checking given a *finite* Kripke structure K and a $\mathsf{HyperCTL}^*_{lp}$ sentence φ, whether $K \models \varphi$. It is plain to see that $\mathsf{HyperCTL}^*_{lp}$ is bisimulation invariant and, in particular, $K \models \varphi$ iff $\mathit{Unw}(K) \models \varphi$.

We consider now two relevant examples from the literature which demonstrate the expressive power of $\mathsf{HyperCTL}^*_{lp}$. Both examples rely on the ability to express observational equivalence in the logic. We fix an observation map Obs. For an agent $a \in \mathsf{Agts}$ and two paths variables x and y in VAR, define $\psi(a, x, y) := \mathsf{G}^-(\bigwedge_{p \in \mathit{Obs}(a)} p[x] \leftrightarrow p[y])$

The first example shows that the logic can express *distributed knowledge*, a notion extensively investigated in [11]. It is crucial for information-flow security requirements as it allows to reason about adversaries who can communicate to share their knowledge: a group of agents $A \subseteq \mathsf{Agts}$ has distributed knowledge of φ, which we will denote by $\mathsf{D}_A\varphi$, if the combined knowledge of the members of A implies φ. It is well known that the modality D_A cannot be expressed by means of modalities K_a [11]. Also, since $\mathsf{HyperCTL}^*$ cannot express the modality K_a (see Section 3.2) and K_a is $\mathsf{D}_{\{a\}}$, it cannot express either D_A. However, D_A is expressible in $\mathsf{HyperCTL}^*_{lp}$. Given a $\mathsf{HyperCTL}^*_{lp}$ formula φ, we have: $\mathsf{D}_A\varphi \equiv \forall^G y.\,[(\bigwedge_{a \in A} \psi(a, x, y)) \rightarrow \varphi]$. Observe that both distinctive features of $\mathsf{HyperCTL}^*_{lp}$ are used here: the linear past modalities to capture observational equivalence, and the general hyper quantifier to range over all the initial paths.

The second example, inspired by [1], is an opacity requirement that we conjecture can be expressed neither in $\mathsf{HyperCTL}^*$ nor in KCTL^*. Assume that agent a can observe the low-security (Boolean) variables p (i.e., $p \in \mathit{Obs}(a)$), but not the high-security variables q (i.e., $q \notin \mathit{Obs}(a)$). Consider the case of a secret

represented by the value `true` of a high variable q_s. Then, the requirement $\forall x.\mathsf{G}(q_s \rightarrow \forall^G y.\psi(a,x,y))$ says that whenever q_s holds at some node in the computation tree, all the nodes at the same level have the same valuations of low variables. Hence, the observer a cannot infer that the secret has been revealed. Here again, both the linear past and the general hyper quantifier are required.

3 Expressiveness issues

In this section, we establish that $\mathsf{HyperCTL}^*$ and KCTL^* are expressively incomparable, and $\mathsf{HyperCTL}^*_{lp}$ is more expressive than both $\mathsf{HyperCTL}^*$ and KCTL^*.

Let $\mathcal{L}$ be a logic interpreted over Kripke structures, $\mathcal{L}'$ be a logic interpreted over *extended* Kripke structures, and C be a class of Kripke structures. For a sentence φ of $\mathcal{L}$, a sentence φ' of $\mathcal{L}'$, and an observation map *Obs*, φ and φ' *are equivalent w.r.t. C and Obs*, written $\varphi \equiv_{C,Obs} \varphi'$ if for all Kripke structures $K \in C$, $K \models \varphi$ iff $(K, Obs) \models \varphi'$. $\mathcal{L}'$ is *at least as expressive as* $\mathcal{L}$ w.r.t. C, written $\mathcal{L} \leq_C \mathcal{L}'$, if for every sentence φ of $\mathcal{L}$, there is an observation map *Obs* and a sentence φ' of $\mathcal{L}'$ such that $\varphi \equiv_{C,Obs} \varphi'$. Conversely, $\mathcal{L}$ is *at least as expressive as* $\mathcal{L}'$ w.r.t. the class C, written $\mathcal{L}' \leq_C \mathcal{L}$, if for every sentence φ' of $\mathcal{L}'$ and for every observation map *Obs*, there is a sentence φ of $\mathcal{L}$ such that $\varphi \equiv_{C,Obs} \varphi'$. Note the obvious asymmetry in the above two definitions due to the fact that for evaluating a sentence in $\mathcal{L}'$, we need to fix an observation map. If $\mathcal{L} \not\leq_C \mathcal{L}'$ and $\mathcal{L}' \not\leq_C \mathcal{L}$, then $\mathcal{L}$ and $\mathcal{L}'$ are *expressively incomparable w.r.t. C*. We denote by *fin* the class of finite Kripke structures.

3.1 HyperCTL* is not subsumed by KCTL*

In this section, we show that $\mathsf{HyperCTL}^*$ and its fragment $\mathsf{HyperLTL}$ are not subsumed by KCTL^* even if we restrict ourselves to *finite* Kripke structures.

Theorem 1. *HyperLTL* $\not\leq_{fin}$ *KCTL**.

The main intuition for Theorem 1 is that unlike $\mathsf{HyperLTL}$, KCTL^* does not allow to relate two initial paths at an unbounded number of positions. Thus, for example, there is no mechanism in KCTL^* to select two distinct paths π and π' such that the evaluations of a given LTL formula along π and π' coincide at every position. Formally, in order to prove Theorem 1, we use the $\mathsf{HyperLTL}$ sentence of Example 2 given by $\varphi_p := \exists x.\exists y.\ p[x]\ \mathsf{U}\ \Big((p[x] \wedge \neg p[y]) \wedge \mathsf{XG}(p[x] \leftrightarrow p[y])\Big)$.

We exhibit two families of *regular* tree structures $(K_n)_{n>1}$ and $(M_n)_{n>1}$ over $2^{\{p\}}$ such that: (i) for all $n > 1$, φ_p distinguishes between K_n and M_n,[4] and (ii) for every KCTL^* sentence ψ, there is $n > 1$ s.t. ψ does *not* distinguish between (K_n, Obs) and (M_n, Obs) for all observation maps *Obs*. Hence, Theorem 1 follows.

In the following, we fix $n > 1$. The regular tree structure K_n is illustrated in Fig. 1, where $\ell_n > 1$. Note that the root has label $\{p\}$ and $2n + 1$ successors

[4] i.e., φ_p evaluates to true on one strucutre and to false on the other one

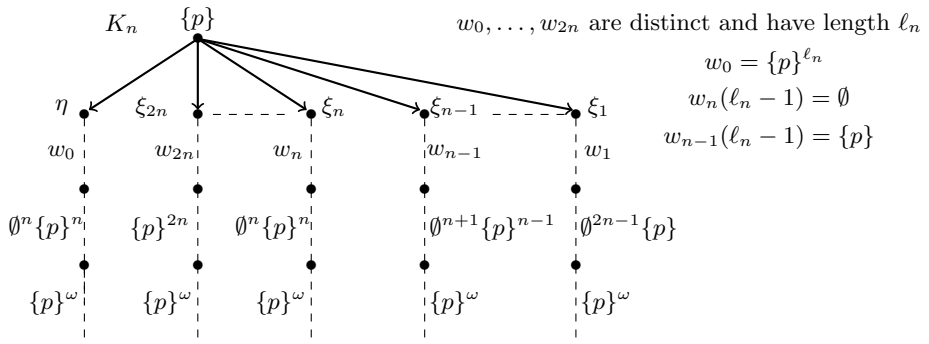

Fig. 1. The regular tree structure K_n for the witness HyperLTL formula φ_p

$\eta, \xi_1, \ldots, \xi_{2n}$, and there is a *unique* initial path visiting η (resp., ξ_k with $k \in [1, 2n]$). We denote this path by $\pi(\eta)$ (resp., $\pi(\xi_k)$). The tree structure M_n is obtained from K_n by replacing the label $\{p\}$ of node $\pi(\xi_n)(\ell_n + 1 + n)$ with $\emptyset$. Note that in M_n, the traces of $\pi(\xi_n)[\ell_n + 1, \infty]$ and $\pi(\xi_{n-1})[\ell_n + 1, \infty]$ coincide.

Proposition 1. *$K_n \models \varphi_p$ and $M_n \not\models \varphi_p$.*

Proof. In the structure K_n, the trace of the finite path $\pi(\eta)[0, \ell_n]$ is $\{p\}^{\ell_n+1}$, the label of $\pi(\xi_n)$ at position ℓ_n is $\emptyset$, and the traces of $\pi(\eta)[\ell_n + 1, \infty]$ and $\pi(\xi_n)[\ell_n + 1, \infty]$ coincide, which make $\pi(\eta)$ and $\pi(\xi_n)$ good candidates to fulfill φ_p. Hence, $K_n \models \varphi_p$. It remains to show that $M_n \not\models \varphi_p$.
By construction, for all distinct initial paths π and π' and $\ell \in [0, \ell_n]$, the traces of $\pi[\ell, \infty]$ and $\pi'[\ell, \infty]$ in M_n are distinct (recall that $\pi(\xi_n)(\ell_n)$ and $\pi(\xi_{n-1})(\ell_n)$ have distinct labels). Moreover, $\pi(\eta)$ is the unique initial path of M_n where p holds at every position in $[0, \ell_n]$. Thus, since $\pi(\eta)(\ell_n + 1)$ has label $\emptyset$ and there is no distinct initial path π'' of M_n such that the traces of $\pi(\eta)[\ell_n + 1, \infty]$ and $\pi''[\ell_n + 1, \infty]$ coincide, by construction of φ_p, $M_n \not\models \varphi_p$. □

A KCTL* formula ψ is *balanced* if for every until subformula $\psi_1 \mathsf{U} \psi_2$ of ψ, it holds that $|\psi_1| = |\psi_2|$. By using the atomic formula $\top$, it is trivial to convert a KCTL* sentence ψ into an *equivalent* balanced KCTL* sentence of size at most $|\psi|^2$. This observation together with Proposition 1, and the following non-trivial result provide a proof of Theorem 1.

Theorem 2. *Let ψ be a* balanced *KCTL* sentence such that $|\psi| < n$. Then, for all observation maps Obs, $(K_n, Obs) \models \psi \Leftrightarrow (M_n, Obs) \models \psi$.*

Proof. Given an observation map *Obs*, it suffices to show that for all initial paths π and positions $i \in [0, \ell_n]$, $\pi, i \models_{K_n, Obs} \psi$ iff $\pi, i \models_{M_n, Obs} \psi$. The key for obtaining this result is that since $|\psi| < n$, ψ cannot distinguish the nodes $\pi(\xi_n)(\ell_n + 1)$ and $\pi(\xi_{n-1})(\ell_n + 1)$ both in (K_n, Obs) and in (M_n, Obs). For M_n, this indistinguishability easily follows from the construction and is independent

of the size of ψ. For K_n, the indistinguishability is non-trivial and is formally proved by defining equivalence relations on the set of nodes at distance $d \in [\ell_n + 1, \ell_n + 2n]$ from the root, which are parameterized by a natural number $h \in [1, n]$, where h intuitively represents the size of the current balanced subformula of ψ in the recursive evaluation of ψ on K_n. □

3.2 KCTL* is not subsumed by HyperCTL*

In this section, we show that KCTL* and its fragment KLTL are not subsumed by HyperCTL* even with respect to finite Kripke structures. The intuitive insight is that unlike KLTL, HyperCTL* cannot express requirements which relate at some position an unbounded number of paths.

For $p \in \mathsf{AP}$, an observation map *Obs* is *p-blind* if for all agents a, $p \notin Obs(a)$.

Theorem 3. *KLTL* $\not\leq_{fin}$ *HyperCTL**.

As witness KLTL sentence for Theorem 3, we use the KLTL sentence of Example 1 given by $\varphi_p := \forall \mathsf{X} \mathsf{F} \mathsf{K}_a \neg p$. We exhibit two families of *regular* tree structures $(K_n)_{n>1}$ and $(M_n)_{n>1}$ over $2^{\{p\}}$ such that the following holds for all $n > 1$: (i) for each *p-blind* observation map *Obs*, φ_p distinguishes between (K_n, Obs) and (M_n, Obs), and (ii) no HyperCTL* formula ψ of size less than n distinguishes between K_n and M_n. Hence, Theorem 3 follows.

Fix $n > 1$. In order to define K_n and M_n, we need additional definitions.

An *n-block* is a word in $\{p\}\emptyset^*$ of length at least $n + 2$. Given finite words $w_1, \ldots, w_k$ over $2^{\{p\}}$ having the same length ℓ, the join $join(w_1, \ldots, w_k)$ of $w_1, \ldots, w_k$ is the word of length ℓ such that $join(w_1, \ldots, w_k)(i) = w_1(i) \cup \ldots \cup w_k(i)$ for all $i \in [0, \ell - 1]$. For a finite word w over $2^{\{p\}}$, the *dual* $\widetilde{w}$ of w is the word over $2^{\{p\}}$ of length $|w|$ such that for all $i \in [0, |w| - 1]$, $p \in \widetilde{w}(i)$ iff $p \notin w(i)$.

Given n finite words $w_1, \ldots, w_n$ over $2^{\{p\}}$ of the same length, the tuple $\langle w_1, \ldots, w_n \rangle$ *satisfies the n-fractal requirement* if for all $k \in [1, n]$,

$$join(w_1, \ldots, w_k) \text{ is of the form } bl_1^k \ldots bl_{m_k}^k \cdot \{p\}$$

where $bl_1^k \ldots bl_{m_k}^k$ are n-blocks. Moreover, $m_1 = n + 4$, and the following holds: if $k < n$, then w_{k+1} is obtained from $join(w_1, \ldots, w_k)$ by replacing the last symbol with $\emptyset$, and by replacing each n-block bl_i^k of $join(w_1, \ldots, w_k)$ by a sequence of $n + 4$ n-blocks preceded by a non-empty word in $\emptyset^*$ of length at least $n + 2$.

Remark 1. Assume that $\langle w_1, \ldots, w_n \rangle$ satisfies the n-fractal requirement and let ℓ be the common length of $w_1, \ldots, w_n$. Then, for all $i \in [0, \ell - 1]$, there is at most one $k \in [1, n]$ such that $p \in w_k(i)$. Moreover, $p \in w_1(0)$ and $p \in w_1(\ell - 1)$.

Definition 1 (The tree structures K_n and M_n). *K_n is illustrated in Fig. 2 where $\ell_n > 1$. The unique initial path visiting node η (resp., ξ_k with $k \in [1, n]$) is denoted by $\pi(\eta)$ (resp., $\pi(\xi_k)$).*

A main position *is a position in $[1, \ell_n]$. Let i_{alert} be the* third *(in increasing order) main position i along $\pi(\xi_1)$ such that the label of $\pi(\xi_1)(i)$ in K_n is $\{p\}$ (note that i_{alert} exists). Then, the regular tree structure M_n is obtained from K_n by replacing the label $\{p\}$ of $\pi(\xi_1)$ at position i_{alert} with $\emptyset$.*

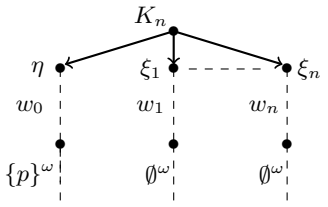

Fig. 2. The regular tree structure K_n for the witness KLTL formula $\varphi_p := \forall \mathsf{X} \mathsf{F} \mathsf{K}_a \neg p$

By construction, in the tree structure K_n, for each non-root level, there is a node where p holds and a node where p does not hold. Hence, $(K_n, Obs) \not\models \varphi_p$. By Remark 1, for each main position i, there is at most one $k \in [1, n]$ such that the label of $\pi(\xi_k)(i)$ in K_n is $\{p\}$. If such a k exists, we say that i is a *main p-position* and ξ_k is the *type* of i. Now, for the level of M_n at distance i_{alert} from the root, p *uniformly* does not hold (i.e., there is no node of M_n at distance i_{alert} from the root where p holds). Thus, we obtain the following result.

Proposition 2. *For each p-blind observation map Obs,* $(K_n, Obs) \not\models \varphi_p$ *and* $(M_n, Obs) \models \varphi_p$.

Theorem 3 directly follows from Proposition 2 and the following result.

Theorem 4. *For all HyperCTL* sentences* ψ *with* $|\psi| < n$, $K_n \models \psi \Leftrightarrow M_n \models \psi$.

Proof. The main idea is that for a HyperCTL* sentence ψ of size less than n, in the recursive evaluation of ψ on the tree structure M_n, there will be $h_* \in [2, n]$ such that the initial path $\pi(\xi_{h_*})$ is not bound by the current path assignment. Then, the n-fractal requirement ensures that in M_n, the main p-position i_{alert} (which in M_n has label $\emptyset$ along $\pi(\xi_1)$) is indistinguishable from the main p-positions j of type ξ_{h_*} which are sufficiently 'near' to i_{alert} (such positions j have label $\emptyset$ along the initial paths $\pi(\xi_k)$ with $k \neq h*$). We formalize this intuition by defining equivalence relations on the set of main positions which are parameterized by h_* and a natural number $\mathfrak{m} \in [0, n]$ and reflect the fractal structure of the main p-position displacement. Since the number of main p-positions of type ξ_1 following i_{alert} is at least n, we then deduce that in all the positions i such that $i \leq i_F$, where i_F is the main p-position of type ξ_1 preceding i_{alert}, no HyperCTL* formula ψ can distinguish M_n and K_n with respect to path assignments such that $|\Pi| + |\psi| < n$, where $|\Pi|$ is the number of initial paths bound by Π. Hence, the result follows. □

3.3 HyperCTL$^*_{lp}$ unifies KCTL* and HyperCTL*

We show that KCTL* can be easily translated in linear time into the two-variable fragment of HyperCTL$^*_{lp}$. Intuitively, the knowledge modalities can be simulated by the general hyper path quantifiers combined with the temporal past modalities. Hence, we obtain the following result.

Theorem 5. *Given a KCTL* sentence ψ and an observation map Obs, one can construct in* linear time *a HyperCTL$^*_{lp}$ sentence φ with just two path variables such that for each Kripke structure K, $K \models \varphi \Leftrightarrow (K, Obs) \models \psi$.*

Note that the KCTL* sentence $\forall \mathsf{XFK}_a \neg p$ used to prove Theorem 3 is equivalent w.r.t. p-blind observation maps to the HyperCTL$^*_{lp}$ sentence $\forall x. \mathsf{XF}(\forall^G y. \neg p[y])$ which does not use past modalities. Thus, by Theorems 1, 3, and 5, we obtain:

Corollary 1. *HyperCTL$^*_{lp}$ is more expressive than both HyperCTL* and KCTL*. Moreover, the* future *fragment of HyperCTL$^*_{lp}$ (where past-time modalities are disallowed) is already more expressive than HyperCTL*.*

4 Model-checking against HyperCTL$^*_{lp}$

In this section, we address the model-checking problem for HyperCTL$^*_{lp}$. Similarly to the proof given in [6] for the less expressive logic HyperCTL*, we show that the above problem is non-elementarily decidable by linear-time reductions from/to satisfiability of *full* Quantified Propositional Temporal Logic (QPTL, for short) [23], which extends LTL with past (PLTL) by quantification over propositions. As main contribution of this section, we address complexity issues for the considered problem by providing optimal complexity bounds in terms of a parameter of the given HyperCTL$^*_{lp}$ formula, we call *strong alternation depth*. For this, we first provide similar optimal complexity bounds for satisfiability of QPTL. As a corollary of our results, we also obtain that for a relevant fragment of HyperCTL$^*_{lp}$, model-checking is EXPSPACE-complete. With regard to QPTL, well-known optimal complexity bounds, in terms of the alternation depth of existential and universal quantifiers, concern the fragment of QPTL in prenex form (quantifiers cannot occur in the scope of temporal modalities) [23]. QPTL formulas can be translated in polynomial time into equisatisfiable QPTL formulas in prenex form, but in this conversion, the nesting depth of temporal modalities in the original formula (in particular, the alternation depth between always and eventually modalities and the nesting depth of until modalities) lead to an equal increasing in the quantifier alternation depth of the resulting formula. We show that this can be avoided by *directly* applying a non-trivial automatic theoretic approach to unrestricted QPTL formulas. Our results also improve in a meaningful way the upper bounds provided in [6] for model-checking of HyperCTL*; indeed, in [6], differently from our approach, occurrences of temporal modalities count as additional alternations.

The logic QPTL [23]. QPTL formulas φ over AP are defined as follows:

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathsf{X}\varphi \mid \mathsf{X}^-\varphi \mid \varphi \mathsf{U} \varphi \mid \varphi \mathsf{U}^- \varphi \mid \exists p\,.\varphi$$

where $p \in \mathsf{AP}$. The *positive normal form* of a QPTL formula φ is obtained by pushing inward negations to propositional literals using De Morgan's laws and the duals R (release), R$^-$ (past release), and $\forall p$ (propositional universal quantifier) of U, U$^-$, and $\exists p$, respectively. A formula is (*pure*) *existential* if its positive normal has no universal quantifier. Analogous notions apply to HyperCTL$^*_{lp}$.

QPTL formulas are interpreted over (infinite) *pointed words* (w, i) over 2^{AP} consisting of an infinite word w over 2^{AP} and a position $i \geq 0$. The semantics of propositional quantification is as follows.

$$(w,i) \models \exists p.\varphi \;\Leftrightarrow\; \text{there is } w' \in (2^{\mathsf{AP}})^{\omega} \text{ such that } w =_{\mathsf{AP}\setminus\{p\}} w' \text{ and } (w',i) \models \varphi$$

where $w =_{\mathsf{AP}\setminus\{p\}} w'$ means that the projections of w and w' over $\mathsf{AP} \setminus \{p\}$ coincide. For a QPTL formula φ, let $\mathcal{L}_{\wp}(\varphi)$ be the set of pointed words satisfying φ, and $\mathcal{L}(\varphi)$ be the set $\{w \mid (w,0) \in \mathcal{L}_{\wp}(\varphi)\}$; φ is satisfiable if $\mathcal{L}(\varphi) \neq \emptyset$.

Optimal bounds for QPTL satisfiability. First, we give a generalization of the standard notion of alternation depth between existential and universal quantifiers, we call *strong alternation depth*. This notion takes into account also the occurrence of temporal modalities between quantifier occurrences, but the nesting depth of temporal modalities is not considered (it is collapsed to one).

Definition 2. *Let* $\mathcal{O} = \{\exists, \forall, \mathsf{U}, \mathsf{U}^{-}, \mathsf{R}, \mathsf{R}^{-}, \mathsf{G}, \mathsf{G}^{-}, \mathsf{F}, \mathsf{F}^{-}\}$. *First, we define the* strong alternation length $\ell(\chi)$ *of finite sequences* $\chi \in \mathcal{O}^*$: $\ell(\varepsilon) = 0$, $\ell(O) = 1$ *for all* $O \in \mathcal{O}$, *and*

$$\ell(OO'\chi) = \begin{cases} \ell(O'\chi) & \text{if } O' \in \mathcal{O} \setminus \{\exists, \forall\} \\ \ell(O'\chi) & \text{if either } O, O' \in \{\exists, \mathsf{F}, \mathsf{F}^{-}\} \text{ or } O, O' \in \{\forall, \mathsf{G}, \mathsf{G}^{-}\} \\ 1 + \ell(O'\chi) & \text{otherwise} \end{cases}$$

[5] *Then, the* strong alternation depth $sad(\varphi)$ *of a QPTL formula* φ *is the maximum over the strong alternation lengths* $\ell(\chi)$, *where* χ *is the sequence of modalities in* $\mathcal{O}$ *along a path in the tree encoding of the positive normal form of* φ. *The* strong alternation depth $sad(\varphi)$ *of a* $\mathsf{HyperCTL}^*_{lp}$ *formula* φ *is defined similarly but we replace quantification over propositions with quantification over path variables. For a QPTL (resp.,* $\mathsf{HyperCTL}^*_{lp}$*) formula* φ, *if there is a subformula* ψ *of the positive normal form of* φ *whose root operator is a universal quantifier and such that* $sad(\psi) = sad(\varphi)$, *then we say that* φ *is a* first-level universal *formula; otherwise, we say that* φ *is a* first-level existential *formula.*

Note that for a QPTL formula φ in prenex form, the strong alternation depth corresponds to the alternation depth of existential and universal quantifiers plus one. For all $n, h \in \mathbb{N}$, $\mathsf{Tower}(h, n)$ denotes a tower of exponentials of height h and argument n: $\mathsf{Tower}(0, n) = n$ and $\mathsf{Tower}(h+1, n) = 2^{\mathsf{Tower}(h,n)}$. We establish the following result, where h-EXPSPACE is the class of languages decided by deterministic Turing machines bounded in space by functions of n in $O(\mathsf{Tower}(h, n^c))$ for some constant $c \geq 1$.

Theorem 6. *For all* $h \geq 1$, *satisfiability of QPTL formulas* φ *with strong alternation depth at most* h *is* h-EXPSPACE*-complete, and* $(h-1)$-EXPSPACE*-complete in case* φ *is* first-level existential *or* pure existential *(even if we only allow temporal modalities in* $\{\mathsf{X}, \mathsf{X}^{-}, \mathsf{F}, \mathsf{F}^{-}, \mathsf{G}, \mathsf{G}^{-}\}$*).*

[5] For example, $\ell(\exists \mathsf{G} \mathsf{U} \exists \mathsf{U}) = \ell(\mathsf{U} \exists \mathsf{U}) = 2$.

Here, we illustrate the upper bounds of Theorem 6. In the automata-theoretic approach for QPTL formulas φ in prenex form, first, one converts the quantifier-free part ψ of φ into an equivalent Büchi nondeterministic automaton (Büchi NWA) accepting $\mathcal{L}(\psi)$. Then, by using the closure of Büchi NWA definable languages under projection and complementation, one obtains a Büchi NWA accepting $\mathcal{L}(\varphi)$. This approach would not work for arbitrary QPTL formulas φ, where quantifiers can occur in the scope of temporal modalities. In this case, for a subformula φ' of φ, we need to keep track of the full set $\mathcal{L}_{\wp}(\varphi')$ of pointed words satisfying φ, and not simply $\mathcal{L}(\varphi')$. Thus, we resort to *two-way* automata $\mathcal{A}$ accepting languages $\mathcal{L}_{\wp}(\mathcal{A})$ of *pointed words*. In particular, the proposed approach is based on a compositional translation of QPTL formulas into a simple two-way extension of Büchi NWA, which we call Büchi SNWA. Essentially, given an input pointed word (w, i), a Büchi SNWA splits in two copies: the first one moves forward along the suffix $w[i, \infty]$ and the second one moves backward along the prefix $w[0, i]$.

Moreover, at each step of the translation into Büchi SNWA, we use as an intermediate formalism a two-way extension of the class of (one-way) *hesitant alternating automata* (HAA, for short) over infinite words introduced in [17]. Like one-way HAA, the set of states Q of a two-way HAA is partitioned into a set of components $Q_1, \ldots, Q_n$ such that moves from states in Q_i lead to states in components Q_j so that $j \leq i$. Moreover, each component is classified as either *past*, or *Büchi*, or *coBüchi*: in a past (resp., Büchi/coBüchi) component Q_i, the unique allowed moves from Q_i to Q_i itself are backward (resp., forward). These syntactical requirements ensure that in a run over a pointed word, every infinite path π of the run gets trapped in some Büchi or coBüchi component, and the path π eventually use only forward moves. Moreover, the acceptance condition of a two-way HAA encodes a particular kind of parity condition of index 2: a Büchi/coBüchi component Q_i has an associated subset $F_i \subseteq Q_i$ of accepting states. Then, a run is accepting if for every infinite path π, denoting with Q_i the Büchi/coBüchi component in which π gets trapped, π satisfies the Büchi/coBüchi acceptance condition associated with Q_i. For two-way HAA $\mathcal{A}$, we establish two crucial results. First, the *dual automaton* $\widetilde{\mathcal{A}}$ obtained from $\mathcal{A}$ by dualizing the transition function, and by converting a Büchi (resp., coBüchi) component into a coBüchi (resp., Büchi) component is still a two-way HAA. Thus, by standard arguments (see e.g. [25]), automaton $\widetilde{\mathcal{A}}$ accepts the complement of $\mathcal{L}_{\wp}(\mathcal{A})$. Second, by using the notion of odd ranking function for standard coBüchi alternating automata [16] (which allows to convert a coBüchi acceptance condition into a Büchi-like acceptance condition) and a non-trivial generalization of the Miyano-Hayashi construction [20], we show that two-way HAA can be converted in singly exponential time into equivalent Büchi SNWA.

Theorem 7. *Given a two-way HAA $\mathcal{A}$ with n states, the following holds:*

1. *the dual automaton $\widetilde{\mathcal{A}}$ of $\mathcal{A}$ is a two-way HAA accepting the complement of $\mathcal{L}_{\wp}(\mathcal{A})$;*
2. *one can build "on the fly" and in singly exponential time a Büchi SNWA accepting $\mathcal{L}_{\wp}(\mathcal{A})$ with $2^{O(n \cdot \log(n))}$ states.*

Finally, by using Theorem 7, we establish the following result from which the upper bounds of Theorem 6 directly follow (note that Büchi SNWA $\mathcal{A}$ can be trivially converted into Büchi NWA accepting the set of infinite words w such that $(w, 0) \in \mathcal{L}_{\wp}(\mathcal{A})$, and checking non-emptiness for Büchi NWA is in NLOGSPACE).

Theorem 8. *Let φ be a first-level existential (resp., first-level universal) QPTL formula and $h = sad(\varphi)$. Then, one can construct "on the fly" a Büchi SNWA $\mathcal{A}_\varphi$ accepting $\mathcal{L}_{\wp}(\varphi)$ in time $\mathsf{Tower}(h, O(|\varphi|))$ (resp., $\mathsf{Tower}(h+1, O(|\varphi|))$).*

Proof. By structural induction on the positive normal form φ_+ of φ. The relevant case is when the outermost operator of φ_+ is a temporal modality (the other cases easily follow from Theorem 7 and the closure of Büchi SNWA definable pointed languages under union, intersection, and projection). This case is handled by first building a two-way HAA $\mathcal{A}$ accepting $\mathcal{L}_{\wp}(\varphi)$ and then by applying Theorem 7(2). The construction of $\mathcal{A}$ is obtained by a generalization of the standard linear-time translation of LTL formulas into Büchi alternating automata which exploits the (inductively built) Büchi SNWA associated with the maximal quantified subformulas of φ_+. □

Optimal bounds for model-checking of HyperCTL$^*_{lp}$. By establishing linear-time reductions from/to satisfiability of QPTL and by exploiting Theorem 6, we provide optimal bounds on the complexity of model-checking for HyperCTL$^*_{lp}$ in terms of the strong alternation depth of the formula. In particular, the linear-time reduction to satisfiability of QPTL generalizes the one given in [6] for the model checking of HyperCTL*.

Theorem 9. *For all $h \geq 1$ and HyperCTL$^*_{lp}$ sentences φ with strong alternation depth at most h, model-checking against φ is h-EXPSPACE-complete, and $(h-1)$-EXPSPACE-complete in case φ is* first-level existential *or* pure existential *(even if we allow only temporal modalities in $\{X, X^-, F, F^-, G, G^-\}$).*

By Theorem 9, for the first-level existential fragment $\mathcal{F}$ of HyperCTL$^*_{lp}$ where the strong alternation depth is at most 2, model-checking is EXPSPACE-complete. Notice that the HyperCTL* fragment $\mathcal{F}'$ of $\mathcal{F}$ can express important classes of information-flow requirements as illustrated in [6], and that the model-checking algorithm in [6] applied to $\mathcal{F}'$ leads to a non-elementary upper bound.

5 Discussion

We plan to extend this work in many directions. First, we intend to identify tractable fragments of HyperCTL$^*_{lp}$ and to investigate their synthesis problem; note that satisfiability of HyperCTL* is already undecidable [6]. Second, we should extend the framework to deal with asynchronicity, as information flows are relevant for security in many asynchronous frameworks, such as distributed systems or cryptographic protocols. In the same line, we would like to investigate the possibility of extending the verification of information-flow requirements to relevant classes of infinite-state systems such as the class of pushdown systems, a model extensively investigated in software verification.

References

1. R. Alur, P. Černỳ, and S. Chaudhuri. Model checking on trees with path equivalences. In *Proc. 13th TACAS*, LNCS 4424, pages 664–678. Springer, 2007.
2. R. Alur, P. Cerný, and S. Zdancewic. Preserving secrecy under refinement. In *Proc. 33rd ICALP*, LNCS 4052, pages 107–118. Springer, 2006.
3. M. Balliu, M. Dam, and G. L. Guernic. Epistemic temporal logic for information flow security. In *Proc. PLAS*, page 6. ACM, 2011.
4. L. Bozzelli, B. Maubert, and S. Pinchinat. Unifying hyper and epistemic temporal logic. *CoRR*, abs/1409.2711, 2014.
5. J. Bryans, M. Koutny, L. Mazaré, and P. Ryan. Opacity generalised to transition systems. *Int. J. Inf. Sec.*, 7(6):421–435, 2008.
6. M. Clarkson, B. Finkbeiner, M. Koleini, K. Micinski, M. Rabe, and C. Sánchez. Temporal logics for hyperproperties. In *Proc. 3rd POST*, LNCS 8414, pages 265–284. Springer, 2014.
7. M. Clarkson and F. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.
8. C. Dima. Revisiting satisfiability and model-checking for CTLK with synchrony and perfect recall. In *Proc. 9th CLIMA*, LNCS 5405, pages 117–131. Springer, 2008.
9. R. Dimitrova, B. Finkbeiner, M. Kovács, M. Rabe, and H. Seidl. Model checking information flow in reactive systems. In *Proc. 13th VMCAI*, LNCS 7148, pages 169–185. Springer, 2012.
10. E. Emerson and J. Halpern. "Sometimes" and "Not Never" revisited: on branching versus linear time temporal logic. *J. ACM*, 33(1):151–178, 1986.
11. R. Fagin, J. Halpern, and M. Vardi. *Reasoning about knowledge*, volume 4. MIT press Cambridge, 1995.
12. J. Goguen and J. Meseguer. Security policies and security models. In *IEEE Symposium on Security and privacy*, volume 12, 1982.
13. J. Halpern and K. O'Neill. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.*, 12(1), 2008.
14. J. Halpern, R. van der Meyden, and M. Vardi. Complete Axiomatizations for Reasoning about Knowledge and Time. *SIAM J. Comput.*, 33(3):674–703, 2004.
15. O. Kupferman, A. Pnueli, and M. Vardi. Once and for all. *J. Comput. Syst. Sci.*, 78(3):981–996, 2012.
16. O. Kupferman and M. Vardi. Weak alternating automata are not that weak. *ACM Transactions on Computational Logic*, 2(3):408–429, 2001.
17. O. Kupferman, M. Vardi, and P. Wolper. An Automata-Theoretic Approach to Branching-Time Model Checking. *J. ACM*, 47(2):312–360, 2000.
18. J. McLean. Proving noninterference and functional correctness using traces. *Journal of Computer Security*, 1(1):37–58, 1992.
19. D. Milushev and D. Clarke. Towards incrementalization of holistic hyperproperties. In *Proc. 1st POST*, LNCS 7215, pages 329–348. Springer, 2012.
20. S. Miyano and T. Hayashi. Alternating finite automata on ω-words. *Theoretical Computer Science*, 32:321–330, 1984.
21. A. Pnueli. The temporal logic of programs. In *Proc. 18th FOCS*, pages 46–57. IEEE Computer Society, 1977.
22. N. Shilov and N. Garanina. Model checking knowledge and fixpoints. In *Proc. FICS*, BRICS Notes Series, pages 25–39, 2002.
23. A. Sistla, M. Vardi, and P. Wolper. The complementation problem for Büchi automata with appplications to temporal logic. *Theoretical Computer Science*, 49:217–237, 1987.
24. R. van der Meyden and N. Shilov. Model checking knowledge and time in systems with perfect recall (extended abstract). In *Proc. 19th FSTTCS*, LNCS 1738, pages 432–445. Springer, 1999.
25. W. Zielonka. Infinite games on finitely coloured graphs with applications to automata on infinite trees. *Theoretical Computer Science*, 200(1-2):135–183, 1998.