The Hierarchy of Hyperlogics: A Knowledge Reasoning Perspective [*]

Norine Coenen , **Bernd Finkbeiner** , **Christopher Hahn** , **Jana Hofmann**
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{norine.coenen, finkbeiner, christopher.hahn, jana.hofmann}@cispa.saarland

Abstract

We discuss the hierarchy of hyperlogics from a knowledge reasoning perspective. Hyperproperties generalize trace properties by relating multiple traces. Recently, logics for hyperproperties have been obtained from standard logics by adding variables for traces or paths to temporal logics like LTL and CTL*, and by adding the equal-level predicate to first-order and second-order logics, like monadic first-order logic of order and MSO. The resulting hierarchy of hyperlogics provides interesting opportunities for knowledge reasoning research: many epistemic properties and system properties in multi-agent systems, like distributivity, are hyperproperties. At the same time, first-order and second-order reasoning methods become applicable to hyperproperties.

Hyperproperties (Clarkson and Schneider 2010) are system properties that relate *multiple* execution traces to each other. Hyperproperties play an important role in security policies, such as information flow control (Goguen and Meseguer 1982), call integrity in smart contracts (Grishchenko, Maffei, and Schneidewind 2018), and secrecy in web-based workflows (Finkbeiner et al. 2017), as well as, beyond security, in areas such as fault-tolerance (Nguyen et al. 2017). As demonstrated by high-profile side-channel attacks like Meltdown and Spectre, hyperproperties have significant practical relevance. There is a lot of recent research on model checking (Finkbeiner, Hahn, and Torfah 2018; Coenen et al. 2019b), synthesis (Finkbeiner et al. 2020a; Finkbeiner et al. 2020b), monitoring (Hahn 2019; Finkbeiner et al. 2019), and program repair (Bonakdarpour and Finkbeiner 2019) from hyperproperties.

The standard logics used in the areas of verification, knowledge representation, and reasoning, like linear-time temporal logic (LTL), computation tree logic (CTL), and monadic first-order logic, cannot express hyperproperties. However, these logics have recently been extended to hyperproperties with two principal extensions: the addition of variables for traces or paths to a temporal logic, and the extension of monadic first-order and second-order logics with a relational predicate.

While the standard temporal logics only refer to a *single* trace or path at a time, the temporal hyperlogics HyperLTL and HyperCTL* quantify over *multiple* traces (or paths) and relate them using a temporal formula. For example, the HyperLTL formula

$$\forall \pi . \forall \pi' . \ \Box \bigwedge_{a \in AP} a_\pi \leftrightarrow a_{\pi'} \tag{1}$$

expresses that *all pairs* of traces must at all times agree on the values of the atomic propositions given as the set AP.

The second extension adds the *equal-level predicate* E (Thomas 2009) to monadic first-order logic of order (FO[$<$]). The equal-level predicate relates points that happen at the same time. The HyperLTL formula (1) is equivalent to the FO[$<, E$] formula

$$\forall x . \forall y . \ E(x,y) \rightarrow \bigwedge_{a \in AP} (P_a(x) \leftrightarrow P_a(y)) \ .$$

A natural question is how the two extensions compare in terms of expressiveness. Kamp's theorem (Kamp 1968) states (in the formulation of Gabbay et al. (Gabbay et al. 1980)) that LTL is expressively equivalent to FO[$<$]. However, the potential analogue of Kamp's theorem for hyperlogics, that HyperLTL might be equivalent to FO[$<, E$], is *not* true (Finkbeiner and Zimmermann 2017).

In the paper "The Hierarchy of Hyperlogics" (Coenen et al. 2019a)[1], we initiated an extensive study of the expressiveness of temporal and first-order/second-order hyperlogics. The standard hierarchy of linear-time and branching-time logics is shown in Figures 1a and 1b, respectively. Each temporal logic corresponds to an equally expressive FO/SO logic, e.g., LTL to FO[$<$], and QPTL to S1S, where the latter two are both able to express all ω-regular languages.

The hierarchy of hyperlogics is shown in Figures 1c and 1d. The picture differs significantly from the standard hierarchy: for almost every pair of a temporal logic and a FO/SO logic that are expressively equivalent in the standard hierarchy, the corresponding FO/SO logic is more expressive in the hierarchy of hyperlogics. The only exception is MSO[E] and HyperQCTL*, which are also equivalent in the hierarchy of hyperlogics. The reason is that HyperQCTL* allows for quantification over

[*] This work was partially supported by the Collaborative Research Center "Foundations of Perspicuous Systems" (TRR 248, 389792660), by G.I.F. grant I-1513-407./2019, and by European Research Council (ERC) Grant OSARES (No. 683300).

[1] https://arxiv.org/pdf/2005.05934.pdf

$$\begin{array}{cccc}
\mathrm{S1S}[E] & \mathrm{MSO} & \mathrm{S1S}[E] & \mathrm{MSO}[E] \\
= & = & \vee & = \\
\mathrm{QPTL} & \mathrm{QCTL}^* & \mathrm{HyperQPTL} & \mathrm{HyperQCTL}^* \\
\vee & \vee & \vee & \vee \\
\mathrm{FO}[<] & \mathrm{MPL} & \mathrm{FO}[<, E] & \mathrm{MPL}[E] \\
= & = & \vee & \vee \\
\mathrm{LTL} & \mathrm{CTL}^* & \mathrm{HyperLTL} & \mathrm{HyperCTL}^* \\
\text{(a)} & \text{(b)} & \text{(c)} & \text{(d)}
\end{array}$$

Figure 1: The linear-time hierarchy of standard logics (a): LTL and its extension with quantification over atomic proposition, QPTL, and their counterparts FO[<] and the monadic second-order logic of one successor (S1S). The branching-time hierarchy of standard logics (b): CTL* and its extension with quantification over atomic propositions, QCTL*, and monadic path logic (MPL) and monadic second-order logic (MSO). The hierarchies of the corresponding hyperlogics (c and d).

atomic propositions, which, on trees, corresponds to full second-order quantification.

The hierarchy of hyperlogics provides interesting opportunities for knowledge reasoning research. The hierarchy can provide a frame of reference for the study of epistemic logics, which reason about the knowledge of agents in multi-agent systems. Consider for example the property "Agent A, who can observe the value of variable a, never knows the value of variable b". To express such a property, one needs to compare computation traces that are equivalent for agent A, it is, thus, a hyperproperty. A common epistemic specification language is LTL extended with the knowledge modality under perfect recall semantics (LTL$_K$). In terms of expressiveness, LTL$_K$ is incomparable to HyperLTL (Bozzelli, Maubert, and Pinchinat 2015). LTL$_K$ is, however, strictly subsumed by HyperQPTL (Rabe 2016), which can express all ω-regular properties. The exact position of LTL$_K$ in the hierarchy of hyperlogics is an open question.

Reasoning about knowledge is especially important in settings where information is distributed over multiple components of a system. In distributed architectures, for example, it is assumed that several processes receive different inputs from the environment and also share information with each other. Which outputs may depend on which inputs can be formalized as a hyperproperty in HyperLTL (Finkbeiner et al. 2020b). Hyperlogics can thus not only express functional correctness and information flow policies, but also describe the structure of the system itself. Similar properties are partial observation and fault tolerance (Finkbeiner et al. 2020b).

Another research opportunity afforded by the hierarchy of hyperlogics is that first-order and second-order reasoning methods become applicable to hyperproperties. There is a rich body of FO/SO reasoning methods, many of which developed for knowledge reasoning, which could be adapted to hyperproperties. Proof systems and tableau methods, for example, have been studied exhaustively for FO logics, but not yet been explored for hyperproperties. Generalizing these techniques to FO hyperlogics could lead to new decision procedures for interesting classes of hyperproperties and to the discovery of new decidable fragments of the hyperlogics.

References

Bonakdarpour, B., and Finkbeiner, B. 2019. Program repair for hyperproperties. In *Int. Symp. on Automated Technology for Verification and Analysis*.

Bozzelli, L.; Maubert, B.; and Pinchinat, S. 2015. Unifying hyper and epistemic temporal logics. In *Int. Conf. on Foundations of Software Science and Computation Structures*.

Clarkson, M. R., and Schneider, F. B. 2010. Hyperproperties. *Journal of Computer Security*.

Coenen, N.; Finkbeiner, B.; Hahn, C.; and Hofmann, J. 2019a. The hierarchy of hyperlogics. In *ACM/IEEE Symp. on Logic in Computer Science*.

Coenen, N.; Finkbeiner, B.; Sánchez, C.; and Tentrup, L. 2019b. Verifying hyperliveness. In *Int. Conf. on Computer-Aided Verification*.

Finkbeiner, B., and Zimmermann, M. 2017. The first-order logic of hyperproperties. In *Symp. on Theoretical Aspects of Computer Science*.

Finkbeiner, B.; Müller, C.; Seidl, H.; and Zalinescu, E. 2017. Verifying security policies in multi-agent workflows with loops. In *ACM Conf. on Computer and Communications Security*.

Finkbeiner, B.; Hahn, C.; Stenger, M.; and Tentrup, L. 2019. Monitoring hyperproperties. *Formal Methods Syst. Des.*

Finkbeiner, B.; Hahn, C.; Hofmann, J.; and Tentrup, L. 2020a. Realizing omega-regular hyperproperties. In *Int. Conf. on Computer-Aided Verification*.

Finkbeiner, B.; Hahn, C.; Lukert, P.; Stenger, M.; and Tentrup, L. 2020b. Synthesis from hyperproperties. *Acta Informatica*.

Finkbeiner, B.; Hahn, C.; and Torfah, H. 2018. Model checking quantitative hyperproperties. In *Int. Conf. on Computer-Aided Verification*.

Gabbay, D.; Pnueli, A.; Shelah, S.; and Stavi, J. 1980. On the temporal analysis of fairness. In *ACM SIGPLAN Symp. on Principles of Programming Languages*.

Goguen, J. A., and Meseguer, J. 1982. Security policies and security models. In *EEE Symp. on Security and Privacy*.

Grishchenko, I.; Maffei, M.; and Schneidewind, C. 2018. A semantic framework for the security analysis of ethereum smart contracts. In *Principles of Security and Trust*.

Hahn, C. 2019. Algorithms for monitoring hyperproperties. In *Int. Conf. on Runtime Verification*.

Kamp, H. W. 1968. *Tense Logic and the Theory of Linear Order*. Ph.D. Dissertation, University of California.

Nguyen, L. V.; Kapinski, J.; Jin, X.; Deshmukh, J. V.; and Johnson, T. T. 2017. Hyperproperties of real-valued signals. In *ACM-IEEE Int. Conf. on Formal Methods and Models for System Design*.

Rabe, M. N. 2016. *A Temporal Logic Approach to Information-Flow Control*. Ph.D. Dissertation, Saarland University.

Thomas, W. 2009. Path logics with synchronization. In *Perspectives in Concurrency Theory*.