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

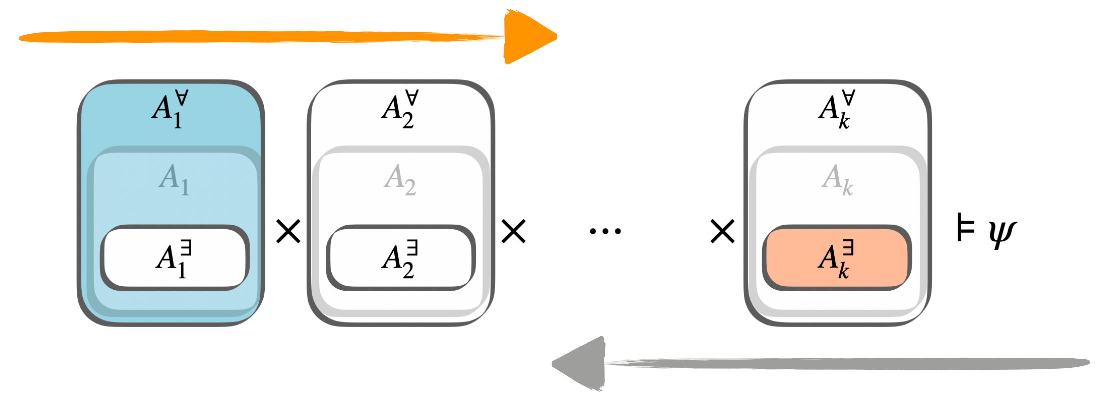
21 July @ CAV 2023

Overview

Hyper²LTL

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

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



Model checking

Trace theory

Asynchronous Hyperproperties

Common knowledge

Hyper²LTL

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

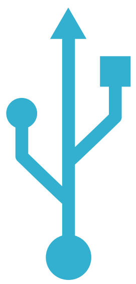
$$\varphi := \exists \pi \in X \,.\, \varphi \mid \forall \pi \in X \,.\, \varphi \mid \exists X \,.\, \varphi \mid \forall X \,.\, \varphi$$

Second-order logic
for the specification of
Hyperproperties

Hyperproperties

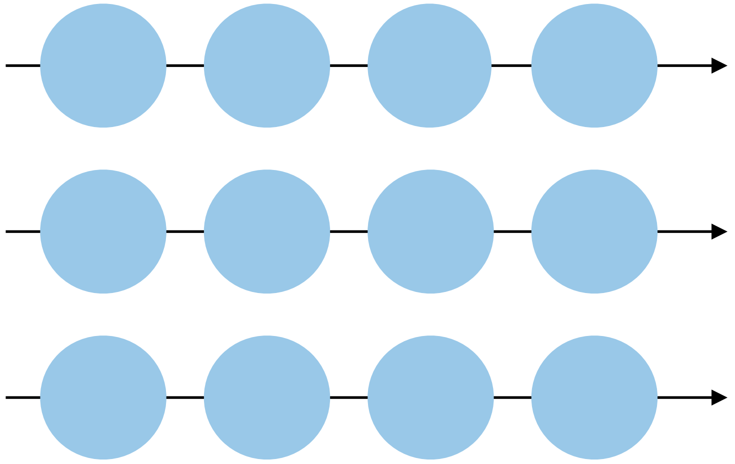
Knowledge

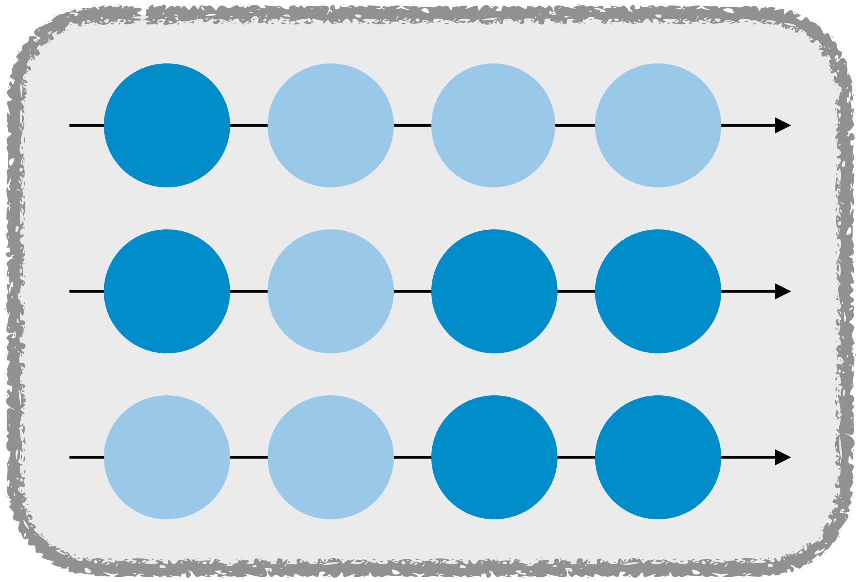
Fairness



Information-flow

Robustness





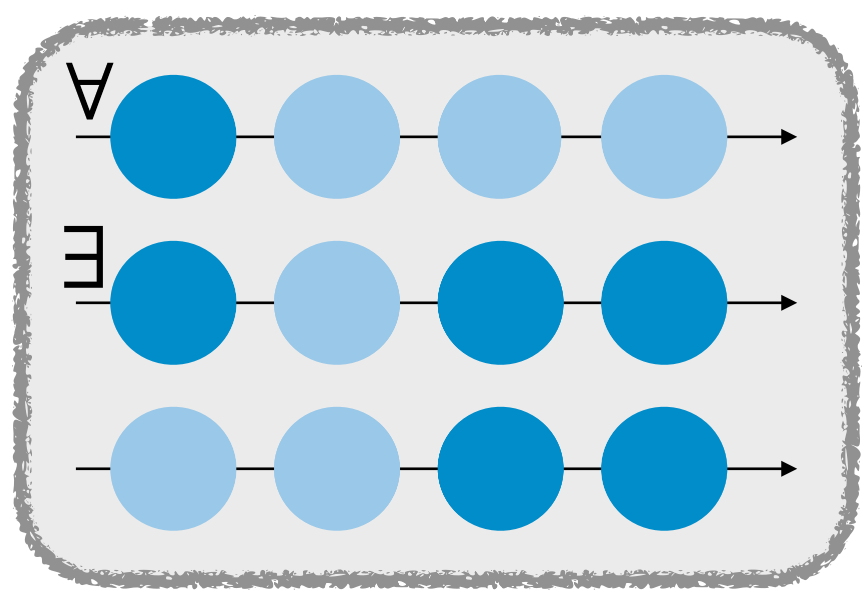
Hyperproperties. Clarkson and Schneider (CSF 2008)

HyperLTL

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

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

trace variable



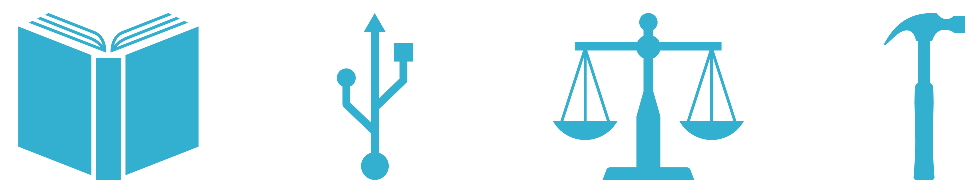
Temporal Logics for Hyperproperties. Clarkson, Finkbeiner, Koleini, Micinski, Rabe, and Sánchez. (POST 2014).

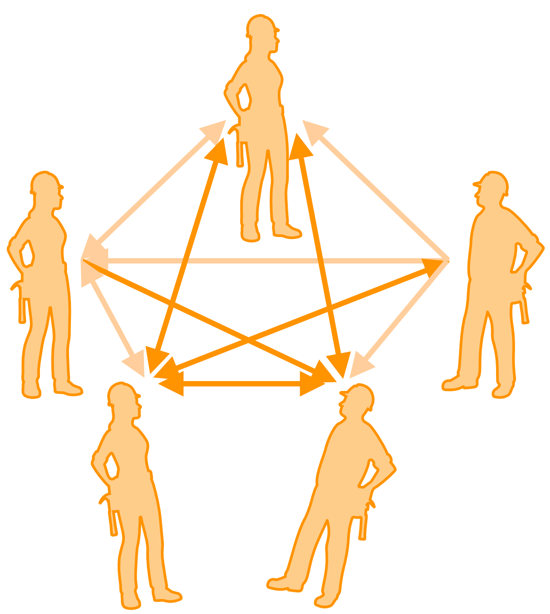
HyperLTL

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

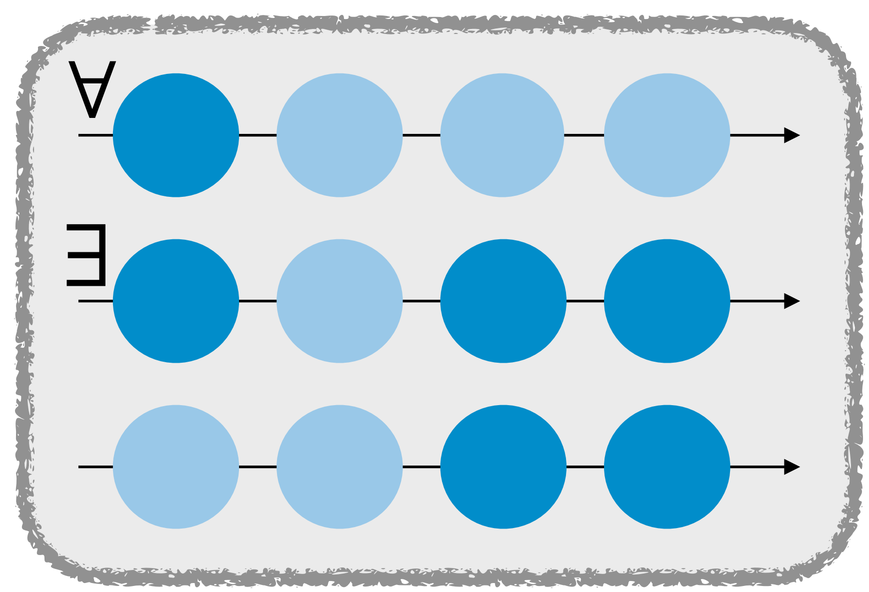
$$\varphi := \exists\pi\,.\,\varphi \mid \forall\pi\,.\,\varphi$$

trace variable





Common Knowledge



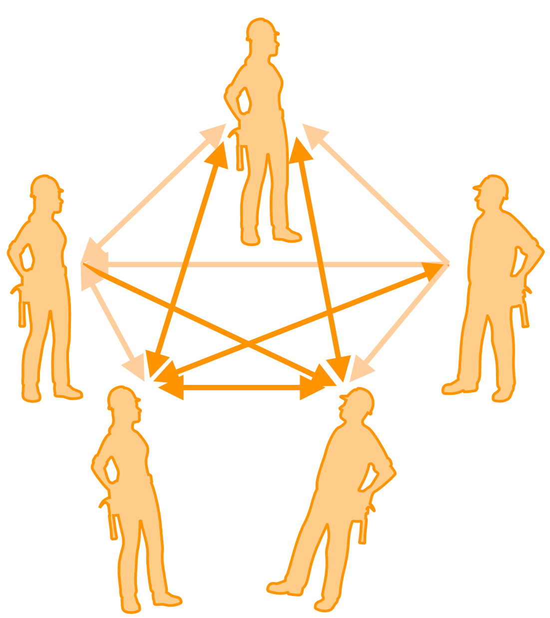
Temporal Logics for Hyperproperties. Clarkson, Finkbeiner, Koleini, Micinski, Rabe, and Sánchez. (POST 2014).

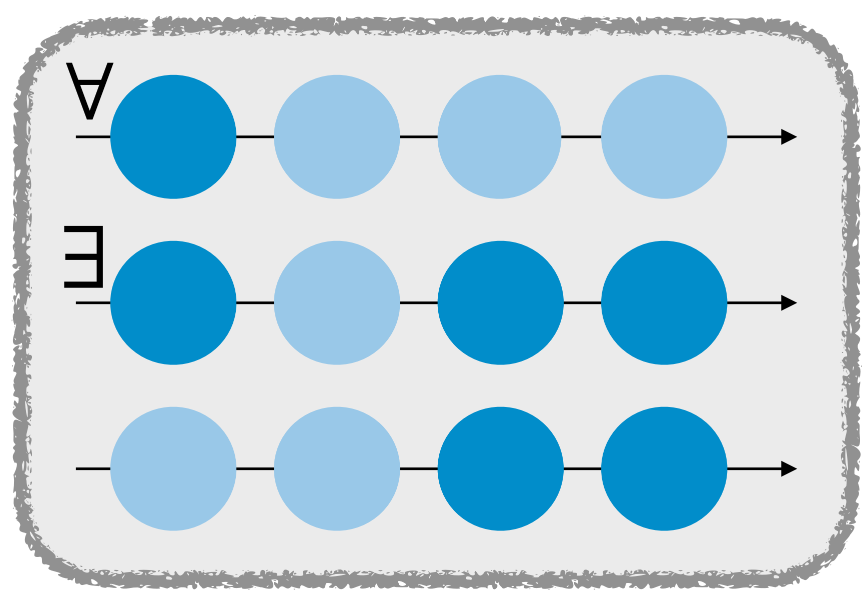
HyperLTL

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

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

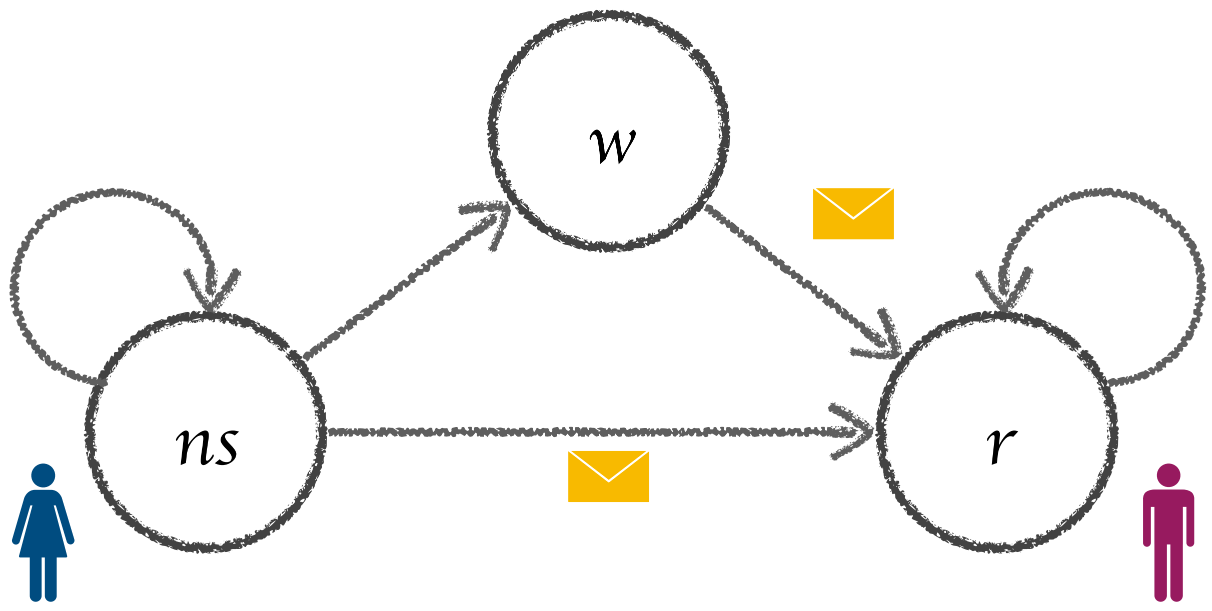
trace variable


Common Knowledge

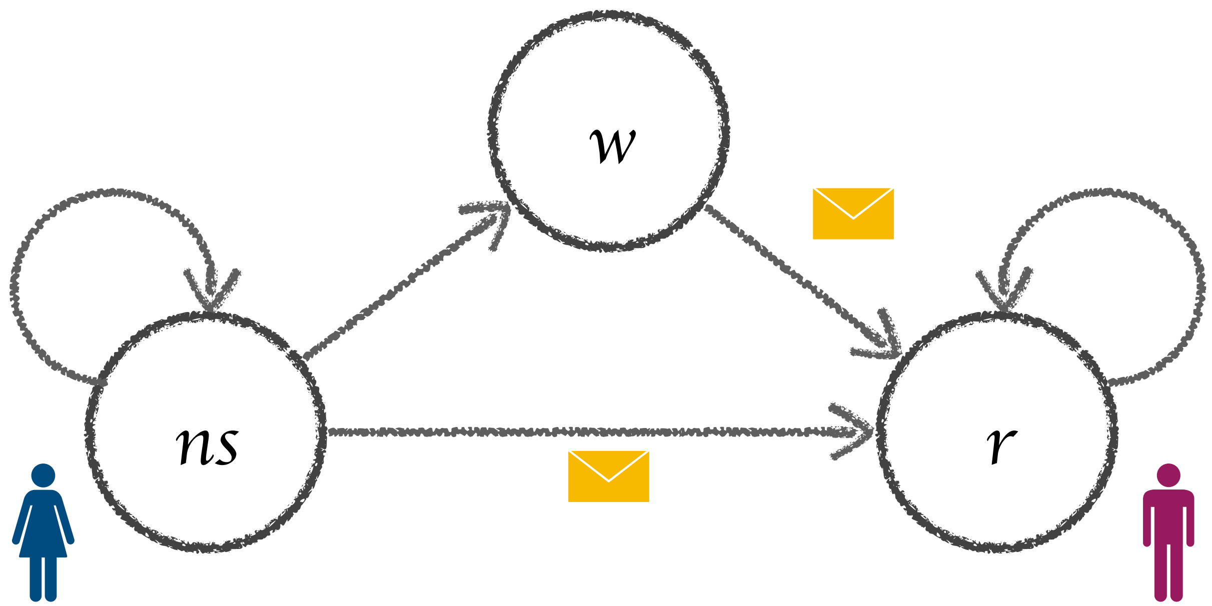


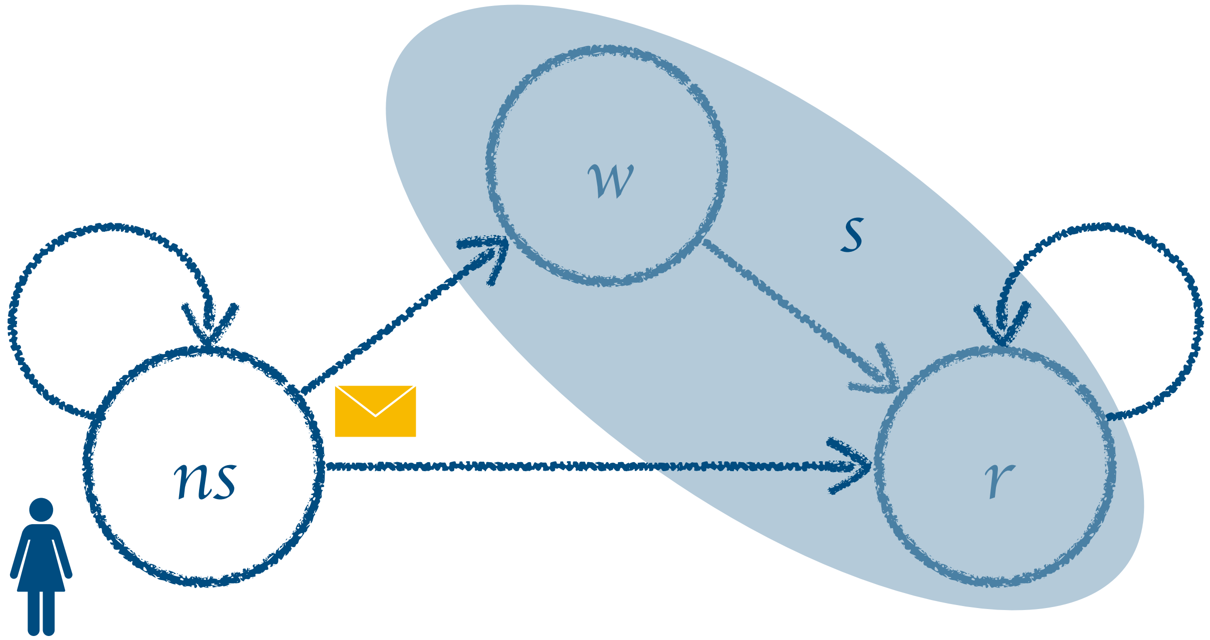
Temporal Logics for Hyperproperties. Clarkson, Finkbeiner, Koleini, Micinski, Rabe, and Sánchez. (POST 2014).

Communication in Multi-Agent Systems

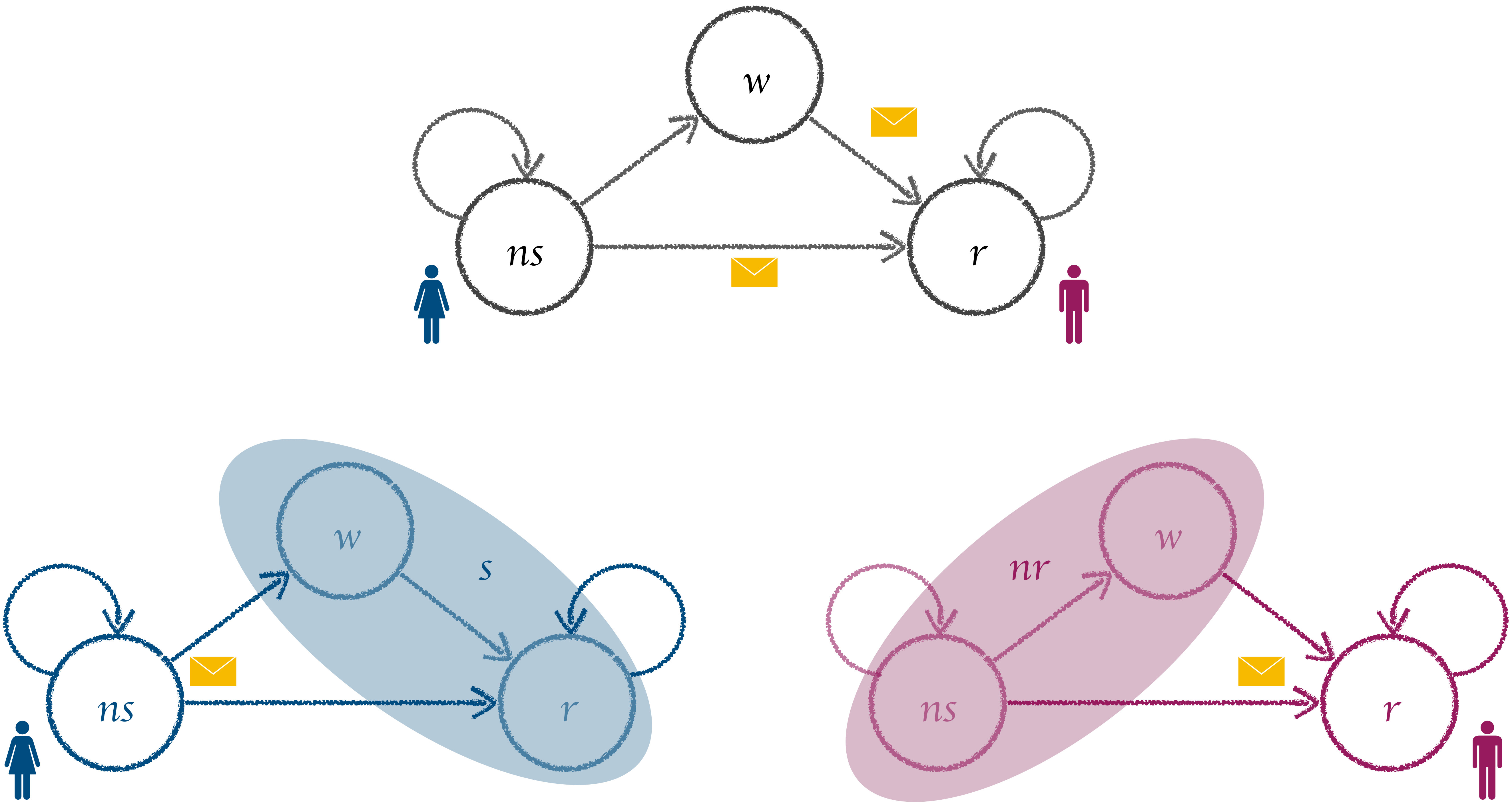


Communication in Multi-Agent Systems

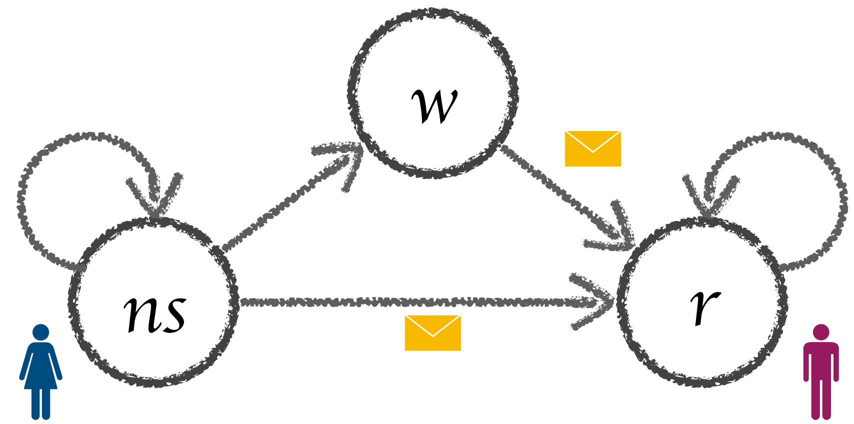


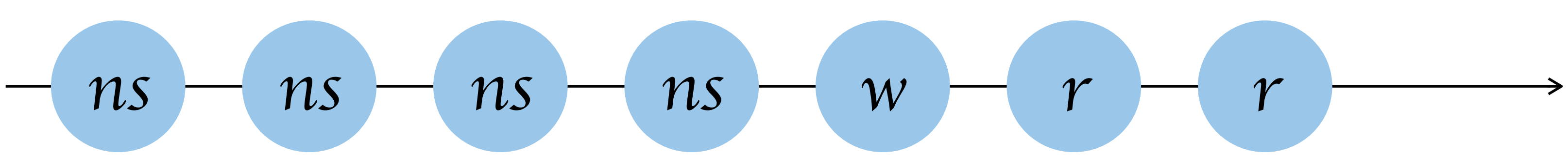


Communication in Multi-Agent Systems



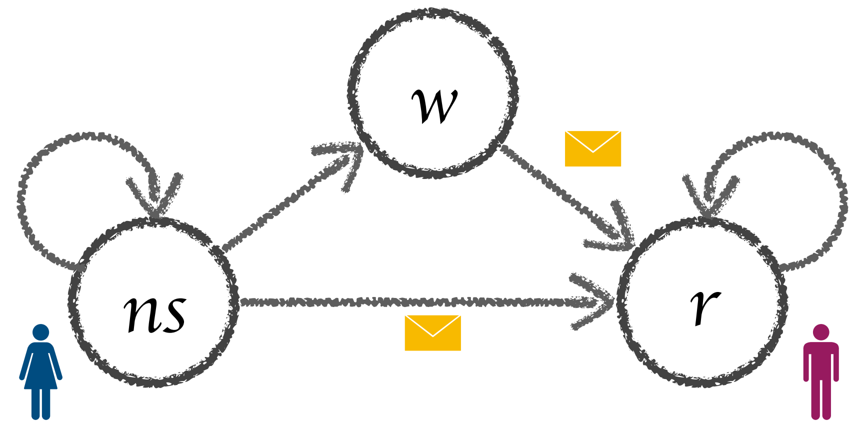
Communication in Multi-Agent Systems

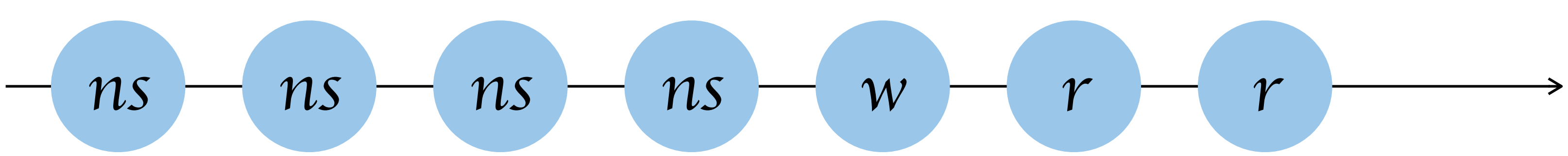




eventually r ?

Communication in Multi-Agent Systems

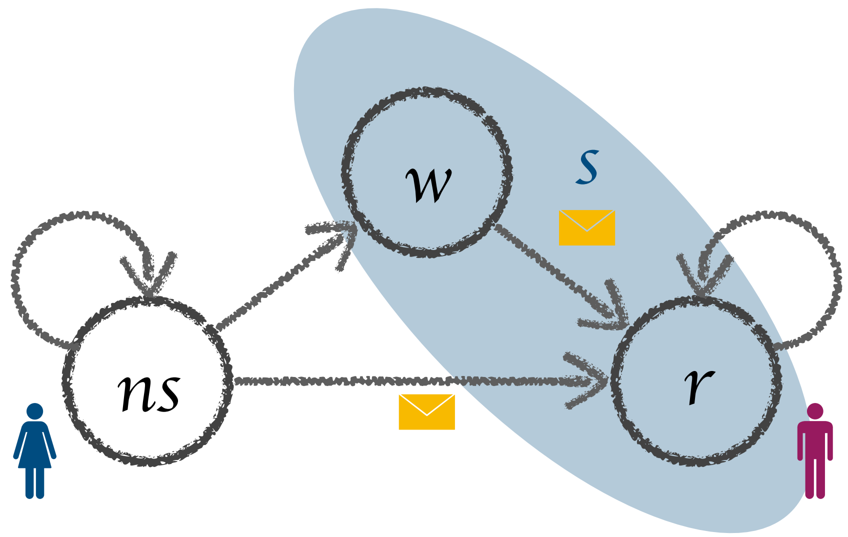


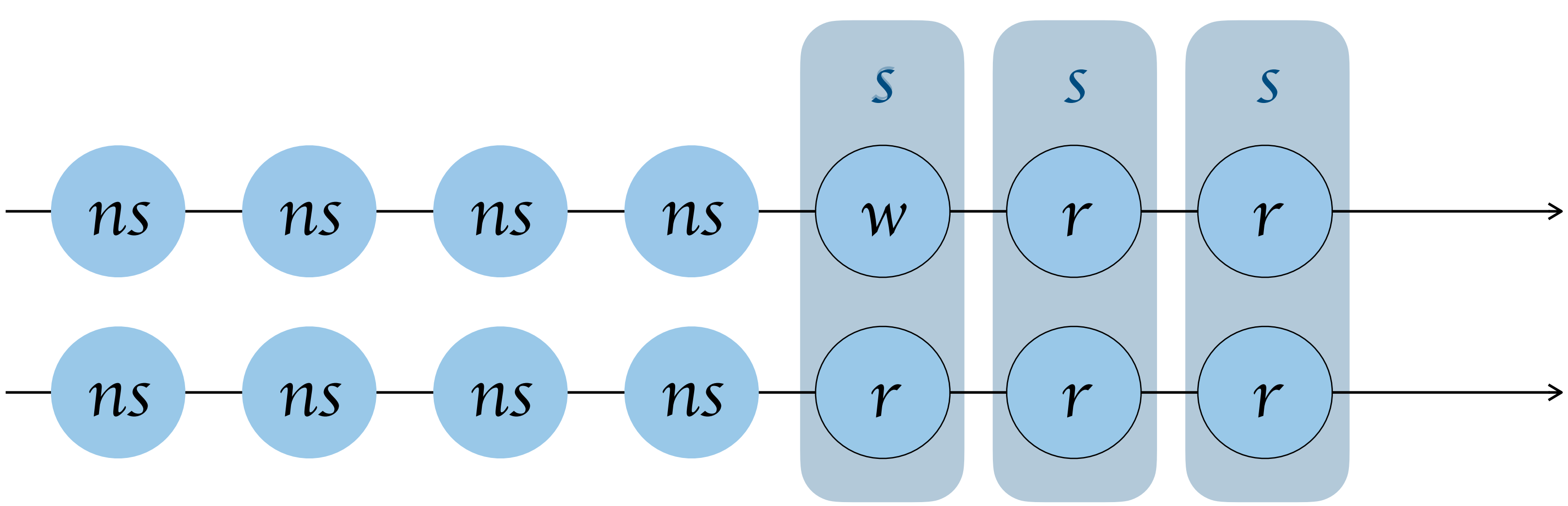


Trace property (LTL)

eventually r ?

Communication in Multi-Agent Systems





Hyperproperty

eventually knows r ?

HyperLTL

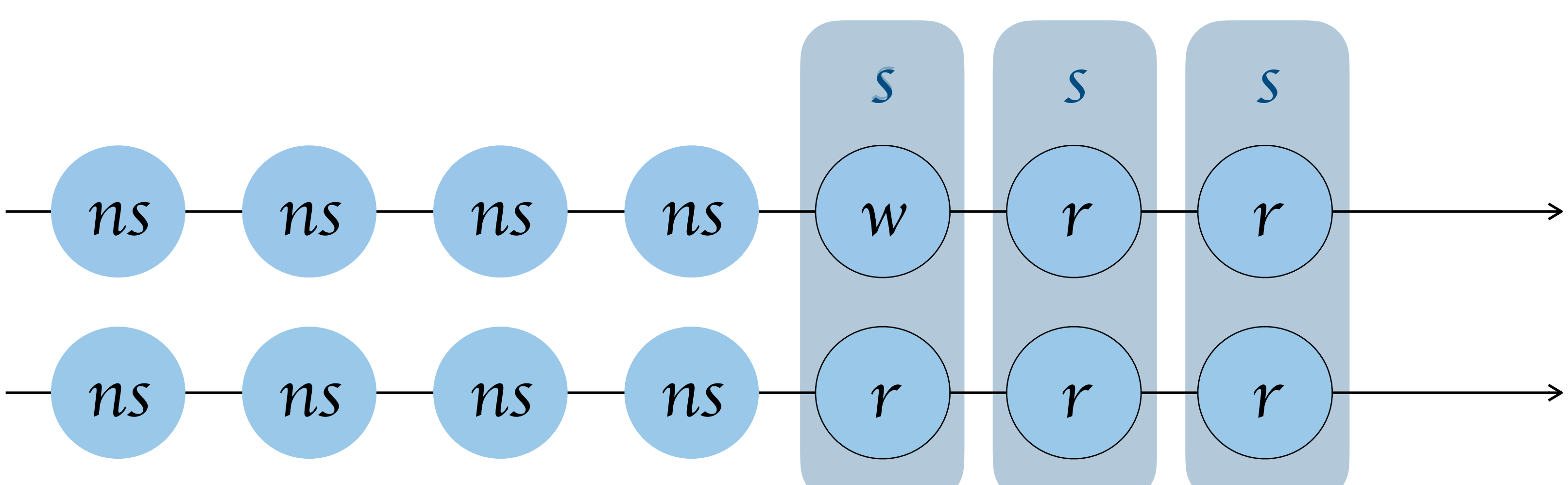
$$\psi := \; a_{\pi} \mid \neg\psi \mid \psi \wedge \psi \mid \bigcirc\psi \mid \psi \, \mathsf{U} \, \psi$$

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

$$\exists \pi \forall \pi' \,.\, (\pi \equiv \pi') \rightarrow \Diamond r_{\pi'}$$

Hyperproperty

eventually knows r ?



HyperLTL

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

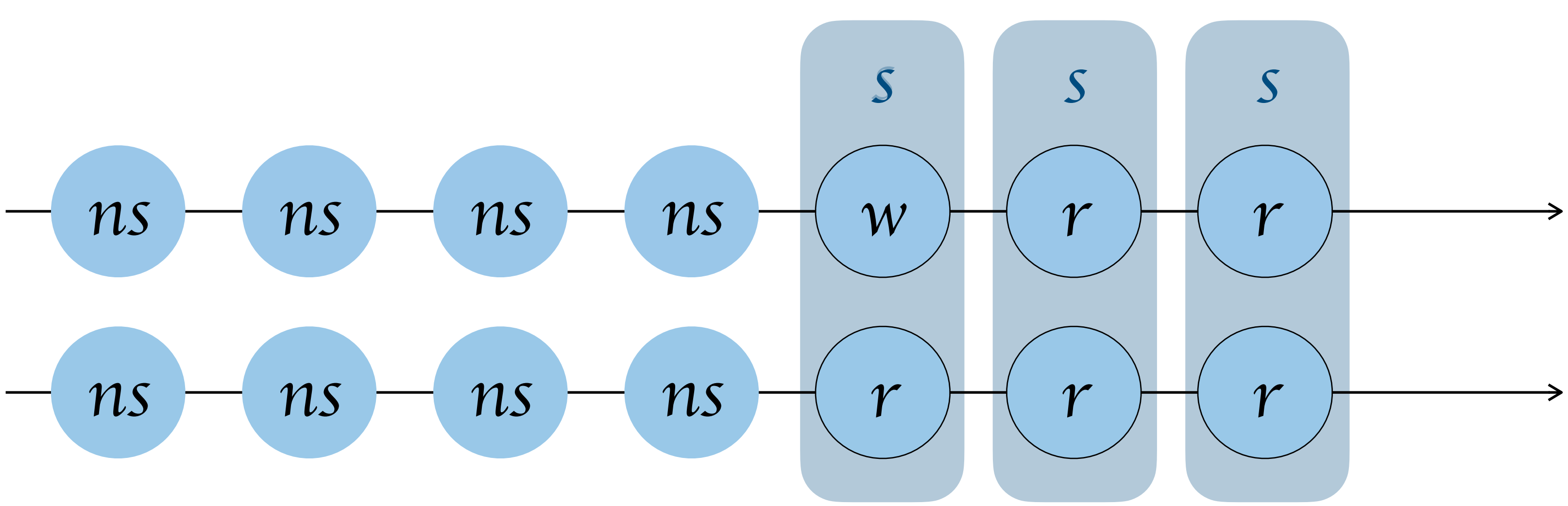
$$\varphi := \exists\pi\,.\,\varphi \mid \forall\pi\,.\,\varphi$$

$$\Box\big((ns_\pi \leftrightarrow ns_{\pi'}) \wedge (s_\pi \leftrightarrow s_{\pi'})\big)$$

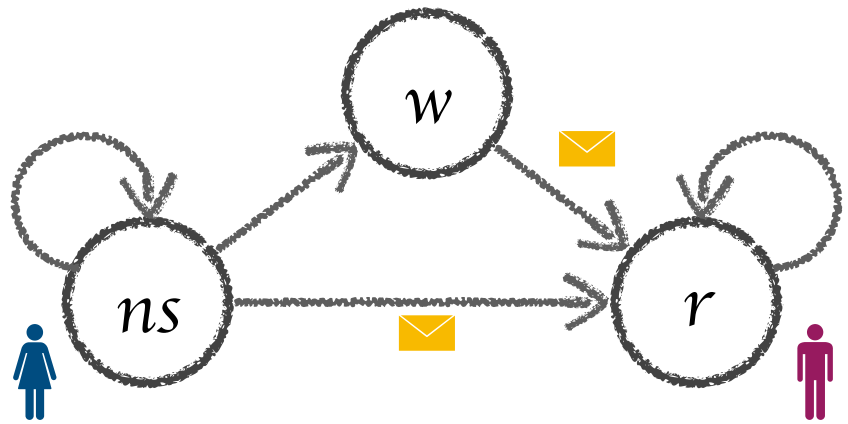
$$\exists\pi\forall\pi'\,.\,(\pi \equiv \pi') \rightarrow \Diamond r_{\pi'}$$

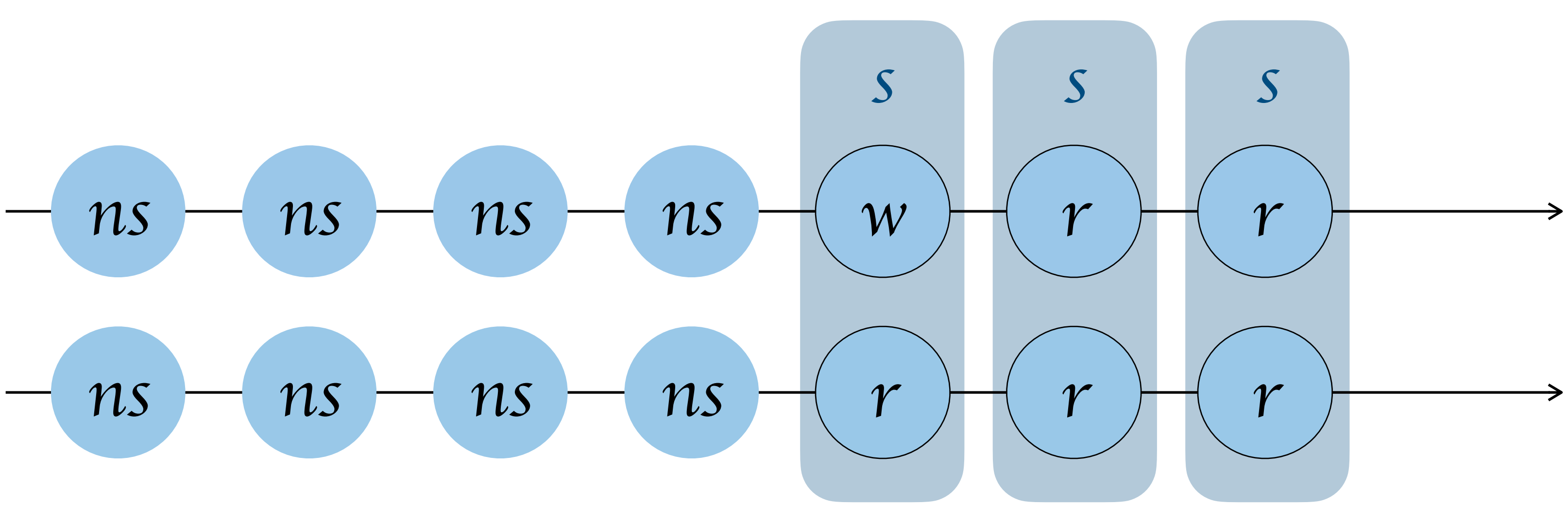
Hyperproperty

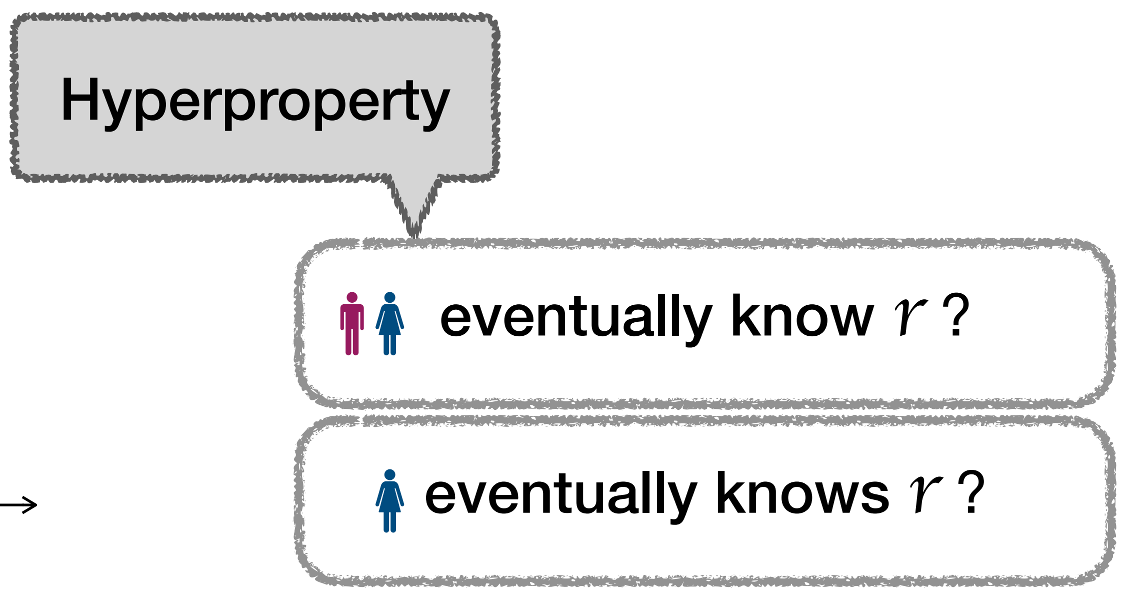
eventually knows r ?



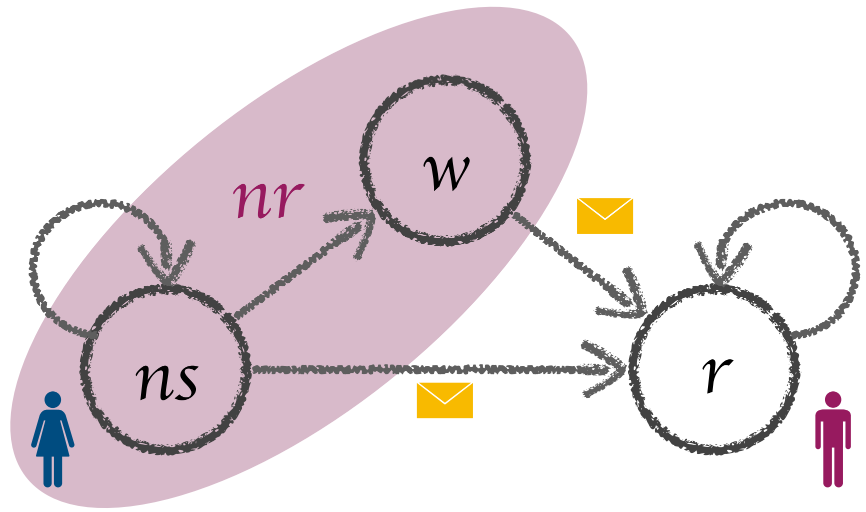
Communication in Multi-Agent Systems

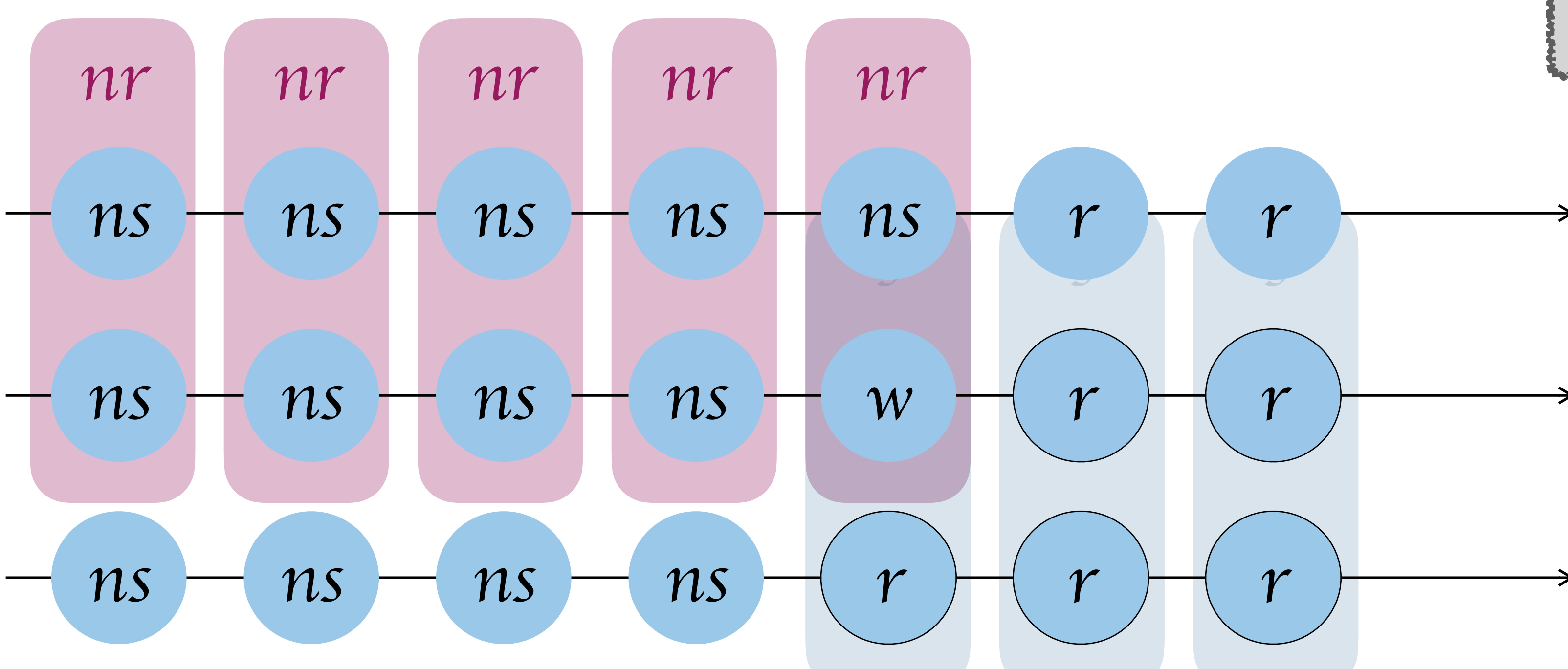






Communication in Multi-Agent Systems



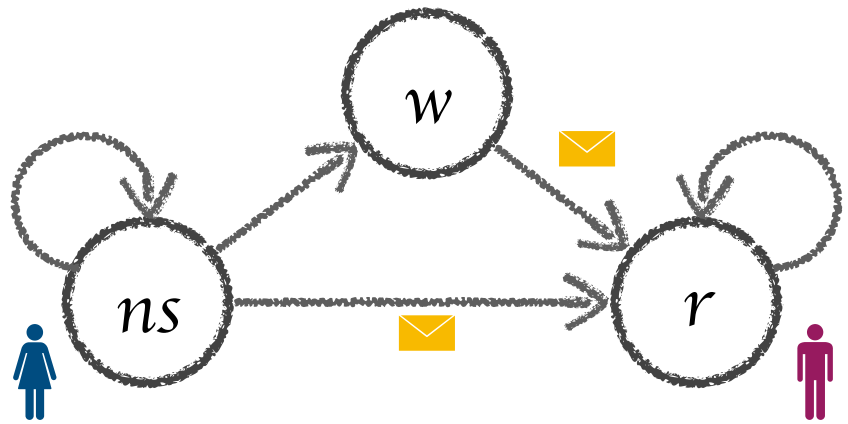


Hyperproperty

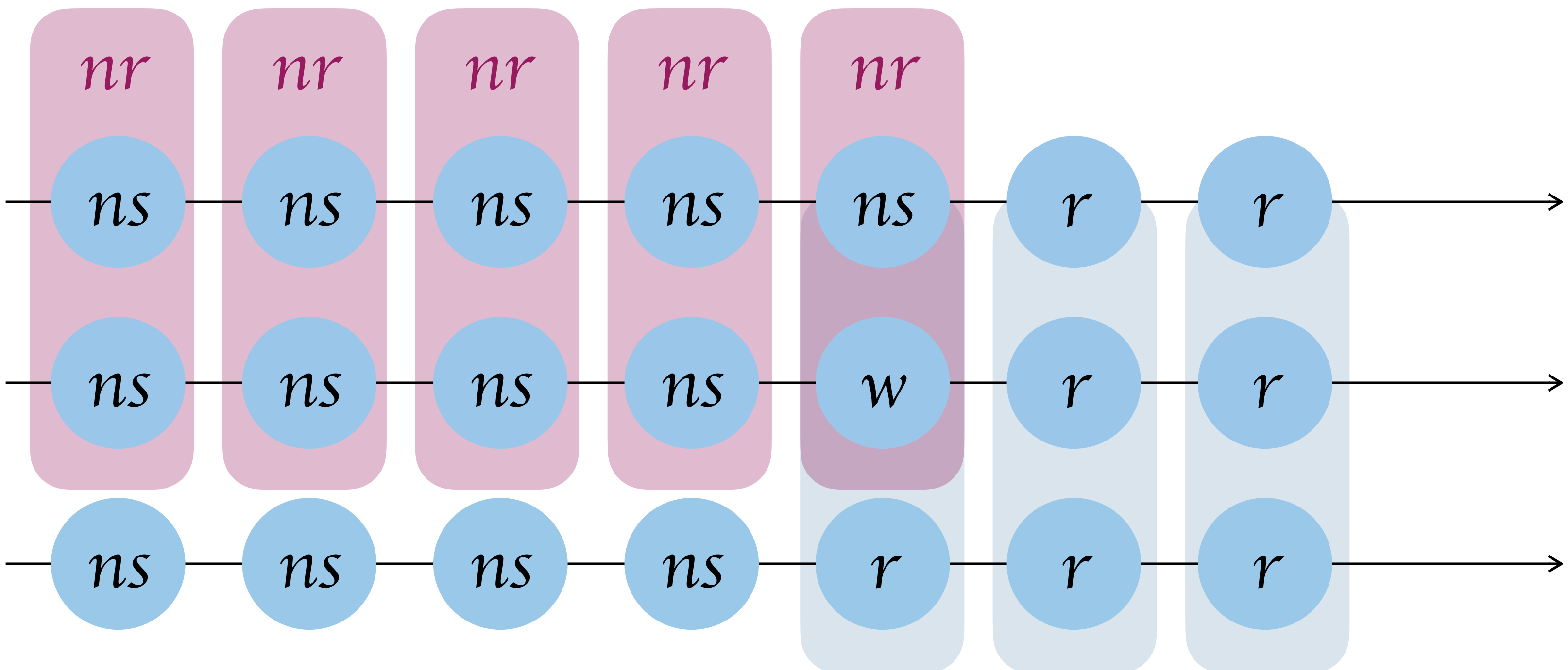
eventually know r ?

eventually knows r ?

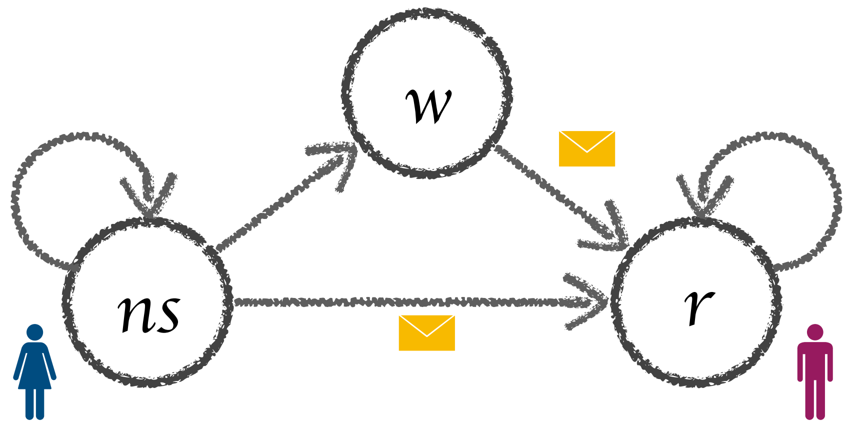
Communication in Multi-Agent Systems



eventually common knowledge r ?



Common Knowledge



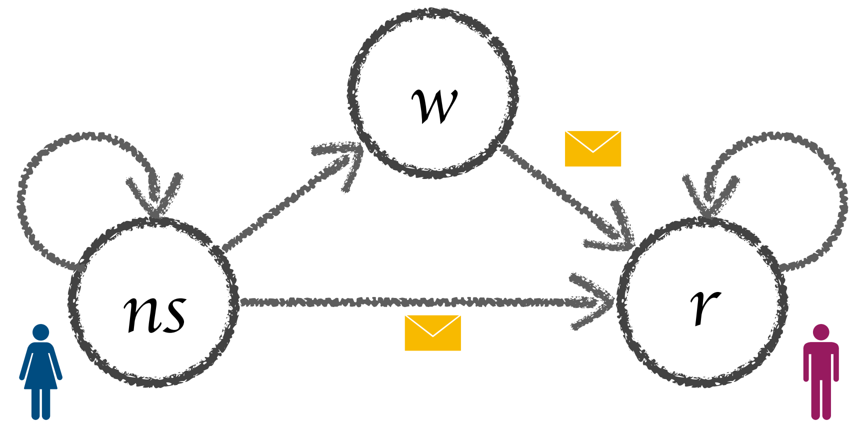
eventually common knowledge r ?

φ common knowledge

$\leftrightarrow$

(know)$^{\omega}$ φ

Common Knowledge



eventually common knowledge r ?

first-order trace quantification is not enough

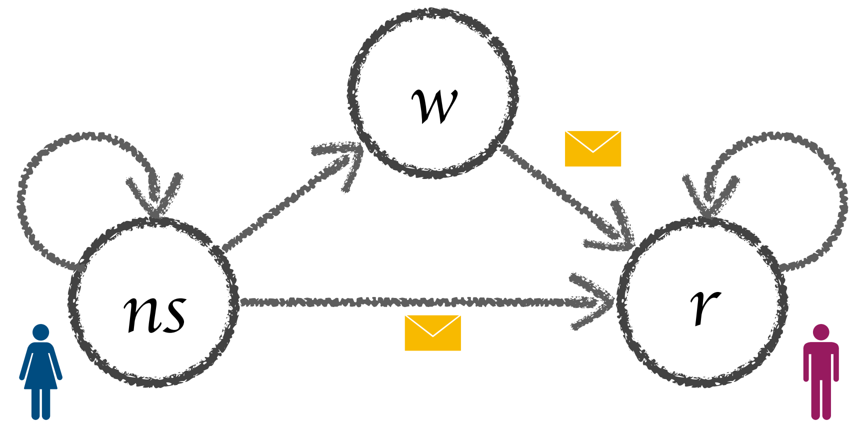
φ common knowledge

$\leftrightarrow$

(know)$^{\omega}$ φ

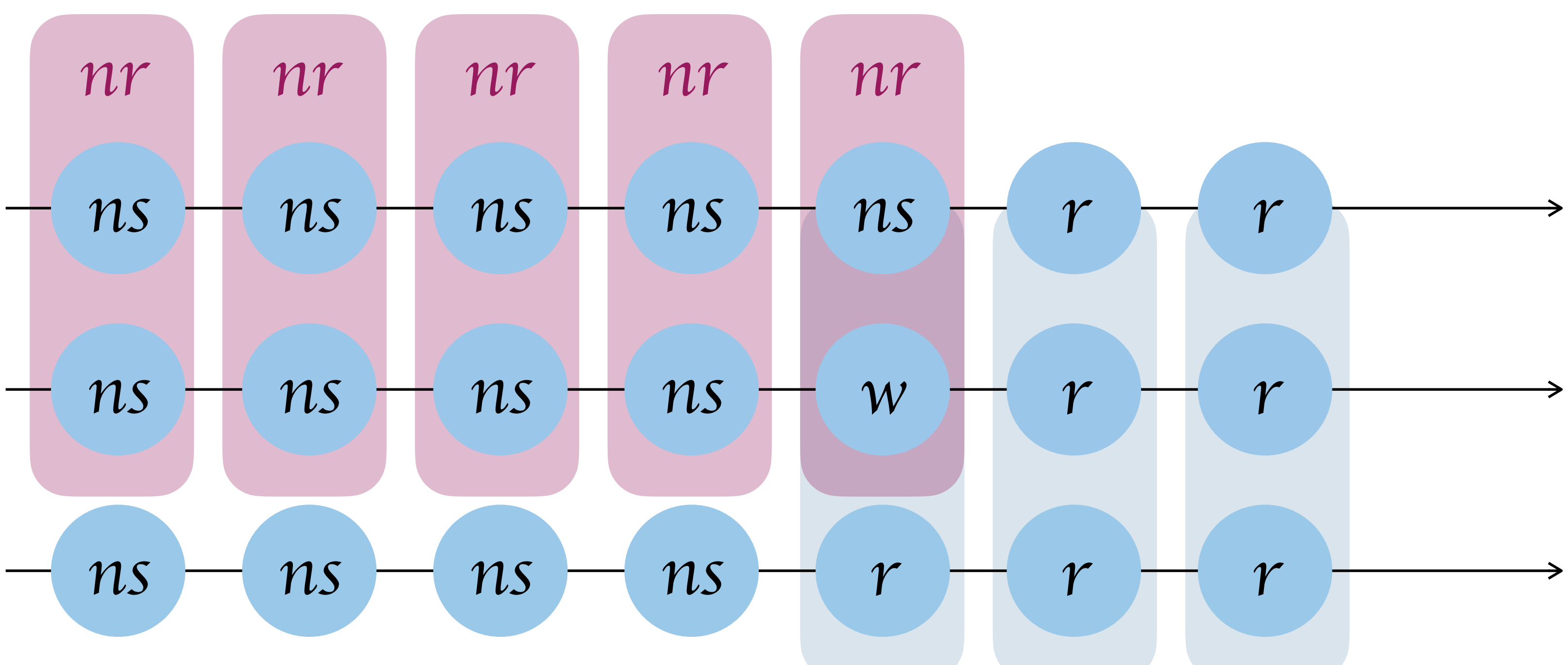
Unifying hyper and epistemic temporal logics. Bozzelli, Maubert, Pinchinat (FoSSaCS 2015)

Communication in Multi-Agent Systems

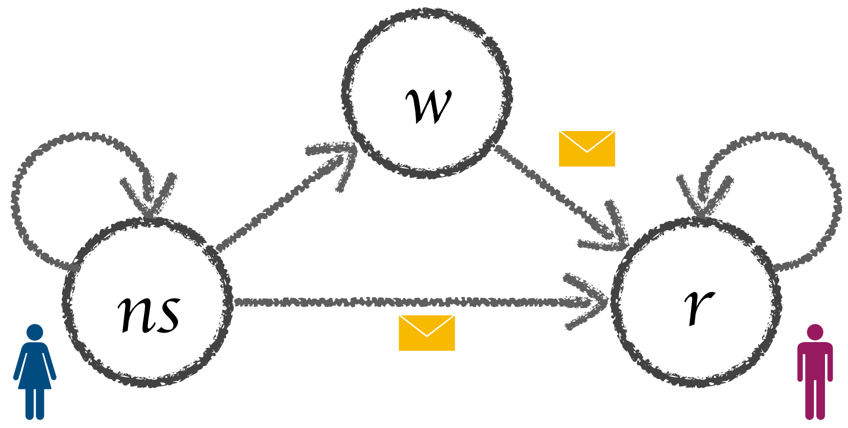


second-order quantification

eventually common knowledge r ?

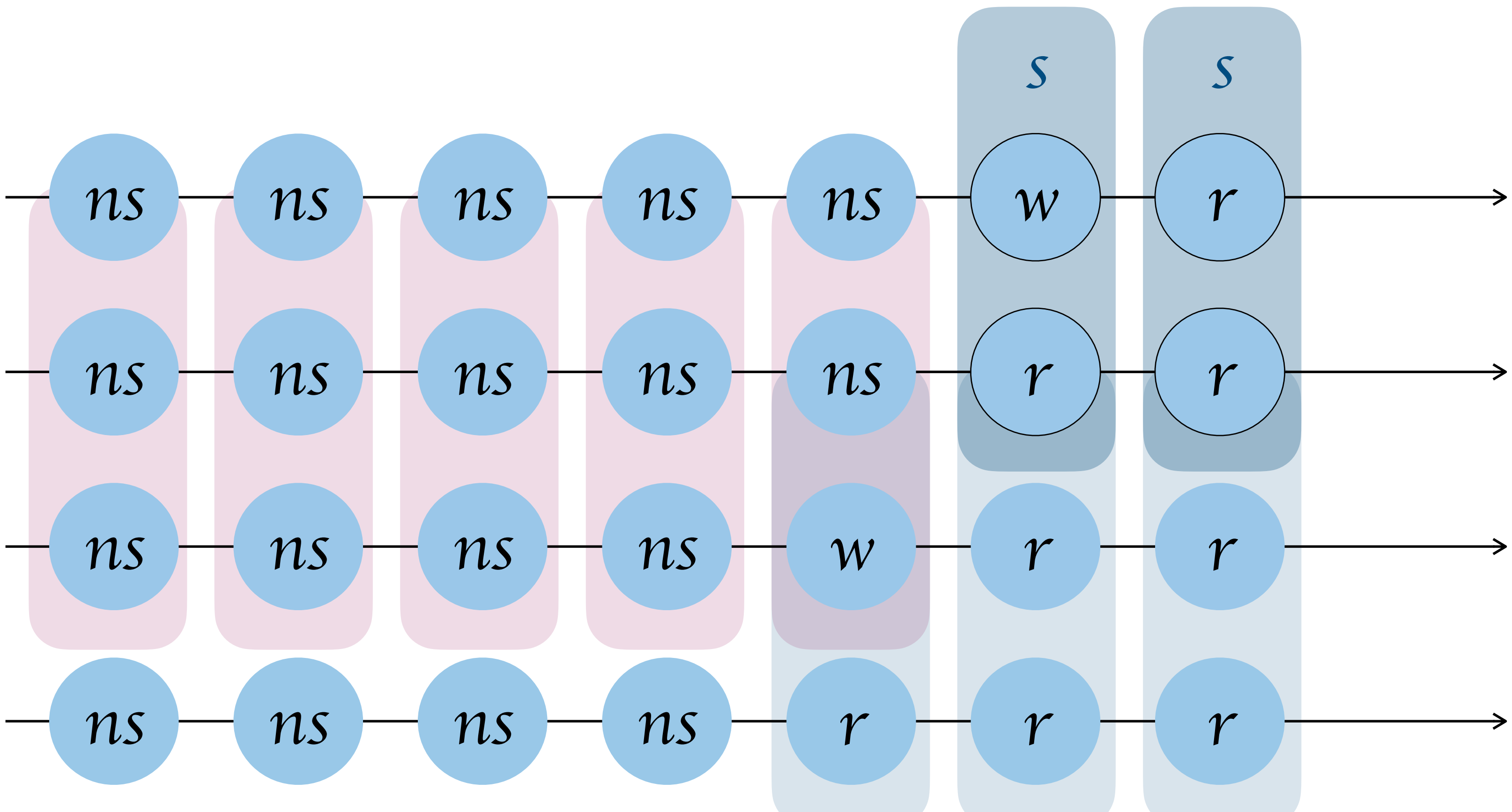


Communication in Multi-Agent Systems

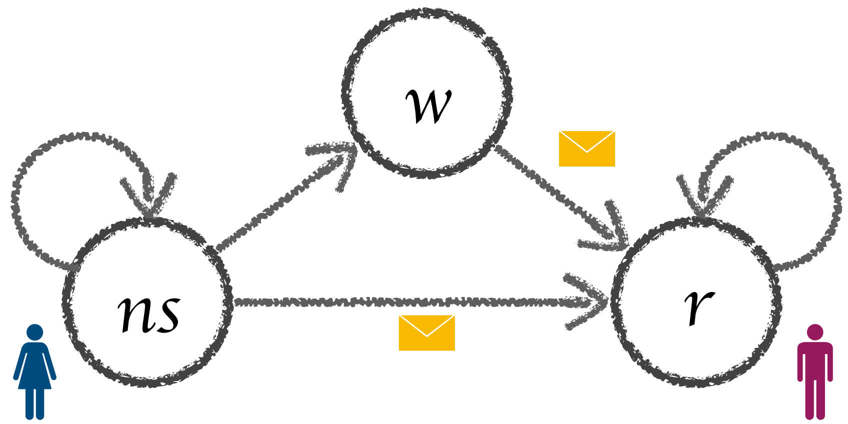


second-order quantification

eventually common knowledge r ?

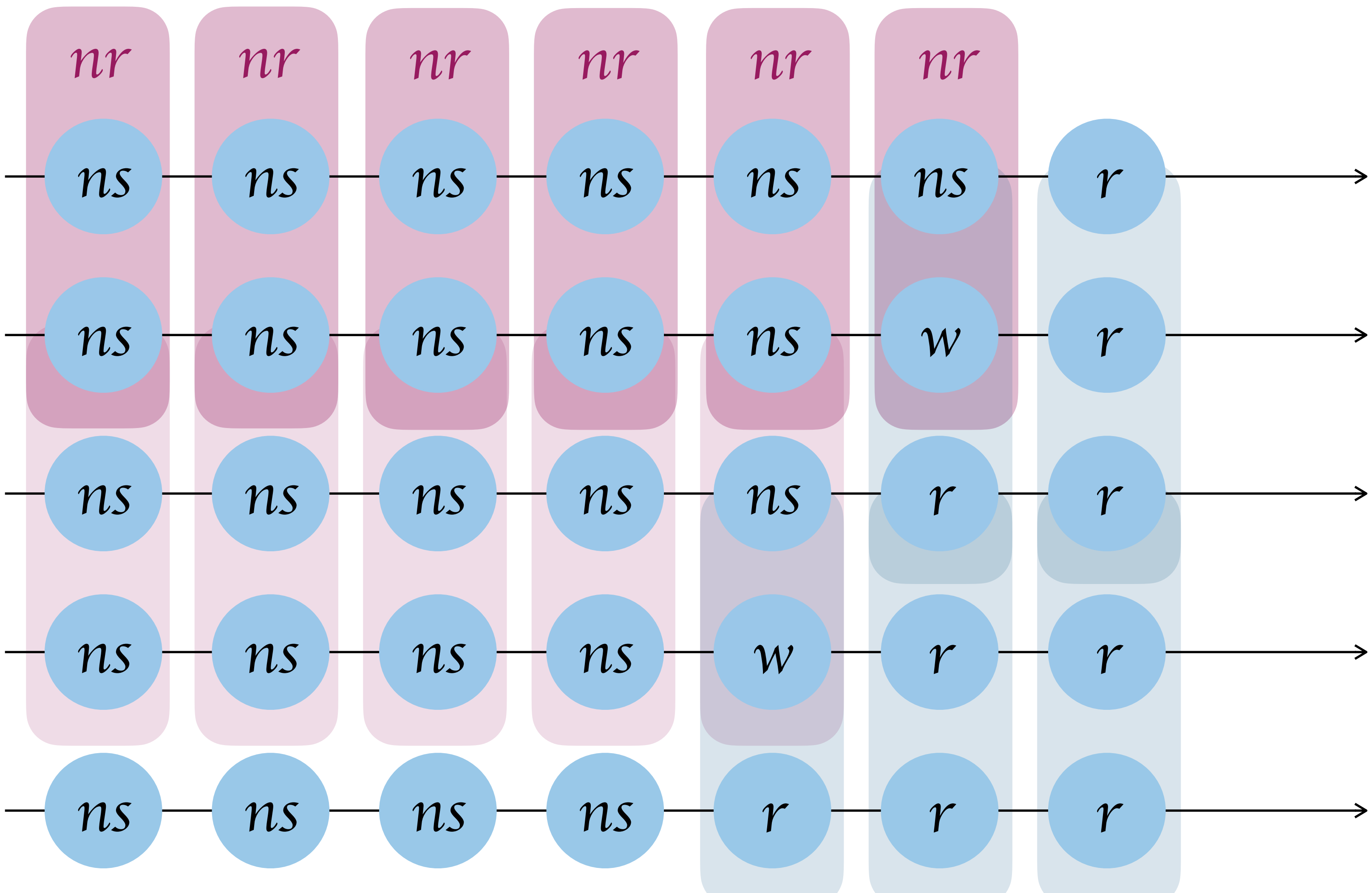


Communication in Multi-Agent Systems

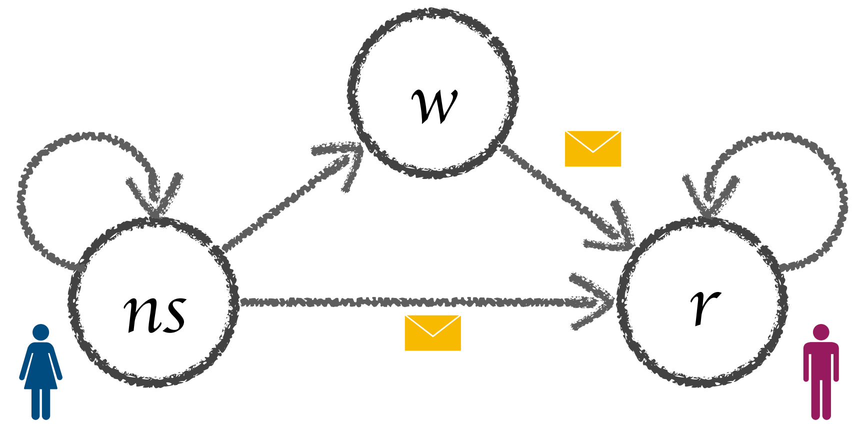


second-order quantification

eventually common knowledge r ?

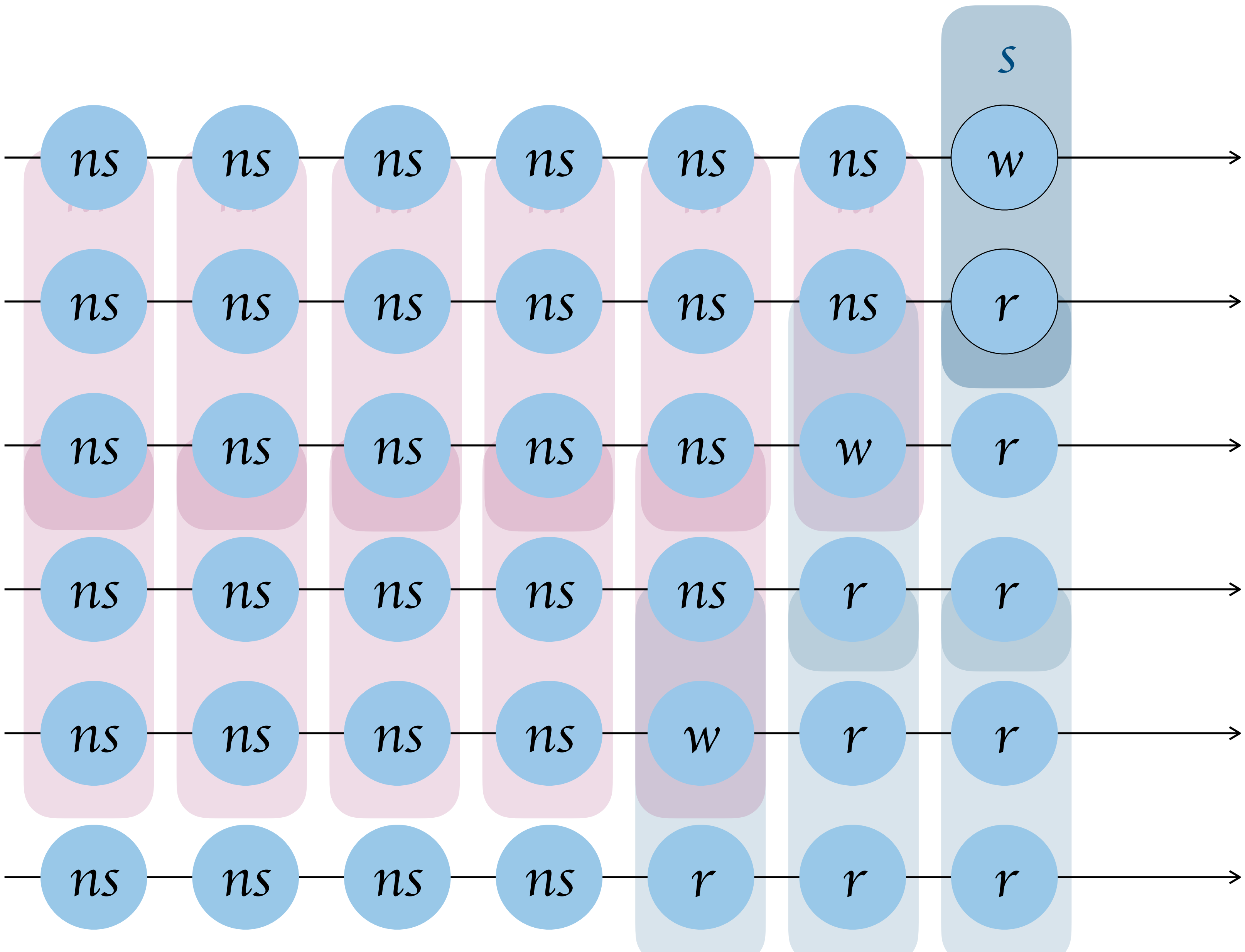


Communication in Multi-Agent Systems

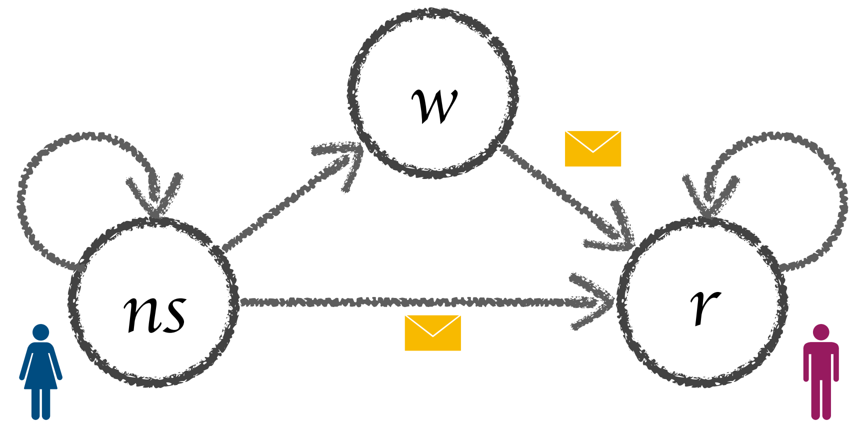


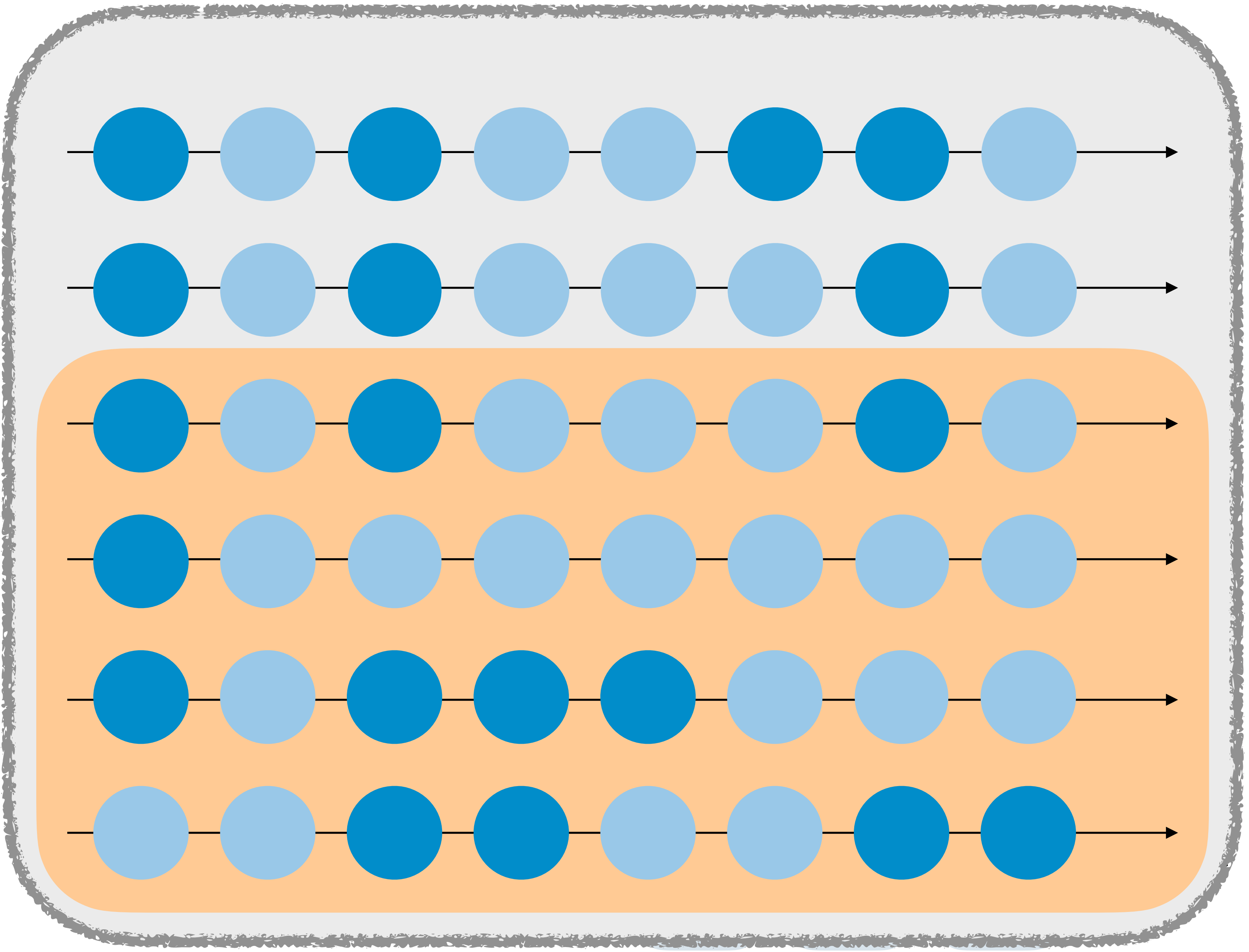
second-order quantification

eventually common knowledge r ?



Communication in Multi-Agent Systems





second-order quantification

eventually common knowledge r ?

Hyper^{2}LTL

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

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

Hyper^{2}LTL

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

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

trace-set variable

Hyper²LTL

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

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

trace-set variable

$\mathcal{G}$ **– system traces**

$\mathcal{U}$ – Σ^ω

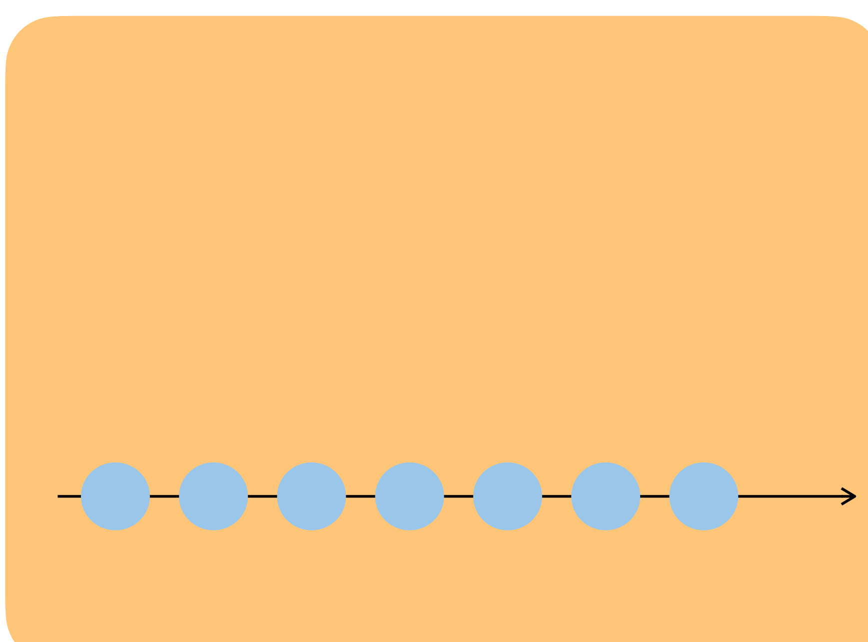
eventually common knowledge r ?

Hyper^{2}LTL

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

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

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



eventually common knowledge r ?

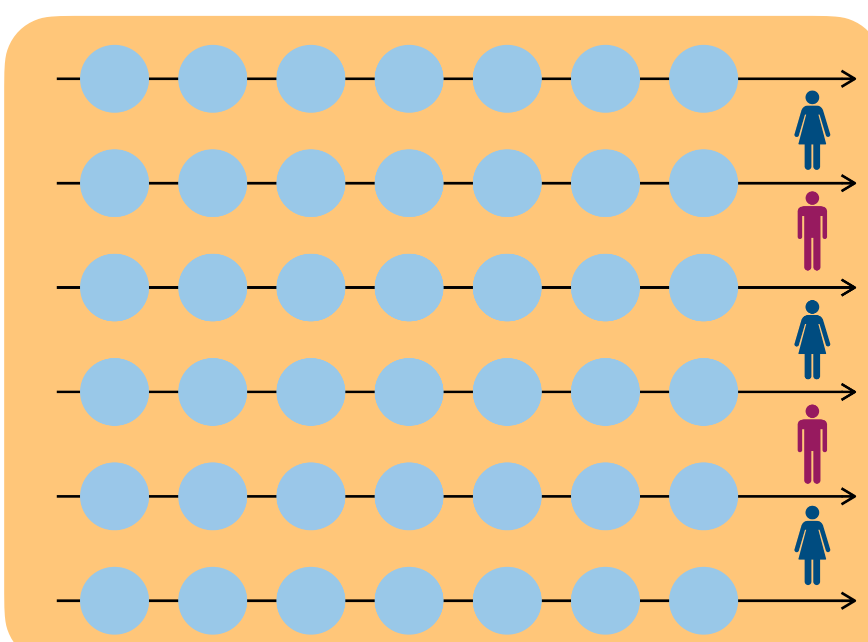
Hyper^{2}LTL

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

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

$$\exists \pi \,.\, \exists X \,.\, \pi \in X \ \wedge$$
$$\forall \pi \in X \,.\, \forall \pi' \in \mathcal{G} \,.\, (\pi \equiv \pi' \vee \pi \equiv \pi') \rightarrow \pi' \in X$$

If π' is indistinguishable from some π in X then π' is also in X



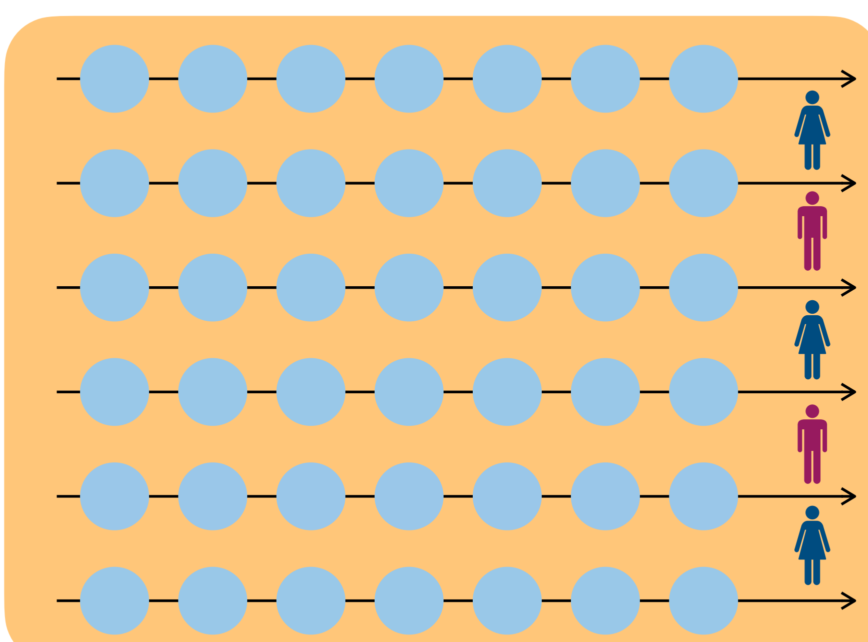
eventually common knowledge r ?

Hyper^{2}LTL

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

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

$$\exists \pi \,.\, \exists X \,.\, \pi \in X \wedge$$
$$\forall \pi \in X \,.\, \forall \pi' \in \mathcal{G} \,.\, (\pi \equiv \pi' \vee \pi \equiv \pi') \rightarrow \pi' \in X$$
$$\forall \pi' \in X \,.\, \Diamond r_{\pi'}$$



If π' is indistinguishable from some π in X then π' is also in X

Hyper²LTL

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

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

Trace theory

Asynchronous Hyperproperties

Common knowledge

Model Checking

Undecidable

Hyper²LTL

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

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

Trace theory

Asynchronous Hyperproperties

Common knowledge

Model Checking

Undecidable

Approximations

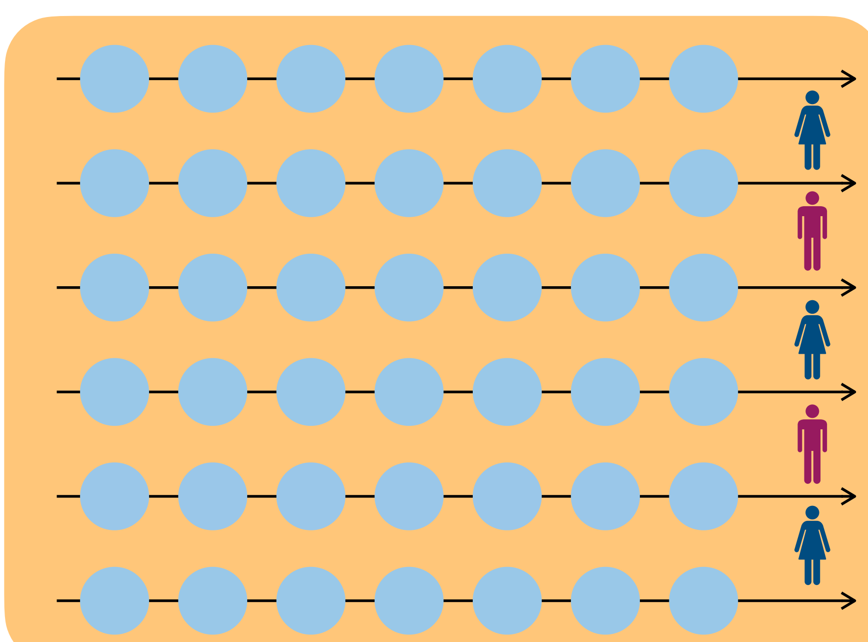
eventually common knowledge r ?

Hyper²LTL

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

$$\forall \pi \in X . \forall \pi' \in \mathcal{G} . (\pi \equiv \pi' \vee \pi \equiv \pi') \rightarrow \pi' \in X$$

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



If π' is indistinguishable from some π in X then π' is also in X

eventually common knowledge r ?

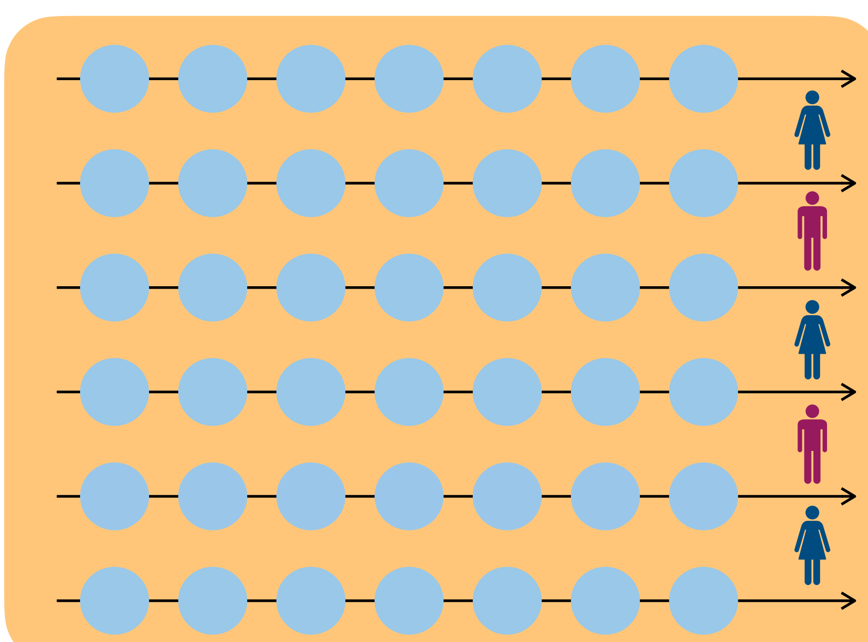
Hyper^{2}LTL

Unique Least Fixpoints

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

$$\forall \pi \in X \,.\, \forall \pi' \in \mathcal{G} \,.\, (\pi \equiv \pi' \lor \pi \equiv \pi') \rightarrow \pi' \in X$$

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



If π' is indistinguishable from some π in X then π' is also in X

Hyper²LTL

Unique Least Fixpoints

eventually common knowledge r ?

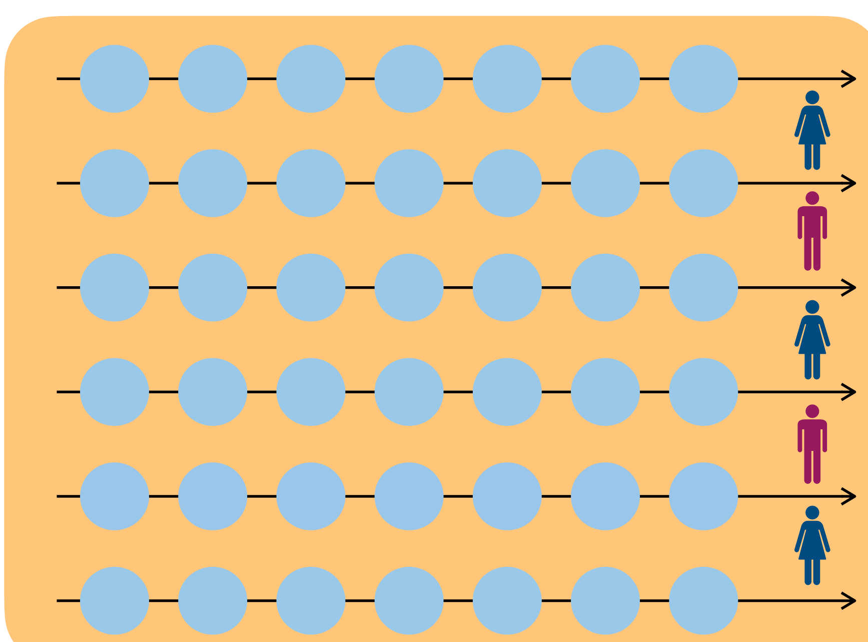
Asynchronous Hyperproperties

Trace theory

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

$$\forall \pi \in X \,.\, \forall \pi' \in \mathcal{G} \,.\, (\pi \equiv \pi' \vee \pi \equiv \pi') \rightarrow \pi' \in X$$

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



If π' is indistinguishable from some π in X then π' is also in X

Model Checking Hyper²LTL

Unique Least Fixpoints

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

Model Checking Hyper²LTL

Unique Least Fixpoints

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

Automaton A_1

Model Checking Hyper^{2}LTL

Unique Least Fixpoints

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

Automaton A_1

Automaton A_k

Model Checking Hyper^{2}LTL

Unique Least 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

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

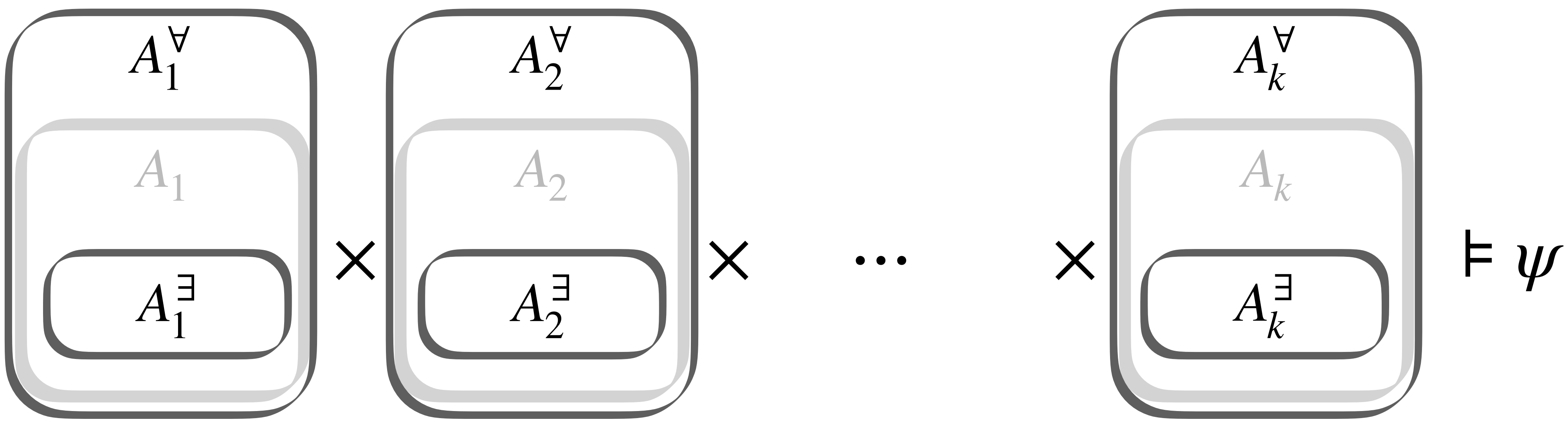
HyperLTL model checking

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

Model Checking Hyper²LTL

Unique Least Fixpoints

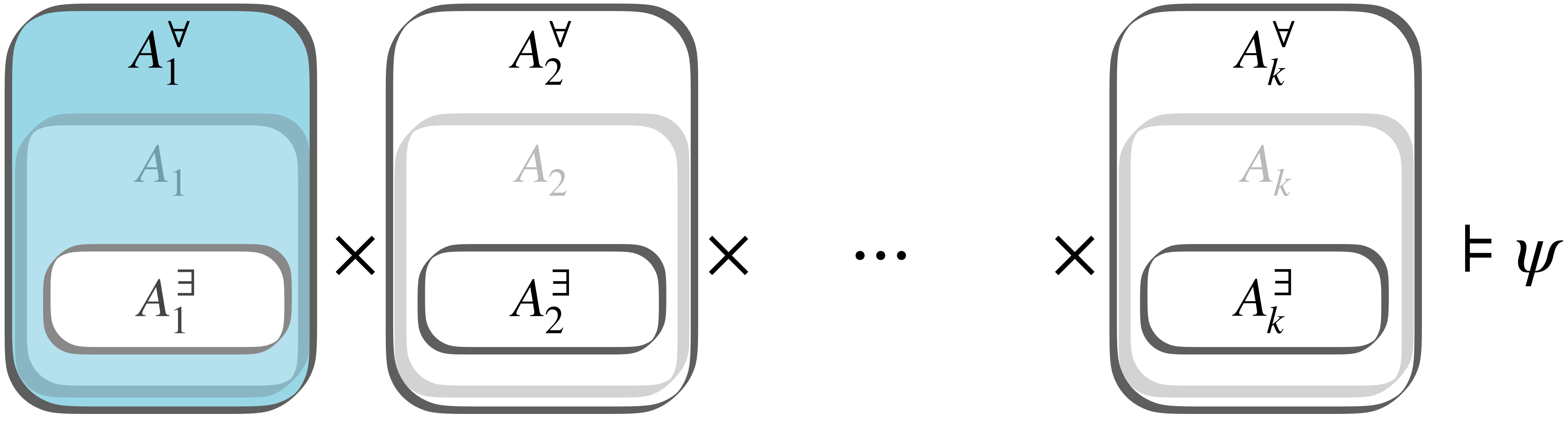
$$\varphi = \exists \pi_1 . \, X_1 . \forall \pi_2 \in X_1 . \ldots . \, X_k . \exists \pi_{k+1} \in X_k . \psi$$



Model Checking Hyper²LTL

Unique Least Fixpoints

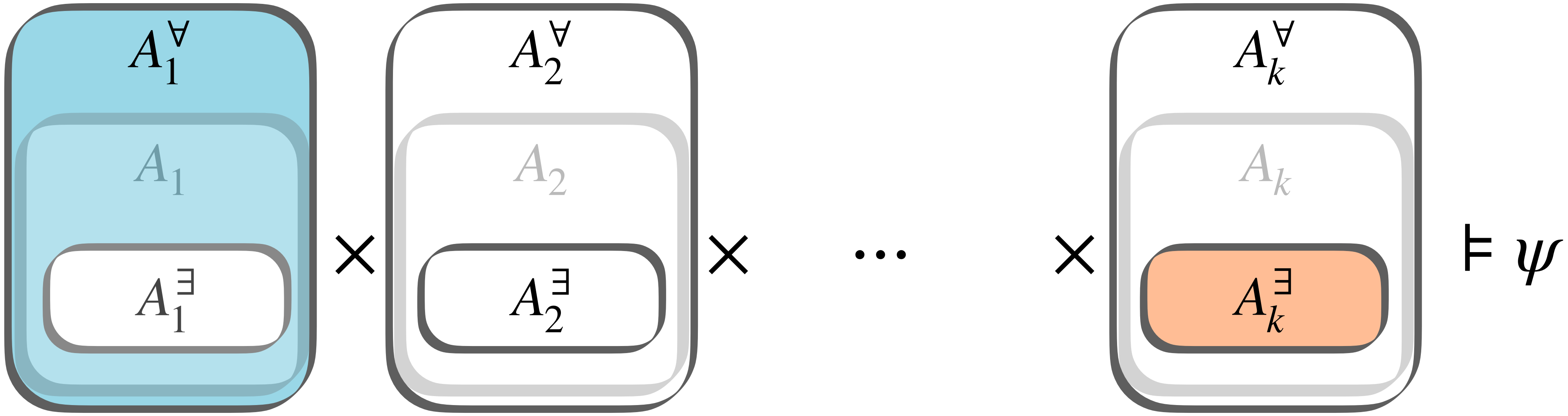
$$\varphi = \exists \pi_1 . \; X_1 . \forall \pi_2 \in X_1 . \ldots . \; X_k . \exists \pi_{k+1} \in X_k . \psi$$



Model Checking Hyper^{2}LTL

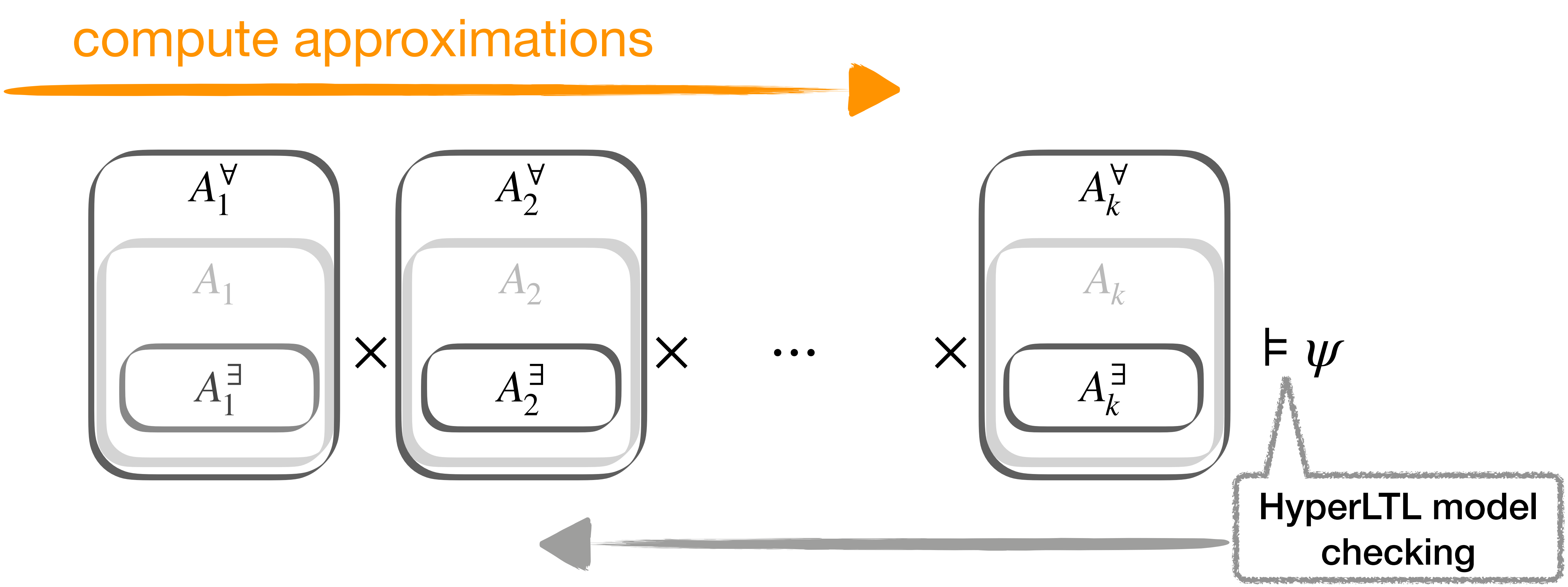
Unique Least Fixpoints

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



Model Checking Hyper²LTL

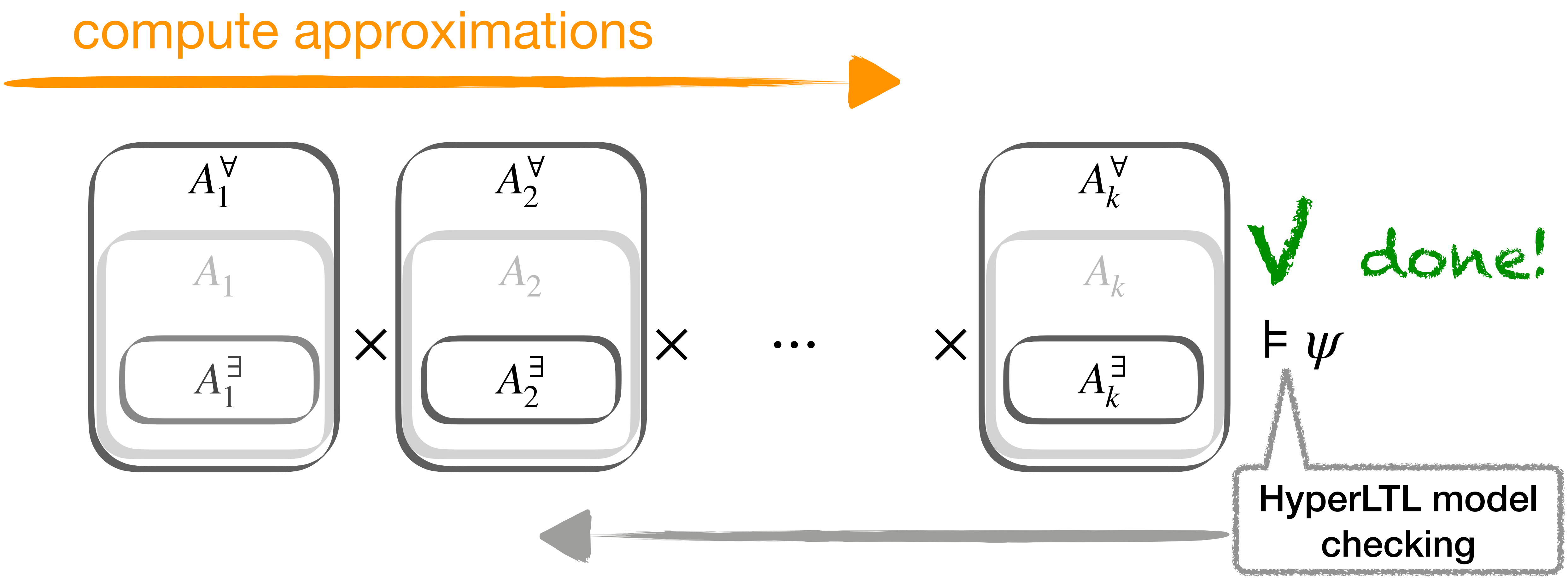
Unique Least Fixpoints



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

Model Checking Hyper²LTL

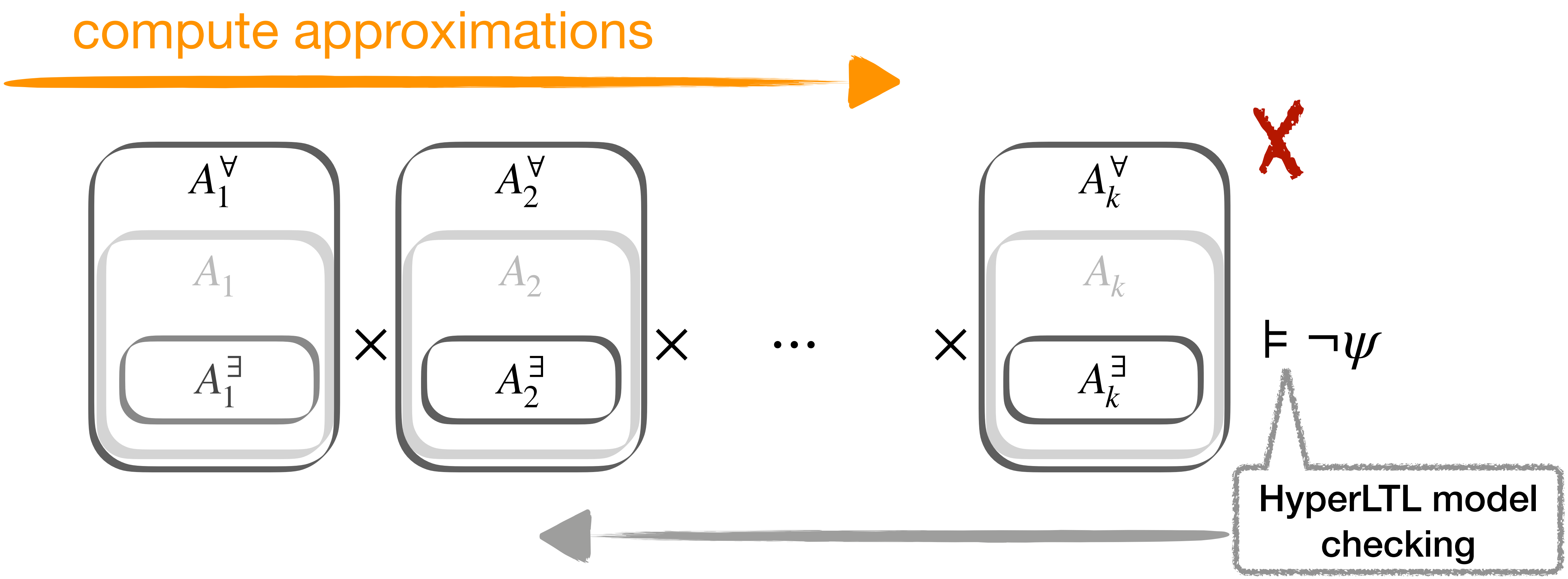
Unique Least Fixpoints



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

Model Checking Hyper²LTL

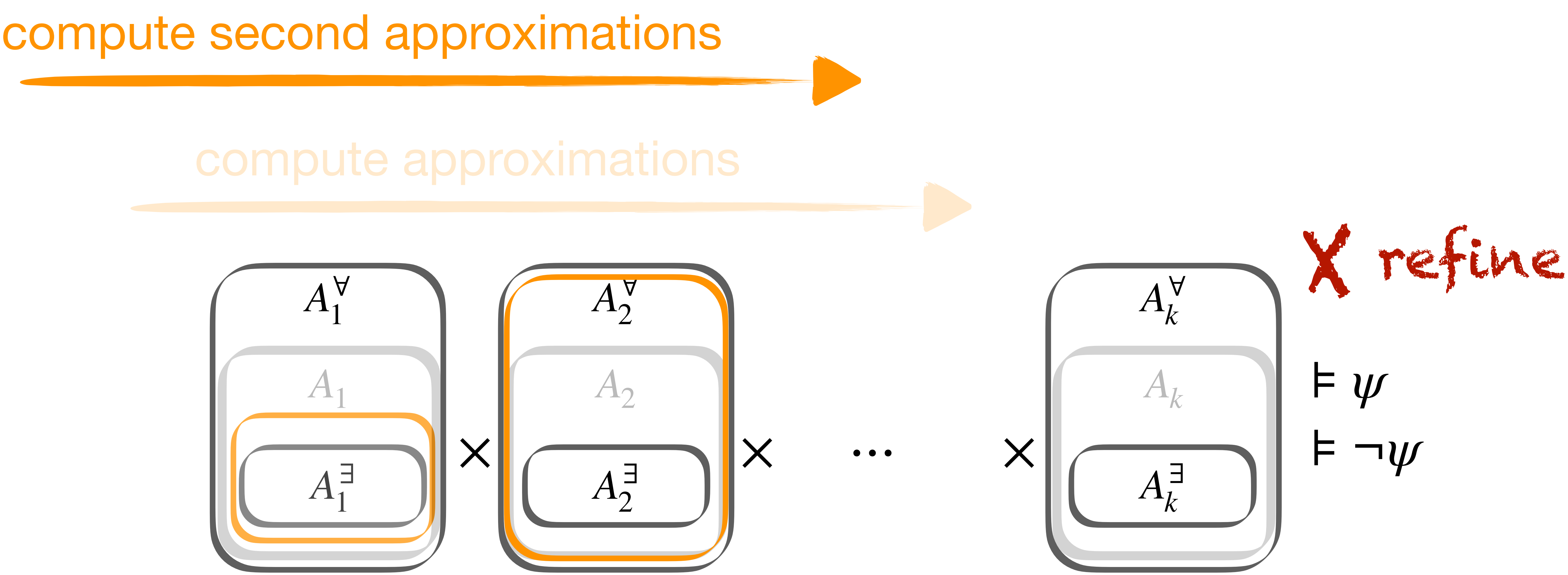
Unique Least Fixpoints



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

Model Checking Hyper^{2}LTL

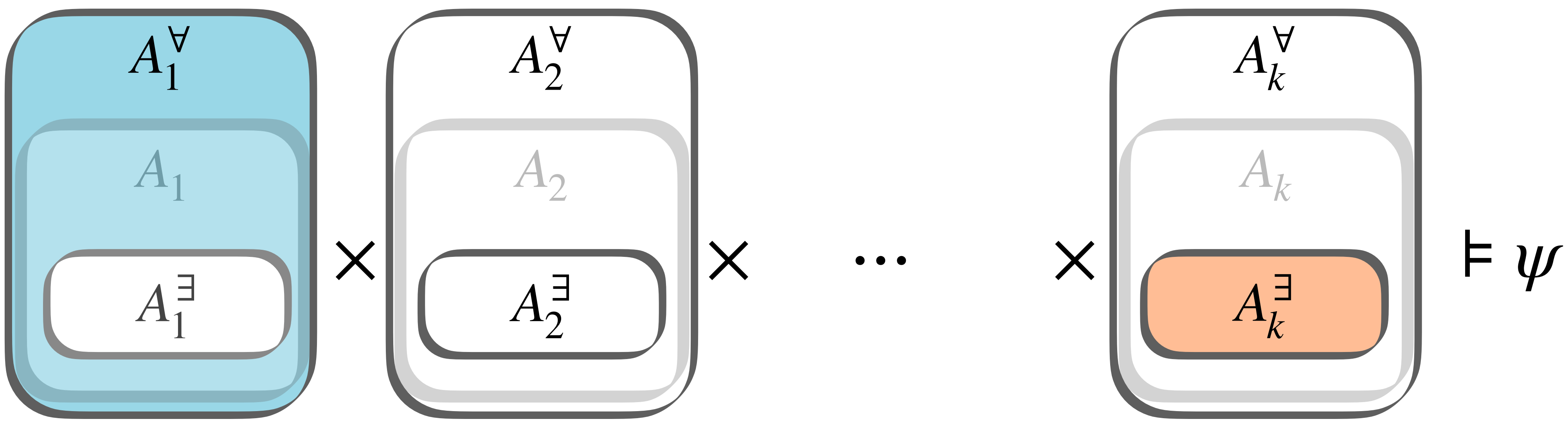
Unique Least Fixpoints



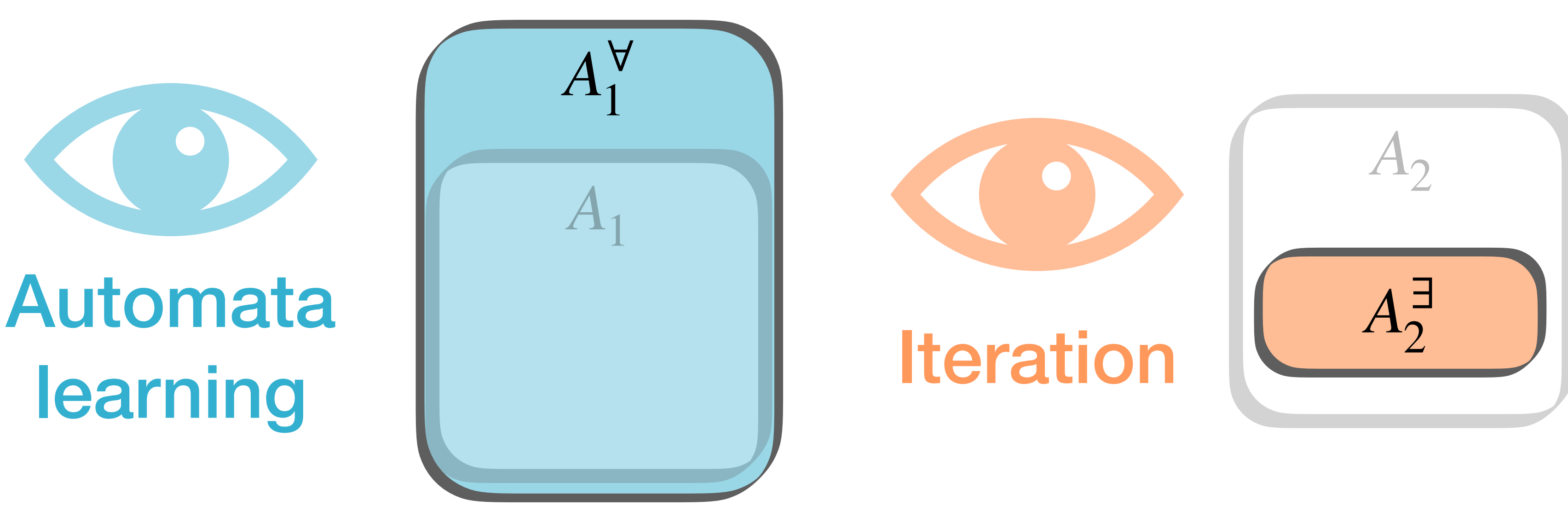
Model Checking Hyper^{2}LTL

Unique Least Fixpoints

$$\varphi = \exists \pi_1 . (X_1, \curlyvee, \varphi_1) . \forall \pi_2 \in X_1 . \ldots . (X_k, \curlyvee, \varphi_k) . \exists \pi_{k+1} \in X_k . \psi$$



Implementation



Implementation

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

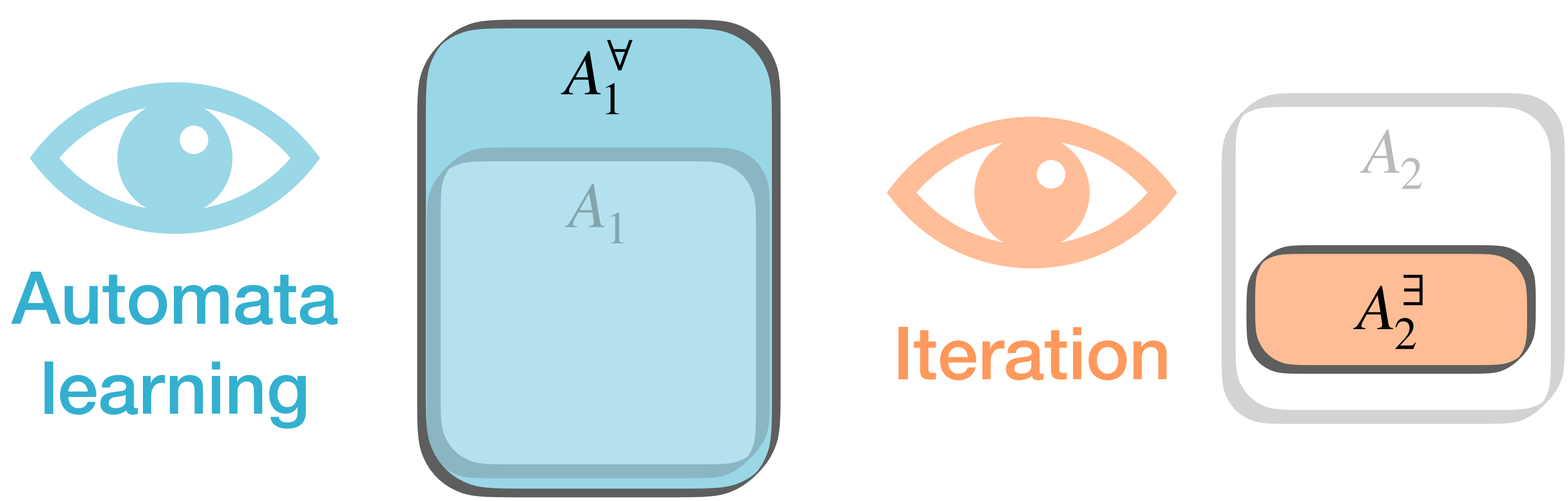
Asynchronous Hyperproperties

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
SwapAViolation$_{15}$	Iter (15)	✗	4.21

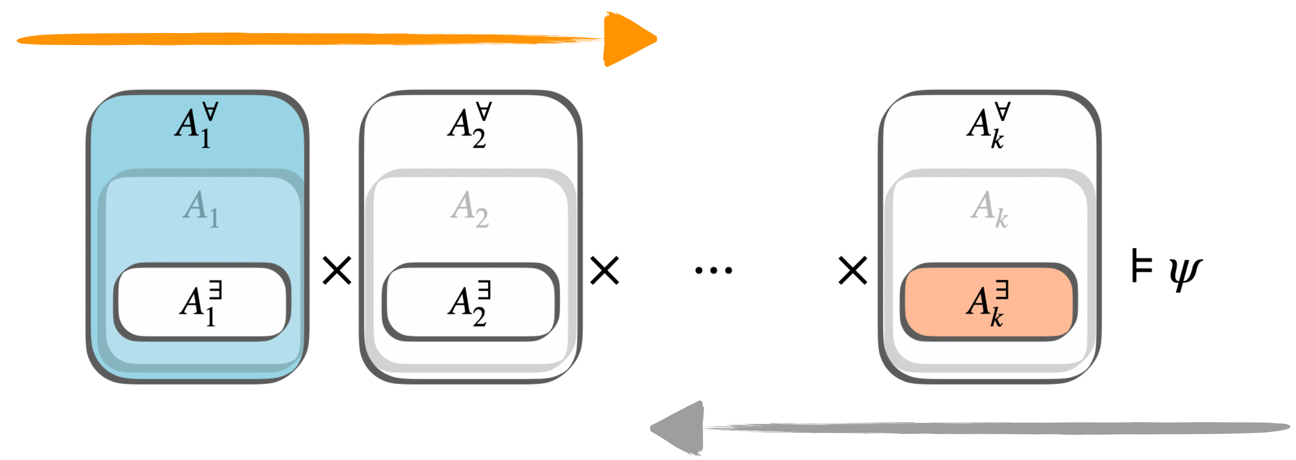
Mazurkiewicz Traces



Hyper^{2}LTL

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

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



Common Knowledge

Asynchronous Hyperproperties

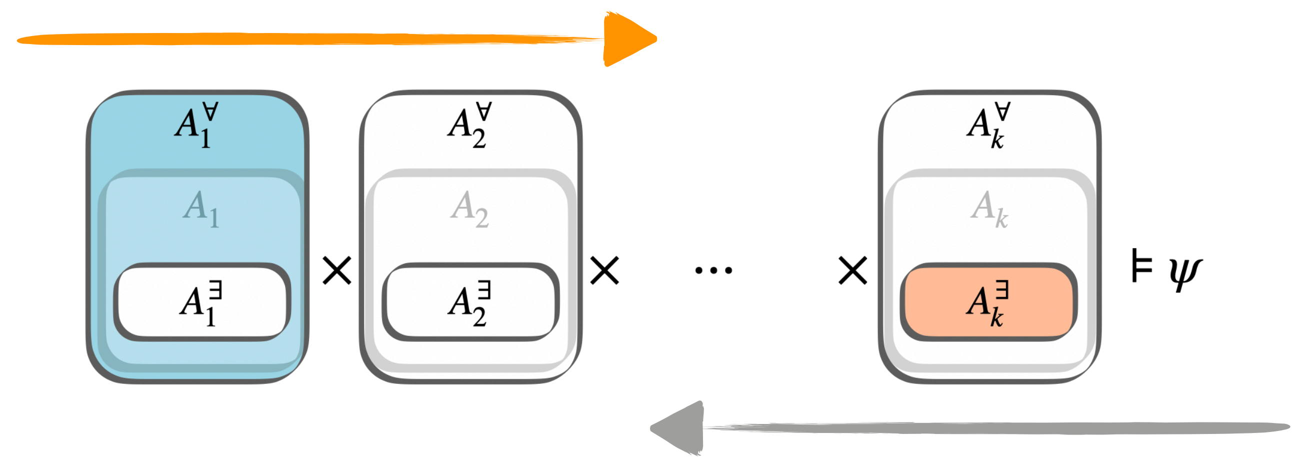
Trace Theory

Generic reasoning and algorithms

Hyper^{2}LTL

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

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



Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Thank you!

Generic reasoning and algorithms