The First-order Logic of Hyperproperties

Joint work with Bernd Finkbeiner (Saarland University)

Martin Zimmermann

Saarland University

September, 13th 2017

Highlights Conference, London, UK

LTL vs. First-order Logic

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

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

HyperLTL

A new logic:

$$\forall\pi\forall\pi'.\,\mathrm{on}_\pi \leftrightarrow \mathrm{on}_{\pi'}$$

- Extend LTL by trace quantifiers to express security, privacy, and information flow properties

HyperLTL

A new logic:

$$\forall\pi\forall\pi'.\,\mathrm{on}_\pi \leftrightarrow \mathrm{on}_{\pi'}$$

- Extend LTL by trace quantifiers to express security, privacy, and information flow properties
- Models are sets of traces!

HyperLTL

A new logic:

$$\forall\pi\forall\pi'.\, \mathrm{on}_\pi \leftrightarrow \mathrm{on}_{\pi'}$$

- Extend LTL by trace quantifiers to express security, privacy, and information flow properties
- Models are sets of traces!

Is there a first-order logic that is expressively equivalent to HyperLTL?

An Example

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

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

An Example

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

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

An Example

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

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

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

An Example

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

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

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

An Example

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

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

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

An Example

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

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

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

An Example

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

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

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

An Example

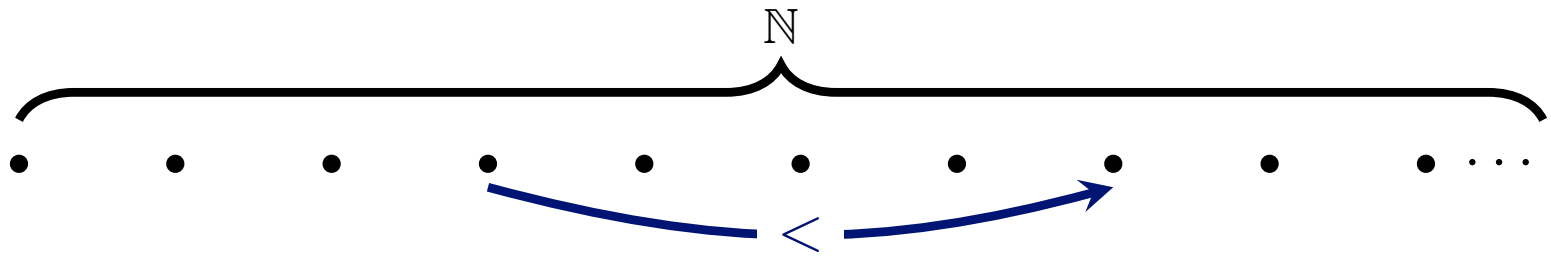
Fix $\mathrm{AP} = \{a\}$ and consider the conjunction φ of

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

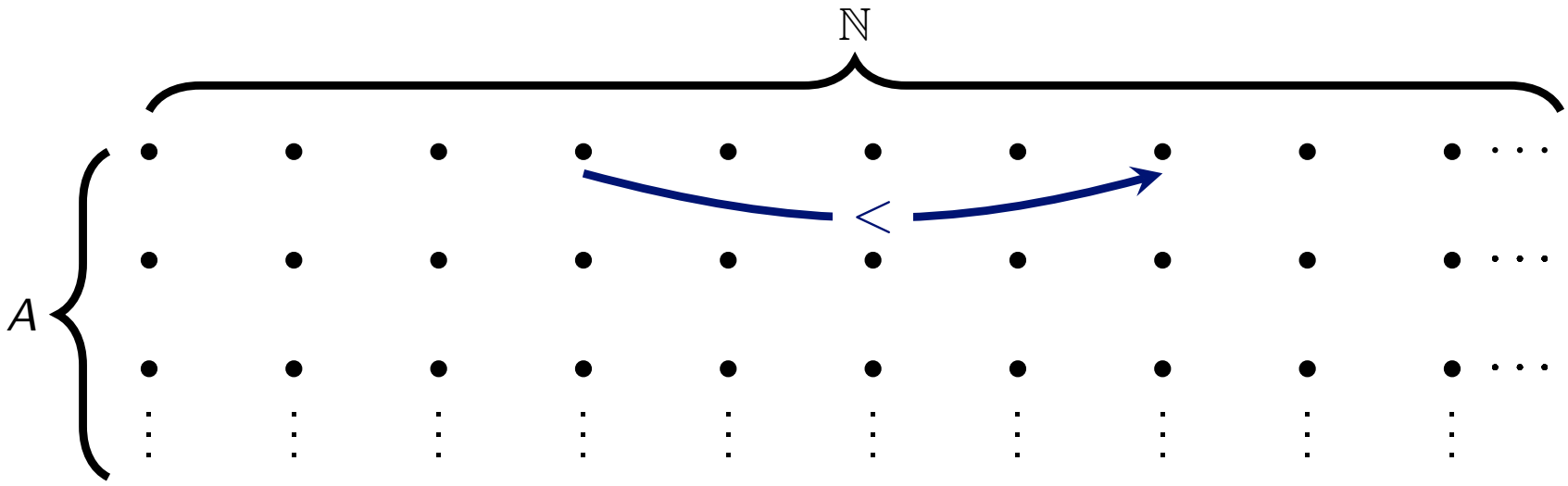
$$
\begin{array}{cccccccccc}
\{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \{a\} & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \cdots \\
\emptyset & \emptyset & \{a\} & \emptyset & \emptyset & \emptyset &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

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

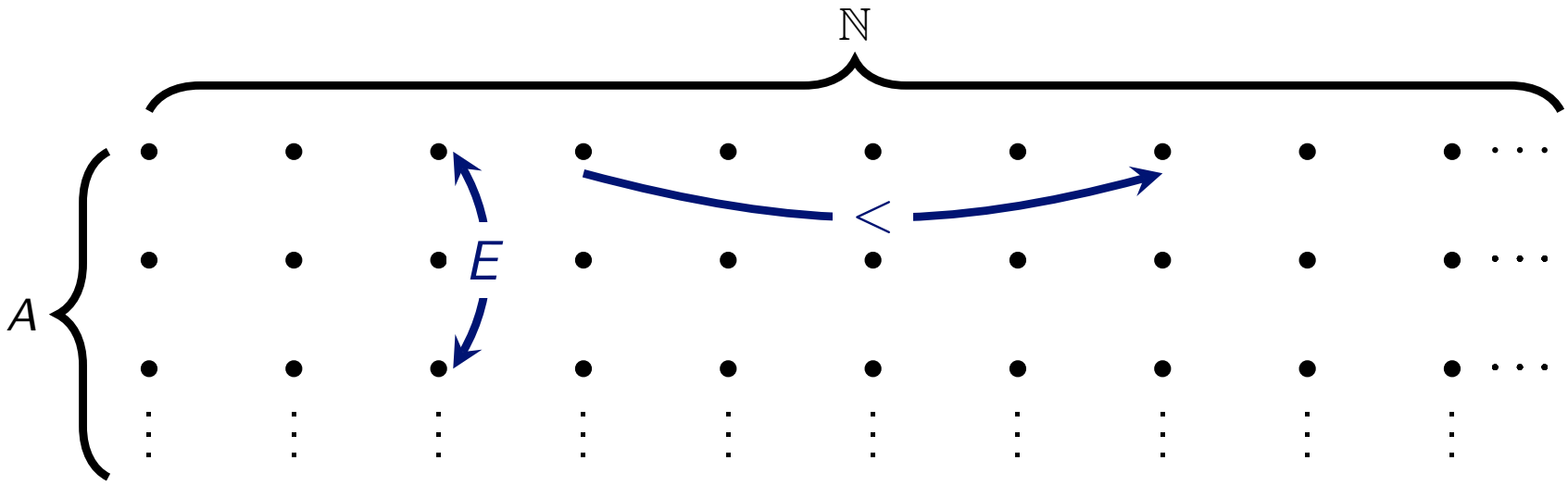
First-order Logic for Hyperproperties



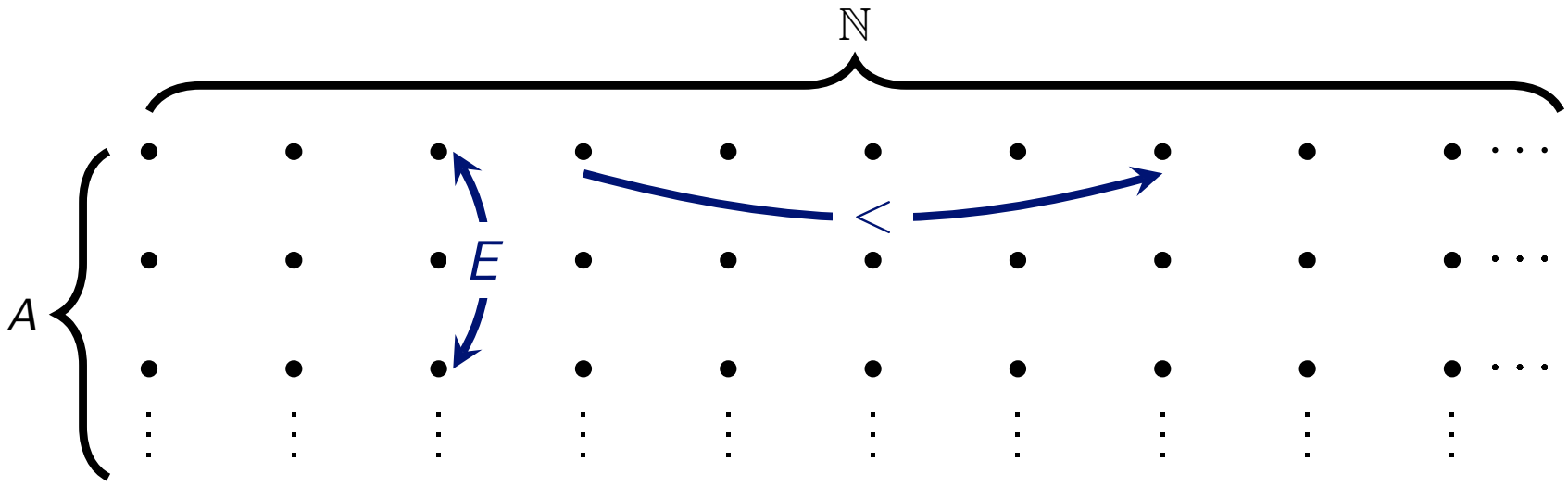
First-order Logic for Hyperproperties



First-order Logic for Hyperproperties

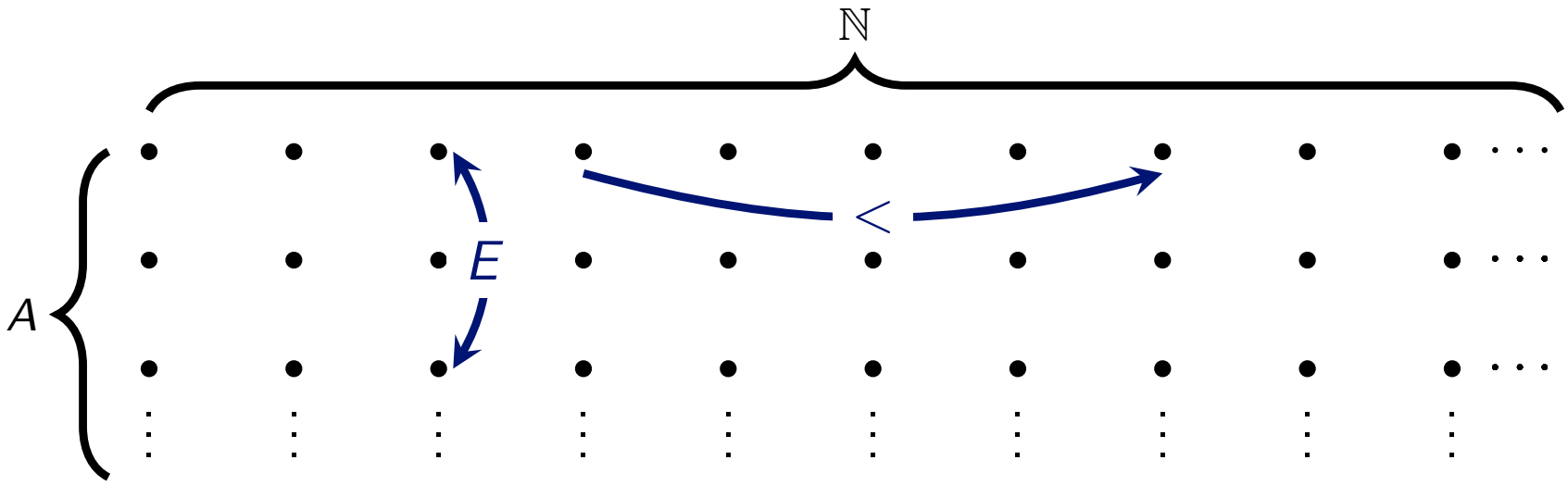


First-order Logic for Hyperproperties



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

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 $A \times \mathbb{N}$.

Proposition

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

A Setback

- Let φ be the following property of sets $T \subseteq (2^{\{a\}})^\omega$:

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

A Setback

- Let φ be the following property of sets $T \subseteq (2^{\{a\}})^\omega$:

  There is an n such that $a \notin t(n)$ 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 $T \subseteq (2^{\{a\}})^\omega$:

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

Theorem (Bozzelli et al. '15)

φ is not expressible in HyperLTL.

- But, φ is easily expressible in FO$[<, E]$:

$$\exists x \, \forall y \, E(x, y) \to \neg P_a(y)$$

Corollary

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

HyperFO

- $\exists^I x$ and $\forall^I x$: 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

- $\exists^I x$ and $\forall^I x$: 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:

$$\forall^I x_1 \, \forall^I x_2 \, \forall^G y_1 \geq x_1 \, \forall^G y_2 \geq x_2 \, E(y_1, y_2) \rightarrow (P_{\mathrm{on}}(y_1) \leftrightarrow P_{\mathrm{on}}(y_2))$$

HyperFO

- $\exists^I x$ and $\forall^I x$: 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:

$$\underbrace{\forall^I x_1 \, \forall^I x_2}_{\substack{\text{quantify initial positions} \\ \cong \\ \text{trace quantification}}} \forall^G y_1 \geq x_1 \, \forall^G y_2 \geq x_2 \, E(y_1, y_2) \rightarrow (P_{\text{on}}(y_1) \leftrightarrow P_{\text{on}}(y_2))$$

HyperFO

- $\exists^I x$ and $\forall^I x$: 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:

$$\underbrace{\forall^I x_1 \, \forall^I x_2}_{\substack{\text{quantify} \\ \text{initial} \\ \text{positions} \\ \cong \\ \text{trace} \\ \text{quantification}}} \underbrace{\forall^G y_1 \geq x_1 \, \forall^G y_2 \geq x_2}_{\substack{\text{quantify arbitrary} \\ \text{positions on} \\ \text{already quantified traces}}} E(y_1, y_2) \rightarrow (P_{\mathtt{on}}(y_1) \leftrightarrow P_{\mathtt{on}}(y_2))$$

HyperFO

- $\exists^I x$ and $\forall^I x$: 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:

$$\underbrace{\forall^I x_1 \, \forall^I x_2}_{\substack{\text{quantify initial positions} \\ \cong \\ \text{trace quantification}}} \underbrace{\forall^G y_1 \geq x_1 \, \forall^G y_2 \geq x_2}_{\substack{\text{quantify arbitrary positions on} \\ \text{already quantified traces}}} \underbrace{E(y_1, y_2) \rightarrow (P_{\mathrm{on}}(y_1) \leftrightarrow P_{\mathrm{on}}(y_2))}_{FO[<, \mathrm{E}] \text{ kernel}}$$

Conclusion

Theorem

HyperLTL and HyperFO are equally expressive.