

Deciding Hyperproperties Combined with Functional Specifications

Raven Beutner¹, David Carral³, Bernd Finkbeiner¹, **Jana Hofmann**¹, Markus Krötzsch²

¹ *CISPA Helmholtz Center for Information Security, Germany*

² *TU Dresden, Germany*

³ *LIRMM, Inria, University of Montpellier, CNRS, France*

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**

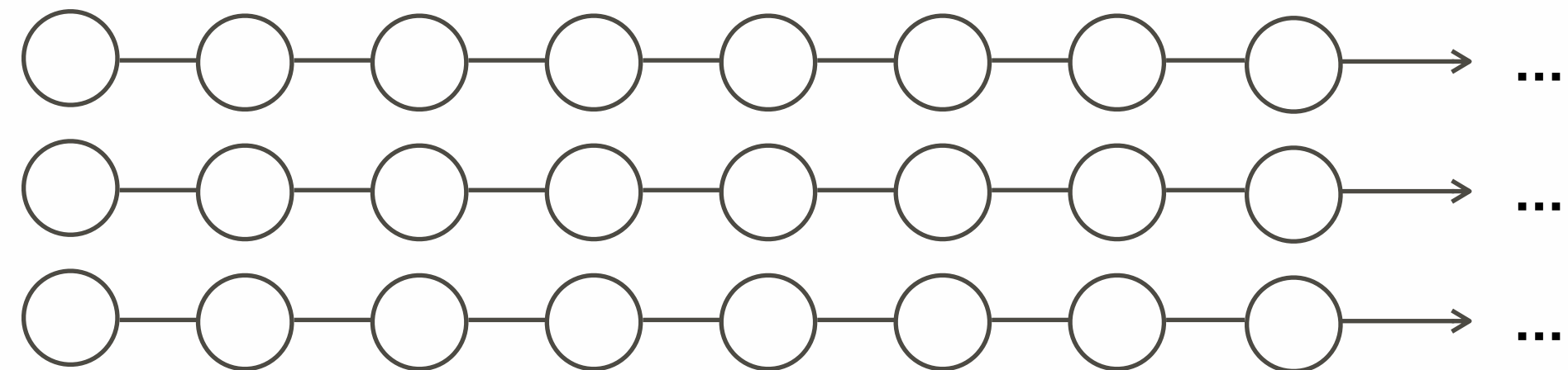
		no LTL spec.	with LTL spec.
Temporal Safety	complete fragment	coRE [Thm. 3.7]	Σ_1^1 [Thm. 3.11]
	$\forall^*\exists^*. \bigcirc^*$	NEXP [Thm. 3.12]	NEXP [Thm. 3.12]
	$\forall^*\exists^*. \square$	NEXP [Lem. 3.13]	Σ_1^1 [Thm. 3.11]
	$\forall^*\exists^*. \square(\bigcirc^*)$	coRE [Lem. 3.10]	Σ_1^1 [Thm. 3.11]
Temporal Liveness	complete fragment	Σ_1^1 [Thm. 4.2]	Σ_1^1 [Thm. 4.2]
	$\forall\exists^*. \text{det-liveness}$	trivial [Prop. 4.15]	Σ_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]	Σ_1^1 [Thm. 4.12]

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

Hyperproperties

Trace property P: set of traces

system



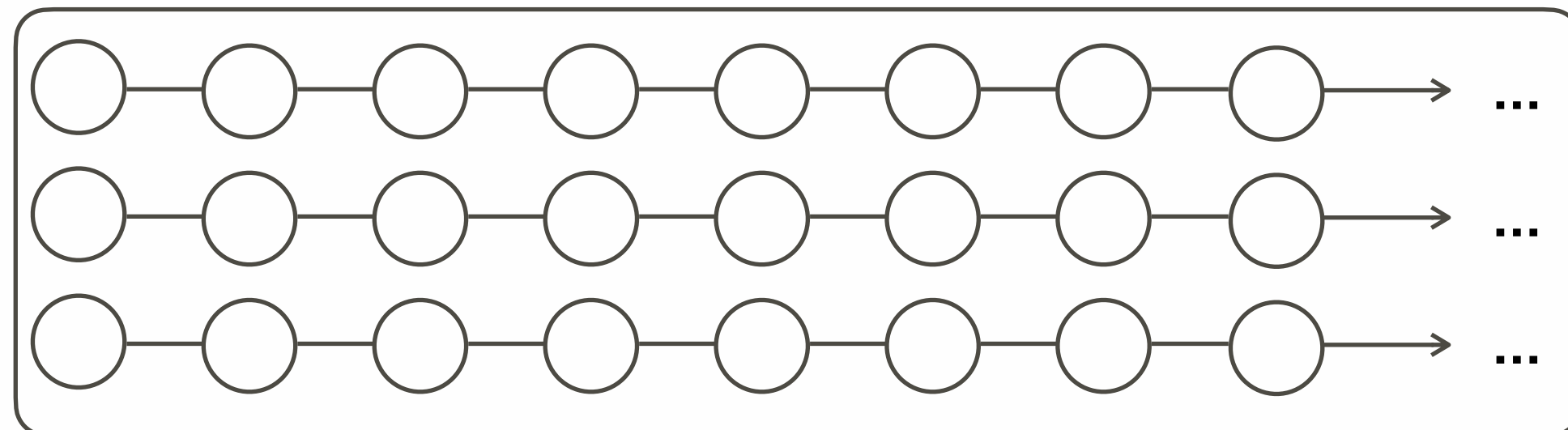
trace \in P?



Functional properties: safety, liveness, ...

Hyperproperty¹ H: set of sets of traces

system



system \in H?



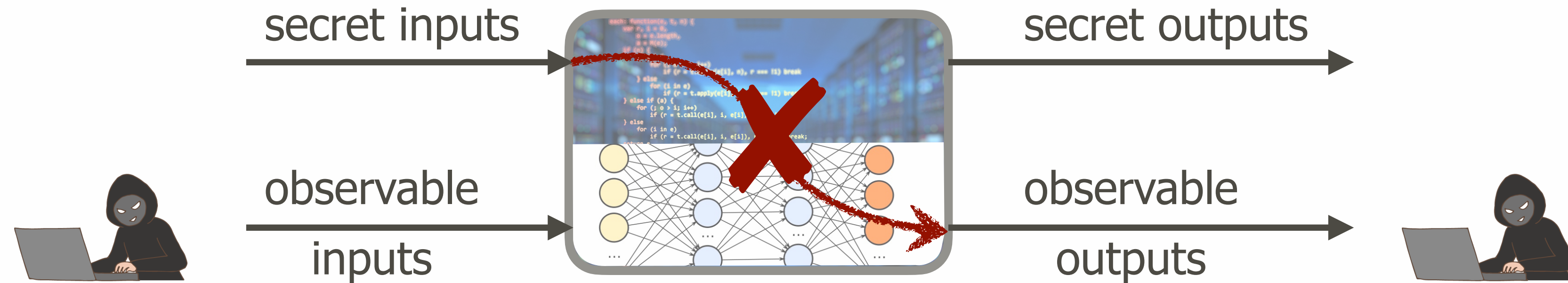
Relational properties:

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

¹Clarkson, Schneider. *Hyperproperties*. CSF 2008.

HyperLTL¹

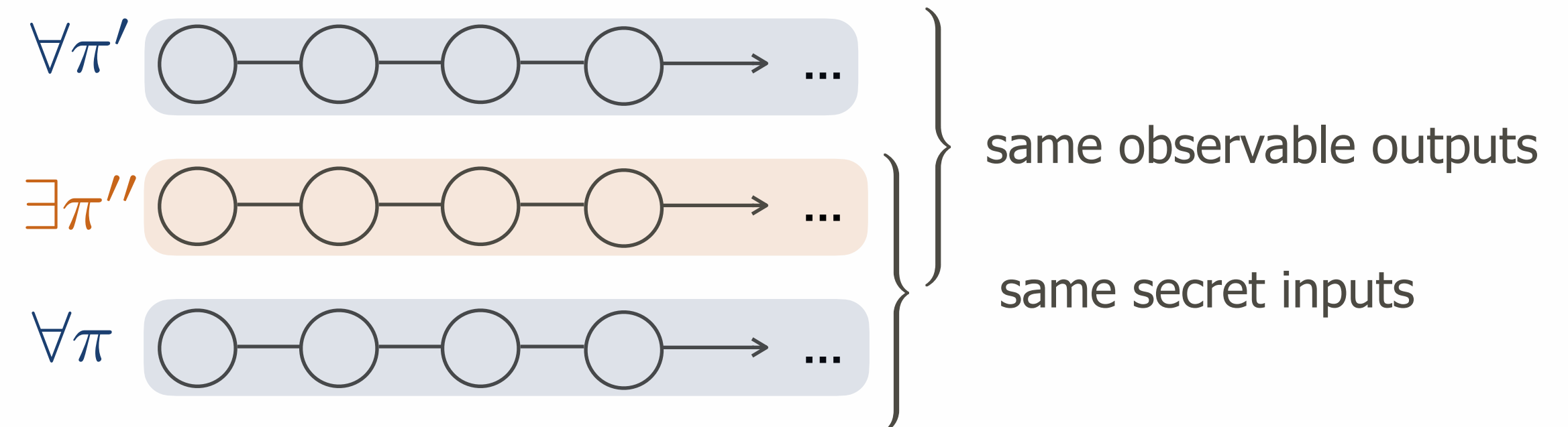
“Secret inputs do not interfere with publicly observable inputs and outputs.”



Generalized noninterference in HyperLTL:

$$\forall \pi. \forall \pi'. \exists \pi''. \square (secretIn_{\pi} = secretIn_{\pi''}) \wedge \square (observableOut_{\pi'} = observableOut_{\pi''})$$

LTL with indexed atomic propositions



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

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

$\exists^* \forall^*$: decidable¹, in general: highly undecidable (in Σ_1^1)²

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

$\forall^2 \exists^*$ + only \square and \diamond , not nested²

$\forall \exists^*$ + arbitrary temporal operators¹

\Rightarrow No easier fragments obtained from syntactic restrictions

\Rightarrow New perspectives on HyperLTL satisfiability?

² Mascle, Zimmermann. *The Keys to Decidable HyperLTL Satisfiability: Small Models or Very Simple Formulas*. CSL 2020.

¹ 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

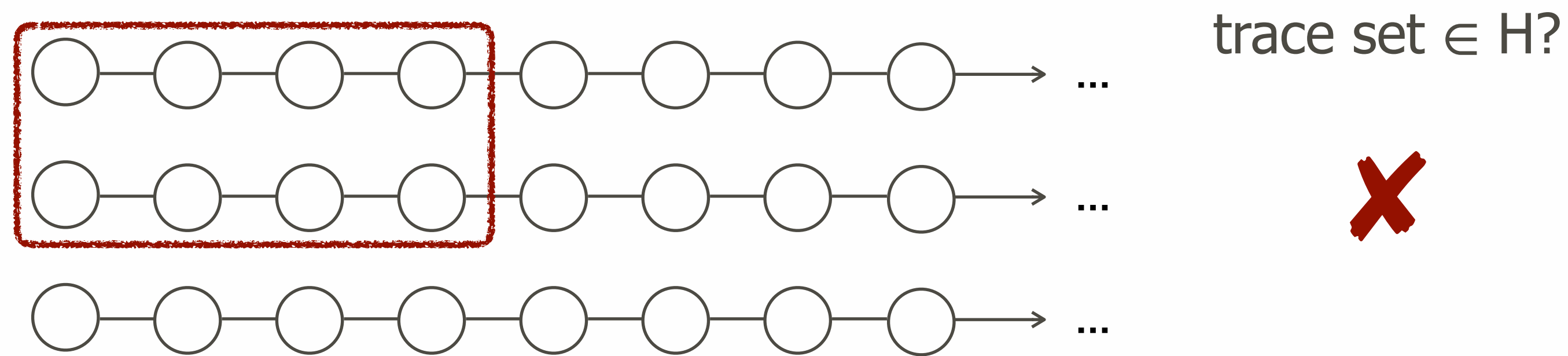
2) Semantic notion of **temporal safety** and **temporal liveness**

Idea: especially safety properties have algorithmic advantages

$\forall^* \exists^* . \psi$ — **safety / liveness LTL formula**

Temporal Safety vs Hypersafety

Hypersafety¹: Does every counterexample have a “finite reason” for being a counterexample?



Hypersafety does not help with satisfiability:

- 1) Whether HyperLTL formula φ is hypersafety is **highly undecidable** (in Π_1^1)²
- 2) If we know that φ is hypersafety, deciding SAT is in PSPACE - **no harder than LTL**

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

¹ Clarkson, Schneider. *Hyperproperties*. CSF 2008.

Results

Reduction to first-order logic

⇒ FO SAT solving becomes applicable

		no LTL spec.	with LTL spec.
Temporal Safety	complete fragment	coRE [Thm. 3.7]	Σ_1^1 [Thm. 3.11]
	$\forall^* \exists^* . \bigcirc^*$	NEXP [Thm. 3.12]	NEXP [Thm. 3.12]
	$\forall^* \exists^* . \square$	NEXP [Lem. 3.13]	Σ_1^1 [Thm. 3.11]
	$\forall^* \exists^* . \square(\bigcirc^*)$	coRE [Lem. 3.10]	Σ_1^1 [Thm. 3.11]
Temporal Liveness	complete fragment	Σ_1^1 [Thm. 4.2]	Σ_1^1 [Thm. 4.2]
	$\forall \exists^* . \text{det-liveness}$	trivial [Prop. 4.15]	Σ_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]	Σ_1^1 [Thm. 4.12]

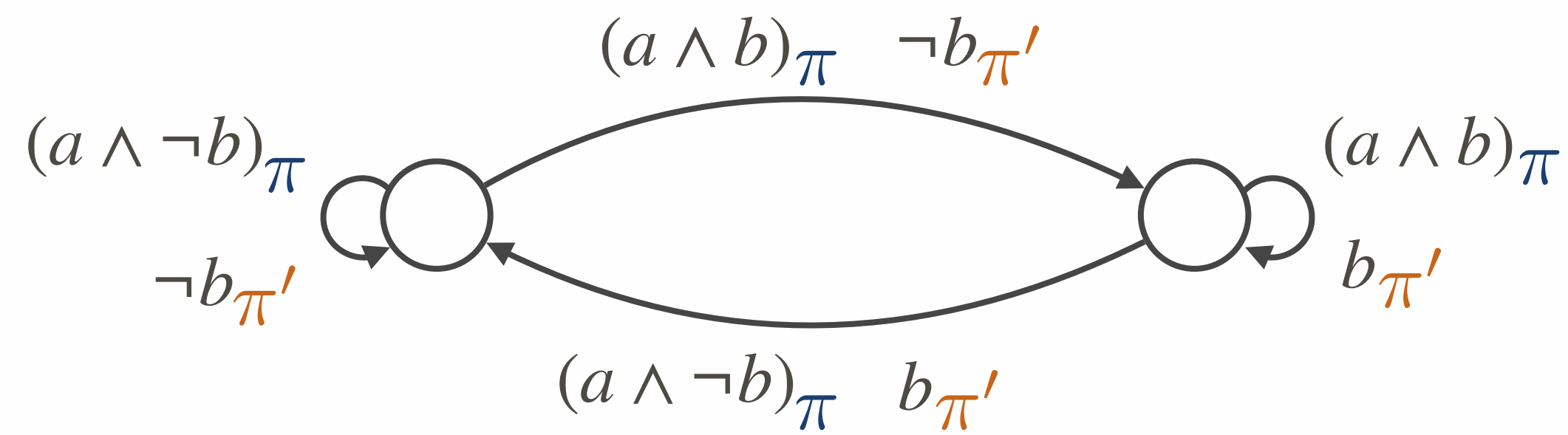
First decidability result for formulas that can enforce models with infinitely many traces

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:    $\mathcal{A}_{\text{new}} := \mathcal{A} \cap \mathcal{A}_{\pi'}^\forall$ ;
7:   FINDMODEL( $\mathcal{A}_{\text{new}}$ );
```

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

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



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

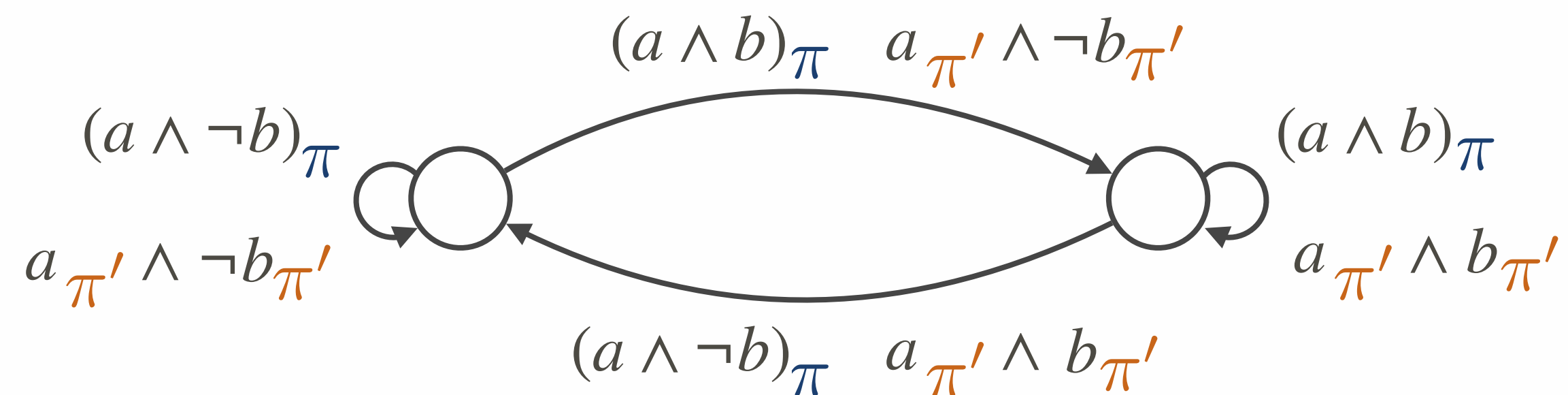
```

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( $\mathcal{A}_{\text{new}}$ );

```

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

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



- Finds largest models
- **Sound** but necessarily **not complete**
- **Evaluation:** finds models that MGHyper¹ does not find, can show **unsatisfiability**

¹Finkbeiner, 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**

		no LTL spec.	with LTL spec.
Temporal Safety	complete fragment	coRE [Thm. 3.7]	Σ_1^1 [Thm. 3.11]
	$\forall^*\exists^*.O^*$	NEXP [Thm. 3.12]	NEXP [Thm. 3.12]
	$\forall^*\exists^*. \square$	NEXP [Lem. 3.13]	Σ_1^1 [Thm. 3.11]
	$\forall^*\exists^*. \square(O^*)$	coRE [Lem. 3.10]	Σ_1^1 [Thm. 3.11]
Temporal Liveness	complete fragment	Σ_1^1 [Thm. 4.2]	Σ_1^1 [Thm. 4.2]
	$\forall\exists^*. \text{det-liveness}$	trivial [Prop. 4.15]	Σ_1^1 [Cor. 4.16]
	$\forall\exists^*. \diamond(O^*)$	NP [Lem. 4.4]	dec. [Thm. 4.6]
	$\forall^*\exists^*. \diamond \wedge \dots \wedge \diamond$	NP [Lem. 4.4]	Σ_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