

# *Deciding Hyperproperties Combined with Functional Specifications*

Raven Beutner<sup>1</sup>, David Carral<sup>3</sup>, Bernd Finkbeiner<sup>1</sup>, **Jana Hofmann<sup>1</sup>**, Markus Krötzsch<sup>2</sup>

<sup>1</sup> CISPA Helmholtz Center for Information Security, Germany

<sup>2</sup> TU Dresden, Germany

<sup>3</sup> LIRMM, Inria, University of Montpellier, CNRS, France



LICS 2022  
Haifa, 2 August 2022

1



# Overview

- Hyperproperties describe many information flow policies like noninterference
- HyperLTL satisfiability is highly undecidable for  $\forall^* \exists^*$  formulas
- 2 new perspectives: temporal safety/liveness + split in functional property and hyperproperty

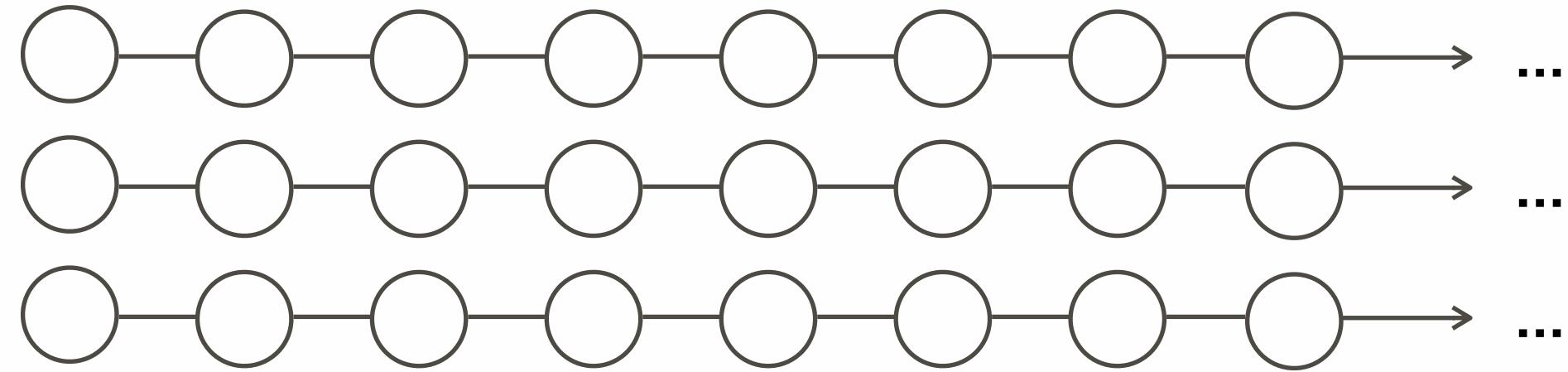
	no LTL spec.	with LTL spec.
Temporal Safety		
complete fragment	coRE [Thm. 3.7]	$\Sigma_1^1$ [Thm. 3.11]
$\forall^* \exists^*. \bigcirc^*$	NEXP [Thm. 3.12]	NEXP [Thm. 3.12]
$\forall^* \exists^*. \Box$	NEXP [Lem. 3.13]	$\Sigma_1^1$ [Thm. 3.11]
$\forall^* \exists^*. \Box(\bigcirc^*)$	coRE [Lem. 3.10]	$\Sigma_1^1$ [Thm. 3.11]
Temporal Liveness		
complete fragment	$\Sigma_1^1$ [Thm. 4.2]	$\Sigma_1^1$ [Thm. 4.2]
$\forall \exists^*. \text{det-liveness}$	trivial [Prop. 4.15]	$\Sigma_1^1$ [Cor. 4.16]
$\forall \exists^*. \Diamond(\bigcirc^*)$	NP [Lem. 4.4]	dec. [Thm. 4.6]
$\forall^* \exists^*. \Diamond \wedge \dots \wedge \Diamond$	NP [Lem. 4.4]	$\Sigma_1^1$ [Thm. 4.12]

- Sound algorithm for largest models for  $\forall \exists^*$  HyperLTL

# Hyperproperties

Trace property  $P$ : set of traces

system



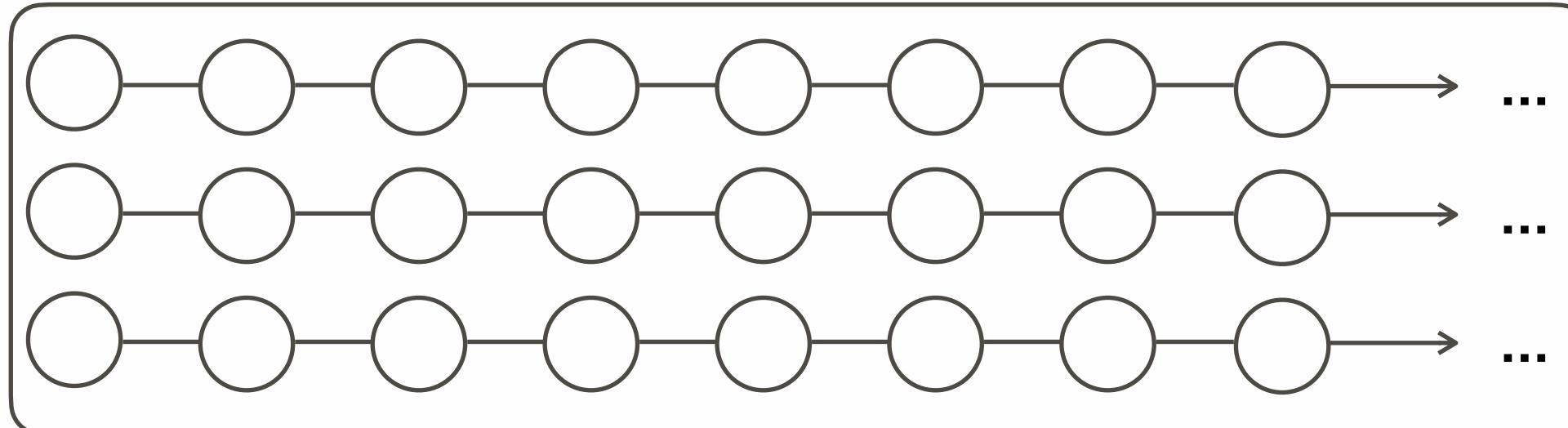
trace  $\in P?$



Functional properties: safety, liveness, ...

Hyperproperty<sup>1</sup>  $H$ : set of sets of traces

system



system  $\in H?$



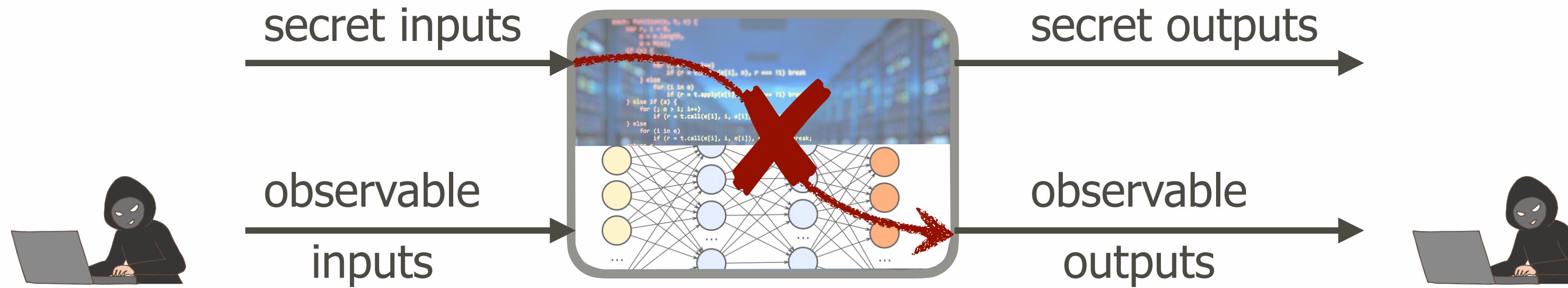
Relational properties:

“Does a change of inputs lead to a change of outputs?”

<sup>1</sup> Clarkson, Schneider. *Hyperproperties*. CSF 2008.

# HyperLTL<sup>1</sup>

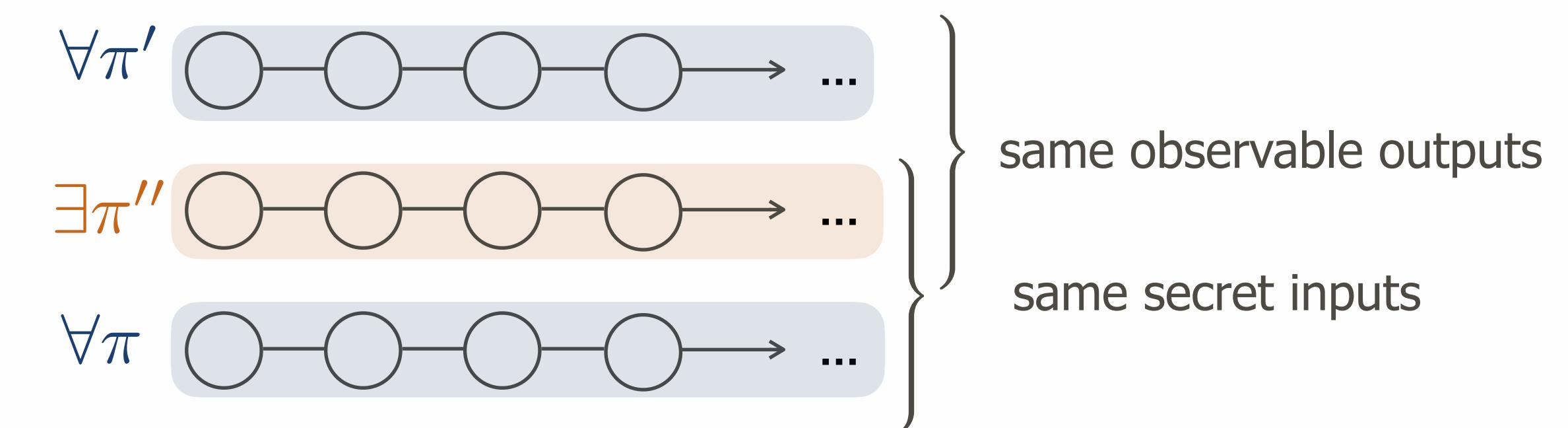
“Secret inputs do not interfere with publicly observable inputs and outputs.”



Generalized noninterference in HyperLTL:

$$\begin{array}{l} \forall \pi. \forall \pi'. \exists \pi''. \square(\text{secretIn}_{\pi} = \text{secretIn}_{\pi''}) \wedge \\ \square(\text{observableOut}_{\pi'} = \text{observableOut}_{\pi''}) \end{array}$$

LTL with indexed atomic propositions



<sup>1</sup> Clarkson, Finkbeiner, Koleini, Micinski, Rabe, Sánchez. *Temporal Logics for Hyperproperties*. POST 2014.

# Satisfiability of $\forall^* \exists^*$ HyperLTL

$\exists^* \forall^*$ : decidable<sup>1</sup>, in general: highly undecidable (in  $\Sigma_1^1$ )<sup>2</sup>

Formulas with  $\forall \exists$  quantifier alternation get **undecidable very quickly**. Undecidable are:

$\forall^2 \exists^*$  + only  $\square$  and  $\diamond$ , not nested<sup>2</sup>

$\forall \exists^*$  + arbitrary temporal operators<sup>1</sup>

- ⇒ No easier fragments obtained from syntactic restrictions
- ⇒ New perspectives on HyperLTL satisfiability?

<sup>2</sup> Masclé, Zimmermann. *The Keys to Decidable HyperLTL Satisfiability: Small Models or Very Simple Formulas*. CSL 2020.

<sup>1</sup> Finkbeiner, Hahn. *Deciding Hyperproperties*. CONCUR 2016.

# New Perspectives on $\forall^* \exists^*$ HyperLTL SAT

## 2 approaches:

- 1) Split hyperproperty into trace property + hyperproperty

Trace property in LTL: describes functional behavior, e.g.: safety properties

Hyperproperty in HyperLTL: simple relational property, e.g.: privacy properties

- 2) Semantic notion of temporal safety and temporal liveness

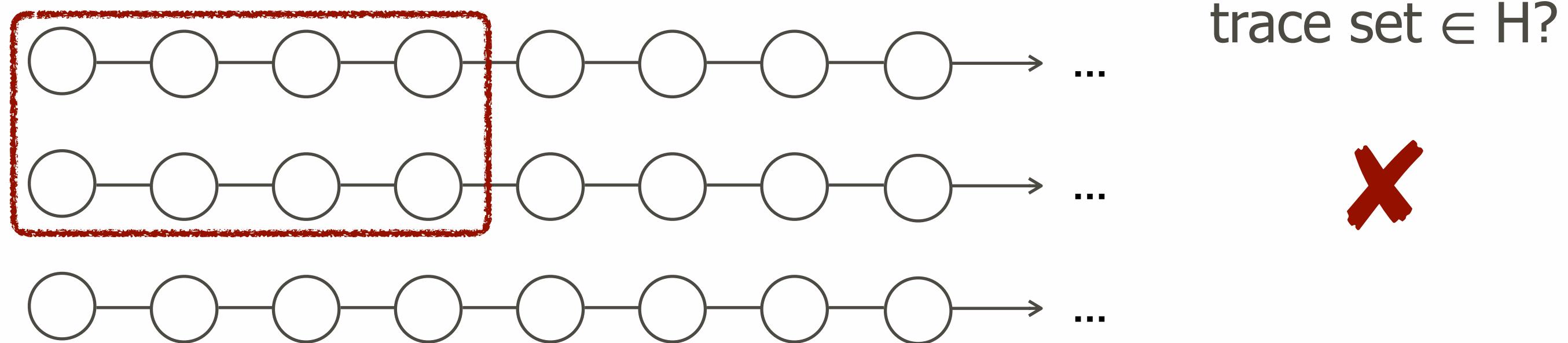
Idea: especially safety properties have algorithmic advantages

$$\forall^* \exists^*. \psi$$

safety / liveness LTL formula

# Temporal Safety vs Hypersafety

**Hypersafety<sup>1</sup>:** Does every counterexample have a “finite reason” for being a counterexample?



Hypersafety does not help with satisfiability:

- 1) Whether HyperLTL formula  $\varphi$  is hypersafety is **highly undecidable** (in  $\Pi_1^1$ )<sup>2</sup>
- 2) If we know that  $\varphi$  is hypersafety, deciding SAT is in PSPACE - no harder than LTL

<sup>2</sup> Finkbeiner, Haas, Torfah. *Canonical Representations of k-Safety Hyperproperties*. CSF 2019.

<sup>1</sup> Clarkson, Schneider. *Hyperproperties*. CSF 2008.

# Results

Reduction to first-order logic

→ FO SAT solving becomes applicable

		<b>no LTL spec.</b>	<b>with LTL spec.</b>
Temporal Safety	complete fragment	coRE [Thm. 3.7]	$\Sigma_1^1$ [Thm. 3.11]
	$\forall^* \exists^*. \bigcirc^*$	NEXP [Thm. 3.12]	NEXP [Thm. 3.12]
	$\forall^* \exists^*. \square$	NEXP [Lem. 3.13]	$\Sigma_1^1$ [Thm. 3.11]
Temporal Liveness	$\forall^* \exists^*. \square(\bigcirc^*)$	coRE [Lem. 3.10]	$\Sigma_1^1$ [Thm. 3.11]
	complete fragment	$\Sigma_1^1$ [Thm. 4.2]	$\Sigma_1^1$ [Thm. 4.2]
	$\forall \exists^*. \text{det-liveness}$	trivial [Prop. 4.15]	$\Sigma_1^1$ [Cor. 4.16]
	$\forall \exists^*. \diamond(\bigcirc^*)$	NP [Lem. 4.4]	dec. [Thm. 4.6]
$\forall^* \exists^*. \diamond \wedge \dots \wedge \diamond$		NP [Lem. 4.4]	$\Sigma_1^1$ [Thm. 4.12]

First decidability result for formulas that can enforce models with infinitely many traces

# Finding Largest Models for $\forall \exists^*$ HyperLTL

---

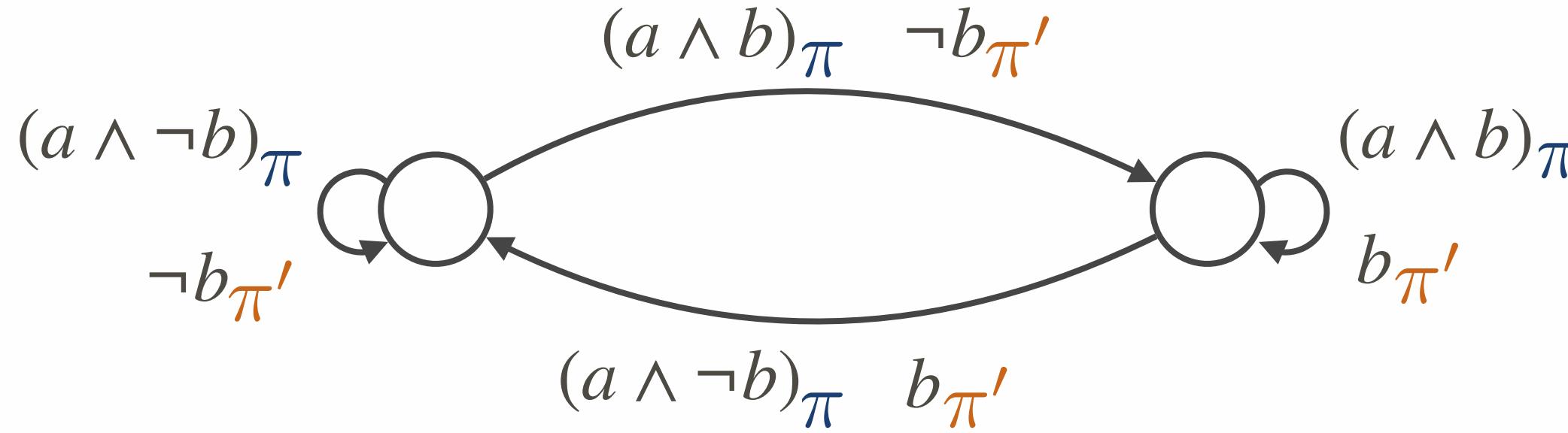
```

1: procedure FINDMODEL( $\mathcal{A}$ )
2:   if  $\mathcal{L}(\mathcal{A}^\forall) = \emptyset$  then
3:     return UNSAT;
4:   if  $\mathcal{L}(\mathcal{A}^\exists) \subseteq \mathcal{L}(\mathcal{A}^\forall)$  then
5:     return SAT, model:  $\mathcal{L}(\mathcal{A}^\forall)$ ;
6:    $\mathcal{A}_{\text{new}} := \mathcal{A} \cap \mathcal{A}_{\pi'}^\forall;$  ━━━━━━━━ Remove  $\forall$ -traces that produce wrong  $\exists$ -traces
7:   FINDMODEL( $\mathcal{A}_{\text{new}}$ );

```

---

$$\forall \pi. \exists \pi'. \underbrace{\square(a_\pi \wedge (b_\pi \leftrightarrow \bigcirc b_{\pi'}))}_{}$$



# Finding Largest Models for $\forall \exists^*$ HyperLTL

---

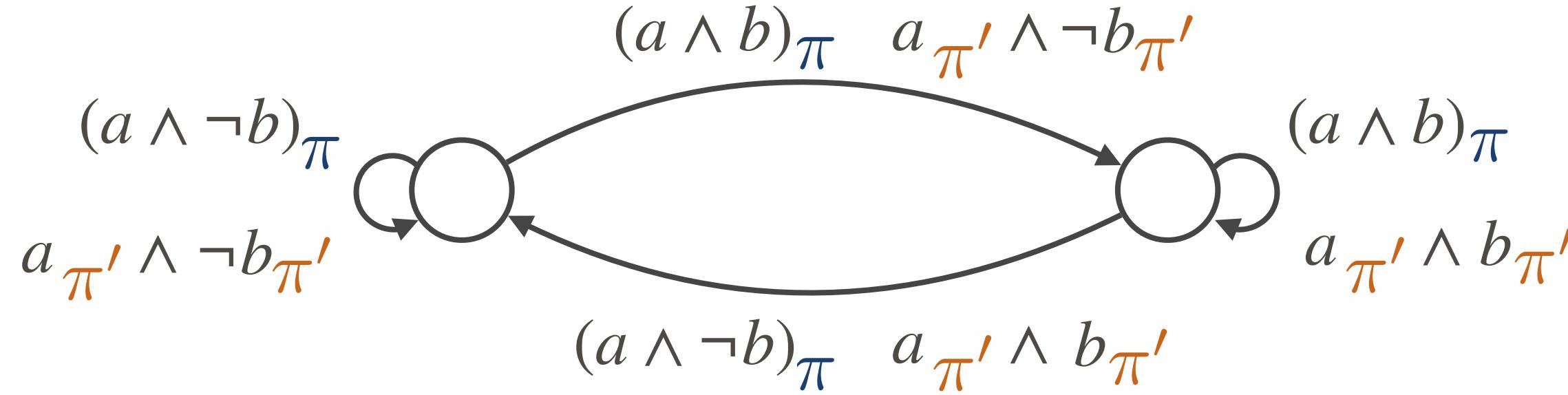
```

1: procedure FINDMODEL( $\mathcal{A}$ )
2:   if  $\mathcal{L}(\mathcal{A}^\forall) = \emptyset$  then
3:     return UNSAT;
4:   if  $\mathcal{L}(\mathcal{A}^\exists) \subseteq \mathcal{L}(\mathcal{A}^\forall)$  then
5:     return SAT, model:  $\mathcal{L}(\mathcal{A}^\forall)$ ;
6:    $\mathcal{A}_{\text{new}} := \mathcal{A} \cap \mathcal{A}_{\pi'}^\forall;$   
7:   FINDMODEL( $\mathcal{A}_{\text{new}}$ );

```

---

$$\forall \pi. \exists \pi'. \square(a_\pi \wedge (b_\pi \leftrightarrow \bigcirc b_{\pi'}))$$



Remove  $\forall$ -traces that produce wrong  $\exists$ -traces

- Finds largest models
- Sound but necessarily not complete
- Evaluation: finds models that MGHyper<sup>1</sup> does not find, can show unsatisfiability

<sup>1</sup> Finkbeiner, Hahn, Hans. MGHyper: Checking Satisfiability of HyperLTL formulas beyond the  $\exists^* \forall^*$  Fragment. ATVA 2018.

# Conclusion

- Syntactic fragments of  $\forall^* \exists^*$  HyperLTL do not make satisfiability easier
- 2 new perspectives: **temporal safety/liveness** + split in **functional property and hyperproperty**

	<b>no LTL spec.</b>	<b>with LTL spec.</b>
Temporal Safety	complete fragment	coRE [Thm. 3.7] $\Sigma_1^1$ [Thm. 3.11]
	$\forall^* \exists^*. \bigcirc^*$	NEXP [Thm. 3.12]      NEXP [Thm. 3.12]
	$\forall^* \exists^*. \square$	NEXP [Lem. 3.13] $\Sigma_1^1$ [Thm. 3.11]
	$\forall^* \exists^*. \square(\bigcirc^*)$	coRE [Lem. 3.10] $\Sigma_1^1$ [Thm. 3.11]
Temporal Liveness	complete fragment	$\Sigma_1^1$ [Thm. 4.2] $\Sigma_1^1$ [Thm. 4.2]
	$\forall \exists^*. \text{det-liveness}$	trivial [Prop. 4.15] $\Sigma_1^1$ [Cor. 4.16]
	$\forall \exists^*. \diamond(\bigcirc^*)$	NP [Lem. 4.4]      dec. [Thm. 4.6]
	$\forall^* \exists^*. \diamond \wedge \cdots \wedge \diamond$	NP [Lem. 4.4] $\Sigma_1^1$ [Thm. 4.12]

New  $\forall^* \exists^*$  decidability results beyond purely syntactic restrictions

Fixpoint algorithm for SAT and UNSAT

- Sound **algorithm** for largest models for  $\forall \exists^*$  HyperLTL