The First-Order Logic of Hyperproperties

Joint work with Bernd Finkbeiner (Saarland University)

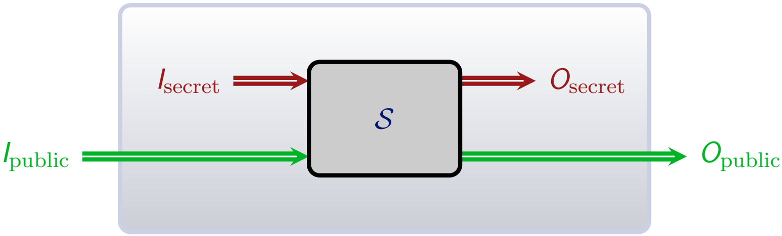
Martin Zimmermann

Saarland University

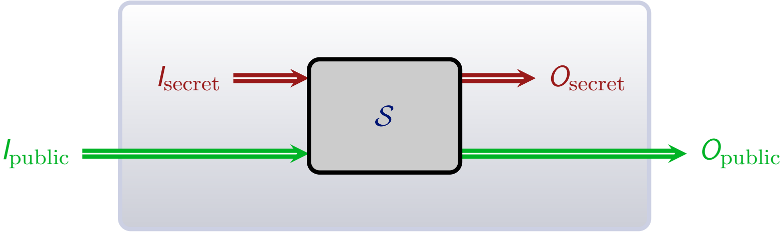
March, 9th 2017

STACS 2017, Hannover, Germany

Hyperproperties



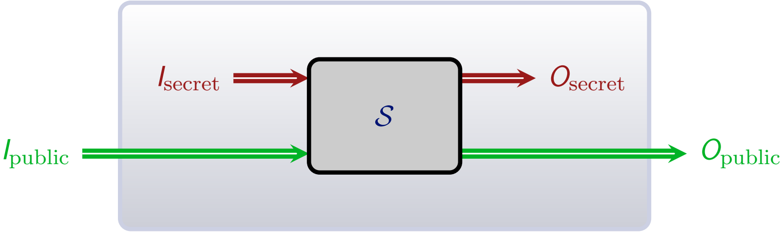
Hyperproperties



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

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

Hyperproperties



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

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

- Noninterference: for all traces t, t' of $\mathcal{S}$

$$t =_{I_{\mathrm{public}}} t' \quad \text{implies} \quad t =_{O_{\mathrm{public}}} t'$$

Hyperproperties

- Both properties are not trace properties, but hyperproperties, i.e., sets of sets of traces.
- A system $\mathcal{S}$ satisfies a hyperproperty H, if $\mathrm{Traces}(\mathcal{S}) \in H$.
- 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 $\mathcal{S}$ satisfies a hyperproperty H, if $\mathrm{Traces}(\mathcal{S}) \in H$.
- 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 +

$$\psi ::= a \quad | \neg\psi \mid \psi \vee \psi \mid \mathbf{X}\,\psi \mid \psi\,\mathbf{U}\,\psi$$

where $a \in \mathrm{AP}$ (atomic propositions)

HyperLTL

HyperLTL = LTL + trace quantification

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

$$\psi ::= a_\pi \mid \neg\psi \mid \psi \vee \psi \mid \mathbf{X}\,\psi \mid \psi\,\mathbf{U}\,\psi$$

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

HyperLTL

HyperLTL = LTL + trace quantification

$$\varphi ::= \exists \pi.\ \varphi \mid \forall \pi.\ \varphi \mid \psi$$
$$\psi ::= a_\pi \mid \neg\psi \mid \psi \vee \psi \mid \mathbf{X}\,\psi \mid \psi\,\mathbf{U}\,\psi$$

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

Shortcuts as usual:

- $\mathbf{F}\,\psi = \mathbf{true}\,\mathbf{U}\,\psi$
- $\mathbf{G}\,\psi = \neg\mathbf{F}\,\neg\psi$

Semantics

$$\varphi = \forall \pi.\, \forall \pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

Semantics

$$\varphi = \forall\pi.\,\forall\pi'.\,\mathbf{G}\,\mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

$$\{\} \models\ \forall\pi.\,\forall\pi'.\,\mathbf{G}\,\mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

Semantics

$$\varphi = \forall\pi.\,\forall\pi'.\,\mathbf{G}\,\mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

$$\{\} \models \forall\pi.\,\forall\pi'.\,\mathbf{G}\,\mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

$$\{\pi \mapsto t\} \models \forall\pi'.\,\mathbf{G}\,\mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } t \in T$$

Semantics

$$\varphi = \forall\pi.\, \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

$$\{\} \models \forall\pi.\, \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

$$\{\pi \mapsto t\} \models \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } t \in T$$

$$\{\pi \mapsto t, \pi' \mapsto t'\} \models \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } t' \in T$$

Semantics

$$\varphi = \forall\pi.\, \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

$$\begin{aligned}
\{\} &\models \forall\pi.\, \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} & \\
\{\pi \mapsto t\} &\models \forall\pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} & \text{for all } t \in T \\
\{\pi \mapsto t, \pi' \mapsto t'\} &\models \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} & \text{for all } t' \in T \\
\{\pi \mapsto t[n,\infty), \pi' \mapsto t'[n,\infty)\} &\models \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} & \text{for all } n \in \mathbb{N}
\end{aligned}$$

Semantics

$$\varphi = \forall \pi.\, \forall \pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

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

$$\{\} \models \forall \pi.\, \forall \pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'}$$

$$\{\pi \mapsto t\} \models \forall \pi'.\, \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } t \in T$$

$$\{\pi \mapsto t, \pi' \mapsto t'\} \models \mathbf{G}\, \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } t' \in T$$

$$\{\pi \mapsto t[n,\infty), \pi' \mapsto t'[n,\infty)\} \models \mathtt{on}_\pi \leftrightarrow \mathtt{on}_{\pi'} \qquad \text{for all } n \in \mathbb{N}$$

$$\mathtt{on} \in t(n) \Leftrightarrow \mathtt{on} \in t'(n)$$

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 $\textsc{PSpace}$-complete.

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 $\textsc{PSpace}$-complete.

Only partial results for HyperLTL.

3a. HyperLTL satisfiability **[F. & Hahn '16]**:

- alternation-free: $\textsc{PSpace}$-complete
- $\exists^*\forall^*$: $\textsc{ExpSpace}$-complete
- $\forall^*\exists^*$: undecidable

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

The Models of HyperLTL

What about Finite Models?

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

- $\forall \pi.\ (\neg a_\pi)\,\mathbf{U}\,(a_\pi \wedge \mathbf{X}\,\mathbf{G}\,\neg a_\pi)$

What about Finite Models?

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

- $\forall\pi.\ (\neg a_\pi)\,\mathbf{U}\,(a_\pi \wedge \mathbf{X}\,\mathbf{G}\,\neg a_\pi)$
- $\exists\pi.\ a_\pi$

What about Finite Models?

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

- $\forall\pi.\ (\neg a_\pi)\,\mathbf{U}\,(a_\pi \wedge \mathbf{X}\,\mathbf{G}\,\neg a_\pi)$
- $\exists\pi.\ a_\pi$

$$\{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \cdots$$

What about Finite Models?

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

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

$$\{a\} \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \cdots$$

What about Finite Models?

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

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

$$\begin{array}{ccccccccc} \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\ \emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \end{array}$$

What about Finite Models?

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

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

$$\begin{array}{ccccccccc}
\{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

The unique model of φ is $\{\emptyset^n\,\{a\}\,\emptyset^\omega \mid n \in \mathbb{N}\}$.

What about Finite Models?

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

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

$$\begin{array}{ccccccccc}
\{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

The unique model of φ is $\{\emptyset^n\,\{a\}\,\emptyset^\omega \mid n \in \mathbb{N}\}$.

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 ω-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 ω-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

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

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

LTL and FO$[<]$ are expressively equivalent.

First-order Logic vs. LTL

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

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

LTL and FO$[<]$ are expressively equivalent.

Example

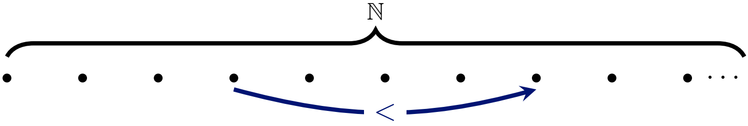
$$\forall x (P_q(x) \wedge \neg P_p(x)) \rightarrow \exists y (x < y \wedge P_p(y))$$

and

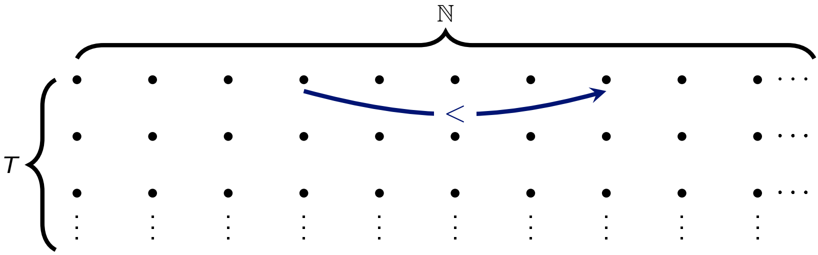
$$\mathbf{G}\,(q \rightarrow \mathbf{F}\,p)$$

are equivalent.

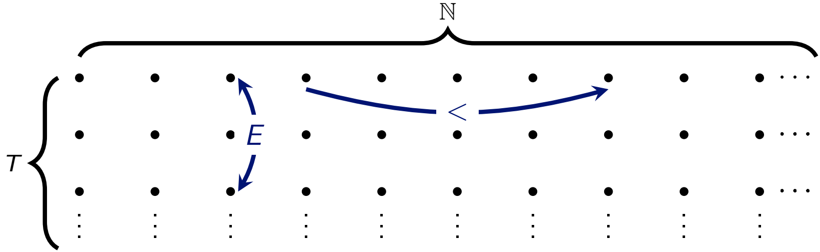
First-order Logic for Hyperproperties



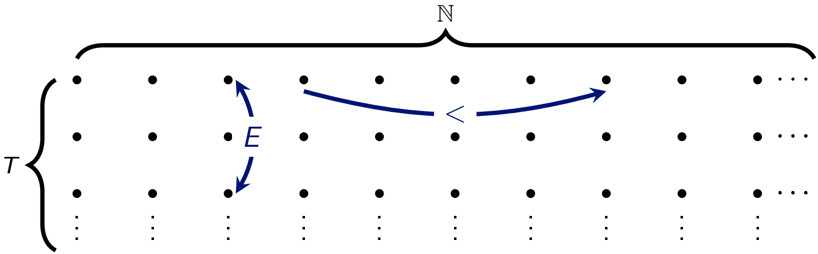
First-order Logic for Hyperproperties



First-order Logic for Hyperproperties



First-order Logic for Hyperproperties

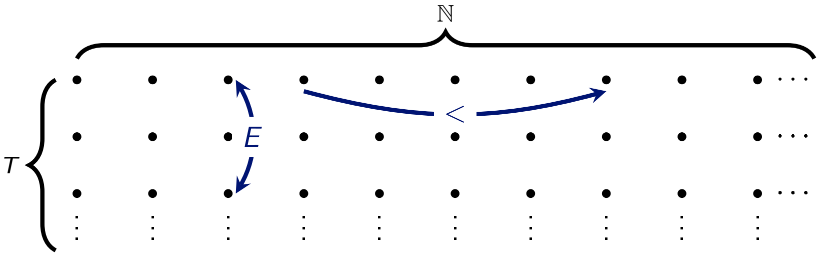


- FO[$<$, E]: first-order logic with equality over the signature $\{<, E\} \cup \{P_a \mid a \in \mathrm{AP}\}$ over structures with universe $T \times \mathbb{N}$.

Example

$$\forall x \forall x' \; E(x, x') \rightarrow (P_{\mathtt{on}}(x) \leftrightarrow P_{\mathtt{on}}(x'))$$

First-order Logic for Hyperproperties



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

Proposition

For every HyperLTL sentence there is an equivalent FO$[<, E]$ sentence.

A Setback

- Let φ 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)

φ is not expressible in HyperLTL.

A Setback

- Let φ 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)

φ is not expressible in HyperLTL.

- But, φ 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

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

- $Q \in \{\exists, \forall\}$,
- $\{x_1, \ldots, x_k\}$ and $\{y_1, \ldots, y_\ell\}$ are disjoint,
- every guard x_{g_j} is in$\{x_1, \ldots, x_k\}$, and
- ψ is quantifier-free over signature $\{<, E\} \cup \{P_a \mid a \in \mathrm{AP}\}$ 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.
- 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 FO[$<$, E]?
- What about HyperCTL*?