Logics for Hyperproperties

Jana Hofmann
CISPA Helmholtz Center for Information Security

joint work with
Norine Coenen, Bernd Finkbeiner, Christopher Hahn and Leander Tentrup

“The Hierarchy of Hyperlogics”, LICS 2019
“Realizing $\omega$-regular Hyperproperties”, CAV 2020

IST Austria, 28 July 2020
Trace Properties vs Hyperproperties

System:

Trace property P?

System:

Hyperproperty H?

70bpm, 65bpm, ...
64bpm, 68bpm, ...
75bpm, 80bpm, ...

Illness!
Information Flow Security

Noninterference: “For any two traces, if they agree on the inputs, they must agree on the outputs.”

$$\forall t, t' \in T. \text{sameInputs}(t, t') \rightarrow \text{sameOutputs}(t, t')$$
Beyond Information Flow Control

Robustness properties: “similar inputs lead to similar outputs”

System properties:
- partial observation
- distributivity
- fault tolerance

… are expressible as hyperproperties

Distributivity:
“on all two traces, if P₁ receives the same inputs, it produces the same outputs”

Finkbeiner, Hahn, Lukert, Stenger, Tentrup
Acta Informatica, 2019
Outline

- model checking
- satisfiability
- synthesis

HyperQPTL

- uniform properties + \( \omega \)-regular properties

HyperLTL

- first-order hyperlogic FO[\(\lt, E\)]

- uniform properties

hierarchy of hyperlogics
HyperLTL

\[ \varphi ::= \exists \pi. \varphi \mid \forall \pi. \varphi \mid \psi \]
\[ \psi ::= a_\pi \mid \bigcirc \psi \mid \psi \bigcup \psi \mid \neg \psi \mid \psi \lor \psi \]

“All traces have the light on at the same time”:

\[ \forall \pi. \forall \pi'. \square (\text{on}_\pi \leftrightarrow \text{on}_{\pi'}) \]

Noninterference:

\[ \forall \pi. \forall \pi'. \square (\bigwedge_{i \in \text{inputs}} i_\pi \leftrightarrow i_{\pi'}) \rightarrow \square (\bigwedge_{o \in \text{outputs}} o_\pi \leftrightarrow o_{\pi'}) \]
HyperLTL Expressiveness

No $\omega$-regular properties

No uniform properties

Uniform Termination: “There is a global bound up to which the system terminates on all traces.”

Hyperlogics beyond HyperLTL?

Bozzelli, Maubert, Pinchinat
FoSSaCS, 2015
Outline

- HyperLTL
  - first-order hyperlogic
  - FO[<,E]
  - uniform properties
  - hierarchy of hyperlogics

HyperLTL
First-Order Hyperlogics

**FO[<,E]: First-Order Monadic Logic of Order with Equal-Level Predicate:**

\[
\begin{align*}
\text{atom} & ::= P(x) \mid x < y \mid E(x, y) \\
\varphi & ::= \text{atom} \mid \neg \varphi \mid \varphi_1 \lor \varphi_2 \mid \varphi_1 \land \varphi_2 \mid \exists x. \varphi \mid \forall x. \varphi
\end{align*}
\]

**Kamp’s Theorem:**

\[\text{LTL} \equiv \text{FO[<]}\]

\[\text{HyperLTL} < \text{FO[<,E]}\]

"All traces globally agree on a":

\[
\forall \pi, \forall \pi'. \quad \square (a_\pi \leftrightarrow a_{\pi'}) \quad \forall x, \forall y. \quad E(x, y) \rightarrow (P_a(x) \leftrightarrow P_a(y))
\]

Finkbeiner, Zimmermann

*STACS, 2017*
HyperLTL $< \text{FO}[^<,E]$}

FO[$<,E$] can express uniform properties:

\[ \exists b \forall x. \ E(x, b) \rightarrow P_{\text{halt}}(x) \]

\[ \forall x. \forall y. \ x < y \land P_{\text{halt}}(x) \rightarrow P_{\text{halt}}(y) \]

**Uniform Termination:** “There is a global bound up to which the system terminates on all traces.”
The Hierarchy of Hyperlogics

linear-time logics

- LTL ≡ FO[<]
- QPTL ≡ S1S

branching-time logics

- CTL* ≡ MPL
- QCTL* ≡ MSO

classic

- FO/SO logic
- temporal logic

hyper

- HyperQCTL*
- HyperQPTL
- HyperLTL
- S1S[E]
- FO[<,E]

- MPL[E]
- HyperCTL*
- HyperQCTL*
- MSO[E]
Omega-regularity

LTL cannot express $\omega$-regular properties

QPTL = LTL + propositional quantification

Counting properties: “On all even positions, a holds.”

$$\exists q. \ q \land \Box(q \leftrightarrow \bigcirc \neg q) \land \Box(q \rightarrow a)$$

HyperQPTL => QPTL instead of LTL?

$$\forall \pi \forall \pi'. \ \Box(\text{on}_\pi \leftrightarrow \text{on}'_\pi)$$

$\omega$-regular properties over n-tuples

We can do better!
HyperQPTL

HyperQPTL = HyperLTL + Propositional Quantification

\[
\varphi ::= \exists \pi \cdot \varphi \mid \forall \pi \cdot \varphi \mid \psi \mid \exists q \cdot \varphi \mid \forall q \cdot \varphi
\]

\[
\psi ::= a_\pi \mid \bigcirc \psi \mid \psi U \psi \mid \neg \psi \mid \psi \lor \psi \mid q
\]

Uniform Termination: “There is a global bound up to which the system terminates on all traces.”

\[
\exists q. \forall \pi. \text{once}(q) \land \Box (halt_\pi \land \diamond q)
\]
HyperQPTL Expressiveness

- Regular properties over n-tuples

Uniform hyperproperties: Uniform termination, promptness

Epistemic properties: HyperQPTL subsumes $\text{LTL}_K$

"An agent that can only observe low security variables can never infer the value of the secret"

$\Box \neg ((K_{\text{low}} \text{ sec}) \leftrightarrow \text{sec})$
HyperQPTL Model Checking

HyperQPTL Model Checking is decidable.

Idea: propositional sequences can be treated as normal traces by modifying the system

Space complexity: \(2^{2^{\phi}}\) number of quantifier alternations \(\exists \Rightarrow \forall / \forall \Rightarrow \exists\)

Uniform termination: 1 quantifier alternation

\[\exists q. \forall \pi. \text{once}(q) \land \Diamond (\text{halt}_\pi \land \Diamond q)\]

S1S[E]: model checking undecidable
HyperQPTL Satisfiability

∀∃ enough to encode
Post’s correspondence problem

Propositional quantifiers do not change decidability of the fragments

Uniform termination in decidable fragment
HyperQPTL Synthesis

No $\forall \pi$: decidable

One $\forall \pi: \exists^*_{q/\pi} \forall^*_{q/\pi} Q^*_q$ decidable

leading to undecidablity:

- $\forall \pi \exists \pi$ inherited from HyperLTL
- $\forall^*_{q/\pi} \exists^*_{q/\pi}$ can encode PCP (even though decidable in HyperLTL)

Two $\forall \pi$: linear fragment decidable

leading to undecidablity:

- information forks in distributed architectures (non-linear)

Propositional quantifiers do change decidability of the fragments

Uniform termination in decidable fragment

Finkbeiner, Hahn, Lukert, Stenger, Tentrup
Acta Informatica, 2019
Conclusion

First/second-order hyperlogics are more expressive than their temporal counterparts

Other FO/SO hyperlogics? Model Checking, SAT, …?

More expressiveness?

HyperQPTL can express $\omega$-regular, uniform, and epistemic properties

Decidable (MC/SAT/SYNT) fragments are expressive