A Complete Proof System for HyperLTL

Naijun Zhan[1,2(✉)], Wen Tang[3], and Dimitar Guelev[4]

[1] School of Computer Science and Key Laboratory of High Confidence Software Technologies of Ministry of Education, Peking University, Beijing, China
njzhan@pku.edu.cn
[2] Zhongguancun Laboratory, Beijing, China
[3] Department of Philosophy, Peking University, Beijing, China
[4] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria

Abstract. HyperLTL extends Linear Temporal Logic (LTL) with explicit trace variables and quantification over traces, allowing formulas to relate multiple executions within a single specification. Consequently, HyperLTL has become an important specification formalism for hyperproperties, i.e., properties of *sets* of traces rather than individual traces. However, the satisfiability of HyperLTL is undecidable, so fully automatic reasoning cannot, in general, replace deductive methods to establish validity. Furthermore, HyperLTL restricts trace quantification to the outermost scope of formulas. In this paper, we study HyperLTL*, a generalization that removes this restriction by allowing trace quantifiers to occur under temporal operators. We present a Gentzen-style sequent calculus for HyperLTL* and establish completeness by means of suitable infinitary rules. We then derive sound finitary principles that are amenable to interactive theorem proving and can serve as a foundation for mechanized reasoning. We illustrate the use of the calculus on representative HyperLTL-style specifications that are difficult to discharge by existing automatic procedures. Finally, we analyze the expressiveness of HyperLTL* and discuss how the calculus can be combined with first-order reasoning infrastructure.

Keywords: HyperLTL · proof system · interactive theorem proving · first-order logic · satisfiability

1 Introduction

Hyperproperties [19] generalize the notion of trace properties [2] from sets of traces (paths) to sets of sets of traces. Requirements on computing systems that are hyperproperties but not trace properties include information flow security policies such as noninterference [36], observational determinism [50], sensitivity and robustness requirements in cyber-physical systems [49], and consistency conditions such as linearizability in concurrent data structures [13], and so on.

Formulas in classical temporal logics, such as Linear Temporal Logic (LTL) [44], Computation Tree Logics (CTL and CTL*) [17,26], and μ-calculus [41],

A. Biere et al. (Eds.): IJCAR 2026, LNAI 16688, pp. 377–395, 2026.
https://doi.org/10.1007/978-3-032-32589-1_23

characterize sets of traces or sets of Kripke models. However, expressing specific properties of sets of traces, such as epistemic properties, typically requires the addition of dedicated modalities to these logics. HyperLTL [18], due to Clarkson *et al.*, extends LTL by introducing trace variables and quantification over the trace domain. This mechanism makes it possible to express relational specifications by correlating the valuations of propositions across multiple traces. Hence, HyperLTL provides a powerful framework for expressing properties over sets of traces. Automatic verification techniques have been developed for HyperLTL, including model- and satisfiability-checking algorithms [27–29,33]. With these techniques, HyperLTL has become a predominant specification logic for hyperproperties and has been successfully applied to fundamental security policies, distributed protocols and coding theories [28,30].

The model-checking complexity of HyperLTL formulas over finite Kripke structures is non-elementary [18]; moreover, neither satisfiability [27] nor synthesis [29] is decidable for the full logic. This inherent complexity makes deductive methods particularly relevant: they provide a complementary reasoning mode when algorithmic procedures diverge or do not apply. In this paper, we consider HyperLTL*, which extends HyperLTL by removing the restriction on quantifiers not to appear in the scope of temporal operators. We propose a complete proof system for HyperLTL*, obtained by extending a Gentzen-style calculus with ω- and Coω-rules. This yields a proof-theoretic basis for interactive theorem proving for HyperLTL*, complementing automated verification techniques and enabling the formal derivation of specifications that remain beyond the reach of fully automatic methods.

Our proof system is presented in the Gentzen style, building upon the one for LTL [35] while incorporating modified temporal rules and extra trace quantifier rules. Additionally, more powerful induction rules, the ω-rule and Coω-rule, are required. This necessity arises because HyperLTL lacks the finite model property [34], rendering the finiteness-of-premise assumption in LTL's proof system [35] inadequate. Consequently, an induction axiom similar to that of LTL [35] is insufficient to guarantee the existence of witnesses for trace quantifiers. Indeed, it is well established that no finitary proof system for a non-compact logic can achieve strong completeness [45]. We provide rigorous proofs for both the soundness and the completeness of our proof system.

Furthermore, we show that HyperLTL* is more expressive than HyperLTL but still strictly subsumed by the first-order logic $FO[<, E]$. To showcase the utility of our proof system, we illustrate its application to formulas with multiple quantifier alternations, which are hard to handle by automatic techniques.

1.1 Related Work

We briefly review prior work on (i) specification formalisms for hyperproperties and (ii) reasoning and verification techniques for such formalisms.

Hyperlogics. Alur *et al.* observed that *opacity* is not expressible in the μ-calculus [4], despite the fact that the μ-calculus subsumes LTL, CTL*, dynamic logic, and

related modal formalisms. This illustrates a general phenomenon: many security and consistency requirements are not properties of a single execution, but rather constrain *sets* of executions (hyperproperties). To capture such requirements, a variety of hyperlogics has been developed, can be briefly summarized as follows:

1. *Encoding via model restrictions.* Structural assumptions on the model (e.g., symmetry) can make certain hyperproperties definable in standard logics; examples include observational determinism [6,39] and noninterference [7].
2. *Adding dedicated modalities.* Examples include path-equivalence modalities in branching-time logics [3], the hide modality H in SecLTL [24], and epistemic modalities [5].
3. *First-order and first-order inspired formalisms.* Monadic first-order logic with the equal-level predicate is studied in [34], and alternative quantifier disciplines are investigated in [8].
4. *Explicit trace/path quantification.* This line includes QLTL [47], HyperPDL-Δ [37], HyperATL* [10], HyperCTL* [18], and so on. In which HyperLTL is a prominent instance.

Further perspectives include team semantics for temporal logics [42,48]. Beyond the synchronous finite-state setting, the high complexity of reasoning about asynchronous systems has motivated dedicated logics [9,14,38]; similarly, quantitative and probabilistic variants have been considered [1,25,33]. A preliminary comparison of these formalisms in terms of expressiveness and algorithmic problems is given in [21].

From a proof-theoretic viewpoint, strong completeness for non-compact logics is typically obtained via infinitary inference principles; examples include intuitionistic temporal logic [15] and higher-order duration calculus [51,52]. However, these systems are Hilbert-style and do not target trace-quantifying temporal hyperlogics; to the best of our knowledge, a strongly complete Gentzen-style calculus in this setting has not previously been developed.

Verification of Hyperproperties. Inspired by the success of classical modal and temporal logics, most of the existing work on hyperlogics focus on automatic verification techniques such as model- and satisfiability-checking, synthesis, and monitoring. Model- and satisfiability-checking tools for HyperLTL were presented in [22,33] and [27,28,30], respectively. Synthesis tools were presented in [29]. Runtime monitoring tools of HyperLTL were reported in [31,32]. Recently, repairing programs w.r.t. HyperLTL was investigated in [11].

In general, the computational complexity of HyperLTL exceeds that of classical temporal logics [27]. It is well known that LTL model checking is PSPACE-COMPLETE [46]. In contrast, HyperLTL model checking over finite Kripke structures is nonelementary [33], and its satisfiability is not semi-decidable [34]. As a consequence, HyperLTL admits no finitary proof system that is strongly complete. The largest known decidable fragment of HyperLTL consists of formulas with quantifier prefix of the form $\exists^*\forall^*$ [21]; important information-flow policies such as general noninterference (GNI) and state opacity lie outside this fragment. This motivates interactive and semi-automated reasoning, for which

a proof system is a prerequisite. To the best of our knowledge, the only proof system available in the literature [20] handles only a fragment of HyperLTL and does not establish full proof-theoretic metatheory such as (strong) completeness. More recently, a set of co-induction proof rules for a fragment of HyperLTL of the type $\forall^*\exists^*\Box\psi$ is reported in [23], where ψ is an LTL formula. This motivates us to investigate this issue in this paper.

Organization. The rest of this paper is organized as follows: Sect. 2 defines the syntax and semantics of HyperLTL*, Sect. 3 presents a proof system in Gentzen style for HyperLTL*, while Sect. 4 proves the completeness of the proof system, Sect. 5 discusses the expressiveness of HyperLTL*, Sect. 6 presents a case study, and finally Sect. 7 draws a conclusion and discusses future work.

2 Syntax and Semantics of HyperLTL*

In this section, we define HyperLTL* by lifting the HyperLTL restriction that trace quantifiers cannot occur within the scope of temporal operators. The logic HyperLTL* has the same syntax as HyperCTL* [18]. However, HyperCTL* is interpreted over Kripke structures, HyperLTL* is interpreted over trace sets, as in HyperLTL.

Definition 1. *A HyperLTL* vocabulary consists of a countable set of trace variables $\mathbb{T}$, and a countable set of propositional letters $\mathbb{P}$. The syntax of HyperLTL* formulas is defined by the following BNF:*

$$\varphi ::= \top \mid a_\pi \mid \exists\pi\varphi \mid \neg\varphi \mid \varphi \wedge \varphi \mid \bigcirc\varphi \mid \varphi\mathcal{U}\varphi$$

where $a \in \mathbb{P}$ and $\pi \in \mathbb{T}$.

In Definition 1, $\bigcirc$ reads *next* and $\mathcal{U}$ reads *until*, as in LTL. The propositional constant $\bot$, the Boolean connectives $\vee$ and $\rightarrow$, the universal quantifier $\forall$, and the temporal operators $\mathcal{R}$, $\Diamond$, $\Box$, and $\mathcal{W}$ are treated as standard abbreviations: $\varphi\mathcal{R}\psi \triangleq \neg(\neg\varphi\mathcal{U}\neg\psi)$, $\Diamond\varphi \triangleq \top\mathcal{U}\varphi$, $\Box\varphi \triangleq \neg\Diamond\neg\varphi$, $\varphi\mathcal{W}\psi \triangleq \Box\varphi \vee (\varphi\mathcal{U}\psi)$.

Let $\Sigma \triangleq 2^{\mathbb{P}}$. A model $\mathcal{M}$ is a pair (T, Π) consisting of a set of traces $T \subseteq \Sigma^\omega$ and a partial *trace assignment* $\Pi : \mathbb{T} \rightarrow T$.

Definition 2. *Given a HyperLTL* formula φ, a model $\mathcal{M} \triangleq (T, \Pi)$, and a reference position $i < \omega$, the satisfaction of φ in $\mathcal{M}$ at position i, denoted by $\mathcal{M}, i \models \varphi$, is defined inductively as follows:*

$$\begin{array}{ll}
\mathcal{M}, i \models \top & \\
\mathcal{M}, i \models a_\pi & \textit{iff} \quad a \in \Pi(\pi)[i] \\
\mathcal{M}, i \models \neg\varphi & \textit{iff} \quad \mathcal{M}, i \not\models \varphi \\
\mathcal{M}, i \models \varphi \vee \psi & \textit{iff} \quad \mathcal{M}, i \models \varphi \textit{ or } \mathcal{M}, i \models \psi \\
\mathcal{M}, i \models \bigcirc\varphi & \textit{iff} \quad \mathcal{M}, i+1 \models \varphi \\
\mathcal{M}, i \models \varphi\mathcal{U}\psi & \textit{iff} \quad \exists j \geq 0. \mathcal{M}, i+j \models \psi \textit{ and } \forall k < j. \mathcal{M}, i+k \models \varphi \\
\mathcal{M}, i \models \exists\pi\varphi & \textit{iff} \quad \textit{there exists } t \in T \textit{ such that } \mathcal{M}[\pi \mapsto t], i \models \varphi
\end{array}$$

where $\mathcal{M}[\pi \mapsto t] \mathrel{\hat{=}} (T, \Pi[\pi \mapsto t])$ *denotes the model obtained from* $\mathcal{M}$ *by updating* Π *to map* π *to* t*. The empty assignment is written* $\Pi_\emptyset$*. Given a sentence* φ*, we write* $T, i \vDash \varphi$ *for* $(T, \Pi_\emptyset), i \vDash \varphi$*. Given a set of formulas* Γ *and a formula* φ*, we write* $\Gamma \vDash \varphi$ *if, for all* $i \in \mathbb{N}$ *and all models* $\mathcal{M}$*,* $\mathcal{M}, i \vDash \gamma$ *for all* $\gamma \in \Gamma$ *implies* $\mathcal{M}, i \vDash \varphi$*.*

The sets $\mathrm{FV}(\varphi)$ and $\mathrm{BV}(\varphi)$ of trace variables which have free and bound occurrences in formula φ, respectively, are defined as usual.

The following coincidence lemma is straightforward.

Lemma 1. *If* $\Pi_1|_{\mathrm{FV}(\varphi)} = \Pi_2|_{\mathrm{FV}(\varphi)}$*, then* $(T, \Pi_1), i \vDash \varphi$ *iff* $(T, \Pi_2), i \vDash \varphi$*.*

In what follows, $\varphi[\pi'/\pi]$ denotes the substitution of π by π' for all free occurrences of π in φ.

Lemma 2. *If* $\pi' \notin \mathrm{BV}(\varphi)$*, then* $\mathcal{M}, i \vDash \varphi[\pi'/\pi]$ *is equivalent to* $\mathcal{M}[\pi \mapsto \Pi(\pi')], i \vDash \varphi$ *for all* $\mathcal{M}$ *and all* $i < \omega$*.*

3 A Sequent Calculus $\mathcal{L}_{H\omega}$ for HyperLTL*

A sequent is a pair of (possibly infinite) sets of HyperLTL* formulas, written $\Gamma \vdash \Delta$. We call $\Gamma \vdash \Delta$ *valid* if, for every model $\mathcal{M}$ and every $i \in \mathbb{N}$, $\mathcal{M}, i \models \Gamma$ implies that there exists $\varphi \in \Delta$ such that $\mathcal{M}, i \models \varphi$. In what follows, we write "Γ, Δ" for $\Gamma \cup \Delta$, "Γ, φ" for $\Gamma \cup \{\varphi\}$, and $\bigcirc^{-1}\Gamma$ for $\{\gamma \mid \bigcirc\gamma \in \Gamma\}$.

We present a Gentzen-style proof system for HyperLTL*, denoted by $\mathcal{L}_{H\omega}$, in Table 1. The system $\mathcal{L}_{H\omega}$ consists of four groups of inference rules, respectively for Boolean connectives, temporal operators, trace quantifiers, and general structures. The rules for connectives $\neg$ and $\wedge$ are standard, the same as in first-order logic. The rules for temporal operators $\bigcirc$, $\Diamond$, and $\mathcal{U}$ (and their combinations) are essentially the same as in LTL, except that we use infinitary rules (ω and Coω) in place of the induction axiom $\Box(\varphi \to \bigcirc\varphi) \to (\varphi \to \Box\varphi)$. We will explain why later. The rules for trace quantifiers are new, but follow standard proof-theoretic patterns. The structural rules are essentially the same as in LTL, but we omit the generalization rule $\dfrac{\vdash \varphi}{\vdash \Box\varphi}$. The role of its infinitary sequent counterpart $\dfrac{\Gamma \vdash \varphi}{\{\Box\gamma \mid \gamma \in \Gamma\} \vdash \Box\varphi}$ is largely assumed by the derived rule $G\Box$ (see below).

3.1 Why ω-Rule

It is well-known that LTL has the small (lasso) model property [40], thus it is reasonable to assume a premise set Δ to be finite. Without this assumption, LTL cannot have a finite complete proof system [15]. A notable counterexample is $\Gamma = \{\bigcirc^k p \mid k \in \mathbb{N}\} \cup \{\Diamond\neg p\}$. Clearly, Γ is infinite and not satisfiable, and for any LTL formula φ, we have $\Gamma \models \varphi$ and $\Gamma \models \neg\varphi$. If LTL has a finite complete proof system without the assumption, it follows $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$,

Table 1. Proof System $\mathcal{L}_{H\omega}$

Boolean rules:

$$(L\neg)\ \frac{\Gamma \vdash \varphi}{\Gamma, \neg\varphi \vdash \chi} \quad (R\neg)\ \frac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi} \quad (L\wedge)\ \frac{\Gamma, \varphi, \psi \vdash \chi}{\Gamma, \varphi \wedge \psi \vdash \chi} \quad (R\wedge)\ \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}$$

Temporal rules:

$$(R\bigcirc)\ \frac{\bigcirc^{-1}\Gamma \vdash \varphi}{\Gamma \vdash \bigcirc\varphi} \qquad (R\neg\bigcirc)\ \frac{\Gamma \vdash \bigcirc\neg\varphi}{\Gamma \vdash \neg\bigcirc\varphi} \qquad (L\neg\bigcirc)\ \frac{\Gamma, \bigcirc\neg\varphi \vdash \chi}{\Gamma, \neg\bigcirc\varphi \vdash \chi}$$

$$(\Diamond\bigcirc)\ \frac{\Gamma \vdash \bigcirc\Diamond\varphi}{\Gamma \vdash \Diamond\bigcirc\varphi} \qquad (\omega)\ \frac{}{\{\bigcirc^k \varphi \mid k \in \mathbb{N}\} \vdash \Box\varphi} \qquad (\mathrm{Co}\omega)\ \frac{}{\Diamond\varphi \vdash \bigcirc^k \varphi, \exists k \in \mathbb{N}}$$

$$(\Diamond\mathcal{U})\ \frac{\Gamma \vdash \varphi\mathcal{U}\psi}{\Gamma \vdash \Diamond\psi} \quad (L\mathcal{U})\ \frac{\Gamma, \psi \vdash \chi \quad \Gamma, \varphi, \neg\psi, \bigcirc(\varphi\mathcal{U}\psi) \vdash \chi}{\Gamma, \varphi\mathcal{U}\psi \vdash \chi} \quad (R\mathcal{U})\ \frac{\Gamma, \neg\varphi \vdash \psi \quad \Gamma, \varphi, \neg\bigcirc(\varphi\mathcal{U}\psi) \vdash \psi}{\Gamma \vdash \varphi\mathcal{U}\psi}$$

Quantifier rules:

$$(R\exists)\ \frac{\Gamma \vdash \varphi[\pi'/\pi]}{\Gamma \vdash \exists\pi\varphi} \qquad (L\exists)\ \frac{\Gamma, \psi[\pi'/\pi] \vdash \varphi}{\Gamma, \exists\pi\psi \vdash \varphi} \quad \pi' \notin \mathrm{FV}(\Gamma \cup \{\exists\pi\psi, \varphi\})$$

$$(R\bigcirc\exists)\ \frac{\Gamma \vdash \bigcirc\exists\pi\varphi}{\Gamma \vdash \exists\pi\bigcirc\varphi} \qquad (L\bigcirc\exists)\ \frac{\Gamma, \bigcirc\exists\pi\varphi \vdash \chi}{\Gamma, \exists\pi\bigcirc\varphi \vdash \chi}$$

Structural rules:

$$(\mathrm{As})\ \frac{}{\Gamma, \varphi \vdash \varphi} \quad (\mathrm{Wk})\ \frac{\Gamma \vdash \chi}{\Gamma, \Delta \vdash \chi} \quad (\mathrm{Cd})\ \frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi} \quad (\bigcirc\bot)\ \frac{\Gamma \vdash \bigcirc\bot}{\Gamma \vdash \chi} \quad (\mathrm{Cut})\ \frac{\Gamma \vdash \psi \quad \Gamma, \psi \vdash \varphi}{\Gamma \vdash \varphi}$$

which is a contradiction. On the other hand, [34] proved that HyperLTL, let alone HyperLTL*, have no established form of small model property. Hence, the proof system $\mathcal{L}_{H\omega}$ has to have two infinitary rules (ω) and (Coω), that relate $\bigcirc$ to $\Box$ (dually $\Diamond$) with infinitely many premises (conclusions). Fortunately, these infinitely many premises can sometimes, if not often, be obtained by induction, which could be proved automatically in interactive theorem provers, like Rocq.

3.2 Proofs and Derivability in $\mathcal{L}_{H\omega}$

A proof P in a proof system with infinitary rules such as $\mathcal{L}_{H\omega}$ is a tree P of height $H(P)$, possibly with infinite width, labeled with sequents, defined as follows:

- any instance of an axiom, that is, a proof rule without premises, is a proof, with $H(P) = 1$;
- if P_is are proofs of all the premises of some instance of a proof rule, where $i \in I$ and I may be finite or infinite, then the tree P is with the conclusion of the rule instance as root, and P_is as immediate descendants, with $H(P) = \sup_{i \in I}(H(P_i) + 1)$.

Sequent $\Gamma \vdash \varphi$ is derivable in $\mathcal{L}_{H\omega}$, written $\Gamma \vdash_{\mathcal{L}_{H\omega}} \varphi$, if it is the label of the root of a proof.

3.3 Soundness of $\mathcal{L}_{H\omega}$

Theorem 1 (Soundness). *For any sequent $\Gamma \vdash \varphi$, $\Gamma \vdash_{\mathcal{L}_{H\omega}} \varphi$ implies $\Gamma \vDash \varphi$.*

Proof. This is done by induction on $H(P)$. We only provide proofs for $(R\exists)$ and $(L\exists)$, the remaining cases are straightforward.

- $(R\exists)$: Suppose $\Gamma \vdash \varphi[\pi'/\pi]$. The induction hypothesis implies $\Gamma \vDash \varphi[\pi'/\pi]$. This means that for any $\mathcal{M}, i$ as given in Definition 2, $\mathcal{M}, i \models \Gamma$ implies $\mathcal{M}, i \models \varphi[\pi'/\pi]$. By Lemma 2, $\mathcal{M}, i \models \varphi[\pi'/\pi]$ means that $\mathcal{M}[\pi \mapsto \Pi(\pi')], i \models \varphi[\pi'/\pi]$, i.e., $\mathcal{M}, i \models \exists\pi\varphi$ according to Definition 2.
- $(L\exists)$: Suppose $\Gamma, \psi[\pi'/\pi] \vdash \varphi$ with π' being not free in $\Gamma, \exists\pi\psi, \varphi$. Thus, it follows $\Gamma, \psi[\pi'/\pi] \vDash \varphi$ by the induction hypothesis. That is, for any $\mathcal{M}, i$, $\mathcal{M}, i \vDash \Gamma$ and $\mathcal{M}, i \vDash \psi[\pi'/\pi]$ implies $\mathcal{M}, i \vDash \varphi$. As π' is not free in $\Gamma, \exists\pi\psi, \varphi$, according to Definition 2, $\mathcal{M}, i \vDash \psi[\pi'/\pi]$ iff $\mathcal{M}, i \vDash \exists\pi\psi$. Whence, for any $\mathcal{M}, i$, $\mathcal{M}, i \vDash \Gamma$ and $\mathcal{M}, i \vDash \exists\pi\psi$ implies $\mathcal{M}, i \vDash \varphi$, i.e., $\Gamma, \exists\pi\psi \vDash \varphi$. □

4 Completeness of $\mathcal{L}_{H\omega}$

We establish the completeness of $\mathcal{L}_{H\omega}$ by the following steps: first showing that, for any set of formulas Δ, if Δ is consistent w.r.t. $\mathcal{L}_{H\omega}$, that is $\Delta \nvdash_{\mathcal{L}_{H\omega}} \bot$, then a maximal $\Delta' \supseteq \Delta$ exists such that $\Delta' \nvdash_{\mathcal{L}_{H\omega}} \bot$ too; then showing how such a Δ' can be used to build a model to refute $\Delta \vDash \bot$; finally, by contraposition, this implies that $\Delta \vdash_{\mathcal{L}_{H\omega}} \varphi$ which is immediately derivable with $\Delta, \neg\varphi \vdash_{\mathcal{L}_{H\omega}} \bot$, follows from $\Delta \vDash \varphi$, by virtue of its equivalence with $\Delta, \neg\varphi \vDash \bot$.

4.1 The Conservativeness of HyperLTL* over LTL

To cut down the parts of the proof which essentially pertain to LTL, we establish and use the fact that $\mathcal{L}_{H\omega}$ extends theoremhood as known for LTL in a conservative way.

Proposition 1. *Every substitution instance of a valid propositional LTL formula is a theorem in $\mathcal{L}_{H\omega}$.*

This means that, e.g., $\vdash_{\mathcal{L}_{H\omega}} \bigcirc\exists\pi\Diamond a_\pi \vee \bigcirc\neg\exists\pi\Diamond a_\pi$ follows from the validity of $\bigcirc q \vee \bigcirc\neg q$ in LTL, regardless of the fact that the position of q in the latter formula is taken by $\exists\pi\Diamond a_\pi$, which is HyperLTL*-specific.

Proof. Induction on the construction of LTL Hilbert-style proofs (cf. e.g., [43]) of the translation

$$t(\alpha[\exists\pi_1\chi_1/q_{\exists\pi_1\chi_1}, \ldots, \exists\pi_N\chi_N/q_{\exists\pi_N\chi_N}, a^1_{\rho_1}/a^1_{\rho_1}, \ldots, a^M_{\rho_M}/a^M_{\rho_M}]) \mathrel{\hat{=}} \alpha$$

of the given LTL substitution instance of LTL formula α which maps every quantified HyperLTL formula $\exists\pi\chi$ or subscripted atomic proposition a_ρ to distinct fresh propositional variables $q_{\exists\pi\chi}$ and (the eponymous) a_ρ, respectively. □

4.2 The Deduction Theorem and Some Derived Rules in $\mathcal{L}_{H\omega}$

Proposition 2 (Deduction Theorem). *For any set of formulas Γ and formula φ, $\Gamma, \varphi \vdash \theta$ iff $\Gamma \vdash \varphi \to \theta$.*

Proof. $\Rightarrow$: $\Gamma, \varphi \vdash \theta$ implies $\Gamma, \varphi, \neg\theta \vdash \bot$ by (L$\neg$). It follows $\Gamma, \varphi \wedge \neg\theta \vdash \bot$ by (L$\wedge$). Hence, it derives $\Gamma \vdash \neg(\varphi \wedge \neg\theta)$ by (R$\neg$), that is $\Gamma \vdash \varphi \to \theta$.
$\Leftarrow$: Clearly, $\Gamma \vdash \varphi \to \theta$ implies $\Gamma \vdash \neg(\varphi \wedge \neg\theta)$, which gives $\Gamma, \varphi \wedge \neg\theta \vdash \bot$ by (L$\neg$). Moreover, we have $\Gamma, \varphi, \neg\theta \vdash \varphi \wedge \neg\theta$ by (As) and $(R\wedge)_2$. It follows that $\Gamma, \varphi, \neg\theta \vdash \bot$ by (Cut). Hence $\Gamma, \varphi \vdash \theta$ by $(R\neg)$. □

Now the rule shown in Table 2 can be easily derived in $\mathcal{L}_{H\omega}$:

Table 2. Some Derived Rules

$$(\neg\bigcirc)^k \quad \frac{\Delta \vdash \neg\bigcirc^k\varphi}{\Delta \vdash \bigcirc^k\neg\varphi}, k \in \mathbb{N} \qquad (L\forall) \quad \frac{\Delta, \psi[\pi'/\pi] \vdash \chi}{\Delta, \forall\pi\psi \vdash \chi}$$

$$(\Diamond\bigcirc)^k \quad \frac{\Delta \vdash \bigcirc^k\Diamond\varphi}{\Delta \vdash \Diamond\bigcirc^k\varphi}, k \in \mathbb{N} \qquad (R\forall) \quad \frac{\Delta \vdash \varphi[\pi'/\pi], \pi' \notin \mathrm{FV}(\Delta \cup \{\forall\pi\varphi\})}{\Delta \vdash \forall\pi\varphi}$$

$$(L\Box) \quad \frac{\Delta, \varphi, \bigcirc\Box\varphi \vdash \chi}{\Delta, \Box\varphi \vdash \chi} \qquad (R\Box) \quad \frac{\Delta \vdash \varphi \quad \Delta, \bigcirc(\top\mathcal{U}\neg\varphi) \vdash \neg\varphi}{\Delta \vdash \Box\varphi}$$

$$(G\Box) \quad \frac{\Delta \vdash \Box(\neg\varphi \vee \bigcirc\varphi)}{\Delta, \varphi \vdash \Box\varphi} \qquad (L\vee) \quad \frac{\Delta, \varphi \vdash \chi, \quad \Delta, \psi \vdash \chi}{\Delta, \varphi \vee \psi \vdash \chi}$$

$$(R\vee_1) \quad \frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi} \qquad (R\vee_2) \quad \frac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}$$

Proof. $R\forall$ and $L\forall$ can be proved by the following proof fragments respectively, for instance:

$$\dfrac{\dfrac{\dfrac{\Delta, \psi[\pi'/\pi] \vdash \chi}{\Delta, \neg\chi \vdash \neg\psi[\pi'/\pi]}\, L\neg, R\neg}{\Delta, \neg\chi \vdash \exists\pi\neg\psi}\, R\exists}{\Delta, \neg\exists\pi\neg\psi \vdash \chi}\, L\neg, R\neg \qquad \dfrac{\dfrac{\dfrac{\Delta \vdash \psi[\pi'/\pi]}{\Delta, \neg\psi[\pi'/\pi] \vdash \bot}\, L\neg}{\Delta, \exists\pi\neg\psi \vdash \bot}\, L\exists}{\Delta \vdash \neg\exists\pi\neg\psi}\, R\neg$$

The other rules can be obtained as single applications of Proposition 1, possibly Proposition 2, and *MP*, using the theoremhood in LTL of the following formulas, given in the order of appearance of the related rules: $\neg\bigcirc^k\varphi \to \bigcirc^k\neg\varphi$, $\bigcirc^k\Diamond\varphi \to \Diamond\bigcirc^k\varphi$, $(\varphi \wedge \bigcirc\Box\varphi \to \chi) \leftrightarrow (\Box\varphi \to \chi)$, $\varphi \to (\Box(\varphi \to \bigcirc\varphi) \to \Box\varphi)$, $\varphi \to ((\varphi \to \neg\bigcirc\Diamond\neg\varphi) \to \Box\varphi)$, $(\varphi \to \chi) \to ((\psi \to \chi) \to (\varphi \vee \psi \to \chi))$, and $\varphi \to \varphi \vee \psi$. □

4.3 A Canonical Model

Definition 3. *A set of formulas Δ is called* consistent*, if $\Delta \nvdash_{\mathcal{L}_{H\omega}} \bot$. Δ is called* a maximal consistent set*, if there does not exist $\Delta' \supsetneq \Delta$ that satisfies $\Delta' \nvdash \bot$.*

In the sequel we often omit the $_{\mathcal{L}_{H\omega}}$ in $\vdash_{\mathcal{L}_{H\omega}}$ to improve readability.

Lemma 3. *Let Δ be a maximal consistent set and φ, ψ be formulas. Then*

(i) $\varphi \notin \Delta$ *iff* $\neg\varphi \in \Delta$, *and* $\Delta \vdash \varphi$ *implies* $\varphi \in \Delta$;
(ii) $\varphi \wedge \psi \in \Delta$ *iff* $\varphi \in \Delta$ *and* $\psi \in \Delta$;
(iii) $\varphi \mathcal{U} \psi \in \Delta$ *iff* $\psi \in \Delta$, *or* $\neg\psi, \varphi, \bigcirc(\varphi \mathcal{U} \psi) \in \Delta$;
(iv) $\neg \bigcirc \varphi \in \Delta$ *iff* $\bigcirc \neg\varphi \in \Delta$;
(v) $\exists\pi \bigcirc \varphi \in \Delta$ *iff* $\bigcirc \exists\pi\varphi \in \Delta$.

Given the consistency of Δ, the first statement of (i) is indeed equivalent to the maximality of Δ.

Proof. The proofs of (i) and (ii) are as in classical propositional logic. We skip the easy directions in the proofs of (iii), (iv) and (v) below too:

(iii) ($\Rightarrow$) Assume $\varphi \mathcal{U} \psi \in \Delta$, $\psi \notin \Delta$ and $\chi \notin \Delta$, for some $\chi \in \{\neg\psi, \varphi, \bigcirc(\varphi \mathcal{U} \psi)\}$.

- $\chi = \neg\psi$: From (i), we have $\neg\psi \in \Delta$ and $\neg\neg\psi \in \Delta$, obviously contradicts to the consistency of Δ.
- $\chi = \varphi$: Also, by (i), we have $\neg\varphi \in \Delta$. Obviously, $\neg\psi, \neg\varphi, \psi \vdash \bot$, and $\neg\psi, \neg\varphi, \varphi, \bigcirc(\varphi \mathcal{U} \psi) \vdash \bot$. Hence, $\neg\psi, \neg\varphi, \varphi \mathcal{U} \psi \vdash \bot$ by $(L\mathcal{U})$, which gives $\neg\varphi, \neg\psi \vdash \neg(\varphi \mathcal{U} \psi)$ by $(R\neg)$. This concludes that $\Delta \vdash \neg(\varphi \mathcal{U} \psi)$, that contradicts to the consistency of Δ.
- $\chi = \bigcirc(\varphi \mathcal{U} \psi)$: Likewise, by (i), we have $\neg \bigcirc(\varphi \mathcal{U} \psi) \in \Delta$. Obviously, $\neg\psi, \neg \bigcirc(\varphi \mathcal{U} \psi), \psi \vdash \bot$, and $\neg\psi, \neg \bigcirc(\varphi \mathcal{U} \psi), \varphi, \bigcirc(\varphi \mathcal{U} \psi) \vdash \bot$. Hence, $\neg\psi, \neg \bigcirc(\varphi \mathcal{U} \psi), \varphi \mathcal{U} \psi \vdash \bot$ by $(L\mathcal{U})$, which gives $\neg\varphi, \neg \bigcirc(\varphi \mathcal{U} \psi) \vdash \neg(\varphi \mathcal{U} \psi)$ by $(R\neg)$. This concludes that $\Delta \vdash \neg(\varphi \mathcal{U} \psi)$ by (Wk), which contradicts the consistency of Δ.

(iv) ($\Rightarrow$): $\bigcirc \neg\varphi \in \Delta$ implies $\Delta \vdash \bigcirc \neg\varphi$ by (As), which implies $\Delta \vdash \neg \bigcirc \varphi$ by $(R\neg\bigcirc)$. Hence, it follows $\neg \bigcirc \varphi \in \Delta$ by (i).
($\Leftarrow$): $\bigcirc \neg\varphi \notin \Delta$ implies $\Delta, \bigcirc \neg\varphi \vdash \bot$ by (i), which implies $\Delta, \neg \bigcirc \varphi \vdash \bot$ by $(L\neg\bigcirc)$. Thus, it follows $\neg \bigcirc \varphi \notin \Delta$ by (i).
(v) Similar to the proof of (iv). □

Lemma 4. *If* Δ *is a maximal consistent set then so is* $\bigcirc^{-1} \Delta$.

Proof. Any hypothetical proof of $\bigcirc^{-1} \Delta \vdash_{\mathcal{L}_{H\omega}} \bot$ can be used to obtain a proof of $\Delta \vdash_{\mathcal{L}_{H\omega}} \bigcirc \bot$ by means of $(R\bigcirc)$, and $(\bigcirc\bot)$ allows deriving $\Delta \vdash_{\mathcal{L}_{H\omega}} \bot$ from that, which gives rise to a contradiction. Maximality is established by observing that the equivalence between $\bigcirc \varphi \in \Delta$ and $\neg \bigcirc \varphi \notin \Delta$ implies the equivalence between $\varphi \in \bigcirc^{-1} \Delta$ and $\neg\varphi \notin \bigcirc^{-1} \Delta$. □

Definition 4. *Let* Δ *be a set of formulas.*

- Δ *has the* $\exists$*-property iff for any* $\exists\pi\varphi \in \Delta$, *there exists a trace variable* π' *such that* $\varphi[\pi'/\pi] \in \Delta$.
- Δ *has the* $\mathcal{U}$*-property iff for any* $\varphi \mathcal{U} \psi \in \Delta$, *there exists a* $k \in \mathbb{N}$ *such that* $\bigcirc^k \psi \in \Delta$.
- Δ *has the strengthened* $\mathcal{U}$*-property iff for any* $\bigcirc^j(\varphi \mathcal{U} \psi) \in \Delta$, *there exists an* $n \geq j$ *such that* $\bigcirc^n \psi \in \Delta$.

Lemma 5. *If a maximal consistent set Δ has the $\exists$-property, then so does $\bigcirc^{-1}\Delta$.*

Proof. For any $\exists\pi\varphi \in \bigcirc^{-1}\Delta$, by the definition of $\bigcirc^{-1}\Delta$, we have $\bigcirc\exists\pi\varphi \in \Delta$. By Lemma 3, we have $\exists\pi \bigcirc \varphi \in \Delta$. Since Δ has the $\exists$-property, $\bigcirc\varphi[\pi'/\pi] \in \Delta$ for some π', and thus $\varphi[\pi'/\pi] \in \bigcirc^{-1}\Delta$. □

Let $\mathbb{T}' \hat{=} \mathbb{T} \cup \{\pi_k : k < \omega\}$, where $\{\pi_k : k < \omega\}$ is a countable set of fresh trace variables.

Definition 5. *Given a set Γ of HyperLTL* formulas over $\mathbb{T}'$, $Cn(\Gamma) \hat{=} \{\varphi \mid \Gamma \vdash \varphi\}$, and $\Gamma + \varphi \hat{=} \{\theta \mid \varphi \to \theta \in Cn(\Gamma)\}$.*

Using this notation, Proposition 2 can be written as $\Gamma + \varphi = Cn(\Gamma \cup \{\varphi\})$.

Lemma 6 (Lindenbaum Lemma). *For any set of formulas Δ in the given vocabulary $\mathbb{T} \cup \mathbb{P}$, if $\Delta \nvdash \bot$, then there exists a maximal consistent set $\Delta_{max} \supset \Delta$ of formulas in $\mathbb{T}' \cup \mathbb{P}$ with the $\exists$-property and the strengthened $\mathcal{U}$-property.*

Proof. As argued in [28] for HyperLTL, the set of HyperLTL* formulas on the vocabulary $\mathbb{T}' \cup \mathbb{P}$ is recursively enumerable, which are assumed to be enumerated by $\varphi_0, \varphi_1, \ldots$. Let $\Delta' = Cn(\Delta)$. Clearly, Δ' is also consistent. In addition, let $\kappa_1, \kappa_2 : \mathbb{N} \mapsto \mathbb{N}$ be the respective left and right functions of a pair function $\kappa : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$. So, for any $k_1, k_2 < \omega$, there is a $k < \omega$ such that $k = \kappa(k_1, k_2)$, $k_1 = \kappa_1(k)$ and $k_2 = \kappa_2(k)$. In what follows, we construct a sequence of consistent sets $\Delta_0, \Delta_1, \ldots, \Delta_n, \ldots$, with $\Delta_0 \subseteq \Delta_1 \subseteq \cdots \subseteq \Delta_n \subseteq \cdots$.

Let $\Delta_0 = \Delta'$, and suppose that we have Δ_k with $k_1 = \kappa_1(k)$ and $k_2 = \kappa_2(k)$, now we construct Δ_{k+1} as follows: $\Delta_{k+1} = \Delta_k$ if $\Delta_k, \varphi_{k_1} \vdash \bot$, otherwise

- $\Delta_{k+1} \hat{=} \Delta_k \cup \{\varphi_{k_1}, \bigcirc^m \psi\}$ for some $m \in \mathbb{N}$ such that $\Delta \cup \{\varphi_{k_1}, \bigcirc^m \psi\} \nvdash \bot$, if $\varphi_{k_1} = \varphi\mathcal{U}\psi$.
- $\Delta_{k+1} \hat{=} \Delta_k \cup \{\varphi_{k_1}, \bigcirc^j \bigcirc^m \psi\}$ for some $m \in \mathbb{N}$ such that $\Delta \cup \{\varphi_{k_1}, \bigcirc^j \bigcirc^m \psi\} \nvdash \bot$, if $\varphi_{k_1} = \bigcirc^j(\varphi\mathcal{U}\psi)$, $j \in \mathbb{N}^+$.
- $\Delta_{k+1} \hat{=} \Delta_k \cup \{\varphi_{k_1}, \bigcirc^m \neg\psi\}$ for some $m \in \mathbb{N}$ such that $\Delta \cup \{\varphi_{k_1}, \bigcirc^m \neg\psi\} \nvdash \bot$, if $\varphi_{k_1} = \neg\Box\psi$.
- $\Delta_{k+1} \hat{=} \Delta_k \cup \{\varphi_{k_1}, \psi[\pi_m/\pi]\}$, where m is the least number such that the fresh variable π_m does not occur in Δ_k, nor in φ_{k_1}, if $\varphi_{k_1} = \exists\pi\psi$;
- $\Delta_{k+1} \hat{=} \Delta_k \cup \{\varphi_{k_1}\}$, otherwise.

We show that Δ_k is consistent for all $k \in \mathbb{N}$ by induction on k. The base case follows immediately from $\Delta_0 = \Delta'$. Suppose Δ_k is consistent, now the inductive step is proved as follows:

- if $\Delta_k \cup \{\varphi_{k_1}\} \vdash \bot$, so $\Delta_{k+1} = \Delta_k$. The consistency is obtained by the hypothesis. Now, suppose $\Delta_k \cup \{\varphi_{k_1}\} \nvdash \bot$, consider the following cases:
  - $\varphi_{k_1} = \varphi\mathcal{U}\psi$: First we show that the desired m always exists. Suppose that for any $m \in \mathbb{N}$, $\Delta, \varphi_{k_1}, \bigcirc^m \psi \vdash \bot$. By $(R\neg)$ we have $\Delta_k, \varphi\mathcal{U}\psi \vdash \neg\bigcirc^m \psi$ for all $m \in \mathbb{N}$. By $(R\neg\bigcirc)$, we have $\Delta_k, \varphi\mathcal{U}\psi \vdash \bigcirc^m \neg\psi$ for all $m \in \mathbb{N}$. Then by (ω) and (Cut), we have $\Delta_k, \varphi\mathcal{U}\psi \vdash \Box\neg\psi$, that is, $\Delta_k, \varphi\mathcal{U}\psi \vdash \neg\Diamond\psi$ by duality. In addition, we have $\Delta_k, \varphi\mathcal{U}\psi \vdash \Diamond\psi$ by $(\Diamond\mathcal{U})$, which contradicts the consistency of $\Delta_k \cup \{\varphi_{k_1}\}$. Hence, there exists always some m such that $\Delta_k \cup \{\varphi_{k_1}, \bigcirc^m \psi\} \nvdash \bot$, i.e. Δ_{k+1} is consistent.

- $\varphi_{k_1} = \bigcirc^j(\varphi \mathcal{U} \psi)$: Similarly, suppose that for any $m \in \mathbb{N}$, $\Delta_k \cup \{\varphi_{k_1}, \bigcirc^j \bigcirc^m \psi\} \vdash \bot$. Then we have $\Delta_k, \bigcirc^j(\varphi \mathcal{U} \psi) \vdash \neg \bigcirc^j \bigcirc^m \psi$ for all $m \in \mathbb{N}$. By $(R \bigcirc \neg)$, it follows that $\Delta_k, \bigcirc^j(\varphi \mathcal{U} \psi) \vdash \bigcirc^m \neg \bigcirc^j \psi$, $\forall m \in \mathbb{N}$. By (ω), we have $\Delta_k, \bigcirc^j(\varphi \mathcal{U} \psi) \vdash \neg \Diamond \bigcirc^j \psi$. On the other hand, by $(\Diamond \mathcal{U})$, it follows that $\varphi \mathcal{U} \psi \vdash \Diamond \psi$. So, by $(R \bigcirc)$, $\bigcirc^j(\varphi \mathcal{U} \psi) \vdash \bigcirc^j \Diamond \psi$. By $(\Diamond \bigcirc)$ and (Wk), it follows $\Delta_k, \bigcirc^j(\varphi \mathcal{U} \psi) \vdash \Diamond \bigcirc^j \psi$, which is a contradiction.
- $\varphi_{k_1} = \neg \Box \psi$: Suppose that there is no such $m \in \mathbb{N}$, that is, for any $m \in \mathbb{N}$, we have $\Delta_k, \varphi_{k_1}, \bigcirc^m \neg \psi \vdash \bot$. Hence, for any $m \in \mathbb{N}$, $\Delta_k, \varphi_{k_1} \vdash \neg \bigcirc^m \neg \psi$ by (R$\neg$), which further implies $\Delta_k, \varphi_{k_1} \vdash \bigcirc^m \psi$ by $(\neg \bigcirc)^k$. Thus, $\Delta_k, \varphi_{k_1} \vdash \Box \psi$ follows by $(\bigcirc \mathbb{N})$ and (Cut). So, it can be concluded that $\Delta_k, \varphi_{k_1} \vdash \bot$ by (As) and duality, which contradicts consistency.
- $\varphi_{k_1} = \exists \pi \psi$: Suppose $\Delta \cup \{\exists \pi \psi, \psi[\pi'/\pi]\} \vdash \bot$, so $\Delta_k, \exists \pi \psi, \psi[\pi'/\pi] \vdash \bot$. Since π' is not free in $\Delta_k, \exists \pi \psi$ and ψ (because Δ uses only finitely many of the new variables), by $(L \exists)$ we have $\Delta_k, \exists \pi \psi, \exists \pi \psi \vdash \bot$, which is a contradiction.
- The last case is straightforward.

Now, let $\Delta_{\max} \mathrel{\hat{=}} \bigcup_{i \in \mathbb{N}} \Delta_i$. Clearly, $\Delta_{\max}$ has the $\exists$-property and the strengthened $\mathcal{U}$-property. So, in what follows, we only need to prove $\Delta_{\max}$ is the maximal consistent set with $\Delta \subseteq \Delta_{\max}$.

Suppose $\Delta_{\max} \vdash \bot$. Then we need to consider the following two cases: 1) there exists a k such that $\cup_{j=0}^{k} \Delta_j \subseteq \Delta_{\max}$ and $\cup_{j=0}^{k} \Delta_j \vdash \bot$. That means that Δ_k is inconsistent with the above construction, which is a contradiction. 2) $\Delta_{\max}$ contains $\neg \Box \varphi$, and for any $k \in \mathbb{N}$, there is $i_k \in \mathbb{N}$ with $\Delta_{i_k} \vdash \bigcirc^k \varphi$. Thus, by the Cut rule, we have $\Delta_{\max} \vdash \Box \varphi$. On the other hand, by $(\text{Co}\omega)$, it follows that $\Delta_{\max} \vdash \bigcirc^{k^*} \neg \varphi$ for some $k^* \in \mathbb{N}$. This implies that there exists $i_{k^*} \in \mathbb{N}$ such that $\bigcirc^{k^*} \neg \varphi \in \Delta_{i_{k^*}}$ due to the maximality of $\Delta_{\max}$. Meanwhile, by assumption, $\bigcirc^{k^*} \varphi \in \Delta_{i_{k'}}$. Let $i_{k''} = \max\{i_{k^*}, i_{k'}\}$. By $(\neg \bigcirc)^k$, it follows that $\Delta_{i_{k''}}$ is inconsistent, which is a contradiction.

Suppose that there exists a consistent Δ^* with $\Delta_{\max} \subseteq \Delta^*$ and $\psi \in \Delta^* \setminus \Delta_{\max}$ for some ψ, which is a formula HyperLTL* over the vocabulary $\mathbb{T}' \cup \mathbb{P}$. So, there is k with $\psi = \varphi_k$. Clearly, $\psi \notin \Delta_{k+1}$, so $\Delta_{k+1} + \psi$ is inconsistent. On the other hand, $\Delta_{k+1} + \psi \subseteq \Delta^*$, which contradicts the consistency of Δ^*. □

Let $\bigcirc^{-j} \Gamma \mathrel{\hat{=}} \{\delta \mid \underbrace{\bigcirc \ldots \bigcirc}_{j \text{ times}} \gamma \in \Gamma\}$.

Lemma 7. *If Δ is maximal consistent and has the strengthened $\mathcal{U}$-property, then so is $\bigcirc^{-j} \Delta$ for all $j \in \mathbb{N}$.*

Proof. By Definition 3, $\bigcirc^j(\varphi \mathcal{U} \psi) \in \Delta$ for all $\varphi \mathcal{U} \psi \in \bigcirc^{-j} \Delta$). By the strengthened $\mathcal{U}$-property, there exists a $n \geq j$ such that $\bigcirc^n \psi \in \Delta$. We can reformulate $\bigcirc^n \psi$ as $\bigcirc^j \bigcirc^k \psi$ with $n = j + k$ and $k \geq 0$, thus $\bigcirc^k \psi \in \bigcirc^{-1} \Delta$, which indicates the strengthened $\mathcal{U}$-property. □

Given a maximal consistent set Δ with the $\exists$-property and the strengthened $\mathcal{U}$-property, consider the canonical trajectory $\langle \bigcirc^{-i} \Delta \rangle_{i \in \mathbb{N}}$. Obviously, this infinite

sequence consists of maximal consistent sets with the $\exists$-property and the reinforced $\mathcal{U}$-property by Definition 3 and Lemmas 4, 5 and 7. For every $\pi \in \mathbb{T}'$, we define $t_\pi(i) \hat{=} \{a \mid a_\pi \in \bigcirc^{-i} \Delta\}$, for $i \in \mathbb{N}$. Consider the model $\mathcal{M}^c_\Delta = (T^c_\Delta, \Pi^c_\Delta)$ where $T^c_\Delta \hat{=} \{t_\pi \mid \pi \in \mathbb{T}'\}$ and $\Pi^c_\Delta(\pi) \hat{=} t_\pi$, $\pi \in \mathbb{T}'$. Models built in the way employed for $\mathcal{M}^c_\Delta$ are called canonical. The following lemma establishes the equivalence between $\varphi \in \bigcirc^{-i} \Delta$ and $\mathcal{M}^c_\Delta, i \vDash \varphi$, which implies that $\mathcal{M}^c_\Delta$ is a model for Δ.

Lemma 8 (Truth Lemma). *For any φ and $i \in \mathbb{N}$, $\mathcal{M}^c_\Delta, i \vDash \varphi$ iff $\varphi \in \bigcirc^{-i} \Delta$.*

Proof. Structural induction on φ.

- $\varphi = a_\pi$: By Definition 2, $\mathcal{M}^c_\Delta, i \vDash a_\pi$ iff $a \in \Pi^c_\Delta(\pi)[i]$; iff $a \in \{a \mid a_\pi \in \bigcirc^{-i} \Delta\}$; iff $a_\pi \in \bigcirc^{-i} \Delta$.
- $\varphi = \neg\psi$: This case follows from Lemma 3 (i), i.e., $\mathcal{M}^c_\Delta, i \vDash \neg\psi$ iff $\mathcal{M}^c_\Delta, i \nvDash \psi$, iff $\psi \notin \bigcirc^{-i} \Delta$, iff $\neg\psi \in \bigcirc^{-i} \Delta$.
- $\varphi = \psi \wedge \chi$: Like the previous case, according to Lemma 3 (ii), $\psi \wedge \chi \in \bigcirc^{-i} \Delta$ iff $\psi, \chi \in \bigcirc^{-i} \Delta$.
- $\varphi = \bigcirc\psi$: Lemma 3 (iv) implies that $\mathcal{M}^c_\Delta, i \vDash \bigcirc\psi$ iff $\mathcal{M}^c_\Delta, i+1 \vDash \psi$, iff $\psi \in \bigcirc^{-(i+1)} \Delta$, iff $\bigcirc\psi \in \bigcirc^{-i} \Delta$.
- $\varphi = \psi \mathcal{U} \chi$: The forward direction follows immediately from the induction hypothesis. For the backward direction, let $\psi \mathcal{U} \chi \in \bigcirc^{-i} \Delta$. Since $\bigcirc^{-i} \Delta$ has the reinforced $\mathcal{U}$-property by Lemma 7, there exists a minimum $k \in \mathbb{N}$ such that $\bigcirc^k \chi \in \bigcirc^{-i} \Delta$. Thus, $\chi \in \bigcirc^{-(i+k)} \Delta$. Consider the following two cases:
  - $\chi \notin \bigcirc^{-(i+j)} \Delta$ for all $j < k$. Lemma 3 (iii) implies $\psi, \bigcirc(\psi \mathcal{U} \chi) \in \bigcirc^{-(i+j)} \Delta$. The induction hypothesis implies $\mathcal{M}, i+k \vDash \chi, \mathcal{M}, i+j \vDash \psi$ for all $j < k$. This implies $\mathcal{M}^c_\Delta, i \vDash \psi \mathcal{U} \chi$;
  - $\chi \in \bigcirc^{-(i+j')} \Delta$ for some $j' < k$. This case admits a similar proof.
- $\varphi = \exists\pi\psi$: $\mathcal{M}^c_\Delta, i \vDash \exists\pi\psi$ iff there exists a $t \in T^c_\Delta$ s.t. $T^c_\Delta, \Pi^c_\Delta[\pi \mapsto t], i \vDash \psi$ by Definition 2; iff there exists a $\pi' \in \mathbb{T}'$ s.t. $\mathcal{M}^c_\Delta[\pi \mapsto \Pi^c_\Delta(\pi')], i \vDash \psi$, as Π^c_Δ is a bijection from $\mathbb{T}'$ to T^c_Δ; iff there exists a $\pi' \in \mathbb{T}'$ s.t. $\mathcal{M}^c_\Delta, i \vDash \psi[\pi'/\pi]$ by Lemma 2; iff there exists a $\pi' \in \mathbb{T}'$ s.t. $\psi[\pi'/\pi] \in \bigcirc^{-i} \Delta$ by the induction hypothesis; iff $\exists\pi\psi \in \Delta$ according to the $\exists$-property and $(R\exists)$. □

Theorem 2 (Completeness of HyperLTL*). *For any Δ and φ, $\Delta \vDash \varphi$ implies $\Delta \vdash \varphi$.*

Proof. Suppose $\Delta \nvDash \varphi$, so $\Delta \cup \{\neg\varphi\}$ is consistent. Hence, $\mathcal{M}^c_{\Delta \cup \{\neg\varphi\}}, 0 \vDash \psi$ for all $\psi \in \Delta \cup \{\neg\varphi\}$ by Lemma 8, which contradicts to $\Delta \vDash \varphi$. □

5 Expressiveness of HyperLTL*

HyperLTL can be viewed as a proper subset of HyperLTL* in which trace quantifiers do not occur in the scope of $\bigcirc$ or $\mathcal{U}$. Consequently, every HyperLTL* formula in prenex normal form is a HyperLTL formula. The following theorem shows that allowing trace quantifiers under temporal operators strictly increases expressiveness.

Theorem 3 ([34]). *There is no HyperLTL formula, that can be equivalent to HyperLTL* formula $\Diamond\forall\pi\neg p_\pi$.*

HyperLTL* is still subsumed by the predicate-logic theory $FO[<, E]$ from [34].

Definition 6. *The syntax of $FO[<, E]$ is defined by the following BNF:*

$$\varphi ::= P_a(x) \mid E(x, y) \mid x = y \mid x < y \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x.\varphi \mid \forall x.\varphi$$

where P_a is a unary predicate, corresponding to the proposition letter a in HyperLTL*, and x, y represents the positions of the trace, interpreted as natural numbers. Given a trace set T, we let $\underline{T} \hat{=} (T \times \mathbb{N}, <^{\underline{T}}, E^{\underline{T}}, P_a^{\underline{T}})$, where the non-logical symbols of $FO[<, E]$ are interpreted in $\underline{T}$, where $<^{\underline{T}} \hat{=} \{(t, n), (t, n') \mid t \in T, n < n'\}$, $E^{\underline{T}} \hat{=} \{(t, n), (t', n) \mid t, t' \in T\}$, $P_a^{\underline{T}} \hat{=} \{(t, n) \mid a \in t[n]\}$.

Next, we define a satisfaction-preserving translation f from HyperLTL* to $FO[<, E]$. Each trace variable π in φ is associated with an individual variable x_π. The translation $f(\varphi)$ is a formula of $FO[<, E]$ with the individual variables x_π and z as its free variables, where $\pi \in \mathrm{FV}(\varphi)$. The variable z is called the time variable of $f(\varphi)$, standing for the reference position.

Definition 7. *The translation function f is inductively defined as follows:*

- $f(a_\pi) \hat{=} \exists y.y \geq x_\pi \wedge E(z, y) \wedge P_a(y)$, *where z is the time-variable for $f(a_\pi)$;*
- $f(\neg\varphi) \hat{=} \neg f(\varphi)$;
- $f(\varphi_1 \wedge \varphi_2) \hat{=} f(\varphi_1) \wedge f(\varphi_2)$;
- $f(\bigcirc\varphi) \hat{=} \exists z_1.Succ(z, z_1) \wedge f(\varphi)[z_1/z]$, *where $Succ(z, z_1)$ stands for $z < z_1 \wedge \forall z_2.z < z_2 \rightarrow z_1 \leq z_2$;*
- $f(\varphi_1 \mathcal{U} \varphi_2) \hat{=} \exists z_2.z \leq z_2 \wedge f(\varphi_2)[z_2/z] \wedge \forall z_1.z \leq z_1 < z_2 \rightarrow f(\varphi_1)[z_1/z]$;
- $f(\exists\pi\varphi) = \exists x_\pi.f(\varphi)$.

The following theorem shows that $FO[<, E]$ subsumes HyperLTL*.

Theorem 4. *Let φ be a HyperLTL* formula and let T be a set of traces. Let $\underline{T}$ be the corresponding $FO[<, E]$-structure. Let the trace assignment Π and the $FO[<, E]$ variable assignment β satisfy the equivalence*

$$\Pi(\pi) = t \text{ iff } \beta(x_\pi) = (t, i) \text{ for } \pi \in \mathrm{FV}(\varphi), \text{ and } \beta(z) = (\lambda, i),$$

where λ in T is a dummy value. Then $(T, \Pi), i \vDash \varphi$ iff $(\underline{T}, \beta) \vDash f(\varphi)$

Proof. Structural induction on φ. □

Moreover, according to the proof of Theorem 8 in [34], clearly the property discussed there is not expressible in HyperLTL* either, so $FO[<, E]$ is strictly more expressive than HyperLTL*.

6 Case Study

We present a revised example of EDAS from [12] and prove that an EDAS model adapted from [11] satisfies the refined noninterference property from [12].

EDAS is a paper-submission system: each execution assigns a submission either `acc` (accepted) or `rej` (rejected) and decides the session to which it is assigned. If the session has not been decided, the system displays "yet to decide", which is represented by a Boolean variable *ses*.

We now provide a simple model of EDAS following the repaired program in [11] in Fig. 1, which can be represented as the HyperLTL formula in Table 3. φ_1 says that any trace whenever passing through the initial state will enter either the accepted state or the rejected state in the next step; φ_2 says that any trace whenever passing through the accepted state cannot enter the rejected state in the next step; symmetrically, φ_3 says that any trace whenever passing through the rejected state cannot enter the accepted state in the next step; φ_4 says that any trace should start from the initial state l_0.

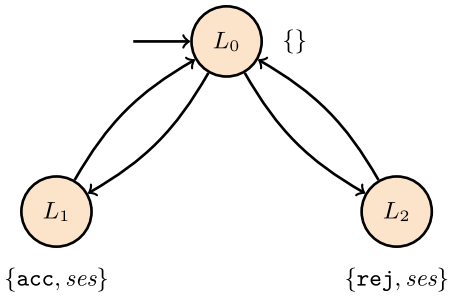

Fig. 1. EDAS: A simple paper submission system

Table 3. HyperLTL formula encoding the EDAS model

$$\varphi_1 = \forall\pi\Box(\neg\mathtt{acc}_\pi \wedge \neg\mathtt{rej}_\pi \wedge \neg ses_\pi \rightarrow \bigcirc(\mathtt{acc}_\pi \wedge \neg\mathtt{rej}_\pi \wedge ses_\pi) \vee \bigcirc(\neg\mathtt{acc}_\pi \wedge \mathtt{rej}_\pi \wedge ses_\pi))$$
$$\varphi_2 = \forall\pi\Box(\mathtt{acc}_\pi \wedge \neg\mathtt{rej}_\pi \wedge ses_\pi \rightarrow \bigcirc(\neg\mathtt{acc}_\pi \wedge \neg\mathtt{rej}_\pi \wedge \neg ses_\pi))$$
$$\varphi_3 = \forall\pi\Box(\neg\mathtt{acc}_\pi \wedge \mathtt{rej}_\pi \wedge ses_\pi \rightarrow \bigcirc(\neg\mathtt{acc}_\pi \wedge \neg\mathtt{rej}_\pi \wedge \neg ses_\pi))$$
$$\varphi_4 = \forall\pi(\neg acc_\pi \wedge \neg rej_\pi \wedge \neg ses_\pi)$$

We are interested in the refined noninterference property given in [12], represented by the following HyperLTL formula

$$\varphi_{ref} \hat{=} \forall\pi_1\exists\pi_2\forall\pi_3\exists\pi_4 \ \ \mathrm{obj}(\pi_1,\pi_2) \wedge \Box(dec_{\pi_4} = dec_{\pi_2}) \wedge \Box(ses_{\pi_4} \leftrightarrow ses_{\pi_3})$$

where $\mathrm{obj}(\pi_1, \pi_2)$ stands for $(\Diamond \mathtt{acc}_{\pi_1} \rightarrow \Diamond \mathtt{acc}_{\pi_2}) \wedge (\Diamond \mathtt{rej}_{\pi_1} \rightarrow \Diamond \mathtt{rej}_{\pi_2})$, and $dec_{\pi_1} = dec_{\pi_2}$ for $(\mathtt{acc}_{\pi_1} \leftrightarrow \mathtt{acc}_{\pi_2}) \wedge (\mathtt{rej}_{\pi_1} \leftrightarrow \mathtt{rej}_{\pi_2})$. Clearly, $\mathrm{obj}(\pi_1, \pi_2)$ says executions π_1 and π_2 make the same decision at last, while $dec_{\pi_1} = dec_{\pi_2}$ says executions π_1 and π_2 share the same decision at the reference position. φ_{ref} (with three quantifier alternations) expresses a refined noninterference with the modification that the universally quantified trace π_1 is replaced by an existentially quantified trace π_2 that satisfies the same objectives.

Now we need to prove the model satisfies the property, i.e., $\Delta \vdash \varphi_{ref}$, where $\Delta = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. Obviously, the satisfiability and validity of the above formula falls into the undecidable fragment of HyperLTL [27], as the number of quantifier alternations in φ_{ref} is three.

For simplicity, we use ψ_1, ψ_2, ψ_3 and ψ_4 to denote the trace quantifier free part of $\varphi_1, \varphi_2, \varphi_3$ and φ_4 in Table 3, respectively.

Now consider the following quantifier-free sequent first.

$$\bigcup_{j \in [1,2]} \{\psi_i[\pi'_j/\pi] \mid i \in [1,4]\} \vdash \quad \mathrm{obj}(\pi'_1, \pi'_1) \wedge \Box(dec_{\pi'_1} = dec_{\pi'_1}) \wedge \Box(ses_{\pi'_1} \leftrightarrow ses_{\pi'_2})$$

We abbreviate the antecedent of the sequent as Δ' and the succedent as φ'. The quantifier-free part of HyperLTL is exactly the same as LTL (taking each combination of propositional letter and trace variable as a unique propositional letter). Therefore, we can use a state-of-the-art automatic tool for LTL such as NuSMV [16] to prove the quantifier-free sequent by checking whether $\bigwedge \Delta' \rightarrow \varphi'$ is valid. We use the symbolic model checker NuSMV for the task. The reader may refer to repository[1] for the NuSMV code. Now, we focus on proving the quantifier-related part of the sequent as follows:

(1) $\psi_i[\pi'_1/\pi], \psi_i[\pi'_2/\pi], i \in [1,4] \vdash \mathrm{obj}(\pi'_1, \pi'_1) \wedge \Box(dec_{\pi'_1} = dec_{\pi'_1}) \wedge \Box(ses_{\pi'_1} \leftrightarrow ses_{\pi'_2})$

(2) $\forall\pi\psi_1, \forall\pi\psi_2, \forall\pi\psi_3, \forall\pi\psi_4 \vdash \mathrm{obj}(\pi'_1, \pi'_1) \wedge \Box(dec_{\pi'_1} = dec_{\pi'_1}) \wedge \Box(ses_{\pi'_1} \leftrightarrow ses_{\pi'_2})$ by (1) and $(\forall L)$ and Boolean rules

(3) $\Delta \vdash \exists\pi_4\, \mathrm{obj}(\pi'_1, \pi'_1) \wedge \Box(dec_{\pi_4} = dec_{\pi'_1}) \wedge \Box(ses_{\pi_4} \leftrightarrow ses_{\pi'_2})$ by (2) and $(R\exists)$

(4) $\Delta \vdash \forall\pi_3\exists\pi_4\, \mathrm{obj}(\pi'_1, \pi'_1) \wedge \Box(dec_{\pi_4} = dec_{\pi'_1}) \wedge \Box(ses_{\pi_4} \leftrightarrow ses_{\pi_3})$ by (3) and $(R\forall)$

(5) $\Delta \vdash \exists\pi_2\forall\pi_3\exists\pi_4\, \mathrm{obj}(\pi'_1, \pi_2) \wedge \Box(dec_{\pi_4} = dec_{\pi_2}) \wedge \Box(ses_{\pi_4} \leftrightarrow ses_{\pi_3})$ by (4) and $(R\exists)$

(6) $\Delta \vdash \forall\pi_1\exists\pi_2\forall\pi_3\exists\pi_4\, \mathrm{obj}(\pi_1, \pi_2) \wedge \Box(dec_{\pi_4} = dec_{\pi_2}) \wedge \Box(ses_{\pi_4} \leftrightarrow ses_{\pi_3})$ by (5) and $(R\forall)$

7 Conclusion and Future Work

In this paper, we present a proof system $\mathcal{L}_{H\omega}$ for HyperLTL*. Our main contribution is the completeness of $\mathcal{L}_{H\omega}$ over trace models. Existing research on hyperlogics has mainly focused on semantic considerations, whereas this paper develops a deductive treatment. The proof system provides a basis for formalizing HyperLTL-style reasoning in proof assistants and thereby facilitates the

[1] https://zenodo.org/records/14885502.

verification of hyperproperties that cannot be handled by fully automatic techniques.

For future work, it deserves to investigate formalization and implementation of the proof system in proof assistants such as Rocq and Isabelle/HOL

Acknowledgments. The authors thank anonymous reviewers for their valuable comments and helpful suggestions. This work is partially funded by the National Key R&D Program under grant No. 2022YFA1005101 and 2022YFA1005102, the NSFC under grant No. 62192732, W2511064 and 62502475, and the CAS Project for Young Scientists in Basic Research under grant No. YSBR-040.

References

1. Ábrahám, E., Bartocci, E., Bonakdarpour, B., Dobe, O.: Probabilistic hyperproperties with nondeterminism. In: Hung, D.V., Sokolsky, O. (eds.) ATVA 2020. LNCS, vol. 12302, pp. 518–534. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-59152-6_29
2. Alpern, B., Schneider, F.B.: Defining liveness. Inf. Process. Lett. **21**(4), 181–185 (1985)
3. Alur, R., Černý, P., Chaudhuri, S.: Model checking on trees with path equivalences. In: Grumberg, O., Huth, M. (eds.) TACAS 2007. LNCS, vol. 4424, pp. 664–678. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71209-1_51
4. Alur, R., Černý, P., Zdancewic, S.: Preserving secrecy under refinement. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 107–118. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_10
5. Balliu, M., Dam, M., Guernic, G.L.: Epistemic temporal logic for information flow security. In: PLAS 2011, p. 6. ACM (2011)
6. Barthe, G., Crespo, J.M., Kunz, C.: Beyond 2-safety: asymmetric product programs for relational program verification. In: Artemov, S., Nerode, A. (eds.) LFCS 2013. LNCS, vol. 7734, pp. 29–43. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-35722-0_3
7. Barthe, G., D'Argenio, P.R., Rezk, T.: Secure information flow by self-composition. In: CSFW-17 2004, pp. 100–114. IEEE Computer Society (2004)
8. Bartocci, E., Ferrère, T., Henzinger, T.A., Nickovic, D., da Costa, A.O.: Flavors of sequential information flow. In: Finkbeiner, B., Wies, T. (eds.) VMCAI 2022. LNCS, vol. 13182, pp. 1–19. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-94583-1_1
9. Baumeister, J., Coenen, N., Bonakdarpour, B., Finkbeiner, B., Sánchez, C.: A temporal logic for asynchronous hyperproperties. In: Silva, A., Leino, K.R.M. (eds.) CAV 2021. LNCS, vol. 12759, pp. 694–717. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-81685-8_33
10. Beutner, R., Finkbeiner, B.: A temporal logic for strategic hyperproperties. In: CONCUR 2021. LIPIcs, vol. 203, pp. 24:1–24:19 (2021)
11. Beutner, R., Hsu, T., Bonakdarpour, B., Finkbeiner, B.: Syntax-guided automated program repair for hyperproperties. In: Gurfinkel, A., Ganesh, V. (eds.) CAV 2024. LNCS, vol. 14683, pp. 3–26. Springer (2024). https://doi.org/10.1007/978-3-031-65633-0_1

12. Bonakdarpour, B., Finkbeiner, B.: The complexity of monitoring hyperproperties. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF), July 2018. IEEE (2018)
13. Bonakdarpour, B., Sanchez, C., Schneider, G.: Monitoring hyperproperties by combining static analysis and runtime verification. In: Margaria, T., Steffen, B. (eds.) ISoLA 2018. LNCS, vol. 11245, pp. 8–27. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03421-4_2
14. Bozzelli, L., Peron, A., Sánchez, C.: Asynchronous extensions of HyperLTL. In: LICS 2021. pp. 1–13. IEEE (2021)
15. Chopoghloo, S., Moniri, M.: A strongly complete axiomatization of intuitionistic temporal logic. J. Logic Comput. **31**(7), 1640–1659 (2021)
16. Cimatti, A.: NuSMV 2: an OpenSource tool for symbolic model checking. In: Brinksma, E., Larsen, K.G. (eds.) CAV 2002. LNCS, vol. 2404, pp. 359–364. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45657-0_29
17. Clarke, E.M., Emerson, E.A.: Design and synthesis of synchronization skeletons using branching time temporal logic. In: Kozen, D. (ed.) Logic of Programs 1981. LNCS, vol. 131, pp. 52–71. Springer, Heidelberg (1982). https://doi.org/10.1007/BFb0025774
18. Clarkson, M.R., Finkbeiner, B., Koleini, M., Micinski, K.K., Rabe, M.N., Sánchez, C.: Temporal logics for hyperproperties. In: Abadi, M., Kremer, S. (eds.) POST 2014. LNCS, vol. 8414, pp. 265–284. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54792-8_15
19. Clarkson, M.R., Schneider, F.B.: Hyperproperties. J. Comput. Secur. **18**(6), 1157–1210 (2010)
20. Coenen, N.: A proof system for HyperLTL. Bachelor's Thesis. University of Saarland (2016)
21. Coenen, N., Finkbeiner, B., Hahn, C., Hofmann, J.: The hierarchy of hyperlogics. In: LICS 2019, pp. 1–13. IEEE (2019)
22. Coenen, N., Finkbeiner, B., Sánchez, C., Tentrup, L.: Verifying hyperliveness. In: Dillig, I., Tasiran, S. (eds.) CAV 2019. LNCS, vol. 11561, pp. 121–139. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25540-4_7
23. Correnson, A., Finkbeiner, B.: Coinductive proofs for temporal hyperliveness. Proc. ACM Program. Lang. **9**(POPL), 1568–1595 (2025)
24. Dimitrova, R., Finkbeiner, B., Kovács, M., Rabe, M.N., Seidl, H.: Model checking information flow in reactive systems. In: Kuncak, V., Rybalchenko, A. (eds.) VMCAI 2012. LNCS, vol. 7148, pp. 169–185. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-27940-9_12
25. Dimitrova, R., Finkbeiner, B., Torfah, H.: Probabilistic hyperproperties of Markov decision processes. In: Hung, D.V., Sokolsky, O. (eds.) ATVA 2020. LNCS, vol. 12302, pp. 484–500. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-59152-6_27
26. Emerson, E.A., Halpern, J.Y.: "Sometimes" and "not never" revisited: on branching versus linear time temporal logic. J. ACM **33**(1), 151–178 (1986)
27. Finkbeiner, B., Hahn, C.: Deciding hyperproperties. In: CONCUR 2016. LIPIcs, vol. 59, pp. 13:1–13:14 (2016)
28. Finkbeiner, B., Hahn, C., Hans, T.: MGHyper: checking satisfiability of HyperLTL formulas beyond the $\exists^*\forall^*$ fragment. In: Lahiri, S.K., Wang, C. (eds.) ATVA 2018. LNCS, vol. 11138, pp. 521–527. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01090-4_31

29. Finkbeiner, B., Hahn, C., Lukert, P., Stenger, M., Tentrup, L.: Synthesizing reactive systems from hyperproperties. In: Chockler, H., Weissenbacher, G. (eds.) CAV 2018. LNCS, vol. 10981, pp. 289–306. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96145-3_16
30. Finkbeiner, B., Hahn, C., Stenger, M.: EAHyper: satisfiability, implication, and equivalence checking of hyperproperties. In: Majumdar, R., Kunčak, V. (eds.) CAV 2017. LNCS, vol. 10427, pp. 564–570. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63390-9_29
31. Finkbeiner, B., Hahn, C., Stenger, M., Tentrup, L.: Monitoring hyperproperties. Formal Meth. Syst. Des. **54**(3), 336–363 (2019). https://doi.org/10.1007/s10703-019-00334-z
32. Finkbeiner, B., Hahn, C., Stenger, M., Tentrup, L.: RVHyper: a runtime verification tool for temporal hyperproperties. In: Beyer, D., Huisman, M. (eds.) TACAS 2018. LNCS, vol. 10806, pp. 194–200. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-89963-3_11
33. Finkbeiner, B., Hahn, C., Torfah, H.: Model checking quantitative hyperproperties. In: Chockler, H., Weissenbacher, G. (eds.) CAV 2018. LNCS, vol. 10981, pp. 144–163. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96145-3_8
34. Finkbeiner, B., Zimmermann, M.: The first-order logic of hyperproperties. In: STACS 2017. LIPIcs, vol. 66, pp. 30:1–30:14 (2017)
35. Gaintzarain, J., Hermo, M., Lucio, P., Navarro, M., Orejas, F.: A cut-free and invariant-free sequent calculus for PLTL. In: Duparc, J., Henzinger, T.A. (eds.) CSL 2007. LNCS, vol. 4646, pp. 481–495. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74915-8_36
36. Goguen, J.A., Meseguer, J.: Security policies and security models. In: 1982 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 26–28 April 1982. pp. 11–20. IEEE Computer Society (1982)
37. Gutsfeld, J.O., Müller-Olm, M., Ohrem, C.: Propositional dynamic logic for hyperproperties. In: CONCUR 2020. LIPIcs, vol. 171, pp. 50:1–50:22 (2020)
38. Gutsfeld, J.O., Müller-Olm, M., Ohrem, C.: Automata and fixpoints for asynchronous hyperproperties. Proc. ACM Program. Lang. **5**(POPL), 1–29 (2021)
39. Huisman, M., Worah, P., Sunesen, K.: A temporal logic characterisation of observational determinism. In: CSFW-19 2006, p. 3. IEEE Computer Society (2006)
40. Kesten, Y., Pnueli, A.: A complete proof systems for QPTL. In: LICS 1995, pp. 2–12. IEEE Computer Society (1995)
41. Kozen, D.: Results on the propositional μ-Calculus. Theor. Comput. Sci. **27**, 333–354 (1983)
42. Krebs, A., Meier, A., Virtema, J., Zimmermann, M.: Team semantics for the specification and verification of hyperproperties. In: MFCS 2018. LIPIcs, vol. 117, pp. 10:1–10:16 (2018)
43. Lichtenstein, O., Pnueli, A.: Propositional temporal logics: decidability and completeness. Logic J. IGPL **8**(1), 55–85 (2000)
44. Pnueli, A.: The temporal logic of programs. In: FOCS 1977, pp. 46–57. IEEE Computer Society (1977)
45. Segerberg, K.: A model existence theorem in infinitary propositional modal logic. J. Philos. Logic **23**(4), 337–367 (1994)
46. Sistla, A.P., Clarke, E.M.: The complexity of propositional linear temporal logics. J. ACM **32**(3), 733–749 (1985)
47. Sistla, A.P., Vardi, M.Y., Wolper, P.: The complementation problem for Büchi automata with applications to temporal logic. Theor. Comput. Sci. **49**, 217–237 (1987)

48. Virtema, J., Hofmann, J., Finkbeiner, B., Kontinen, J., Yang, F.: Linear-time temporal logic with team semantics: expressivity and complexity. In: FSTTCS 2021. LIPIcs, vol. 213, pp. 52:1–52:17 (2021)
49. Wang, Y., Zarei, M., Bonakdarpour, B., Pajic, M.: Statistical verification of hyperproperties for cyber-physical systems. ACM Trans. Embed. Comput. Syst. **18**(5s), 92:1–92:23 (2019)
50. Zdancewic, S., Myers, A.C.: Observational determinism for concurrent program security. In: 16th IEEE Computer Security Foundations Workshop (CSFW-16 2003), 30 June–2 July 2003, Pacific Grove, CA, USA, p. 29. IEEE Computer Society (2003)
51. Zhan, N.: Completeness of higher-order duration calculus. In: Clote, P.G., Schwichtenberg, H. (eds.) CSL 2000. LNCS, vol. 1862, pp. 442–456. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44622-2_30
52. Zhou, C., Guelev, D.P., Zhan, N.: A higher-order duration calculus. In: Millennial Perspectives in Computer Science, pp. 407–416 (1999)