Why do we need Second-Order Hyperlogics?

Hadar Frenkel

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

HYPER workshop
18 July @ CAV 2023
Second-Order Hyperproperties

Raven Beutner, Bernd Finkbeiner, Hadar Frenkel, and Niklas Metzger

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{raven.beutner, finkbeiner, hadar.frenkel, niklas.metzger}@cispa.de

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

Second-Order Hyperproperties. Beutner, Finkbeiner, F., Metzger (CAV 2023)
\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \bigcirc \psi \mid \psi \lor \psi \]

\[ \phi := \exists \pi \in X. \phi \mid \forall \pi \in X. \phi \mid \exists X. \phi \mid \forall X. \phi \]
Hyper²LTL

Why?

\[
\psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \lor \psi
\]

\[
\phi := \exists \pi \in X. \phi \mid \forall \pi \in X. \phi \mid \exists X. \phi \mid \forall X. \phi
\]

Generic reasoning and algorithms
Hyper²LTL

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

\[ \varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality

Generic reasoning and algorithms
Hyper$^2$LTL

\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \bigcirc \psi \mid \psi \cup \psi \]

\[ \varphi := \exists \pi. \varphi \mid \forall \pi. \varphi \]
Hyper$^2$LTL

$\psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \lor \psi$

$\phi := \exists \pi \in X. \phi \mid \forall \pi \in X. \phi \mid \exists X. \phi \mid \forall X. \phi$
Hyper²LTL

\[ \psi := a_\pi | \neg \psi | \psi \land \psi | \bigcirc \psi | \psi \cup \psi \]

\[ \varphi := \exists \pi \in X. \varphi | \forall \pi \in X. \varphi | \exists X. \varphi | \forall X. \varphi \]

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems

eventually knows \( r \)?
eventually \( r \)?
Communication in Multi-Agent Systems

Eventually knows r?

Eventually know r?

Eventually r?
Communication in Multi-Agent Systems

eventually knows $r$?

eventually common knowledge $\exists r$?

eventually know $r$?

eventually knows $r$?

eventually $r$?
Communication in Multi-Agent Systems

A trace property}

eventually \( r \) ?
Communication in Multi-Agent Systems

A hyperproperty

eventually knows $r$?
eventually $r$?
Communication in Multi-Agent Systems

A hyperproperty

eventually know \( r \)?

eventually knows \( r \)?

eventually \( r \)?
Communication in Multi-Agent Systems

A hyperproperty

- eventually know r?
- eventually knows r?
- eventually r?
Communication in Multi-Agent Systems

Eventually knows $r$?

Eventually common knowledge $r$?

Eventually know $r$?

Eventually $r$?
Communication in Multi-Agent Systems

Eventually knows $r$?

Eventually common knowledge $r$?

Simultaneous action

Consensus

Eventually know $r$?

Eventually knows $r$?

Eventually $r$?
Communication in Multi-Agent Systems

eventually common knowledge?

eventually know r?

eventually knows r?

eventually r?
Communication in Multi-Agent Systems

eventually common knowledge

eventually know r?

eventually knows r?

eventually r?
Communication in Multi-Agent Systems

eventually know $r$?
eventually knows $r$?
eventually $r$?
Temporal Epistemic Logics

- $\text{LTL}_{K,C}$
  LTL + (common) knowledge

- $\text{HyperCTL}^*_{lp}$
  HyperCTL$^*$ + knowledge

- MCK, MCMAS
  Model checking knowledge and time

The complexity of reasoning about knowledge and time. Halpern and Vardi (STOC 1986)
Unifying hyper and epistemic temporal logics. Bozzelli, Maubert, Pinchinat (FoSSaCS 2015)
MCK: model checking the logic of knowledge. Gammie, van der Meyden (CAV 2004)
$\psi := a_{\pi} \mid \neg \psi \mid \psi \land \psi \mid \Box \psi \mid \psi \lor \psi$

$\varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi$

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality
Hyper$^2$LTL

$\psi := a_\pi \mid \neg\psi \mid \psi \land \psi \mid \bigcirc\psi \mid \psi \lor \psi$

$\varphi := \exists \pi . \varphi \mid \forall \pi . \varphi$

$\exists \pi \forall \pi'. (\pi \equiv \pi') \rightarrow \lozenge (r_\pi \land r_{\pi'})$

eventually knows $r$?
Hyper²LTL

\[ \psi ::= a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \lor \psi \]

\[ \phi ::= \exists \pi. \phi \mid \forall \pi. \phi \]

\[ \Box \left( (ns_\pi \leftrightarrow ns_{\pi'}) \land (s_\pi \leftrightarrow s_{\pi'}) \right) \]

\[ \exists \pi \forall \pi'. (\pi \equiv \pi') \rightarrow \Diamond (r_\pi \land r_{\pi'}) \]

eventually knows \( r \)?
Hyper²LTL

\[ \psi := a_\pi | \neg \psi | \psi \land \psi | \bigcirc \psi | \psi \cup \psi \]

\[ \varphi := \exists \pi \in X . \varphi | \forall \pi \in X . \varphi | \exists X . \varphi | \forall X . \varphi \]

- trace-set variable
- \( \mathcal{G} \) — system traces
- \( \mathcal{U} \) — \( \Sigma^\omega \)
Hyper²LTL

\[ \psi ::= a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \lor \psi \]

\[ \varphi ::= \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

eventually common knowledge

r?
Hyper²LTL

\[ \psi ::= a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \lor \psi \]

\[ \varphi ::= \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

\[ \exists \pi. \exists X. \pi \in X \]

Eventually common knowledge \( r \)?
\textbf{Hyper}^2\text{LTL}

\[ \psi := a_\pi | \neg \psi | \psi \land \psi | \Box \psi | \psi \lor \psi \]

\[ \varphi := \exists \pi \in X. \varphi | \forall \pi \in X. \varphi | \exists X. \varphi | \forall X. \varphi \]

\[ \exists \pi. \exists X. \pi \in X \land \forall \pi \in X. \forall \pi' \in \mathcal{G}. (\pi \equiv \pi' \lor \pi \equiv \pi') \rightarrow \pi' \in X \]

Eventually common knowledge \( r \)?
Hyper²LTL

\[ \psi := a_{\pi} | \neg \psi | \psi \land \psi | \Diamond \psi | \psi \lor \psi \]

\[ \varphi := \exists \pi \in X. \varphi | \forall \pi \in X. \varphi | \exists X. \varphi | \forall X. \varphi \]

\[ \exists \pi. \exists X. \pi \in X \land \forall \pi \in X. \forall \pi' \in \mathcal{G}. (\pi \equiv \pi' \lor \pi \equiv \pi') \rightarrow \pi' \in X \]

\[ \forall \pi' \in X. \Diamond r_{\pi'} \]

eventually common knowledge \( r \) ?
Hyper$^2$LTL

\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Box \psi \mid \psi \lor \psi \]

\[ \varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality
Asynchronous Hyperproperties

Observational determinism

\[ \forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \square (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]
Asynchronous Hyperproperties

Observational determinism

\[ \forall \pi_1. \forall \pi_2. (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \square (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]

```
l := 0
if h then
  l := 1
else
  l := l + 1
```
Asynchronous Hyperproperties

Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```plaintext
l := 0
if h then
  l := 1
else
  l := l + 1

reg := l + 1
l := reg
```

States:

- 0 1
- 0 1
- 0 1 1
- 0 0 1

Asynchronous Hyperproperties

Observational determinism

\[ \forall \pi_1. \forall \pi_2. (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]

\begin{align*}
  l &:= 0 \\
  \text{if } h \text{ then} \\
  \quad l &:= 1 \\
  \text{else} \\
  \quad l &:= l + 1
\end{align*}

Access to shared resources

Scheduler decisions

Compiler optimizations
Asynchronous Hyperproperties

- HyperLTL$_S$
  HyperLTL + stuttering w.r.t a set of LTL formulas

- AHLTL
  HyperLTL + trajectories

- $H_\mu$
  fixpoint-based logic

Asynchronous extensions of HyperLTL. Bozzelli, Peron, Sánchez (LICS 2021)
A temporal logic for asynchronous hyperproperties. Baumeister, Coenen, Bonakdarpour, Finkbeiner, Sánchez (CAV 2021)
Automata and fixpoints for asynchronous hyperproperties. Gutsfeld, Müller-Olm, Ohrem (POPL 2021)
Asynchronous Hyperproperties

Observational determinism

\[ \forall \pi_1 \cdot \forall \pi_2 \cdot (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]
Asynchronous Hyperproperties

Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

$$\forall \pi_i . \exists X_i . \pi_i \in X_i$$

$X_i$ — all stutter-equivalent traces to $\pi_i$
Asynchronous Hyperproperties

Observational determinism

\[ \forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]

\[ \forall \pi_i . \exists X_i . \pi_i \in X_i \]

\[ \forall \pi \in X_i . \forall \pi' \in \mathcal{U} . (\pi =_{AP} \pi') \cup \]

\[ (\pi =_{AP} \pi' \land \Box \bigwedge_{a \in \mathcal{AP}} a_{\pi} \leftrightarrow \Diamond a_{\pi'}) \rightarrow \pi' \in X \]
Asynchronous Hyperproperties

Observational determinism
\[ \forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]

\[ l := 0 \quad \rightarrow \quad 0 \quad 1 \]
\[ \text{if } h \text{ then} \]
\[ l := 1 \quad \rightarrow \quad 0 \quad 1 \]
\[ \text{else} \]
\[ l := l + 1 \]

\[ \forall \pi_i . \exists X_i . \pi_i \in X_i \]

\[ X_i \] — all stutter-equivalent traces to \( \pi_i \)

\[ \exists \pi_1 \in X_1 . \exists \pi_2 \in X_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2}) \]

\[ l := 0 \quad \rightarrow \quad 0 \quad 1 \quad 1 \]
\[ \text{if } h \text{ then} \]
\[ l := 1 \quad \rightarrow \quad 0 \quad 0 \quad 1 \]
\[ \text{else} \]
\[ \text{reg := } l + 1 \]
\[ l := \text{reg} \]
Hyper\(^2\)LTL

\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \square \psi \mid \psi \lor \psi \]

\[ \phi := \exists \pi \in \mathbb{X}. \phi \mid \forall \pi \in \mathbb{X}. \phi \mid \exists \mathbb{X}. \phi \mid \forall \mathbb{X}. \phi \]

Generic reasoning
Hyper\textsuperscript{2}LTL

\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \Diamond \psi \mid \psi \cup \psi \]

\[ \varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality

trace property = set of traces

Generic reasoning
Hyper²LTL

\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \bigcirc \psi \mid \psi \cup \psi \]

\[ \varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi \]

- Common Knowledge
- Asynchronous Hyperproperties
- Trace Theory
- Causality

Generic reasoning and algorithms
Model Checking Hyper\(^2\)LTL\(_{fp}\)

\[ \varphi = \exists \pi_1 \cdot \forall X_1 \cdot \forall \pi_2 \in X_1 \ldots \exists X_k \cdot \exists \pi_k \in X_k \cdot \psi \]

Interpreted over general set assignments
Model Checking Hyper$^2$LTL$^{fp}$

Friday afternoon
@CAV

$\varphi = \exists \pi_1 . \forall X_1 . \forall \pi_2 \in X_1 . \ldots \exists X_k . \exists \pi_k \in X_k . \psi$

under some conditions

under some conditions
Model Checking Hyper²LTL_{fp}

\[ \varphi = \exists \pi_1 \cdot \forall X_1 \cdot \forall \pi_2 \in X_1 \cdot \ldots \exists X_k \cdot \exists \pi_k \in X_k \cdot \psi \]

under some conditions

under some conditions
Why do we need Second-Order Hyperlogics?
Why do we need Second-Order Hyperlogics?

Hyper\(^2\)LTL

\[\psi := a_\pi | \neg \psi | \psi \land \psi | \diamond \psi | \psi \lor \psi\]

\[\varphi := \exists \pi . \varphi | \forall \pi . \varphi | \exists X . \varphi | \forall X . \varphi\]

Trace properties

First-order Hyperproperties

Common knowledge

Information-flow

Causality

Knowledge

Asynchronous properties

Second-order Hyperproperties

\[\vdash \psi\]
Why do we need Second-Order Hyperlogics?

Thank you!