Second-Order Hyperproperties

Raven Beutner, Bernd Finkbeiner, Hadar Frenkel, Niklas Metzger

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

21 July @ CAV 2023
Overview

Hyper\(^{2}\)LTL

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

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

Model checking

Trace theory

Asynchronous Hyperproperties

Common knowledge
Hyper$^2$LTL

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

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

Second-order logic
for the specification of
Hyperproperties
Hyperproperties

Knowledge

Fairness

Information-flow

Robustness

Hyperproperties. Clarkson and Schneider (CSF 2008)
\[ \psi := a_\pi \mid \neg \psi \mid \psi \land \psi \mid \bigcirc \psi \mid \psi \cup \psi \]

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

*trace variable*

**HyperLTL**

HyperLTL

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

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

Common Knowledge

HyperLTL

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

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

Common Knowledge

Communication in Multi-Agent Systems
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems

[Diagram of communication in multi-agent systems]
Communication in Multi-Agent Systems

Eventually $r$?
Communication in Multi-Agent Systems

![Diagram of communication in multi-agent systems](image)

Trace property (LTL)

eventually $r$?
Communication in Multi-Agent Systems

Hyperproperty

eventually knows $r$?
HyperLTL

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

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

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

Hyperproperty

eventually knows \( r \)?
HyperLTL

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

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

\[
\square (ns_\pi \leftrightarrow ns_{\pi'}) \land (s_\pi \leftrightarrow s_{\pi'})
\]

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

Hyperproperty

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

Hyperproperty

eventually know $r$?

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

Hyperproperty

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

Eventually common knowledge?

nr ns nr ns nr ns nr ns
ns ns ns ns ns ns r r
ns ns ns ns ns w r r
ns ns ns ns ns r r

eventually common knowledge 🤖 r?
Common Knowledge

\[ \varphi \text{ common knowledge} \iff (\text{know})^\omega \varphi \]

eventually common knowledge
**Common Knowledge**

\[ \phi \text{ common knowledge} \iff (\text{know})^\omega \phi \]

- Eventually common knowledge?
  - First-order trace quantification is not enough.
Communication in Multi-Agent Systems

Eventually common knowledge

Second-order quantification

Eventually common knowledge?
Communication in Multi-Agent Systems

Eventually common knowledge?

Second-order quantification
Communication in Multi-Agent Systems
Communication in Multi-Agent Systems

Eventually common knowledge

Second-order quantification

 Eventually common knowledge 🤔
Communication in Multi-Agent Systems

Eventually common knowledge

Second-order quantification

Eventually common knowledge $r$?
Hyper²LTL

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

$$\varphi := \exists \pi \in X. \varphi \mid \forall \pi \in X. \varphi \mid \exists X. \varphi \mid \forall X. \varphi$$
Hyper$^2$LTL

\[ \psi := a_{\pi} \mid \neg \psi \mid \psi \land \psi \mid \square \psi \mid \psi \cup \psi \]

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

trace-set variable
Hyper\textsuperscript{2}LTL

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

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

- trace-set variable
- $\mathcal{G} \quad \text{system traces}$
- $\mathcal{U} \quad \Sigma^\omega$
Hyperl²LTL

ψ := a_π | ¬ψ | ψ ∧ ψ | ◯ψ | ψ U ψ

φ := ∃π ∈ X. φ | ∀π ∈ X. φ | ∃X. φ | ∀X. φ

∃π. ∃X. π ∈ X
Hyper²LTL

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

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

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

If \( \pi' \) is indistinguishable from some \( \pi \) in \( X \) then \( \pi' \) is also in \( X \)
Hyper²LTL

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

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

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

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

If \( \pi' \) is indistinguishable from some \( \pi \) in \( X \) then \( \pi' \) is also in \( X \)
Hyper\textsuperscript{2}LTL

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

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

Trace theory
Asynchronous Hyperproperties
Common knowledge

Model Checking
Undecidable
Hyper\textsuperscript{2}LTL

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

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

- Trace theory
- Asynchronous Hyperproperties
- Common knowledge

Model Checking
Undecidable

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

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

If \( \pi' \) is indistinguishable from some \( \pi \) in \( X \) then \( \pi' \) is also in \( X \)
Hyper²LTL
Unique Least Fixpoints

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

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

If \( \pi' \) is indistinguishable from some \( \pi \) in \( X \) then \( \pi' \) is also in \( X \)
Hyper²LTL

Unique Least Fixpoints

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

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

If \( \pi' \) is indistinguishable from some \( \pi \) in \( X \) then \( \pi' \) is also in \( X \)
Model Checking Hyper²LTL

Unique Least Fixpoints

\[ \varphi = \exists \pi_1 . X_1 . \forall \pi_2 \in X_1 . \ldots . X_k . \exists \pi_{k+1} \in X_k . \psi \]
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

$$\varphi = \exists \pi_1 \cdot X_1 \cdot \forall \pi_2 \in X_1 \cdot \ldots \cdot X_k \cdot \exists \pi_{k+1} \in X_k \cdot \psi$$

Automaton $A_1$
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

$\varphi = \exists \pi_1 \cdot X_1 \cdot \forall \pi_2 \in X_1 \cdot \ldots \cdot X_k \cdot \exists \pi_{k+1} \in X_k \cdot \psi$

Automaton $A_1$

Automaton $A_k$

$A_1 \times A_2 \times \ldots \times A_k \models \psi$

HyperLTL model checking

*Algorithms for Model Checking HyperLTL and HyperCTL*+. Finkbeiner, Rabe, Sánchez (CAV 2015)
Model Checking Hyper\(^2\)LTL

Unique Least Fixpoints

\[ \varphi = \exists \pi_1 \cdot X_1 \cdot \forall \pi_2 \in X_1 \cdot \ldots \cdot X_k \cdot \exists \pi_{k+1} \in X_k \cdot \psi \]
Model Checking Hyper²LTL

Unique Least Fixpoints

\[ \varphi = \exists \pi_1 . X_1 . \forall \pi_2 \in X_1 . \ldots . X_k . \exists \pi_{k+1} \in X_k . \psi \]
Model Checking Hyper\(^2\)LTL

Unique Least Fixpoints

\[ \varphi = \exists \pi_1 . X_1 . \forall \pi_2 \in X_1 . \ldots . X_k . \exists \pi_{k+1} \in X_k . \psi \]

\[ A_1^\forall \times A_1^\exists \times A_2^\forall \times A_2^\exists \times \ldots \times A_k^\forall \times A_k^\exists \begin{array}{c} \vdash \psi \end{array} \]
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

compute approximations

$A_1^\forall \times A_1^\exists \times \cdots \times A_k^\forall \models \psi$

HyperLTL model checking

Algorithms for Model Checking HyperLTL and HyperCTL*. Finkbeiner, Rabe, Sánchez (CAV 2015)
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

compute approximations

$A_1^\forall$
$A_1$
$A_1^\exists$
$A_2^\forall$
$A_2$
$A_2^\exists$
$\cdots$
$A_k^\forall$
$A_k$
$A_k^\exists$

$\models \psi$

$V$ done!

HyperLTL model checking

*Algorithms for Model Checking HyperLTL and HyperCTL*. Finkbeiner, Rabe, Sánchez (CAV 2015)
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

compute approximations

$\forall k A_1 \times A_2 \times \cdots \models \neg \psi$

HyperLTL model checking

Algorithms for Model Checking HyperLTL and HyperCTL*. Finkbeiner, Rabe, Sánchez (CAV 2015)
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

compute second approximations

compute approximations

$\forall 1 \ A \ ∀ 2 \ A \ ∀ k \ A \ ∀ 1 \ A \ ∀ 2 \ A \ ∀ k \ A$

$x$ refine

$\models \neg \psi$

$\models \psi$
Model Checking Hyper$^2$LTL

Unique Least Fixpoints

\[ \varphi = \exists \pi_1 \cdot (X_1, \forall \varphi_1) \cdot \forall \pi_2 \in X_1 \cdot \ldots \cdot (X_k, \forall \varphi_k) \cdot \exists \pi_{k+1} \in X_k \cdot \psi \]
Implementation
## Implementation

### Asynchronous Hyperproperties

<table>
<thead>
<tr>
<th>Instance</th>
<th>Method</th>
<th>Res</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{T}<em>{\text{syn}}, \varphi</em>{OD}$</td>
<td>-</td>
<td>✓</td>
<td>0.26</td>
</tr>
<tr>
<td>$\mathcal{T}<em>{\text{async}}, \varphi</em>{OD}$</td>
<td>-</td>
<td>x</td>
<td>0.31</td>
</tr>
<tr>
<td>$\mathcal{T}<em>{\text{syn}}, \varphi</em>{OD}^{\text{async}}$</td>
<td>Iter (0)</td>
<td>✓</td>
<td>0.50</td>
</tr>
<tr>
<td>$\mathcal{T}<em>{\text{async}}, \varphi</em>{OD}^{\text{async}}$</td>
<td>Iter (1)</td>
<td>✓</td>
<td>0.78</td>
</tr>
<tr>
<td>$Q_{1}, \varphi_{OD}$</td>
<td>-</td>
<td>x</td>
<td>0.34</td>
</tr>
<tr>
<td>$Q_{1}, \varphi_{OD}^{\text{async}}$</td>
<td>Iter (1)</td>
<td>✓</td>
<td>0.86</td>
</tr>
</tbody>
</table>

### Common Knowledge

<table>
<thead>
<tr>
<th>$n$</th>
<th>Method</th>
<th>Res</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Iter (1)</td>
<td>✓</td>
<td>0.51</td>
</tr>
<tr>
<td>2</td>
<td>Iter (3)</td>
<td>✓</td>
<td>0.83</td>
</tr>
<tr>
<td>3</td>
<td>Iter (5)</td>
<td>✓</td>
<td>1.20</td>
</tr>
<tr>
<td>10</td>
<td>Iter (19)</td>
<td>✓</td>
<td>3.81</td>
</tr>
<tr>
<td>100</td>
<td>Iter (199)</td>
<td>✓</td>
<td>102.8</td>
</tr>
</tbody>
</table>

### Mazurkiewicz Traces

<table>
<thead>
<tr>
<th>Instance</th>
<th>Method</th>
<th>Res</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWAPA</td>
<td>Learn</td>
<td>✓</td>
<td>1.07</td>
</tr>
<tr>
<td>SWAPATWICE</td>
<td>Learn</td>
<td>✓</td>
<td>2.13</td>
</tr>
<tr>
<td>SWAPA$_5$</td>
<td>Iter (5)</td>
<td>✓</td>
<td>1.15</td>
</tr>
<tr>
<td>SWAPA$_{15}$</td>
<td>Iter (15)</td>
<td>✓</td>
<td>3.04</td>
</tr>
<tr>
<td>SWAPAVIOLATION$_5$</td>
<td>Iter (5)</td>
<td>x</td>
<td>2.35</td>
</tr>
<tr>
<td>SWAPAVIOLATION$_{15}$</td>
<td>Iter (15)</td>
<td>x</td>
<td>4.21</td>
</tr>
</tbody>
</table>

---

### Automata learning

- $A_1^\forall$
- $A_1$
- $A_2^\exists$

### Iteration

- $A_1$
- $A_2$
Hyper\textsuperscript{2}LTL

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

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

Generic reasoning and algorithms
Hyper$^2$LTL

$\psi := a \pi | \neg \psi | \psi \land \psi | \Box \psi | \psi \cup \psi$

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

Thank you!

Generic reasoning and algorithms