The First-Order Logic of Hyperproperties

Joint work with Bernd Finkbeiner (Saarland University)

Martin Zimmermann

Saarland University

March, 9th 2017

STACS 2017, Hannover, Germany
The system $S$ is input-deterministic: for all traces $t, t'$ of $S$, $t = I \iff t' = \Phi$.

Noninterference: for all traces $t, t'$ of $S$, $t = I \iff t' = \Phi_{public}$.
The system $S$ is input-deterministic: for all traces $t, t'$ of $S$

$t =_I t'$ implies $t =_O t'$
Hyperproperties

The system $S$ is input-deterministic: for all traces $t, t'$ of $S$

$$t =_I t' \quad \text{implies} \quad t =_O t'$$

Noninterference: for all traces $t, t'$ of $S$

$$t =_{I_{\text{public}}} t' \quad \text{implies} \quad t =_{O_{\text{public}}} t'$$
Both properties are not trace properties, but hyperproperties, i.e., sets of sets of traces.

A system $S$ satisfies a hyperproperty $H$, if $\text{Traces}(S) \in H$.

Many information flow properties can be expressed as hyperproperties.
Hyperproperties

- Both properties are not trace properties, but hyperproperties, i.e., sets of sets of traces.
- A system $S$ satisfies a hyperproperty $H$, if $\text{Traces}(S) \in H$.
- Many information flow properties can be expressed as hyperproperties.

Specification languages for hyperproperties [Clarkson et al. ’14]

HyperLTL: Extend LTL by trace quantifiers.
HyperCTL*: Extend CTL* by trace quantifiers.
HyperLTL

HyperLTL = LTL +

\[ \psi ::= a \mid \neg \psi \mid \psi \lor \psi \mid X \psi \mid \psi U \psi \]

where \( a \in AP \) (atomic propositions)
HyperLTL

HyperLTL = LTL + trace quantification

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

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

where \( a \in AP \) (atomic propositions) and \( \pi \in V \) (trace variables).
HyperLTL

HyperLTL = LTL + trace quantification

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

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

where \( a \in AP \) (atomic propositions) and \( \pi \in \mathcal{V} \) (trace variables).

**Shortcuts as usual:**

- \( F \psi = \text{true} U \psi \)
- \( G \psi = \neg F \neg \psi \)
Semantics

\[ \varphi = \forall \pi. \forall \pi'. \text{G on}_\pi \leftrightarrow \text{on}_\pi' \]

\( T \subseteq (2^{AP})^\omega \) is a model of \( \varphi \) iff
\[ \varphi = \forall \pi. \forall \pi'. G \text{ on}_\pi \leftrightarrow \text{ on}_{\pi'} \]

\( T \subseteq (2^{AP})^\omega \) is a model of \( \varphi \) iff

\[ \{ \} \models \forall \pi. \forall \pi'. G \text{ on}_\pi \leftrightarrow \text{ on}_{\pi'} \]
Semantics

\[ \varphi = \forall \pi. \forall \pi'. \mathsf{G} \text{ on}_\pi \leftrightarrow \text{on}_\pi' \]

\( T \subseteq (2^{2^\mathsf{AP}})^\omega \) is a model of \( \varphi \) iff

\[ \{\} \models \forall \pi. \forall \pi'. \mathsf{G} \text{ on}_\pi \leftrightarrow \text{on}_\pi' \]

\[ \{\pi \mapsto t\} \models \forall \pi'. \mathsf{G} \text{ on}_\pi \leftrightarrow \text{on}_\pi' \quad \text{for all } t \in T \]
\[ \varphi = \forall \pi. \forall \pi'. \mathbf{G} \text{on}_\pi \leftrightarrow \text{on}_{\pi'} \]

\( T \subseteq (2^{\mathbf{AP}})^\omega \) is a model of \( \varphi \) iff

\[
\{ \} \models \forall \pi. \forall \pi'. \mathbf{G} \text{on}_\pi \leftrightarrow \text{on}_{\pi'}
\]

\[
\{ \pi \mapsto t \} \models \forall \pi'. \mathbf{G} \text{on}_\pi \leftrightarrow \text{on}_{\pi'} \quad \text{for all } t \in T
\]

\[
\{ \pi \mapsto t, \pi' \mapsto t' \} \models \mathbf{G} \text{on}_\pi \leftrightarrow \text{on}_{\pi'} \quad \text{for all } t' \in T
\]
\[ \varphi = \forall \pi. \forall \pi'. \text{G on}_\pi \leftrightarrow \text{on}_\pi' \]

\( T \subseteq (2^{AP})^\omega \) is a model of \( \varphi \) iff

\[ \{ \} \models \forall \pi. \forall \pi'. \text{G on}_\pi \leftrightarrow \text{on}_\pi' \]

\[ \{ \pi \mapsto t \} \models \forall \pi'. \text{G on}_\pi \leftrightarrow \text{on}_\pi' \quad \text{for all } t \in T \]

\[ \{ \pi \mapsto t, \pi' \mapsto t' \} \models \text{G on}_\pi \leftrightarrow \text{on}_\pi' \quad \text{for all } t' \in T \]

\[ \{ \pi \mapsto t[n, \infty), \pi' \mapsto t'[n, \infty) \} \models \text{on}_\pi \leftrightarrow \text{on}_\pi' \quad \text{for all } n \in \mathbb{N} \]
Semantics

\[ \varphi = \forall \pi. \forall \pi'. G_{on_\pi} \leftrightarrow on_{\pi'} \]

\( T \subseteq (2^{AP})^\omega \) is a model of \( \varphi \) iff

\[ \{ \} \models \forall \pi. \forall \pi'. G_{on_\pi} \leftrightarrow on_{\pi'} \]

\[ \{ \pi \mapsto t \} \models \forall \pi'. G_{on_\pi} \leftrightarrow on_{\pi'} \quad \text{for all } t \in T \]

\[ \{ \pi \mapsto t, \pi' \mapsto t' \} \models G_{on_\pi} \leftrightarrow on_{\pi'} \quad \text{for all } t' \in T \]

\[ \{ \pi \mapsto t[n, \infty), \pi' \mapsto t'[n, \infty) \} \models on_\pi \leftrightarrow on_{\pi'} \quad \text{for all } n \in \mathbb{N} \]

\[ on \in t(n) \leftrightarrow on \in t'(n) \]
LTL vs. HyperLTL

LTL has many desirables properties.

1. Every satisfiable LTL formula is satisfied by an ultimately periodic trace, i.e., by a finite and finitely-represented model.
2. LTL and FO[<] are expressively equivalent.
3. LTL satisfiability and model-checking are \text{PSPACE}-complete.

Only partial results for HyperLTL.

3a. HyperLTL satisfiability [F. & Hahn '16]: alternation-free: \text{PSPACE}-complete
   \exists \ast \forall \ast: \text{ExpSpace}-complete
   \forall \ast \exists \ast: \text{undecidable}

3b. HyperLTL model-checking is decidable [F. et al. '15].
LTL vs. HyperLTL

LTL has many desirables properties.

1. Every satisfiable LTL formula is satisfied by an ultimately periodic trace, i.e., by a finite and finitely-represented model.
2. LTL and $\text{FO}[^<]$ are expressively equivalent.
3. LTL satisfiability and model-checking are $\text{PSPACE}$-complete.

Only partial results for HyperLTL.

3a. HyperLTL satisfiability [F. & Hahn ’16]:
   - alternation-free: $\text{PSPACE}$-complete
   - $\exists^*\forall^*$: $\text{EXPSPACE}$-complete
   - $\forall^*\exists^*$: undecidable

3b. HyperLTL model-checking is decidable [F. et al. ’15].
The Models of HyperLTL
What about Finite Models?

Fix $\text{AP} = \{a\}$ and consider the conjunction $\varphi$ of

$\forall \pi. (\neg a_\pi) \mathbf{U} (a_\pi \land \mathbf{X} \mathbf{G} \neg a_\pi)$
What about Finite Models?

Fix $\text{AP} = \{a\}$ and consider the conjunction $\varphi$ of

- $\forall \pi. (\neg a_\pi) \mathbin{U} (a_\pi \land X G \neg a_\pi)$
- $\exists \pi. a_\pi$
What about Finite Models?

Fix $\text{AP} = \{a\}$ and consider the conjunction $\varphi$ of

- $\forall \pi. (\neg a_\pi) \cup (a_\pi \land \mathbf{X} \mathbf{G} \neg a_\pi)$
- $\exists \pi. a_\pi$

\[
\begin{align*}
\{a\} & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \emptyset & \quad \ldots
\end{align*}
\]
What about Finite Models?

Fix $\text{AP} = \{a\}$ and consider the conjunction $\varphi$ of

- $\forall \pi. \ (\neg a_\pi) \ U \ (a_\pi \land X G \neg a_\pi)$
- $\exists \pi. \ a_\pi$
- $\forall \pi. \exists \pi'. \ F \ (a_\pi \land X a_{\pi'})$

\[
\{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \cdots
\]
What about Finite Models?

Fix $AP = \{a\}$ and consider the conjunction $\varphi$ of

- $\forall \pi. (\neg a_\pi) \mathbf{U} (a_\pi \land X G \neg a_\pi)$
- $\exists \pi. a_\pi$
- $\forall \pi. \exists \pi'. F (a_\pi \land X a_{\pi'})$

\[
\begin{array}{cccccccccc}
\{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\
\emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\
\ldots & & & & & & & & & \\
\end{array}
\]
What about Finite Models?

Fix \( AP = \{a\} \) and consider the conjunction \( \varphi \) of

- \( \forall \pi. (\neg a_\pi) \cup (a_\pi \land X G \neg a_\pi) \)
- \( \exists \pi. a_\pi \)
- \( \forall \pi. \exists \pi'. F (a_\pi \land X a_{\pi'}) \)

\[
{\{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \ldots \}
\]
\[
{\emptyset \quad \{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \ldots \}
\]
\[
{\emptyset \quad \emptyset \quad \{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \ldots \}
\]
\[
{\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \ldots \}
\]

The unique model of \( \varphi \) is \( \{\emptyset^n \{a\} \emptyset^\omega \mid n \in \mathbb{N}\} \).
What about Finite Models?

Fix $AP = \{a\}$ and consider the conjunction $\varphi$ of

- $\forall \pi. (\neg a_{\pi}) \mathsf{U} (a_{\pi} \land X G \neg a_{\pi})$
- $\exists \pi. a_{\pi}$
- $\forall \pi. \exists \pi'. F (a_{\pi} \land X a_{\pi'})$

The unique model of $\varphi$ is $\{\emptyset^n \{a\} \emptyset^\omega | n \in \mathbb{N}\}$.

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any finite set of traces.*
What about Countable Models?

**Theorem**

*Every satisfiable HyperLTL sentence has a countable model.*
What about Countable Models?

**Theorem**

*Every satisfiable HyperLTL sentence has a countable model.*

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any ω-regular set of traces.*
What about Countable Models?

**Theorem**

*Every satisfiable HyperLTL sentence has a countable model.*

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any $\omega$-regular set of traces.*

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any set of traces that contains an ultimately periodic trace.*
What about Countable Models?

**Theorem**

*Every satisfiable HyperLTL sentence has a countable model.*

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any $\omega$-regular set of traces.*

**Theorem**

*There is a satisfiable HyperLTL sentence that is not satisfied by any set of traces that contains an ultimately periodic trace.*

One can even encode the prime numbers in HyperLTL!
First-order Logic for Hyperproperties
First-order Logic vs. LTL

\[ \text{FO}[\prec]: \text{first-order order logic over signature } \{\prec\} \cup \{P_a \mid a \in \text{AP}\} \]
over structures with universe \( \mathbb{N} \).

**Theorem (Kamp '68, Gabbay et al. '80)**

\( \text{LTL and FO}[\prec] \) are expressively equivalent.
First-order Logic vs. LTL

FO[<]: first-order order logic over signature \{<\} \cup \{P_a \mid a \in AP\} over structures with universe \mathbb{N}.

Theorem (Kamp ’68, Gabbay et al. ’80)
\(LTL \text{ and } FO[<] \text{ are expressively equivalent.}\)

Example

\[
\forall x (P_q(x) \land \lnot P_p(x)) \rightarrow \exists y (x < y \land P_p(y))
\]

and

\[
G (q \rightarrow F p)
\]

are equivalent.
First-order Logic for Hyperproperties

\[ \mathbb{N} \]

\[ \cdots \]
First-order Logic for Hyperproperties

\[ T \subseteq \mathbb{N} \]

\[
\begin{array}{ccccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{array}
\]
First-order Logic for Hyperproperties

\[ \text{T}\{ \ldots \} \quad \downarrow \quad E \quad \downarrow \quad < \quad \uparrow \quad \mathbb{N} \quad \uparrow \quad \ldots \]
First-order Logic for Hyperproperties

\[ \text{FO}[<, E]: \text{first-order logic with equality over the signature } \{<, E\} \cup \{P_a \mid a \in \text{AP}\} \text{ over structures with universe } T \times \mathbb{N}. \]

**Example**

\[ \forall x \forall x' \ E(x, x') \rightarrow (P_{on}(x) \leftrightarrow P_{on}(x')) \]
First-order Logic for Hyperproperties

- $\text{FO}[<, E]$: first-order logic with equality over the signature $\{<, E\} \cup \{P_a \mid a \in \text{AP}\}$ over structures with universe $T \times \mathbb{N}$.

**Proposition**

*For every HyperLTL sentence there is an equivalent $\text{FO}[<, E]$ sentence.*
Let $\varphi$ be the following property of sets $T \subseteq (2\{p\})^\omega$:

There is an $n$ such that $p \notin t(n)$ for every $t \in T$.

**Theorem (Bozzelli et al. ’15)**

$\varphi$ is not expressible in HyperLTL.
A Setback

Let $\varphi$ be the following property of sets $T \subseteq (2^\{p\})^\omega$:

There is an $n$ such that $p \notin t(n)$ for every $t \in T$.

**Theorem (Bozzelli et al. ’15)**

$\varphi$ is not expressible in HyperLTL.

But, $\varphi$ is easily expressible in FO[$<, E$]:

$$\exists x \forall y E(x, y) \rightarrow \neg p$$

**Corollary**

$FO[<, E]$ strictly subsumes HyperLTL.
HyperFO

- $\exists^M x$ and $\forall^M x$: quantifiers restricted to initial positions.
- $\exists^G y \geq x$ and $\forall^G y \geq x$: if $x$ is initial, then quantifiers restricted to positions on the same trace as $x$. 
HyperFO

- $\exists^M x$ and $\forall^M x$: quantifiers restricted to initial positions.
- $\exists^G y \geq x$ and $\forall^G y \geq x$: if $x$ is initial, then quantifiers restricted to positions on the same trace as $x$.

HyperFO: sentences of the form

$$\varphi = Q_1^M x_1 \cdots Q_k^M x_k \cdot Q_1^G y_1 \geq x_{g_1} \cdots Q_\ell^G y_\ell \geq x_{g_\ell} \cdot \psi$$

- $Q \in \{\exists, \forall\}$,
- $\{x_1, \ldots, x_k\}$ and $\{y_1, \ldots, y_\ell\}$ are disjoint,
- every guard $x_{g_j}$ is in $\{x_1, \ldots, x_k\}$, and
- $\psi$ is quantifier-free over signature $\{<, E\} \cup \{P_a \mid a \in AP\}$ with free variables in $\{y_1, \ldots, y_\ell\}$.
Equivalence

Theorem

HyperLTL and HyperFO are equally expressive.
Equivalence

Theorem

HyperLTL and HyperFO are equally expressive.

Proof

- From HyperLTL to HyperFO: structural induction.
- From HyperFO to HyperLTL: reduction to Kamp’s theorem.
Conclusion

Our Results

- The models of HyperLTL are rather not well-behaved, i.e., in general (countably) infinite, non-regular, and non-periodic.
- FO[$<, E$] is strictly more expressive than HyperLTL.
- HyperFO is expressively equivalent to HyperLTL.
Conclusion

Our Results

- The models of HyperLTL are rather not well-behaved, i.e., in general (countably) infinite, non-regular, and non-periodic.
- $\text{FO}[<, E]$ is strictly more expressive than HyperLTL.
- HyperFO is expressively equivalent to HyperLTL.

Open Problems

- Is there a class of languages $\mathcal{L}$ such that every satisfiable HyperLTL sentence has a model from $\mathcal{L}$?
- Is there a temporal logic that is expressively equivalent to $\text{FO}[<, E]$?
- What about HyperCTL*?