CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Second-Order Hyperproperties

Raven Beutner, Bernd Finkbeiner, **Hadar Frenkel**, Niklas Metzger

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

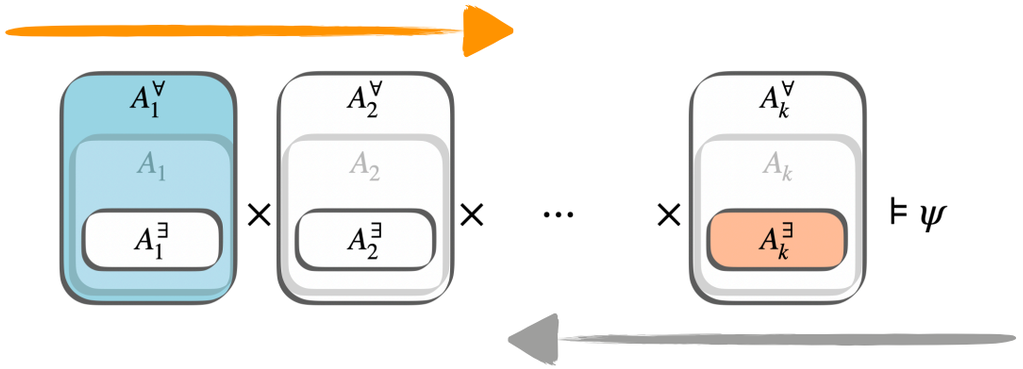
21 July @ CAV 2023

Overview

Hyper^{2}LTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathcal{U} \psi$$

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



Model checking

Trace theory

Asynchronous Hyperproperties

Common knowledge

Hyper^{2}LTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathbin{\mathsf{U}} \psi$$

$$\varphi := \exists \pi \in X . \varphi \mid \forall \pi \in X . \varphi \mid \exists X . \varphi \mid \forall X . \varphi$$

Second-order logic
for the specification of
Hyperproperties

Hyperproperties

Knowledge

Information-flow

Fairness

Robustness

Test of Time Award

Presented to

Michael R. Clarkson & Fred B. Schneider

for their paper

Hyperproperties

published in CSF 2008

July 12, 2023 at the
36th IEEE Computer Security Foundations Symposium

IEEE computer society

IEEE

Hyperproperties. Clarkson and Schneider (CSF 2008)

HyperLTL

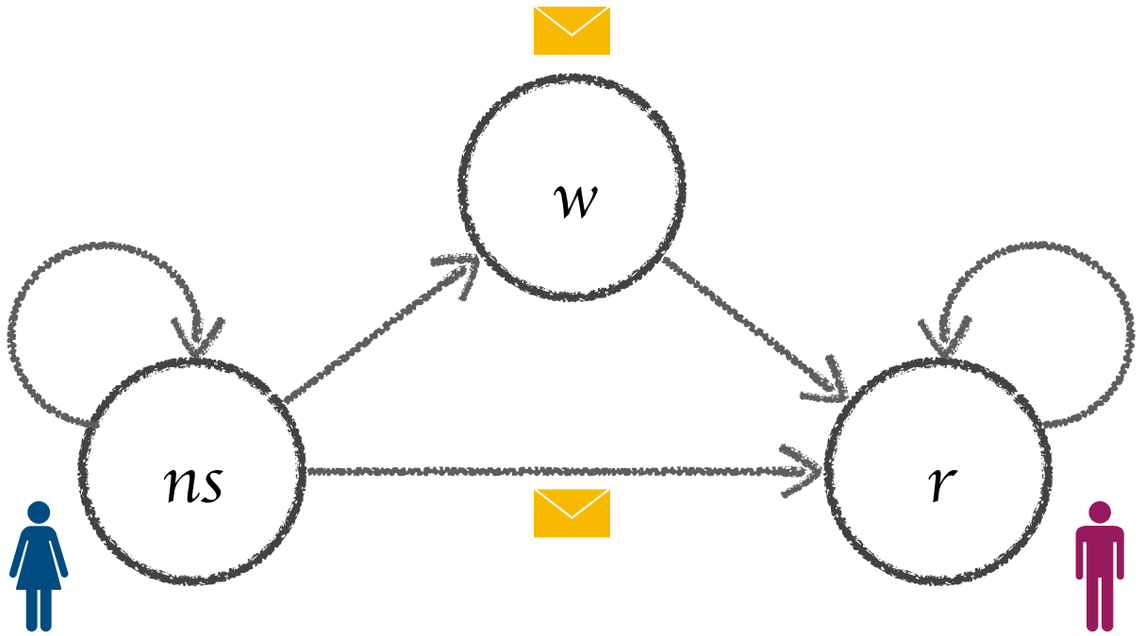
$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathbin{\mathsf{U}} \psi$$

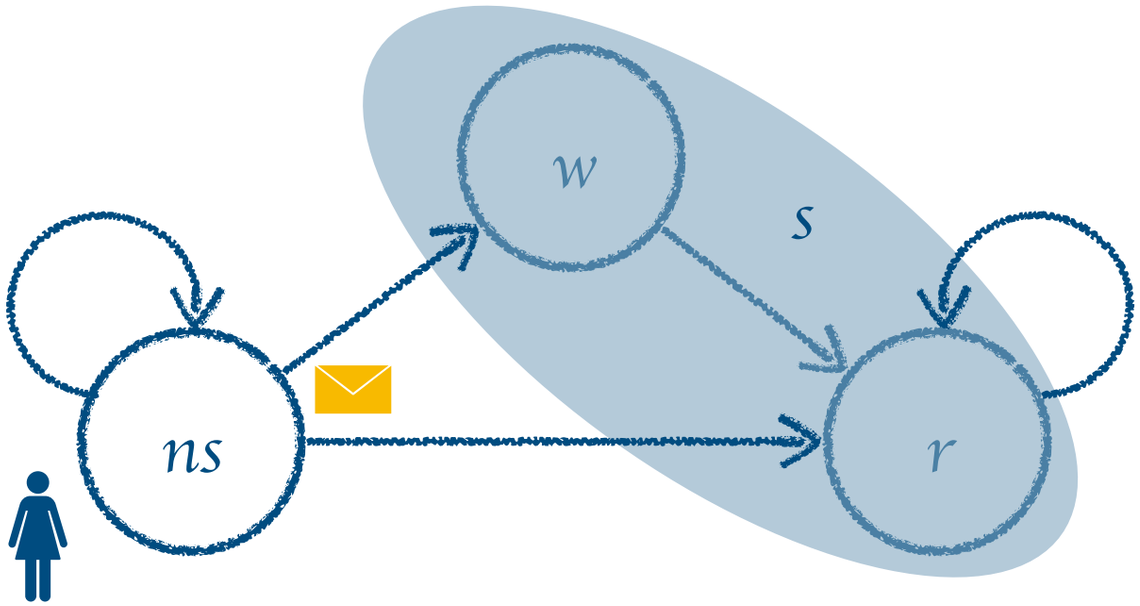
$$\varphi := \exists \pi . \varphi \mid \forall \pi . \varphi$$

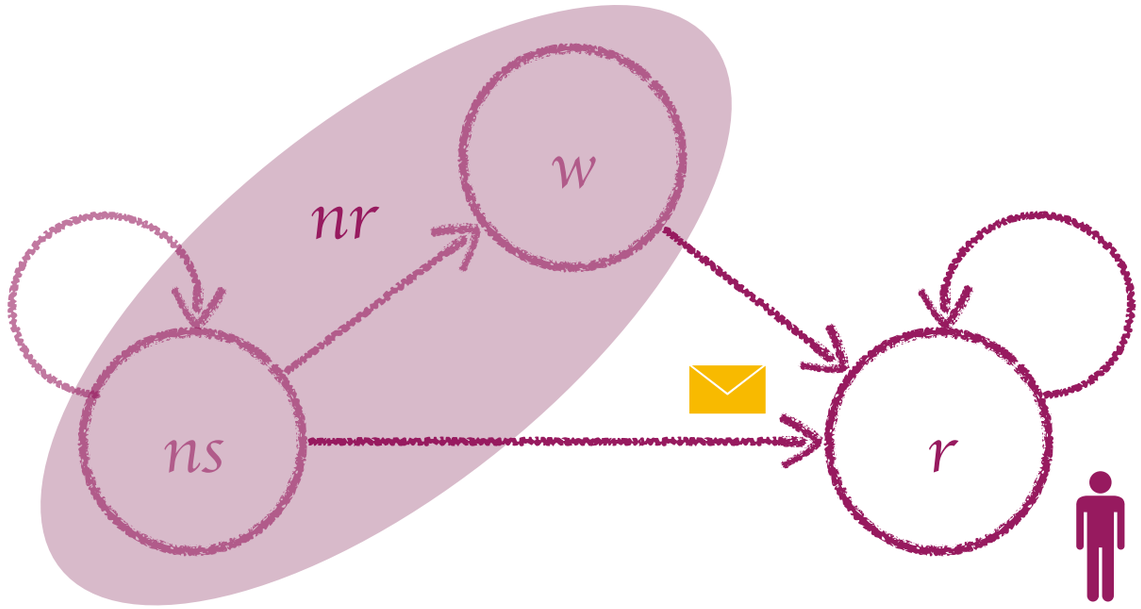
trace variable

Temporal Logics for Hyperproperties. Clarkson, Finkbeiner, Koleini, Micinski, Rabe, and Sánchez. (POST 2014).

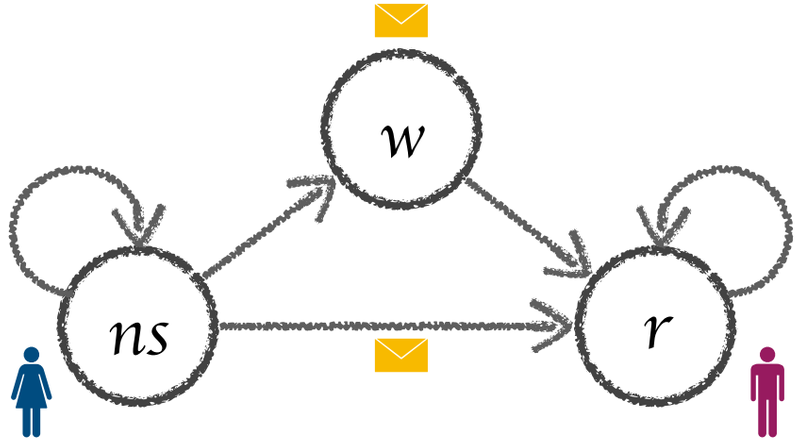
Communication in Multi-Agent Systems

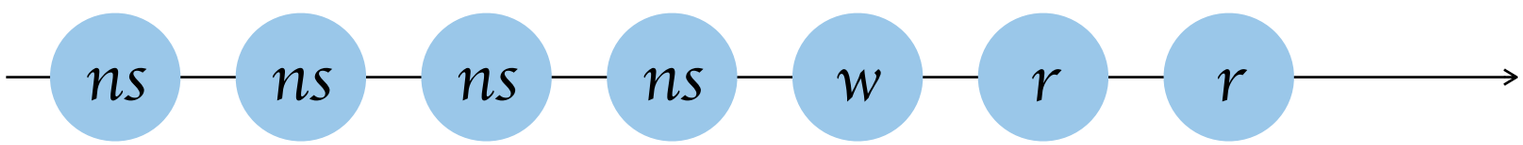






Communication in Multi-Agent Systems





Trace property (LTL)

eventually r ?

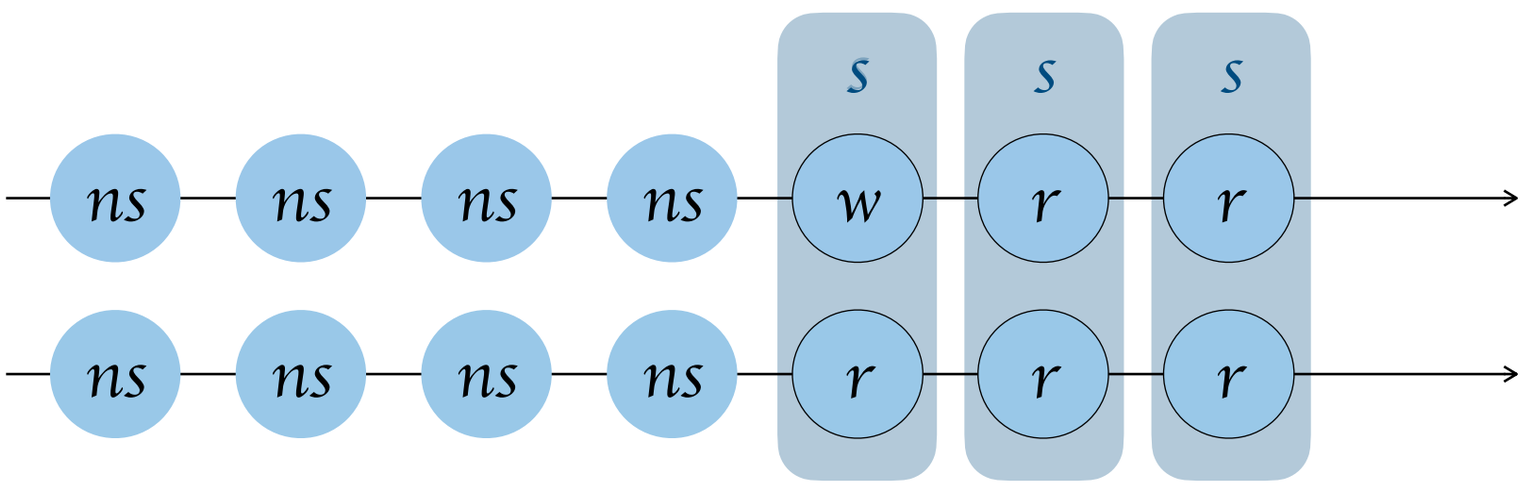
HyperLTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \,\mathsf{U}\, \psi$$

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

$$\square\left((ns_\pi \leftrightarrow ns_{\pi'}) \wedge (s_\pi \leftrightarrow s_{\pi'})\right)$$

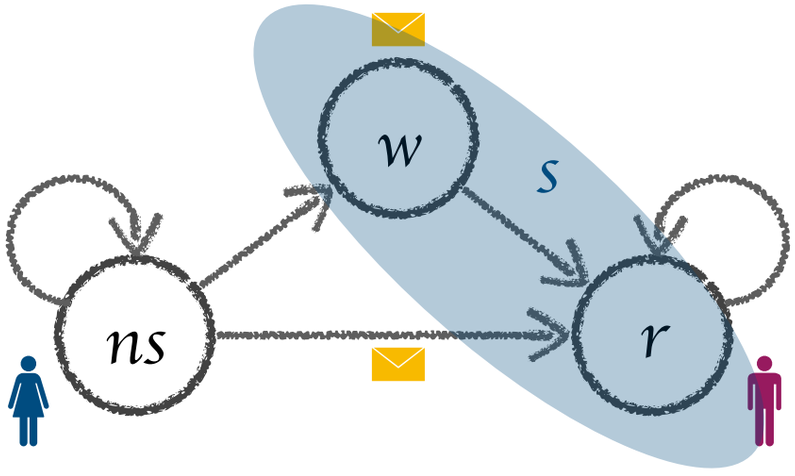
$$\exists \pi \forall \pi' \,.\, (\pi \equiv_{\text{👩}} \pi') \rightarrow \Diamond(r_\pi \wedge r_{\pi'})$$

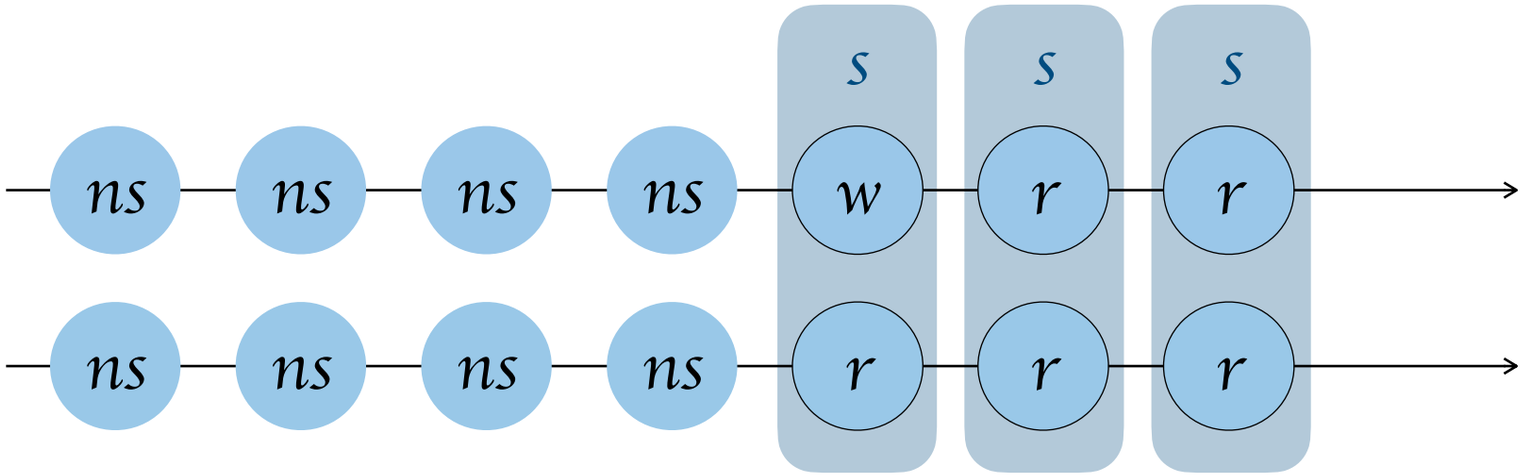


Hyperproperty

👩 eventually knows r ?

Communication in Multi-Agent Systems



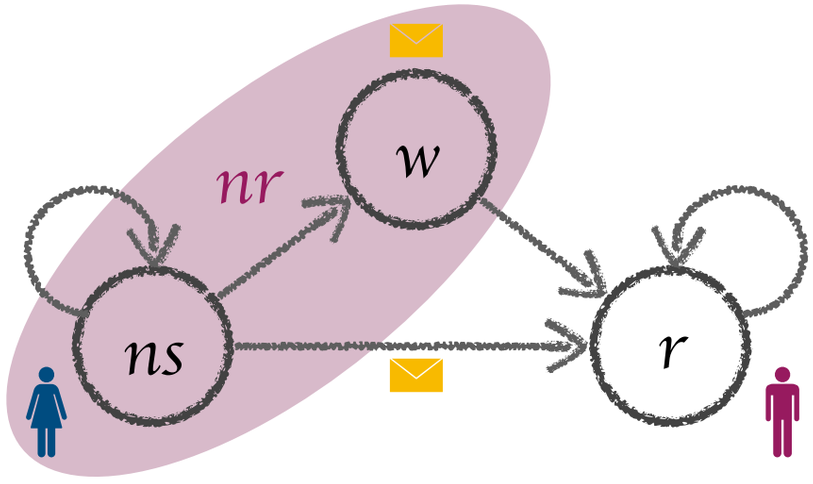


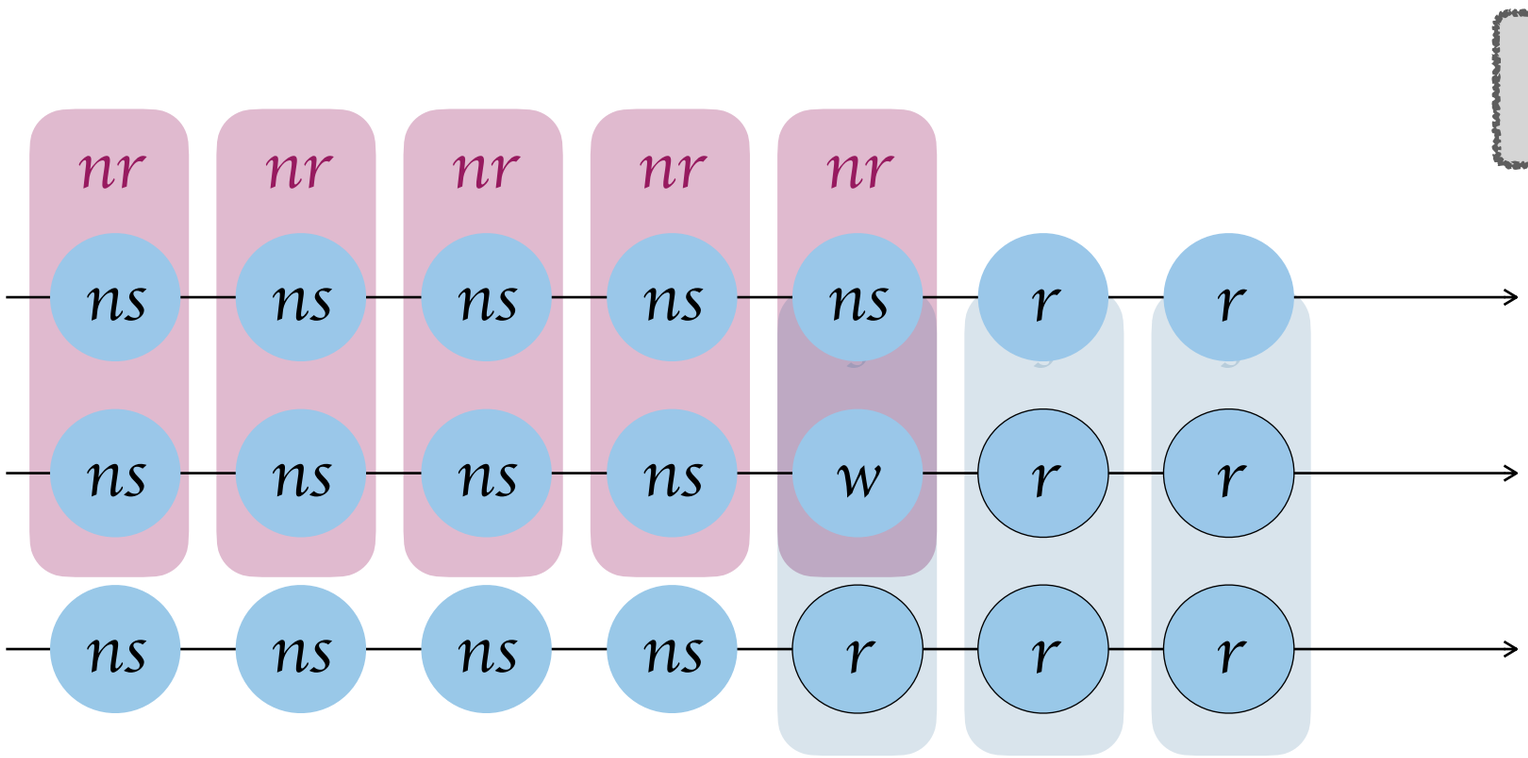
Hyperproperty

eventually know r ?

eventually knows r ?

Communication in Multi-Agent Systems



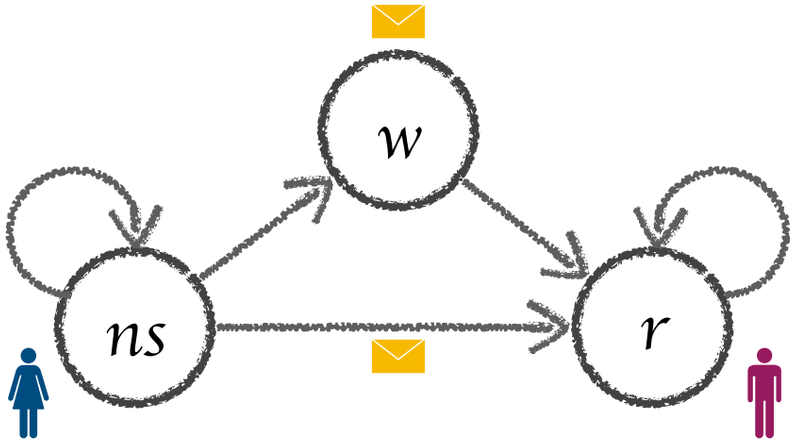


Hyperproperty

eventually know r ?

eventually knows r ?

Common Knowledge



second-order quantification

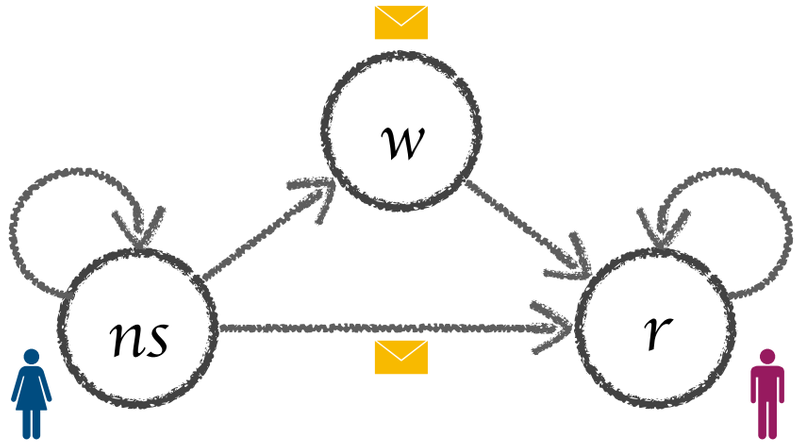
eventually common knowledge  r ?

φ common knowledge

$\leftrightarrow$

(everybody knows)$^{\omega}$ φ

Common Knowledge



second-order quantification

Trace theory

Asynchronous Hyperproperties

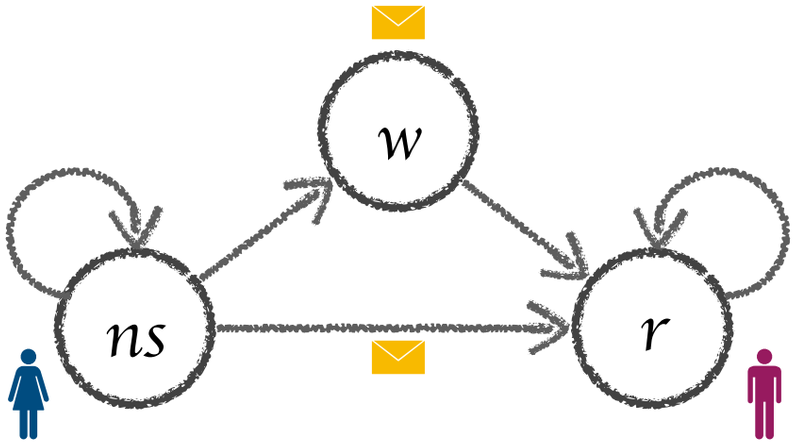
eventually common knowledge 👫 r ?

φ common knowledge

$\leftrightarrow$

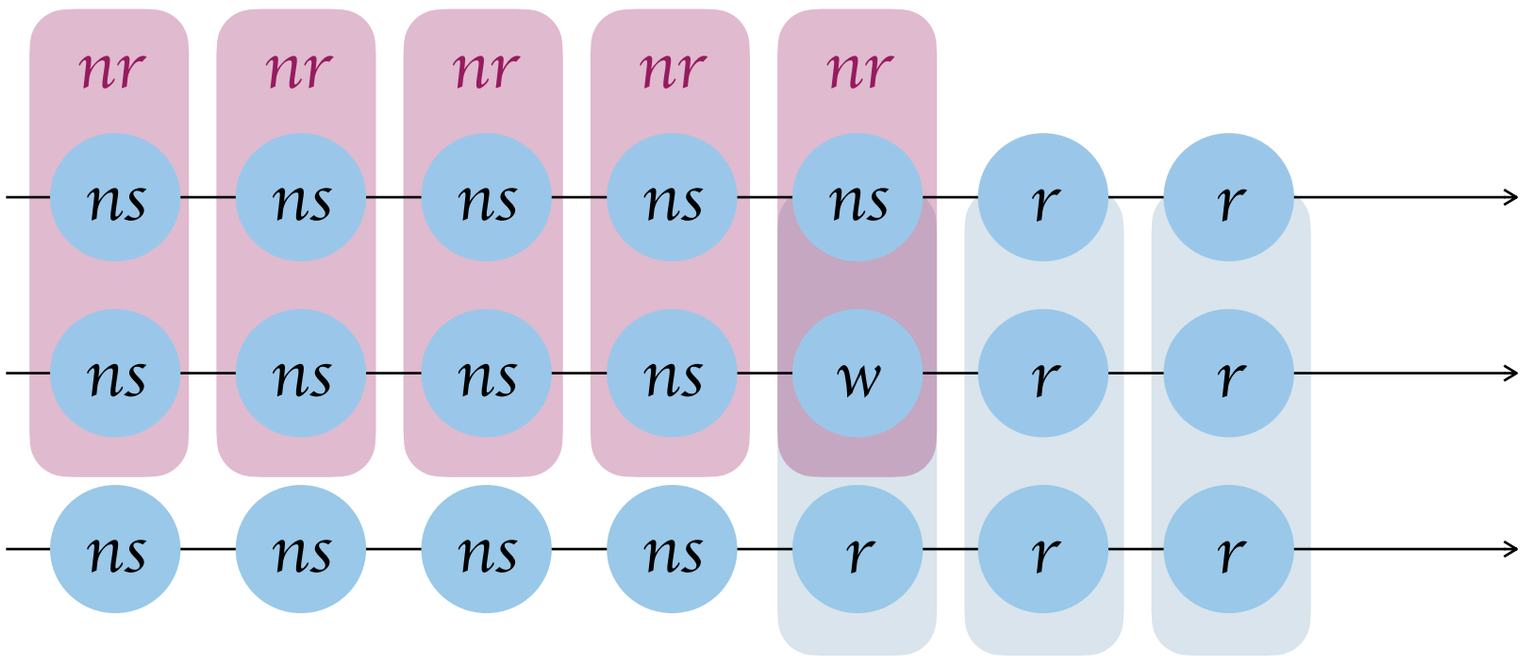
(everybody knows)$^{\omega}$ φ

Communication in Multi-Agent Systems

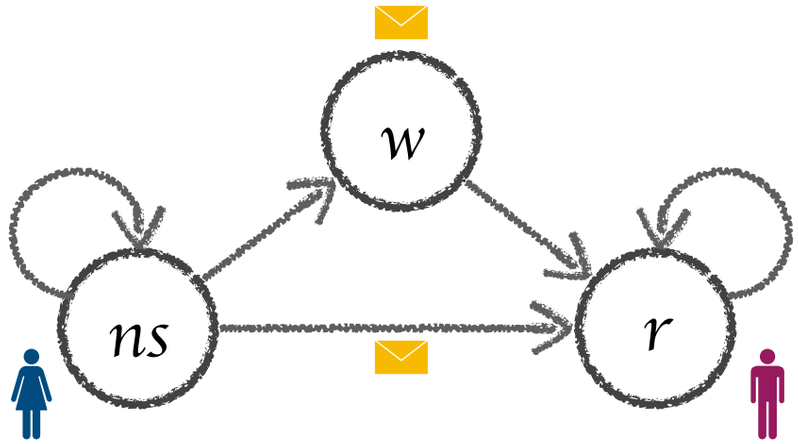


second-order quantification

eventually common knowledge r?

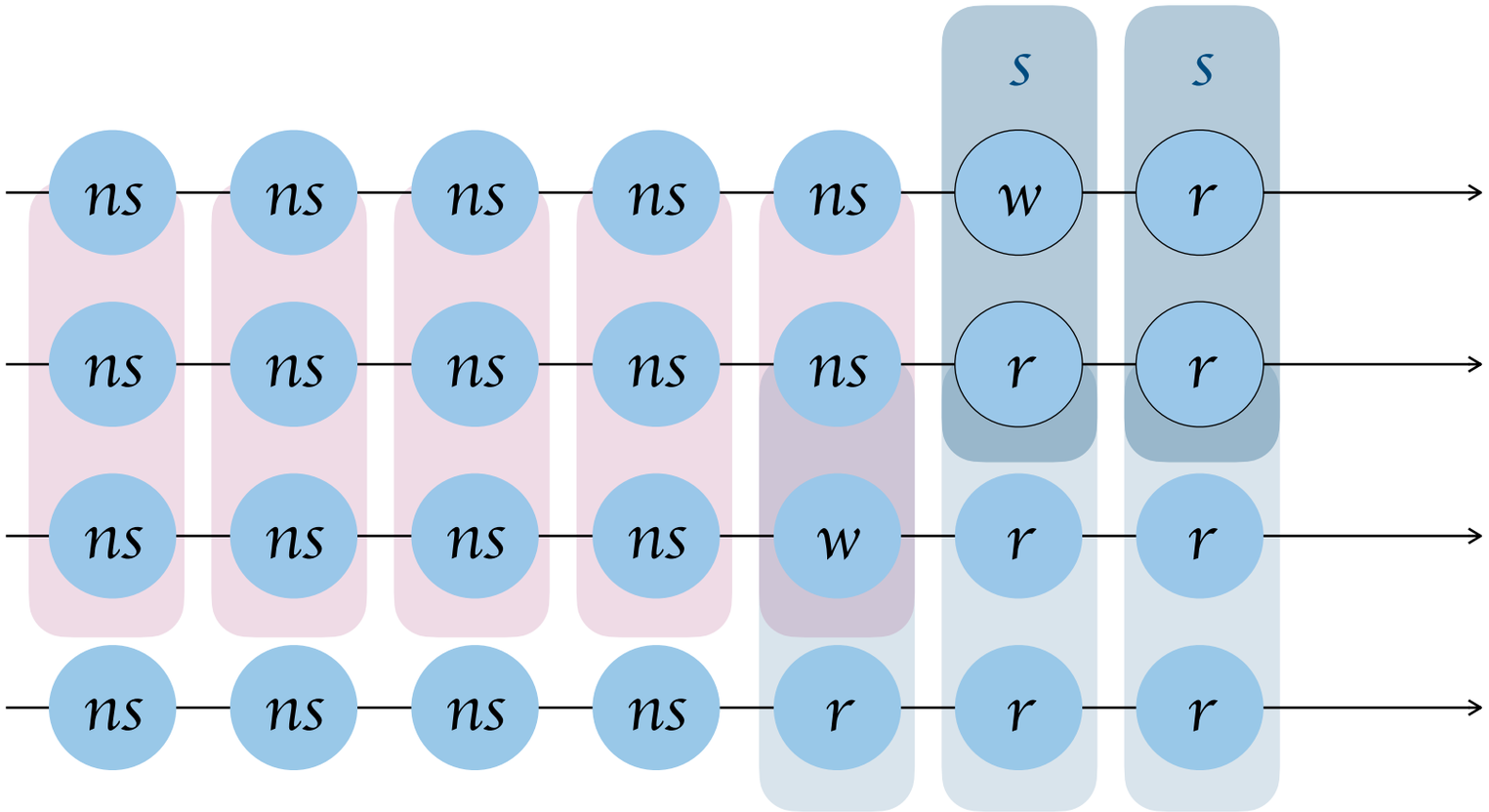


Communication in Multi-Agent Systems

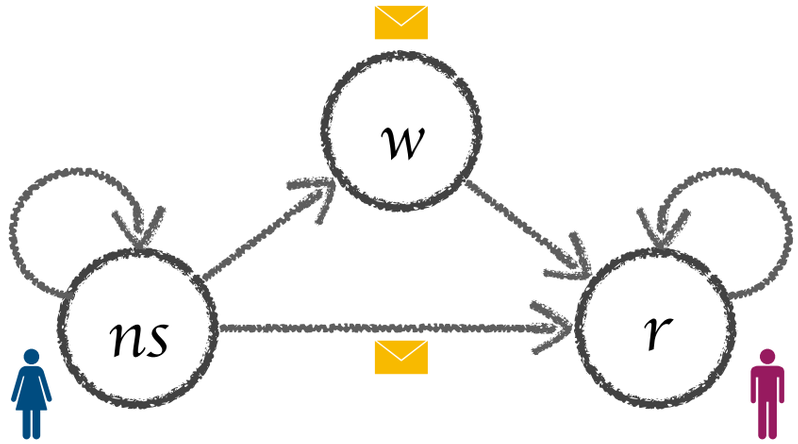


second-order quantification

eventually common knowledge r?

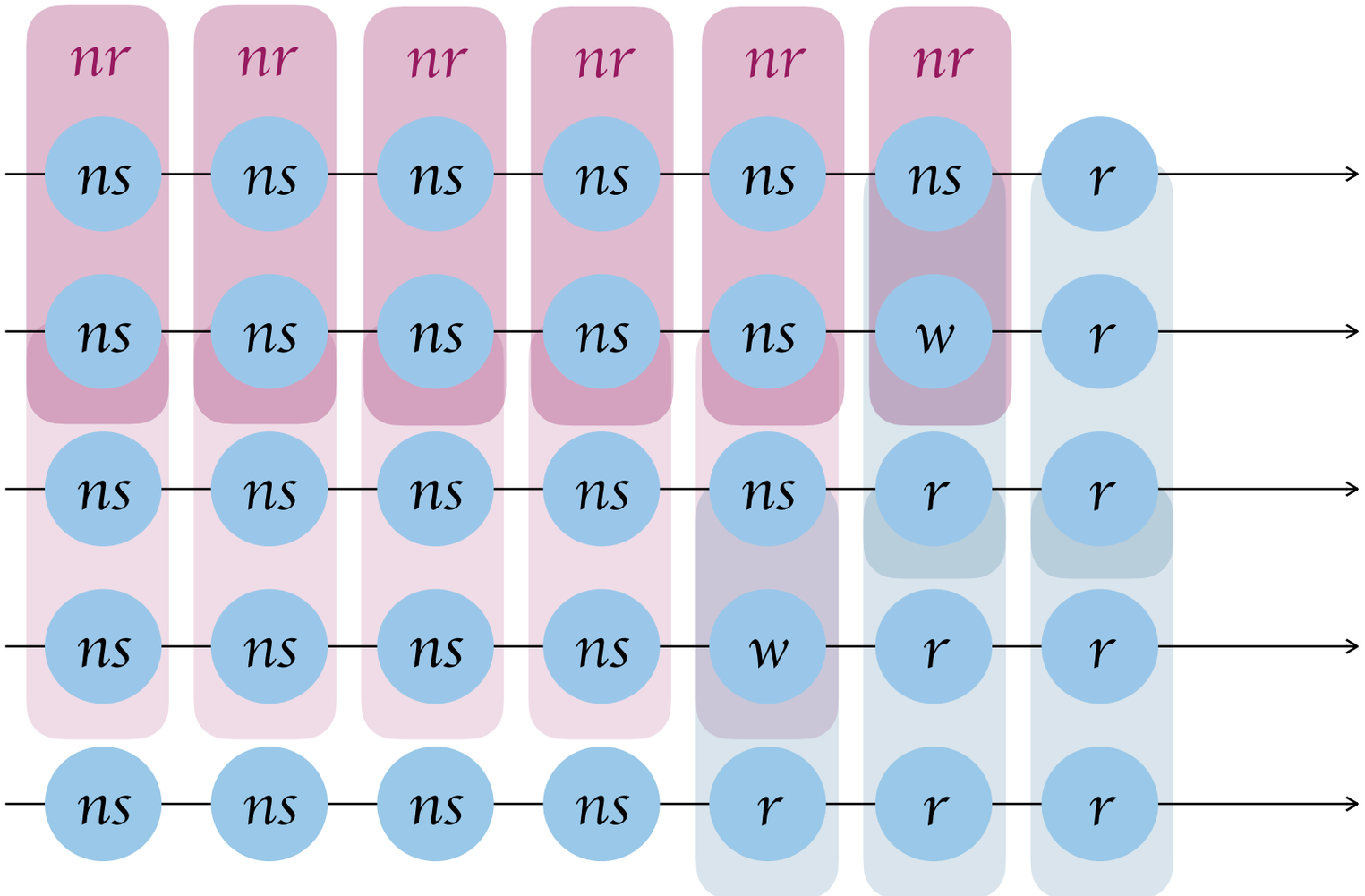


Communication in Multi-Agent Systems

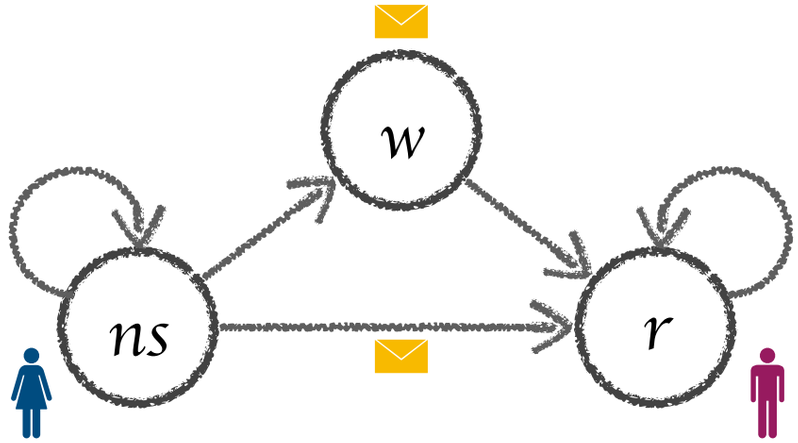


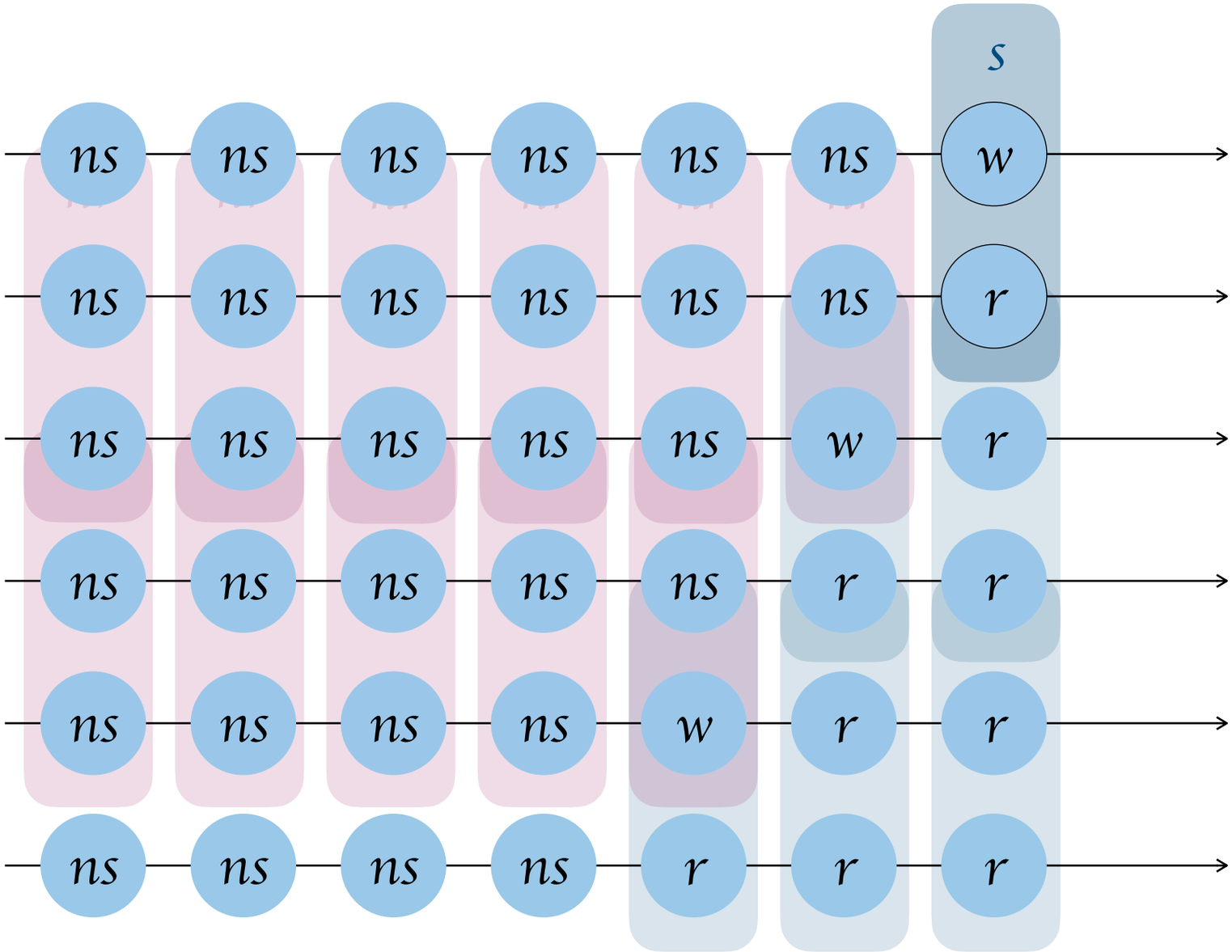
second-order quantification

eventually common knowledge 👫 r ?



Communication in Multi-Agent Systems





second-order quantification

eventually common knowledge r?

Hyper^{2}LTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathbin{\mathsf{U}} \psi$$

$$\varphi := \exists \pi \in X . \varphi \mid \forall \pi \in X . \varphi \mid \exists X . \varphi \mid \forall X . \varphi$$

trace-set variable

$\mathcal{G}$ – system traces
$\mathcal{U}$ – Σ^ω

Hyper^{2}LTL

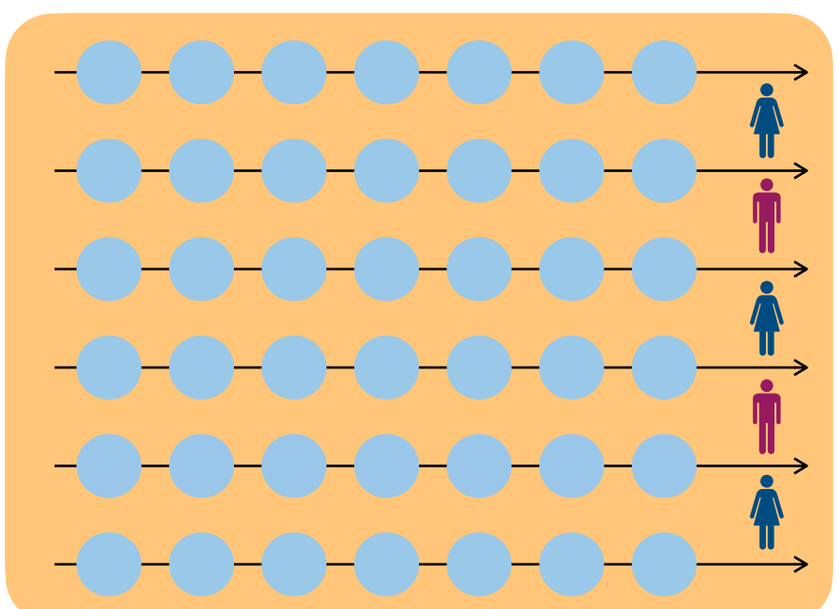
$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathbin{\mathsf{U}} \psi$$

$$\varphi := \exists \pi \in X . \varphi \mid \forall \pi \in X . \varphi \mid \exists X . \varphi \mid \forall X . \varphi$$

$$\exists \pi . \exists X . \pi \in X \wedge$$

$$\forall \pi \in X . \forall \pi' \in \mathcal{G} . (\pi \equiv_{\text{♀}} \pi' \vee \pi \equiv_{\text{♂}} \pi') \rightarrow \pi' \in X$$

$$\forall \pi' \in X . \Diamond r_{\pi'}$$



eventually common knowledge ♀♂ r ?

Hyper^{2}LTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathbin{\mathsf{U}} \psi$$

$$\varphi := \exists \pi \in X . \varphi \mid \forall \pi \in X . \varphi \mid \exists X . \varphi \mid \forall X . \varphi$$

Trace theory

Asynchronous Hyperproperties

Common knowledge

Model Checking Undecidable

Approximations?

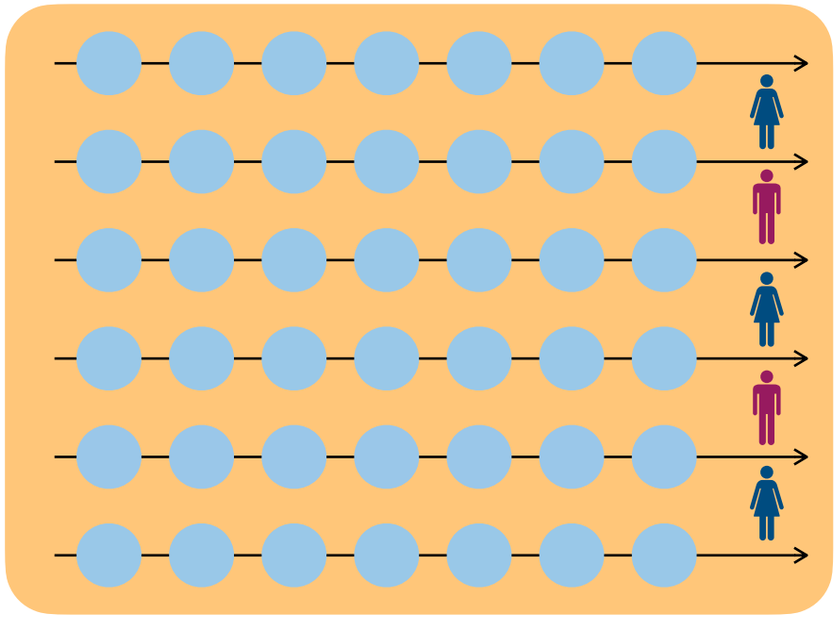
Hyper²LTL

Unique Fixpoints

$$\exists \pi \,.\, \exists X \,.\, \pi \in X \;\wedge$$

$$\forall \pi \in X \,.\, \forall \pi' \in \mathcal{G} \,.\, (\pi \equiv_{\text{♀}} \pi' \vee \pi \equiv_{\text{♂}} \pi') \rightarrow \pi' \in X$$

$$\forall \pi' \in X \,.\, \Diamond r_{\pi'}$$



eventually common knowledge ♂♀ r ?

Trace theory

Asynchronous Hyperproperties

Model Checking Hyper^{2}LTL

Unique Fixpoints

$$\varphi = \exists \pi_1 . \; X_1 \; . \forall \pi_2 \in X_1 . \ldots . \; X_k \; . \exists \pi_{k+1} \in X_k . \psi$$

Automaton A_1

Automaton A_k

$$A_1 \times A_2 \times \cdots \times A_k \models \psi$$

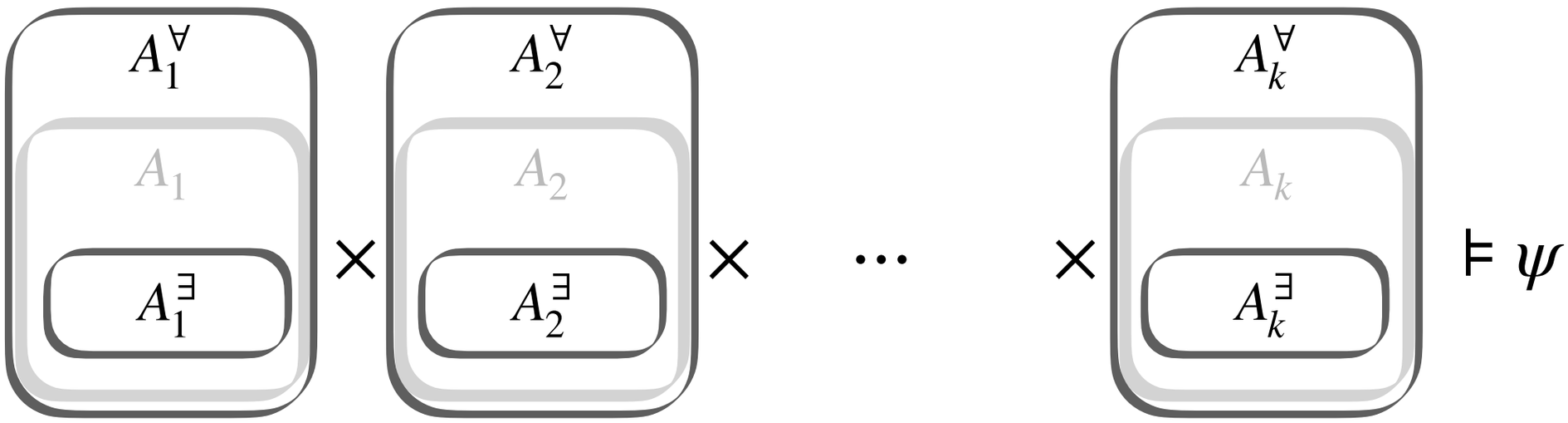
HyperLTL model checking

*Algorithms for Model Checking HyperLTL and HyperCTL**. Finkbeiner, Rabe, Sánchez (CAV 2015)

Model Checking Hyper^{2}LTL

Unique Fixpoints

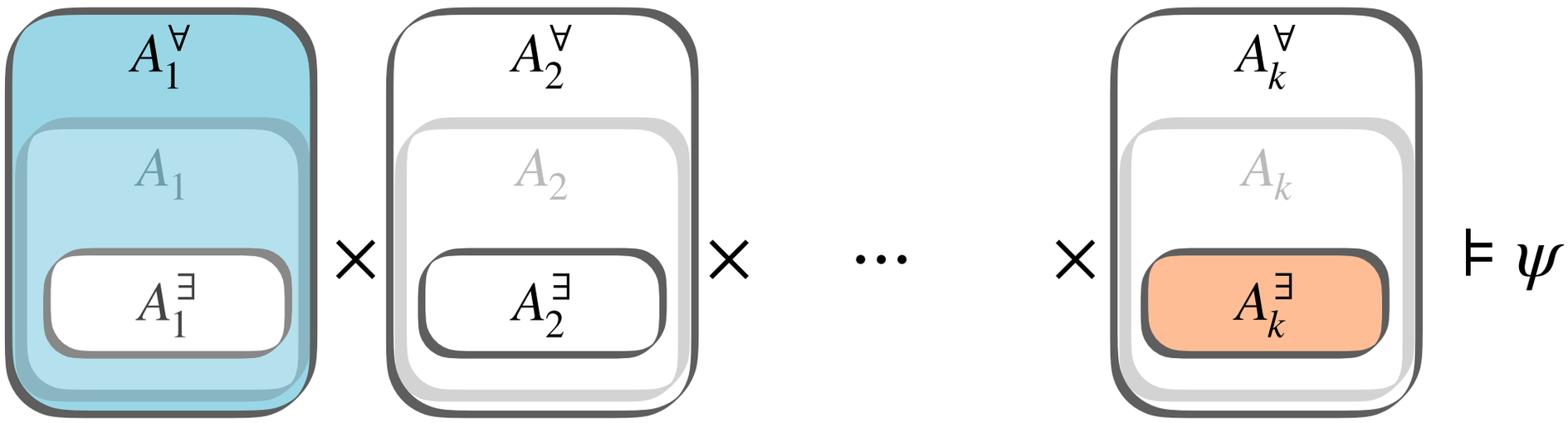
$$\varphi = \exists \pi_1 . \; X_1 \; . \forall \pi_2 \in X_1 . \ldots . \; X_k \; . \exists \pi_{k+1} \in X_k . \psi$$



Model Checking Hyper^{2}LTL

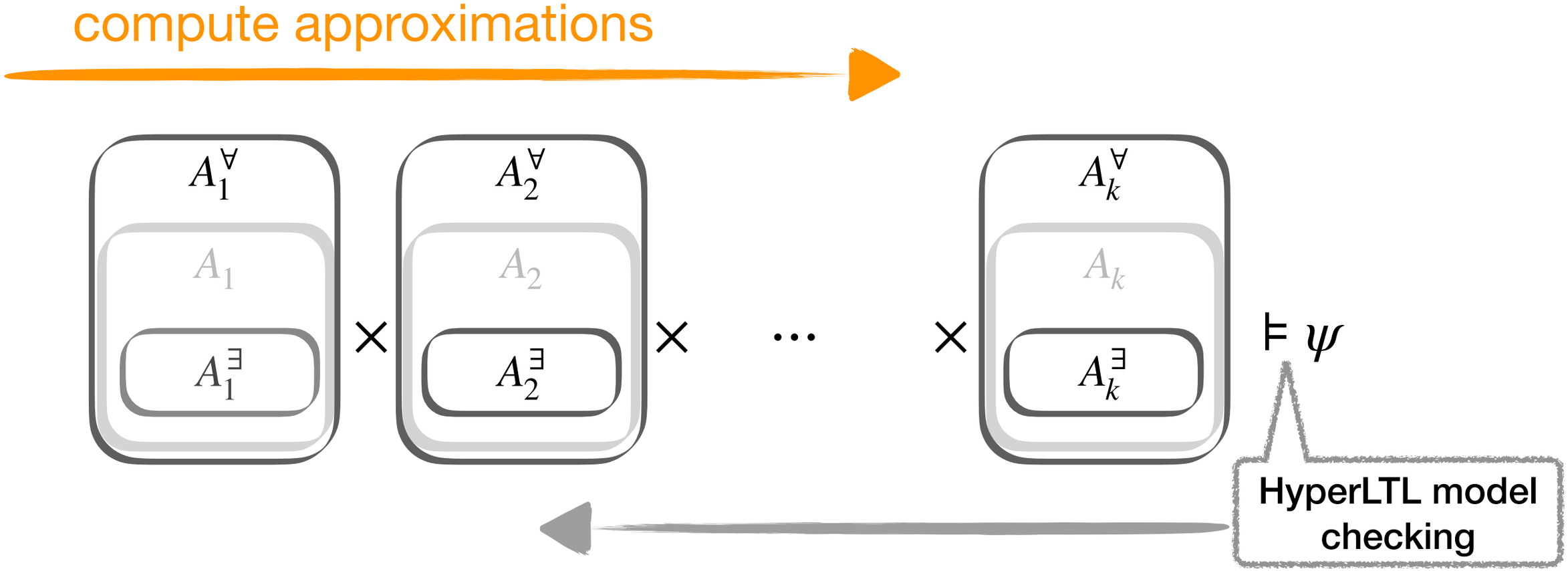
Unique Fixpoints

$$\varphi = \exists \pi_1 . \; X_1 . \forall \pi_2 \in X_1 . \ldots . \; X_k . \exists \pi_{k+1} \in X_k . \psi$$



Model Checking Hyper^{2}LTL

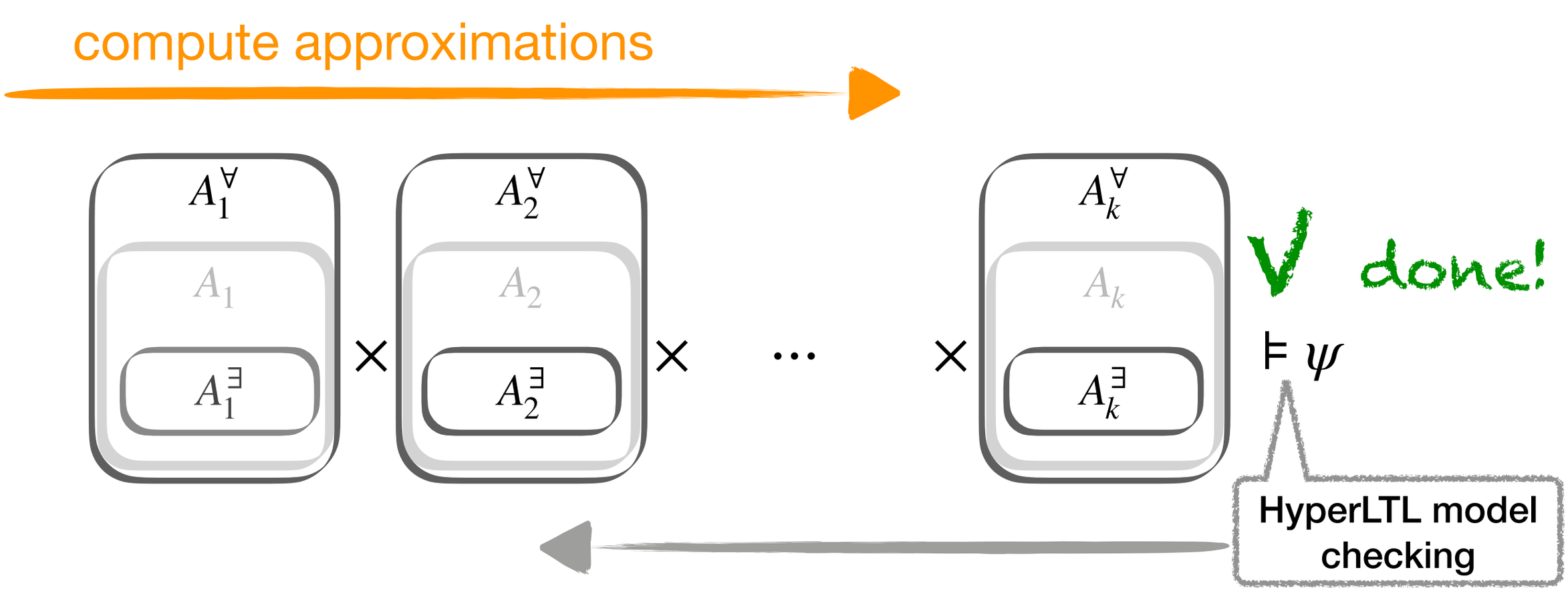
Unique Fixpoints



*Algorithms for Model Checking HyperLTL and HyperCTL**. Finkbeiner, Rabe, Sánchez (CAV 2015)

Model Checking Hyper^{2}LTL

Unique Fixpoints

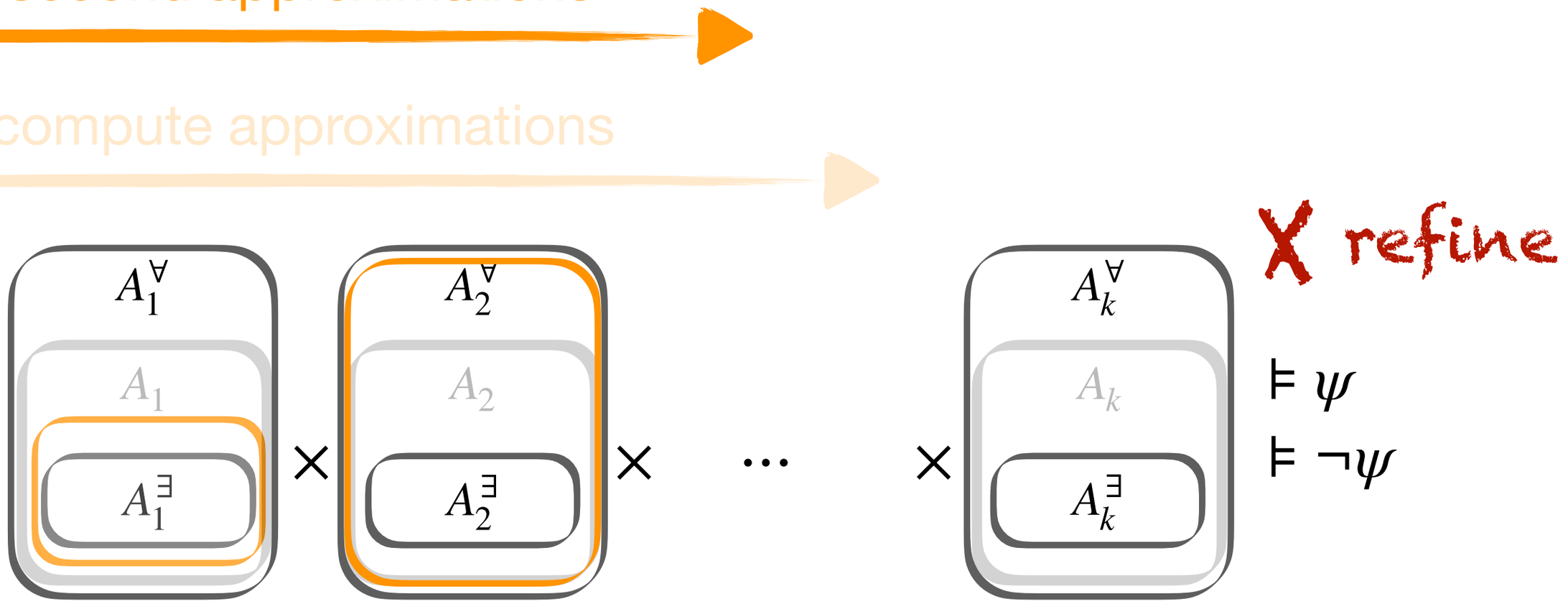


*Algorithms for Model Checking HyperLTL and HyperCTL**. Finkbeiner, Rabe, Sánchez (CAV 2015)

Model Checking Hyper^{2}LTL

Unique Fixpoints

compute second approximations



Implementation

Instance	Method	Res	t
$\mathcal{T}_{syn}$, φ_{OD}	-	✓	0.26
$\mathcal{T}_{asyn}$, φ_{OD}	-	✗	0.31
$\mathcal{T}_{syn}$, φ_{OD}^{asyn}	Iter (0)	✓	0.50
$\mathcal{T}_{asyn}$, φ_{OD}^{asyn}	Iter (1)	✓	0.78
Q1, φ_{OD}	-	✗	0.34
Q1, φ_{OD}^{asyn}	Iter (1)	✓	0.86

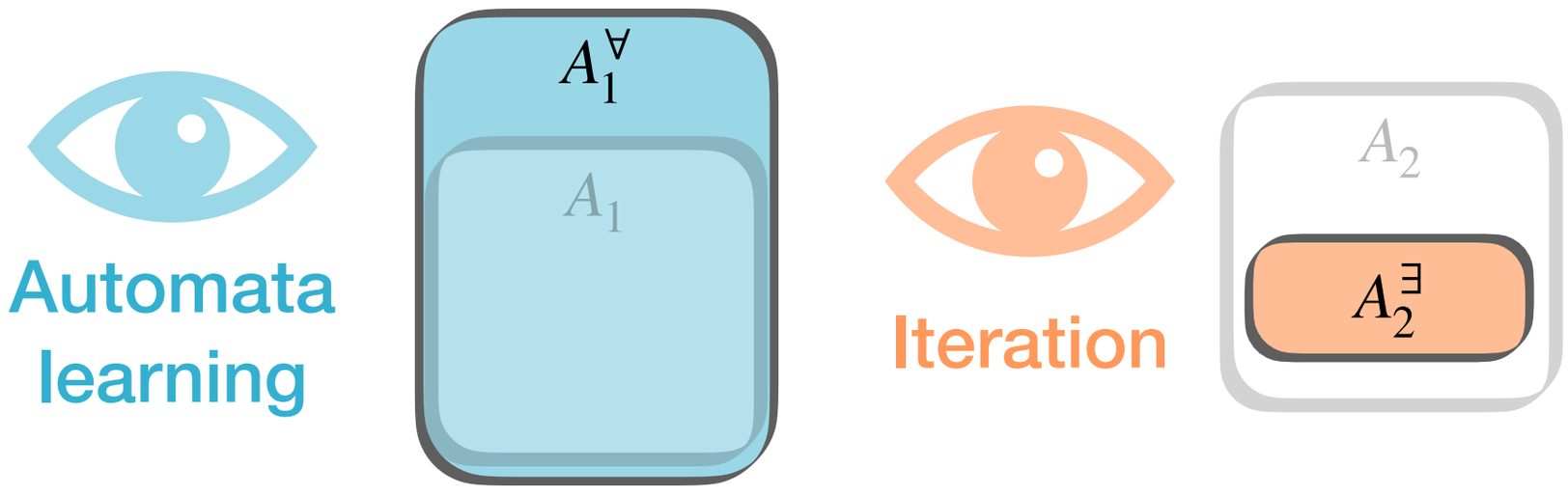
Asynchronous Hyperproperties

n	Method	Res	t
1	Iter (1)	✓	0.51
2	Iter (3)	✓	0.83
3	Iter (5)	✓	1.20
10	Iter (19)	✓	3.81
100	Iter (199)	✓	102.8

Common Knowledge

Instance	Method	Res	t
SwapA	Learn	✓	1.07
SwapATwice	Learn	✓	2.13
SwapA_5	Iter (5)	✓	1.15
SwapA_{15}	Iter (15)	✓	3.04
SwapAViolation_5	Iter (5)	✗	2.35
$\text{SwapAViolation}_{15}$	Iter (15)	✗	4.21

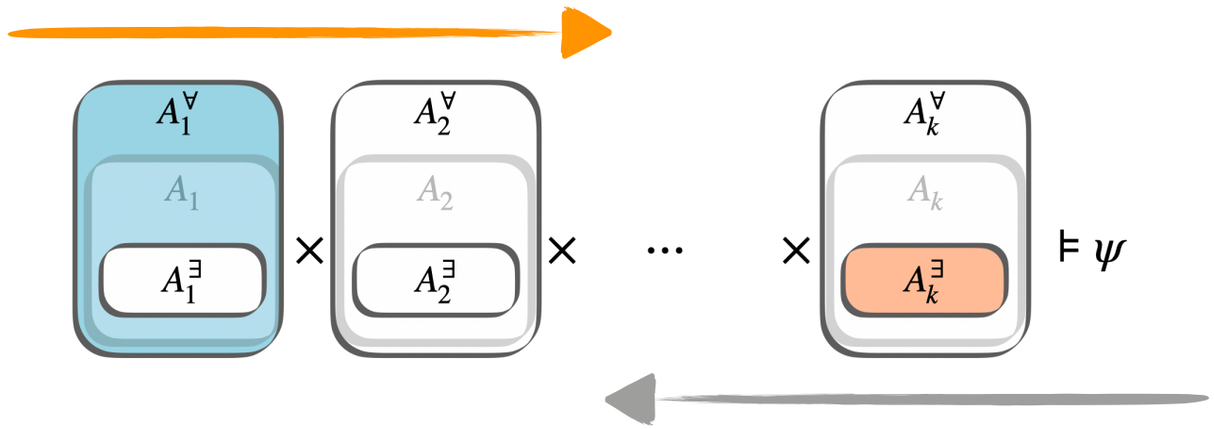
Mazurkiewicz Traces

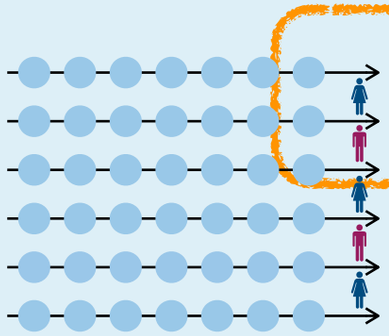


Hyper²LTL

$$\psi := a_\pi \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \mathcal{U} \psi$$

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





Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Thank you!

Generic reasoning and algorithms