CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

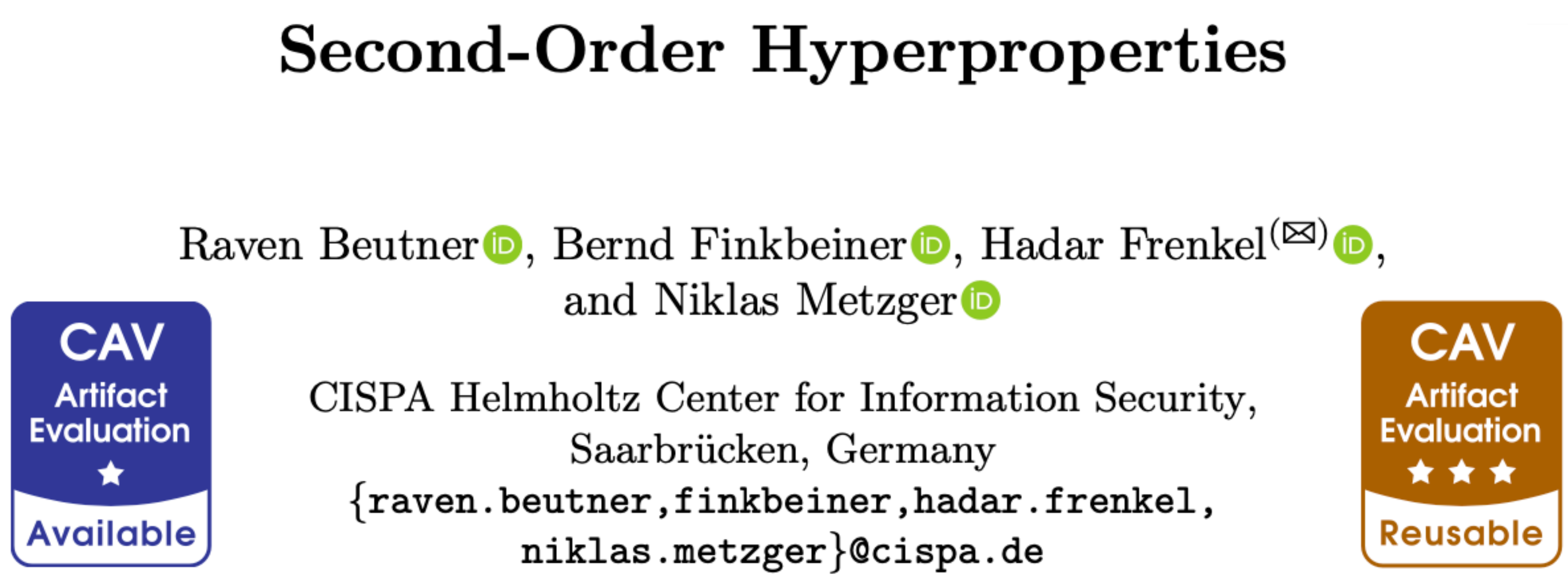
Why do we need Second-Order Hyperlogics?

Hadar Frenkel

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

HYPER workshop
18 July @ CAV 2023

Joint work with



Raven Beutner **Bernd Finkbeiner** **Niklas Metzger**

CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

Friday afternoon!

Second-Oder Hyperproperties. Beutner, Finkbeiner, **F.**, Metzger (CAV 2023)

Hyper^{2}LTL

Why?

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

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

Hyper²LTL

Why?

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality

Generic reasoning and algorithms

Hyper^{2}LTL

Why?

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality

Generic reasoning and algorithms

Hyper^{2}LTL

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

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

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

Hyper^{2}LTL

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

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

Hyper²LTL

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

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

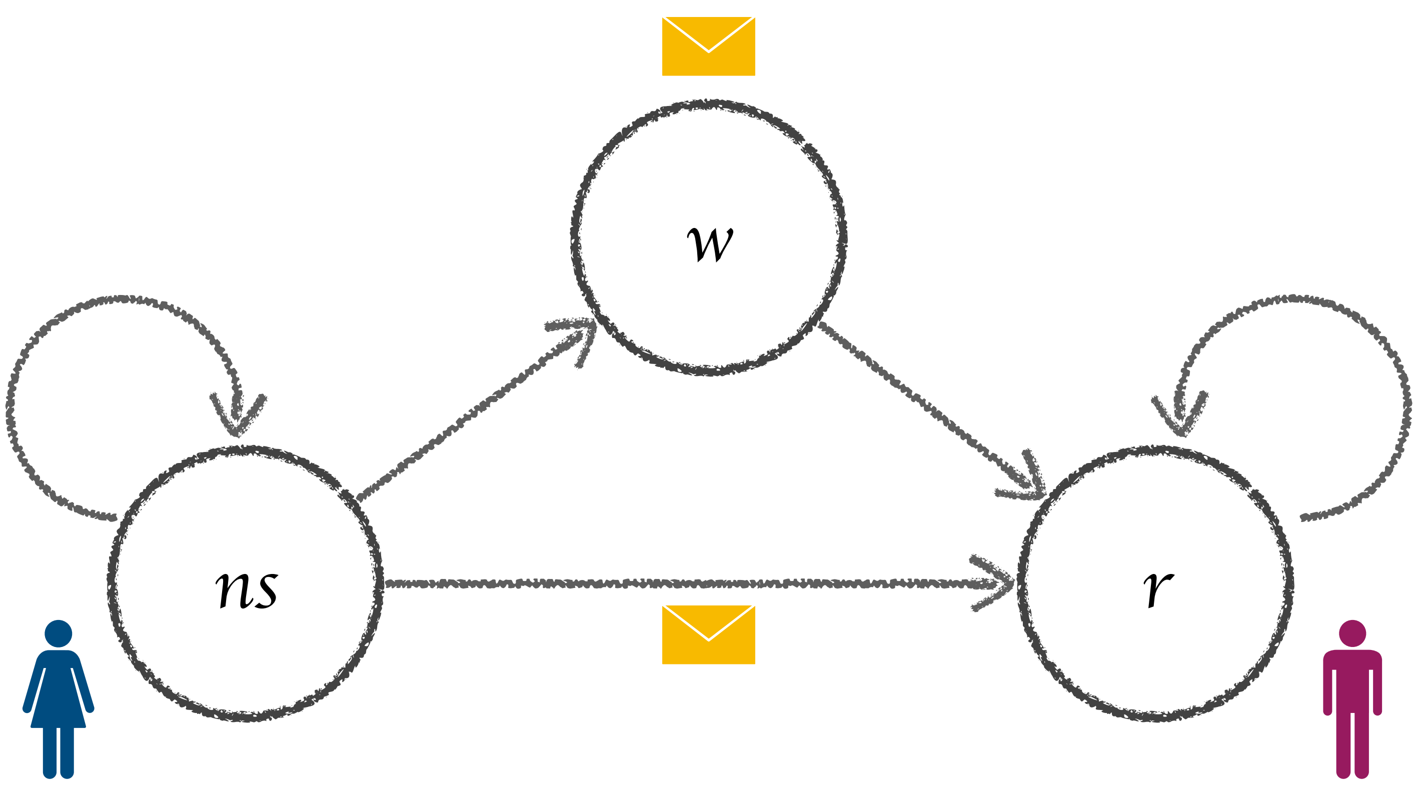
Common Knowledge

Asynchronous Hyperproperties

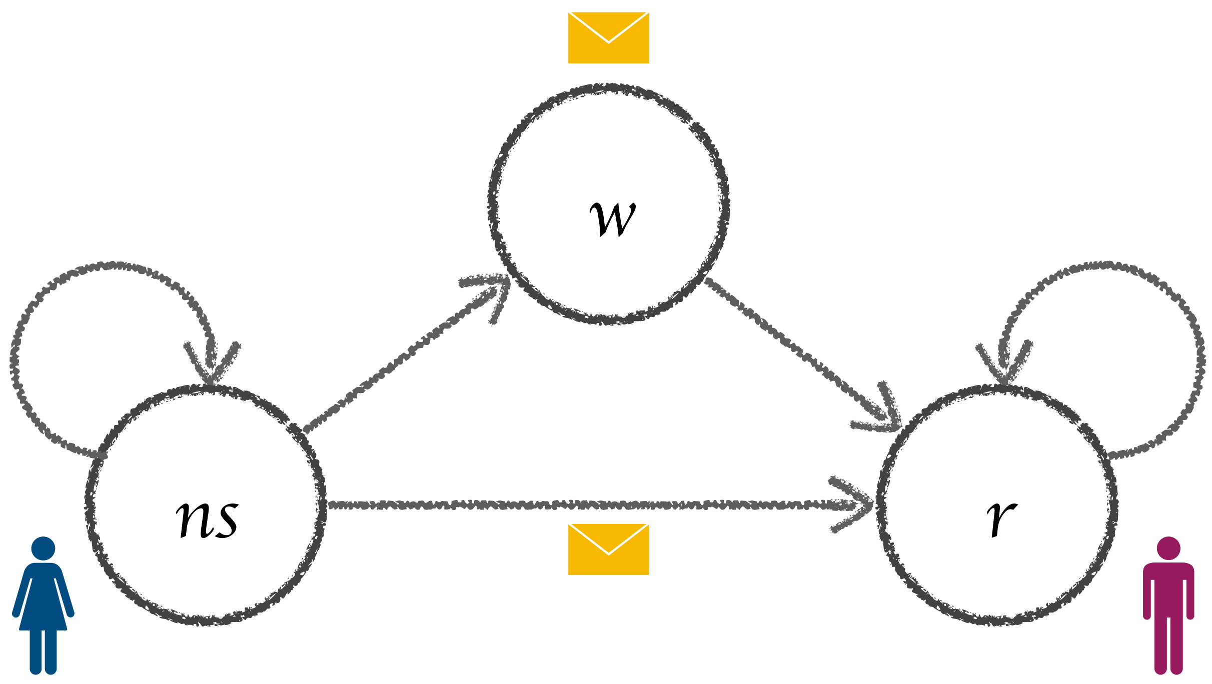
Trace Theory

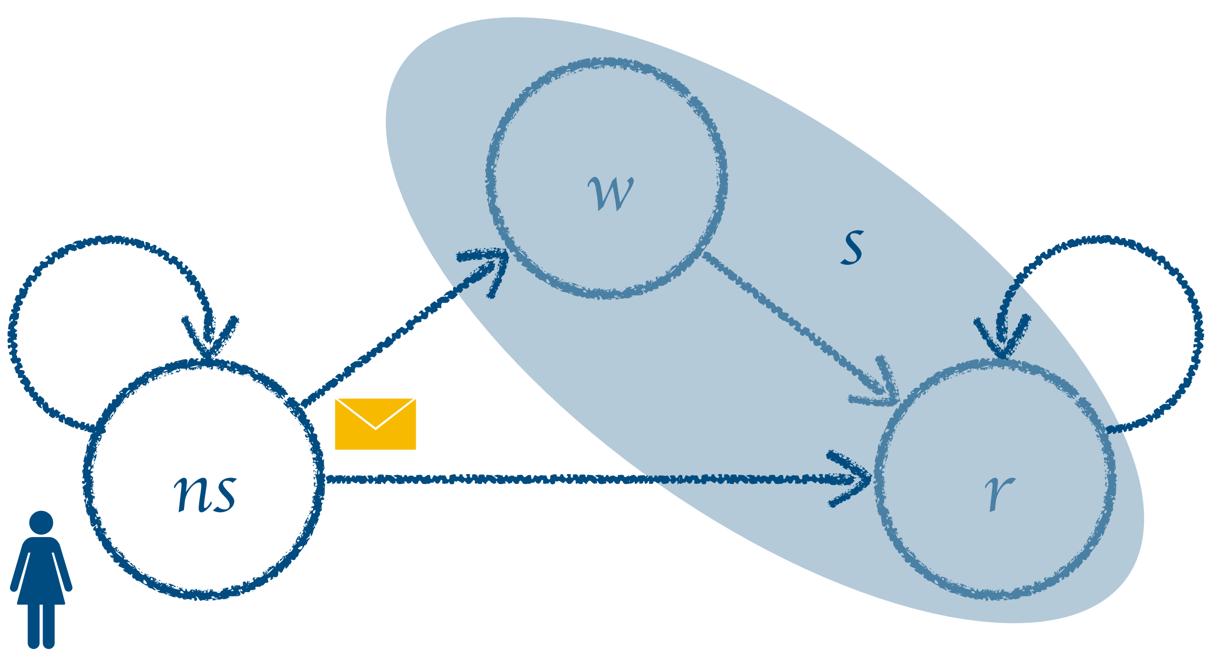
Causality

Communication in Multi-Agent Systems

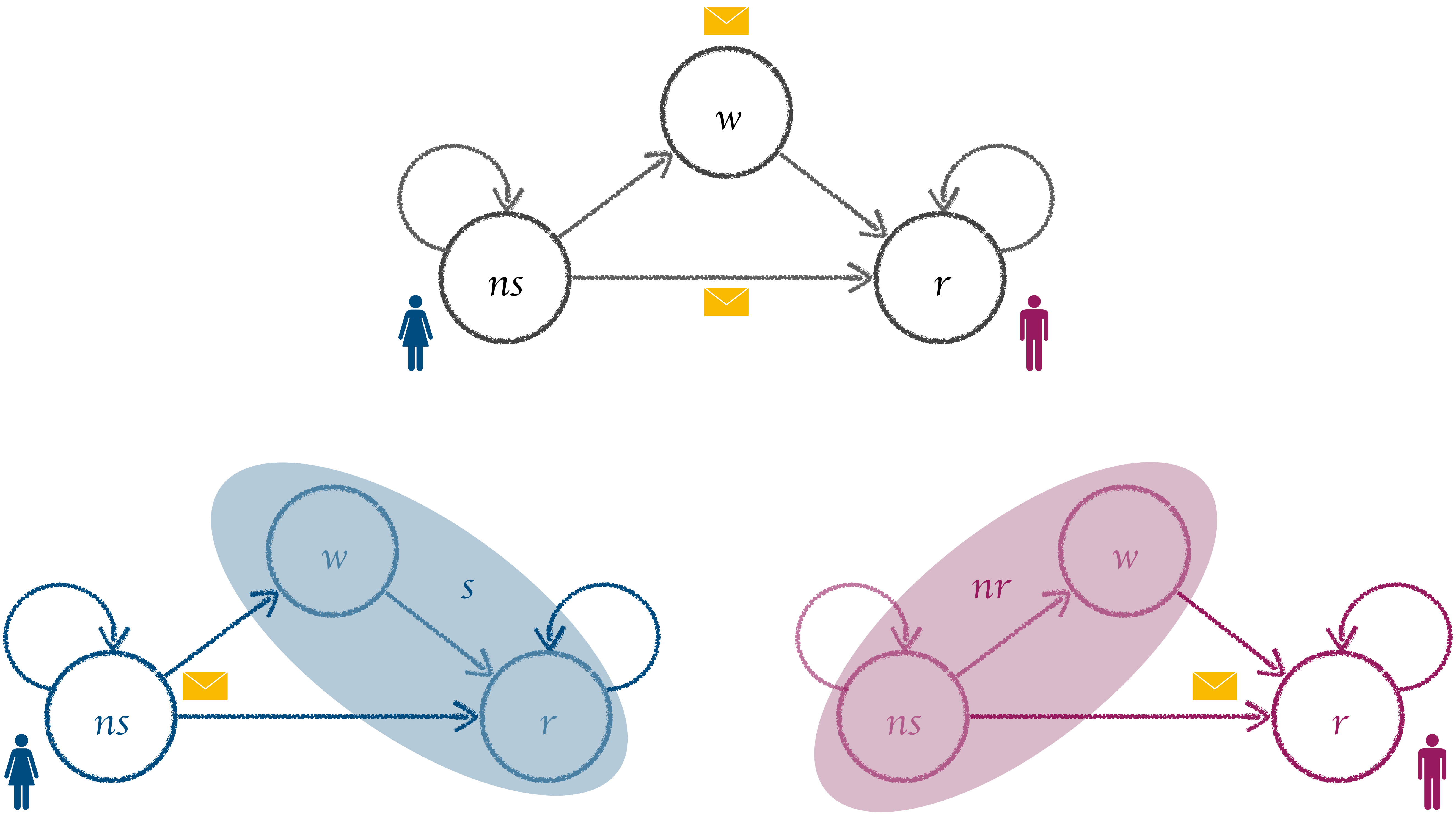


Communication in Multi-Agent Systems

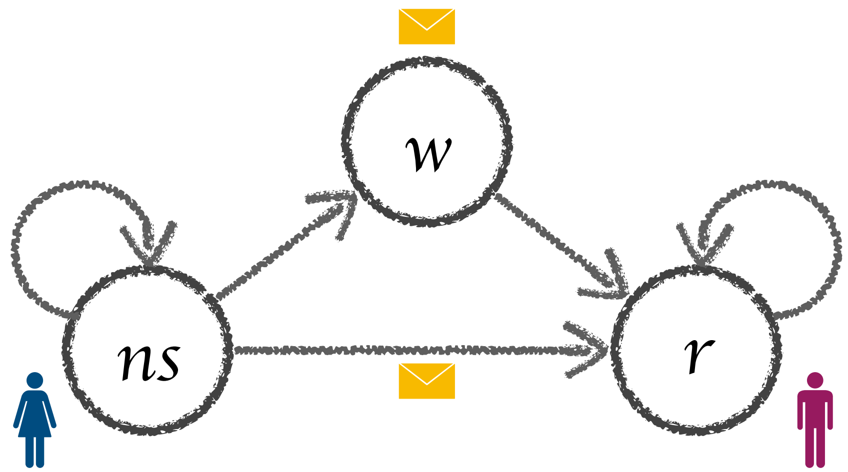


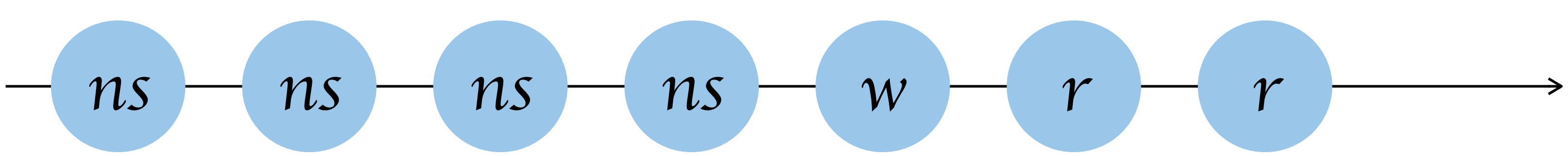


Communication in Multi-Agent Systems

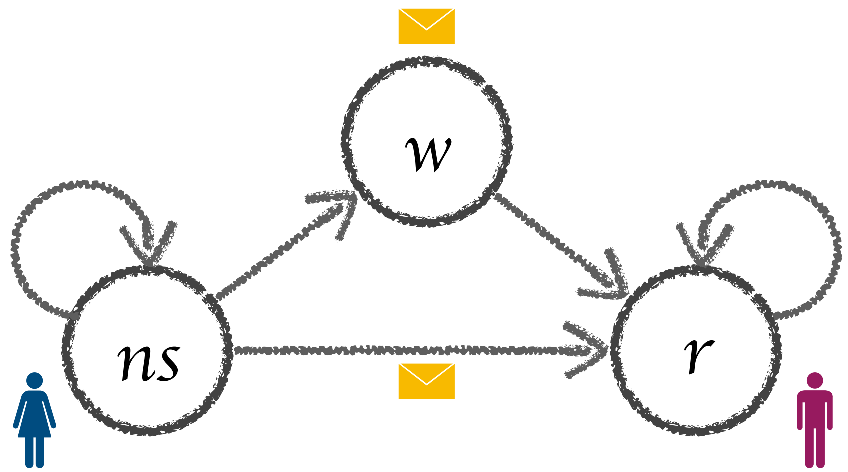


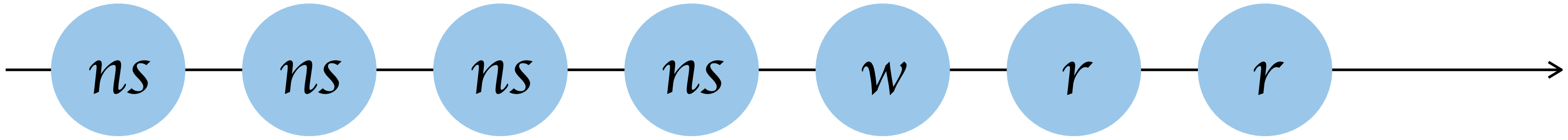
Communication in Multi-Agent Systems





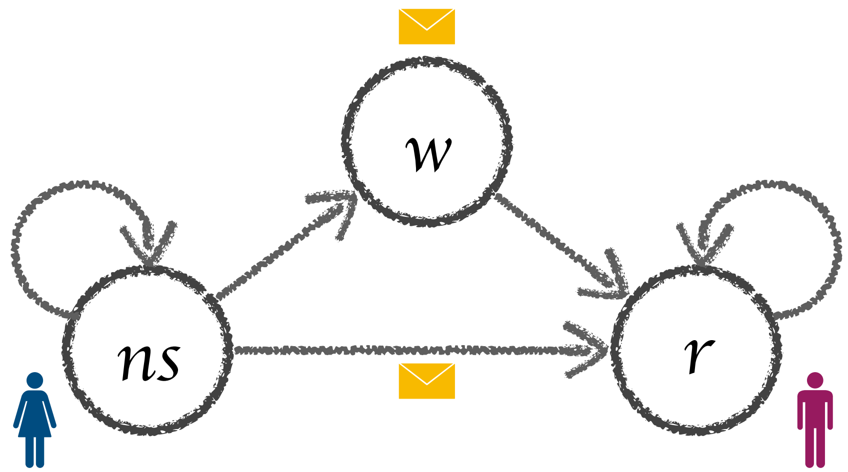
Communication in Multi-Agent Systems

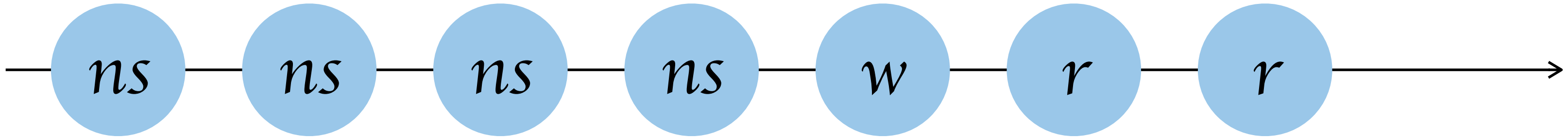




eventually r ?

Communication in Multi-Agent Systems

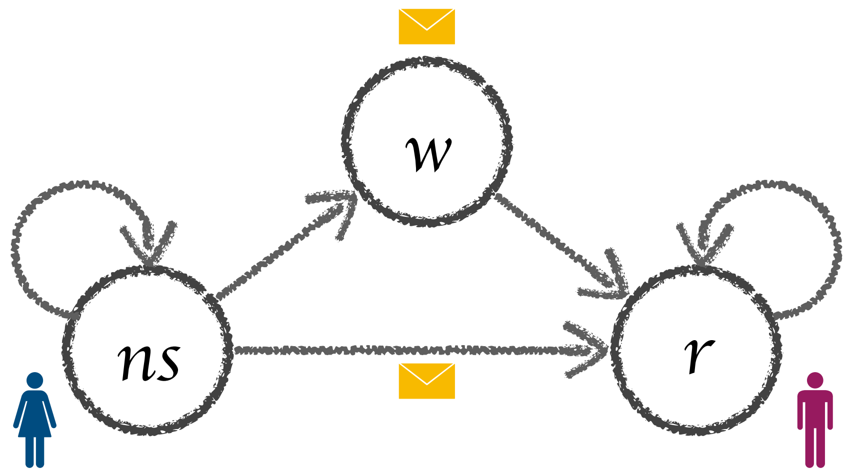


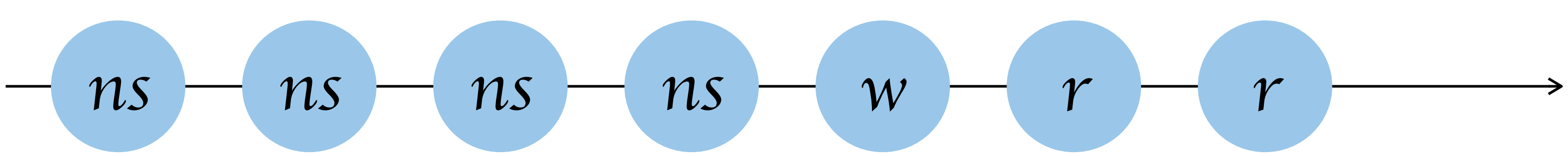


eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems



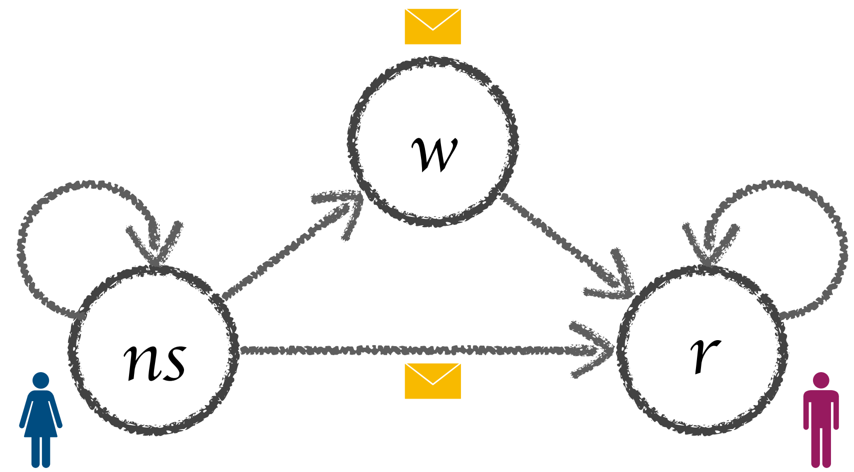


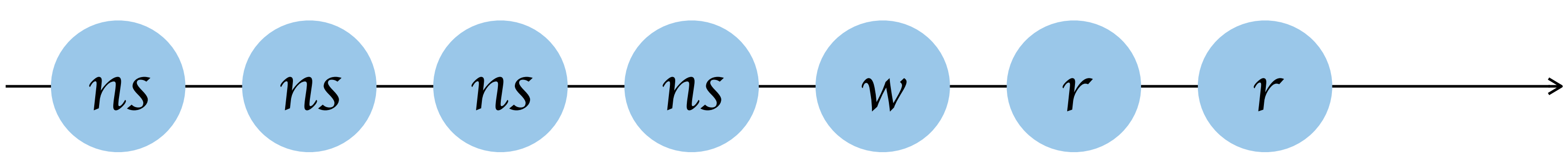
eventually know r ?

eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems





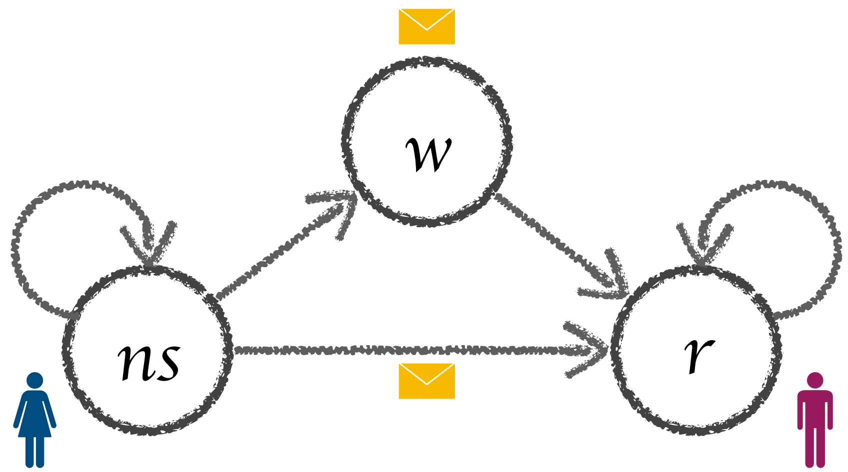
eventually common knowledge r ?

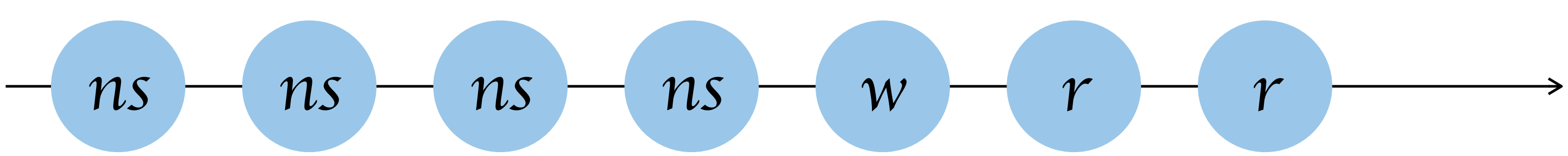
eventually know r ?

eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems

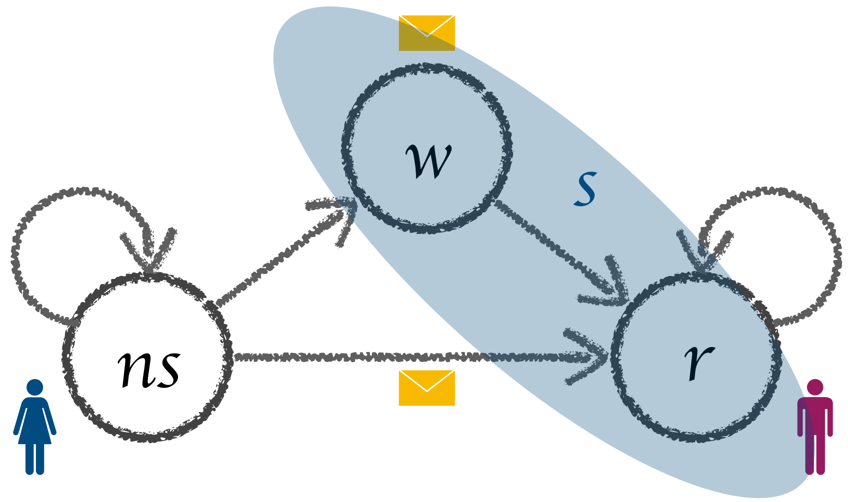




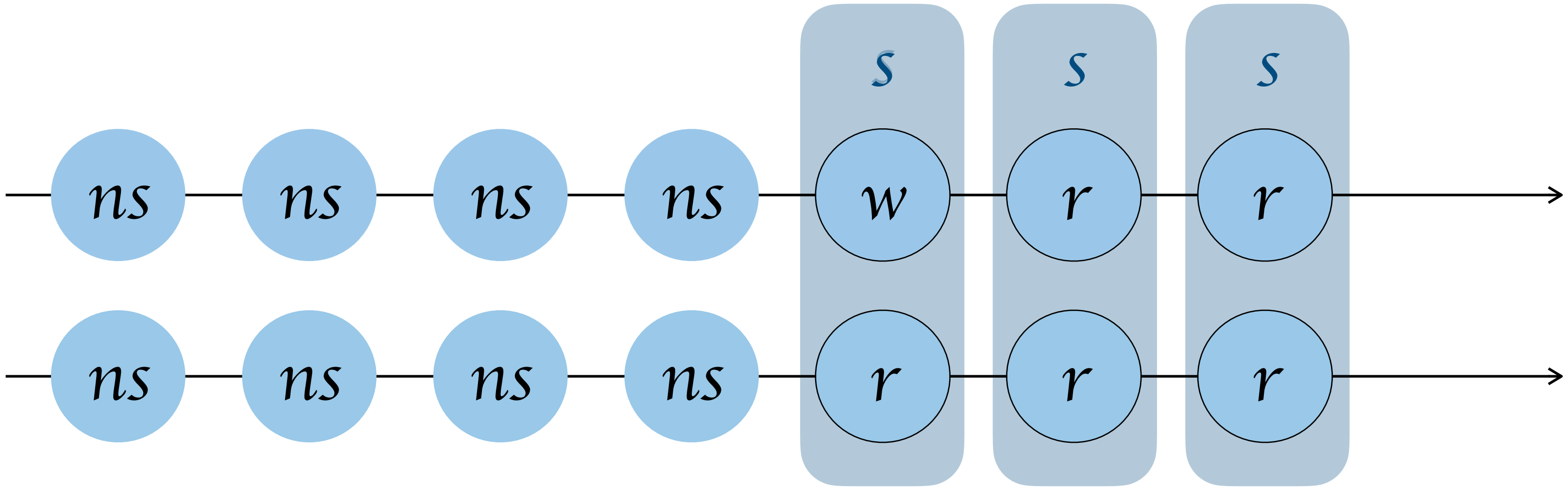
A trace property

eventually r ?

Communication in Multi-Agent Systems



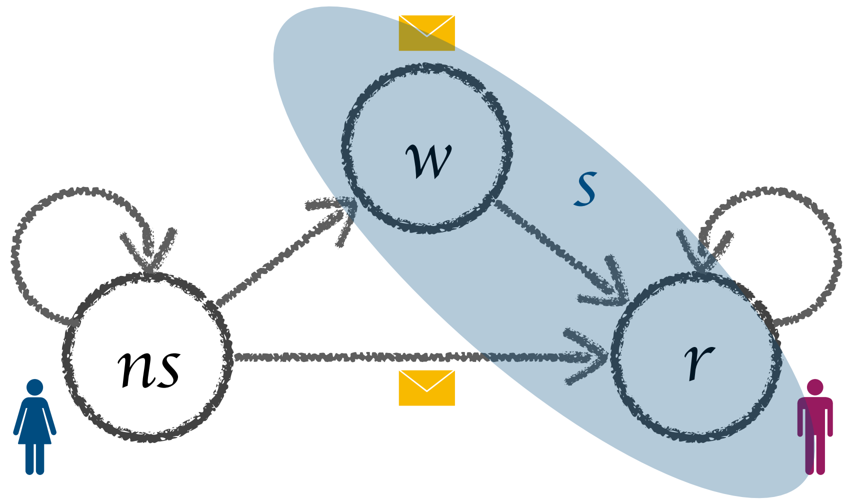
A hyperproperty

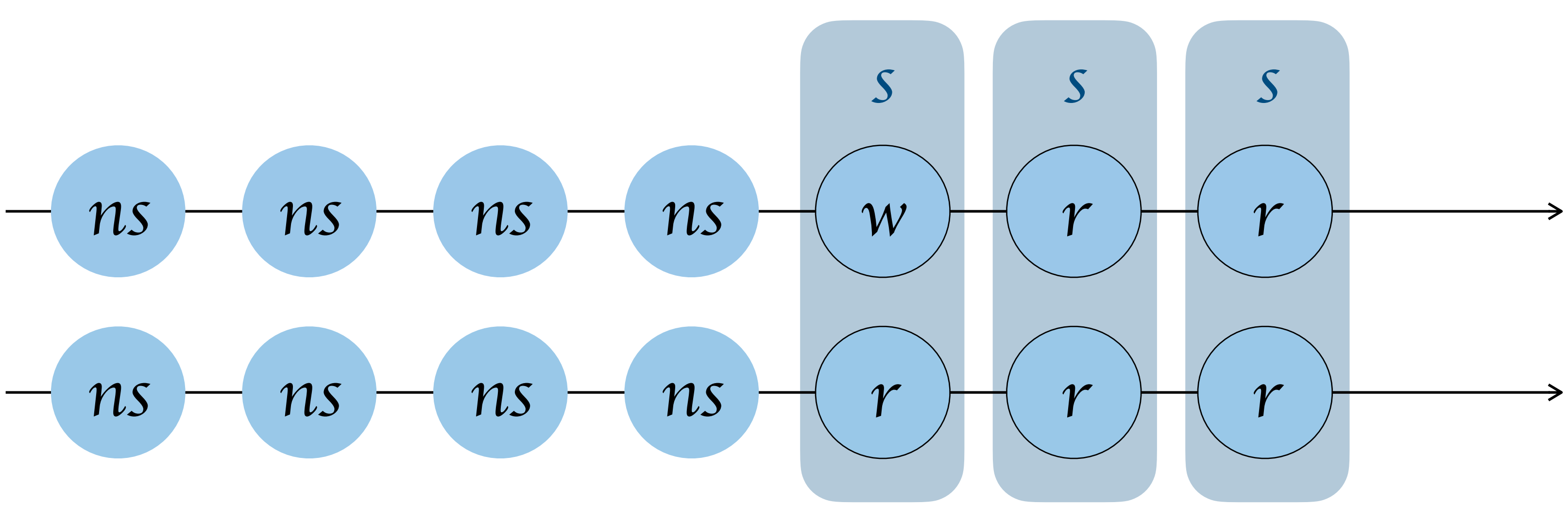


eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems





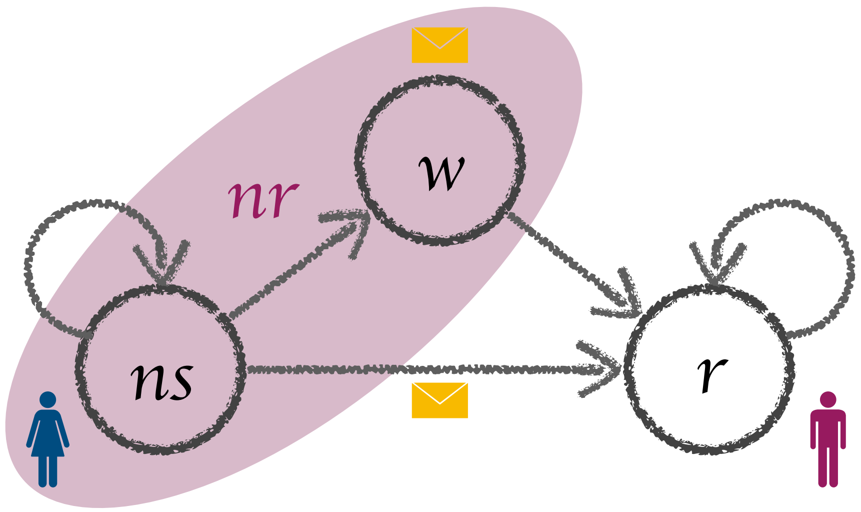
A hyperproperty

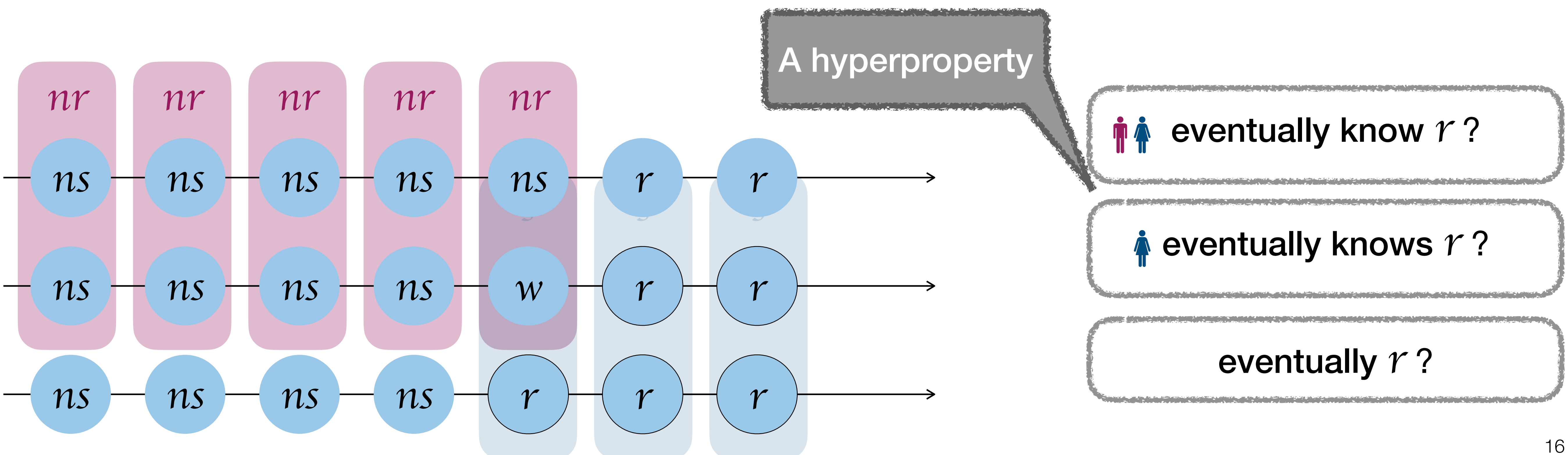
eventually know r ?

eventually knows r ?

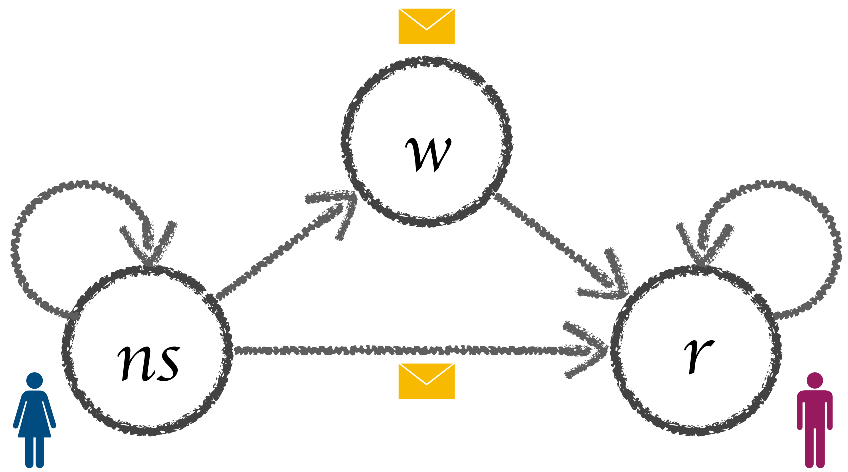
eventually r ?

Communication in Multi-Agent Systems

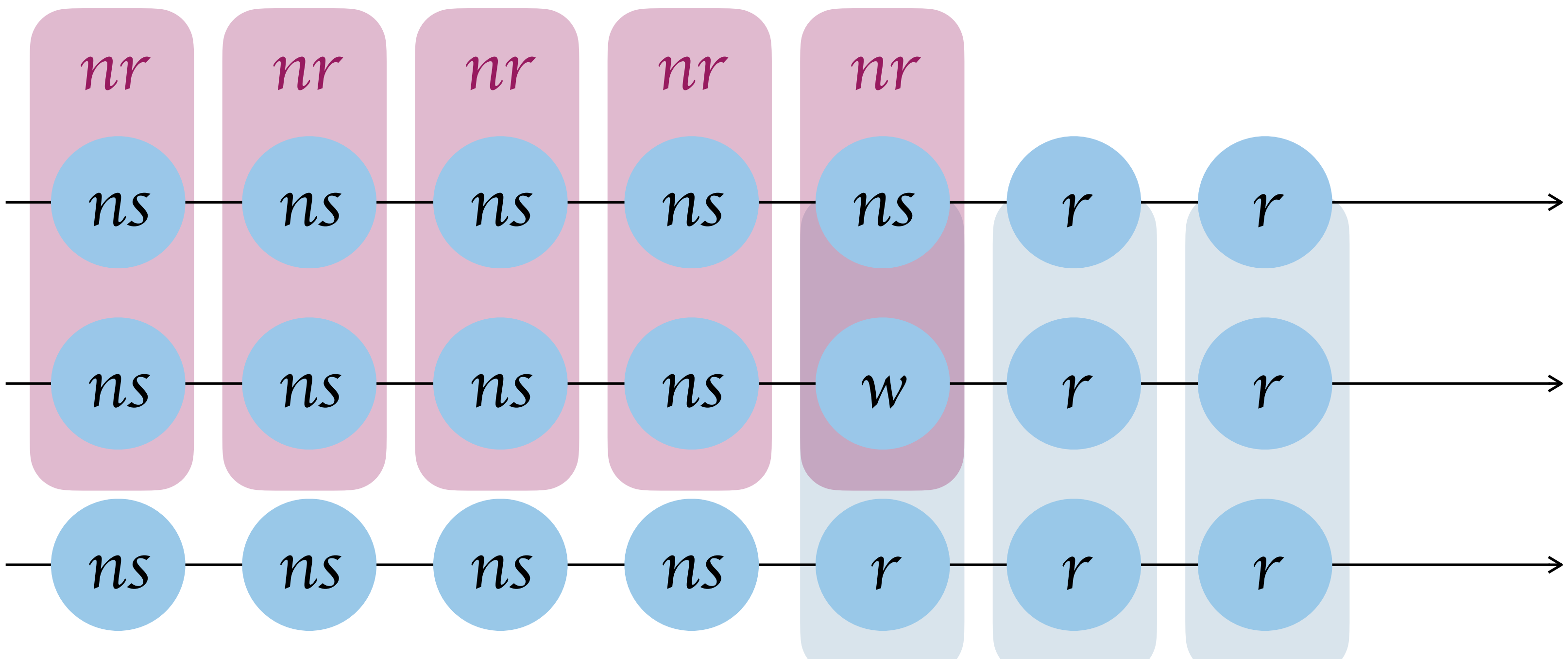




Communication in Multi-Agent Systems



eventually common knowledge r ?

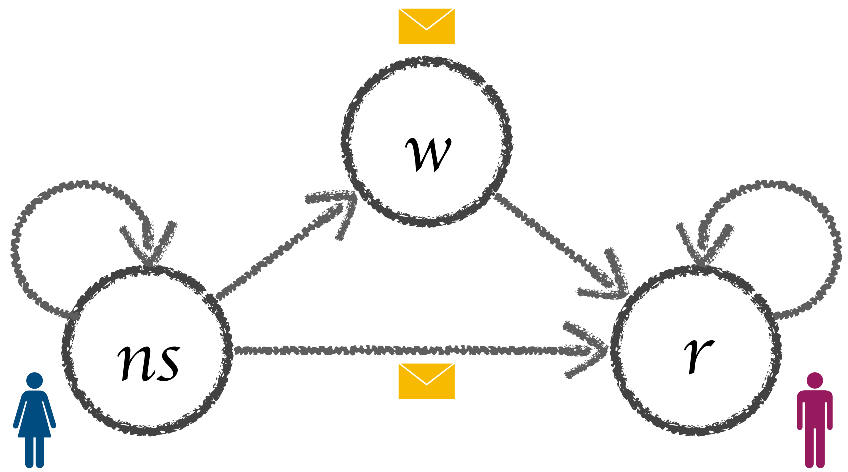


eventually know r ?

eventually knows r ?

eventually r ?

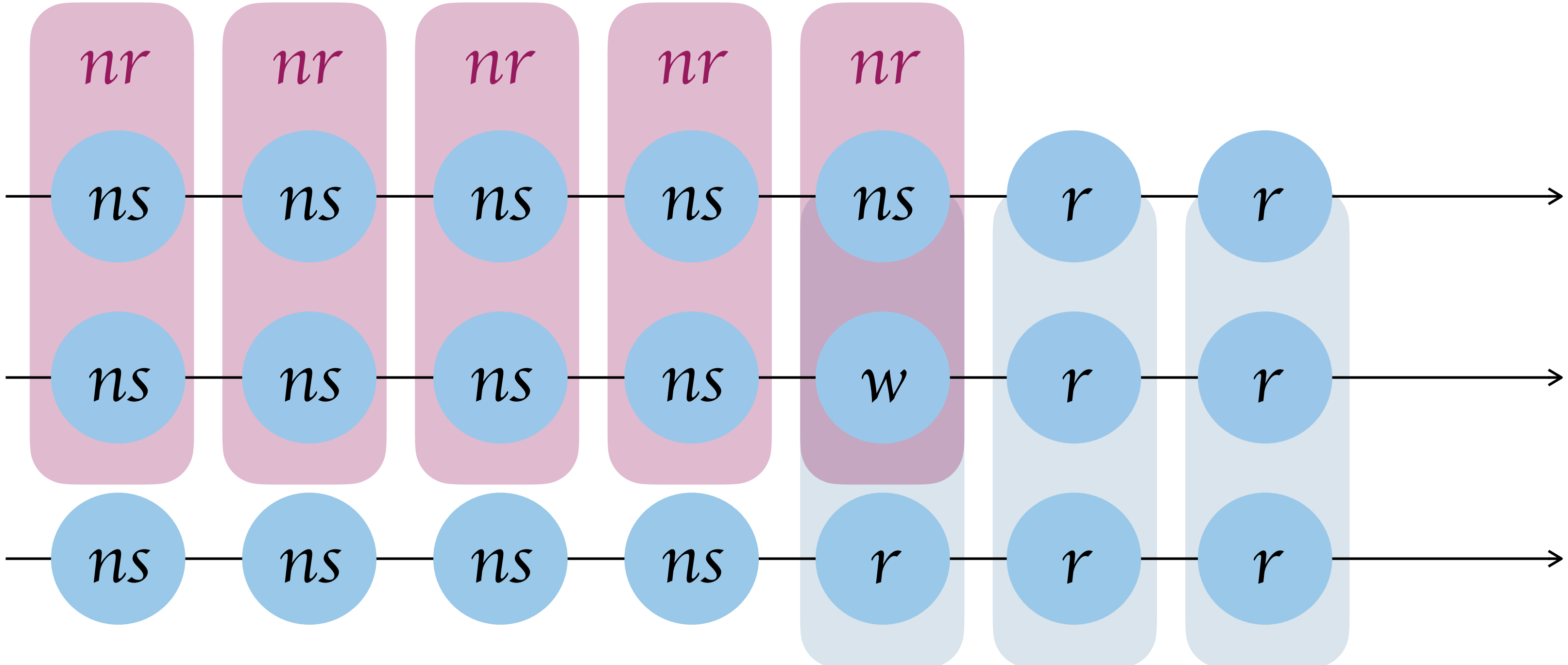
Communication in Multi-Agent Systems



Simultaneous action

Consensus

eventually common knowledge r ?

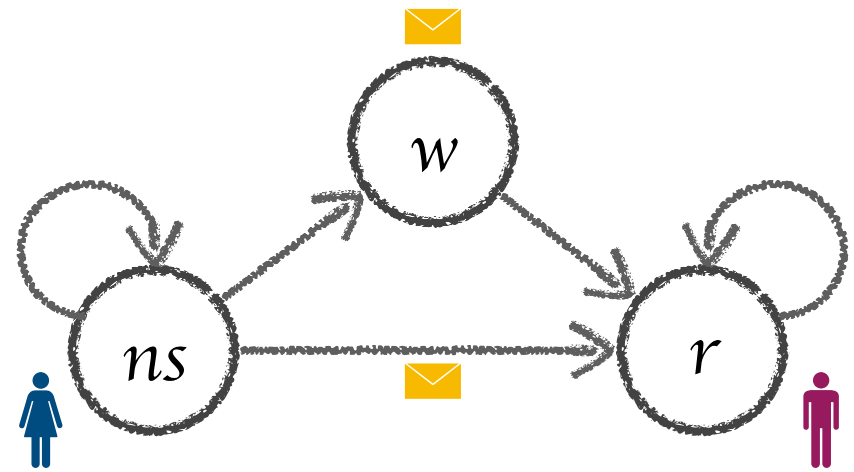


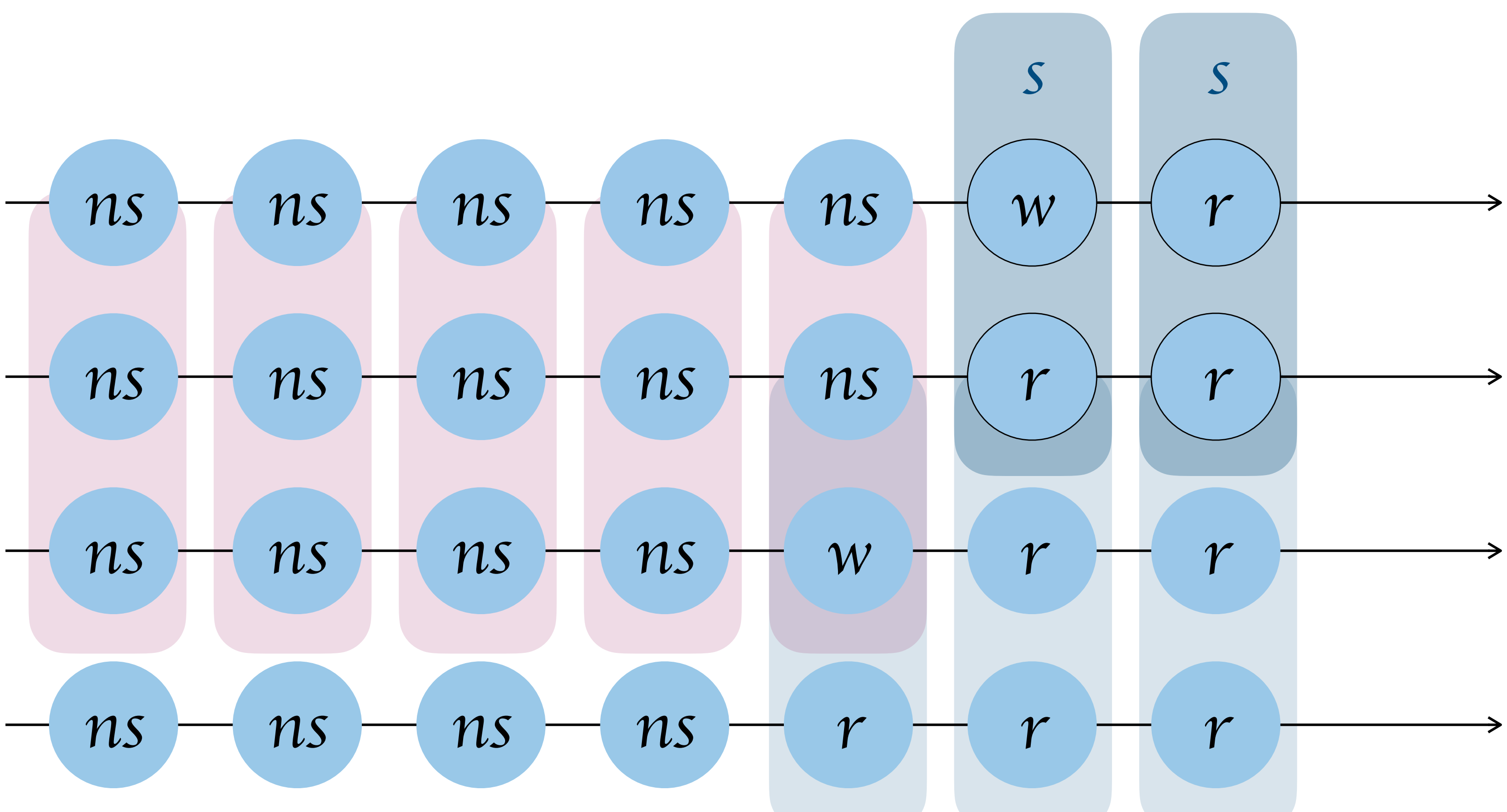
eventually know r ?

eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems





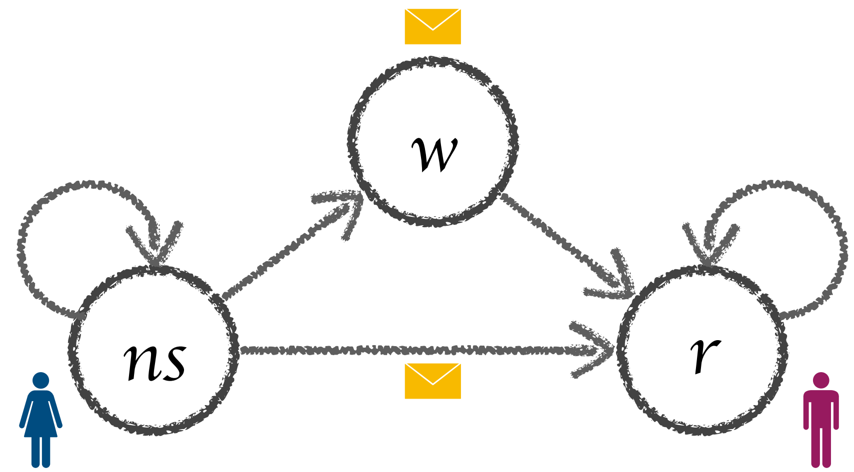
eventually common knowledge r ?

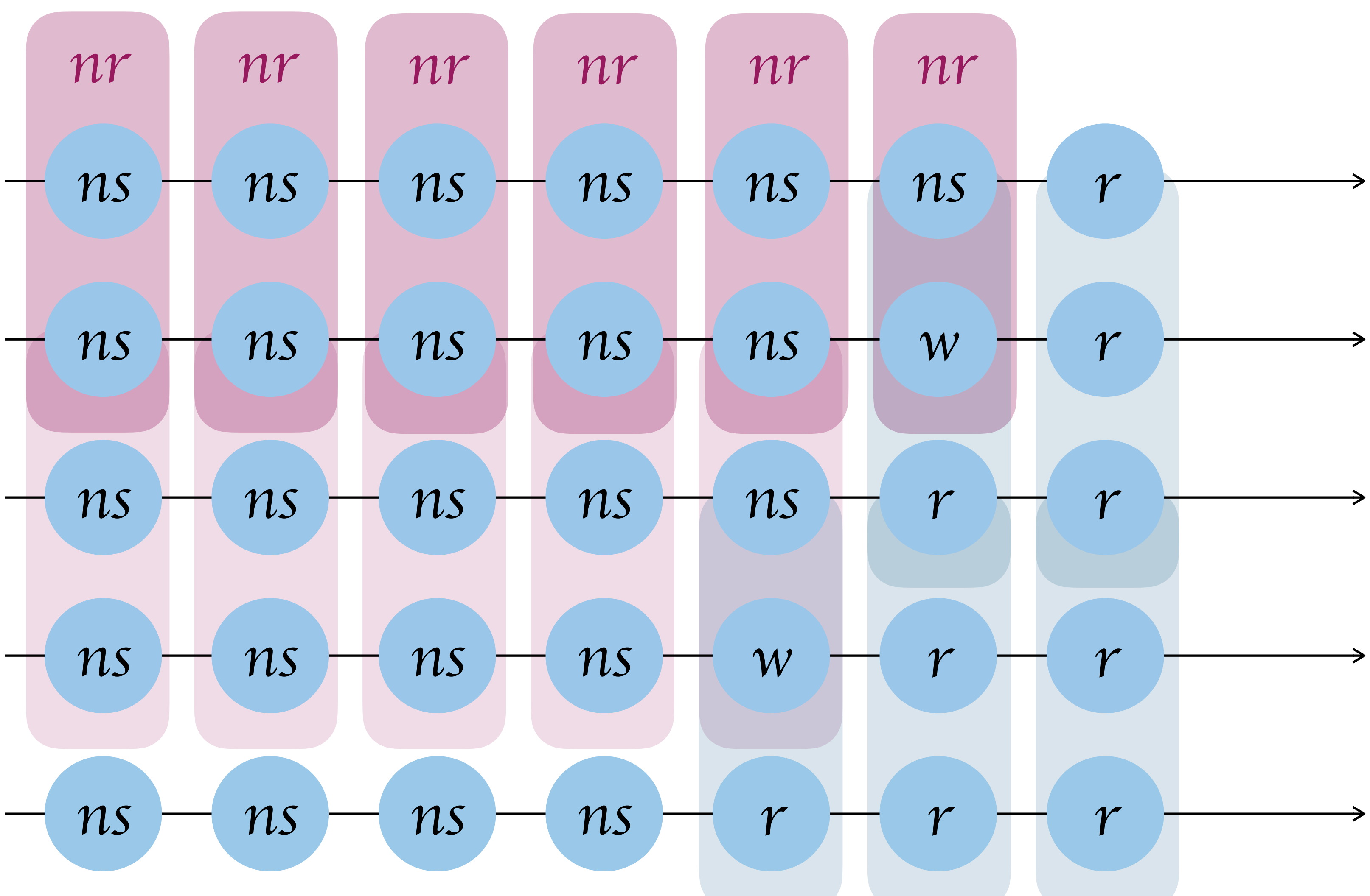
eventually know r ?

eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems





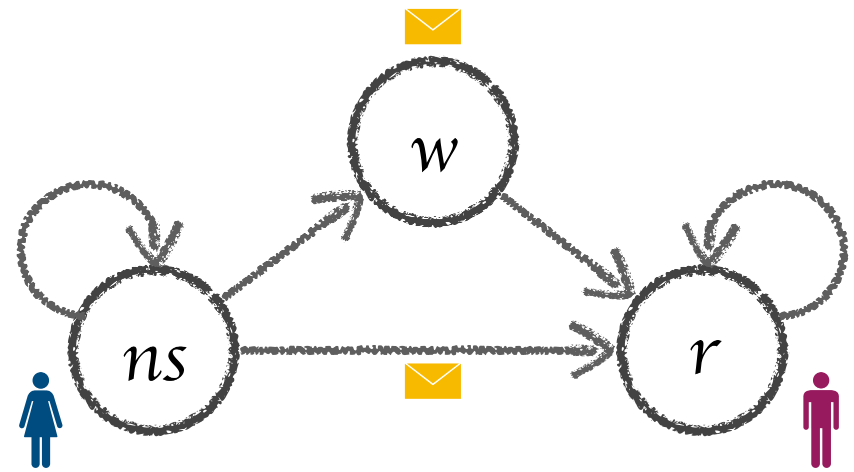
eventually common knowledge r ?

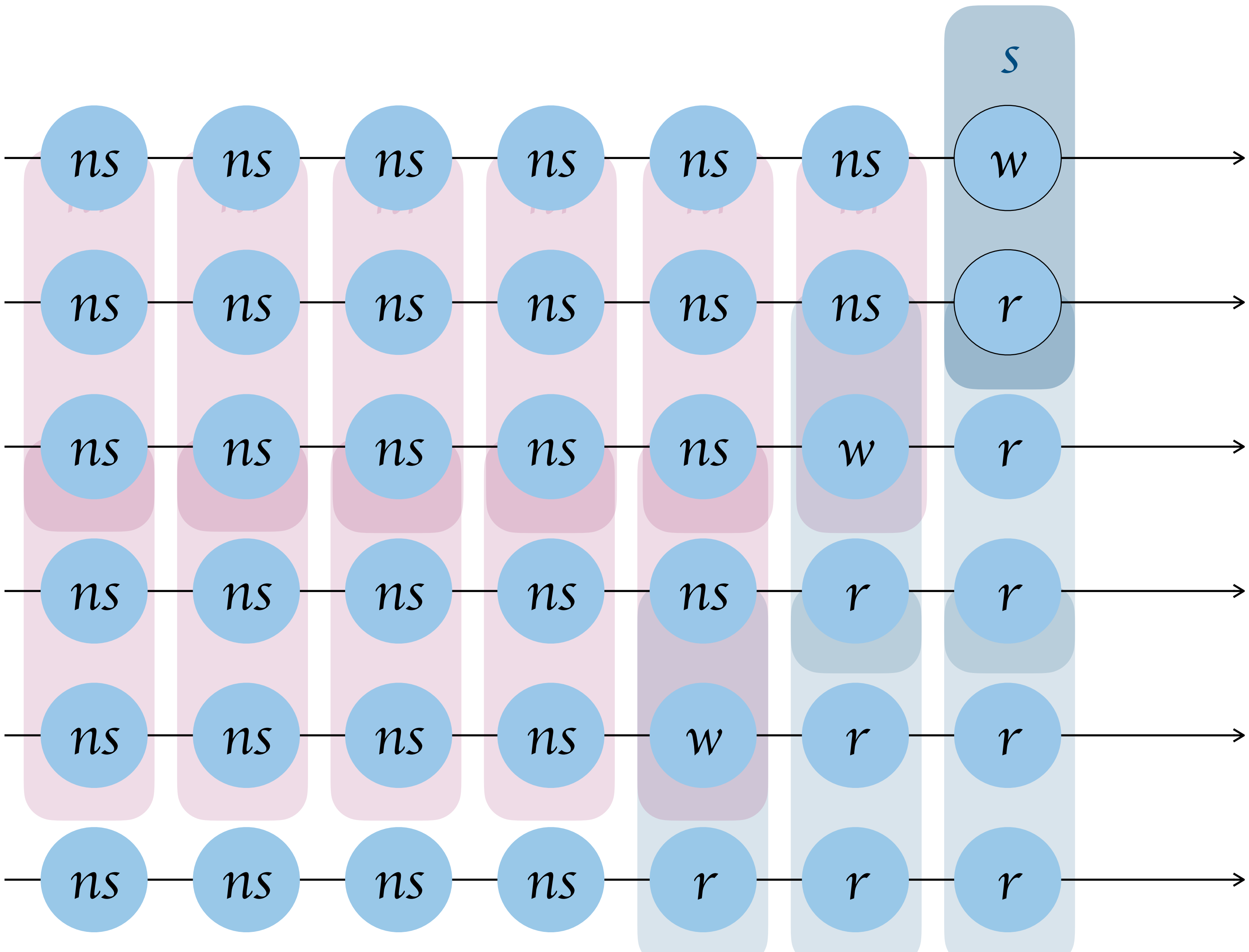
eventually know r ?

eventually knows r ?

eventually r ?

Communication in Multi-Agent Systems





eventually common knowledge r ?

eventually know r ?

eventually knows r ?

eventually r ?

Temporal Epistemic Logics

- $\text{LTL}_{K,C}$
  LTL + (common) knowledge

- HyperCTL^*_{lp}
  HyperCTL^* + knowledge

- MCK, MCMAS
  Model checking knowledge and time

The complexity of reasoning about knowledge and time. Halpern and Vardi (STOC 1986)

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

MCK: model checking the logic of knowledge. Gammie, van der Meyden (CAV 2004)

MCMAS: an open-source model checker for the verification of multi-agent systems. Lomuscio, Qu, Raimondi (Int. J. Softw. Tools Technol. 2015)

Hyper²LTL

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

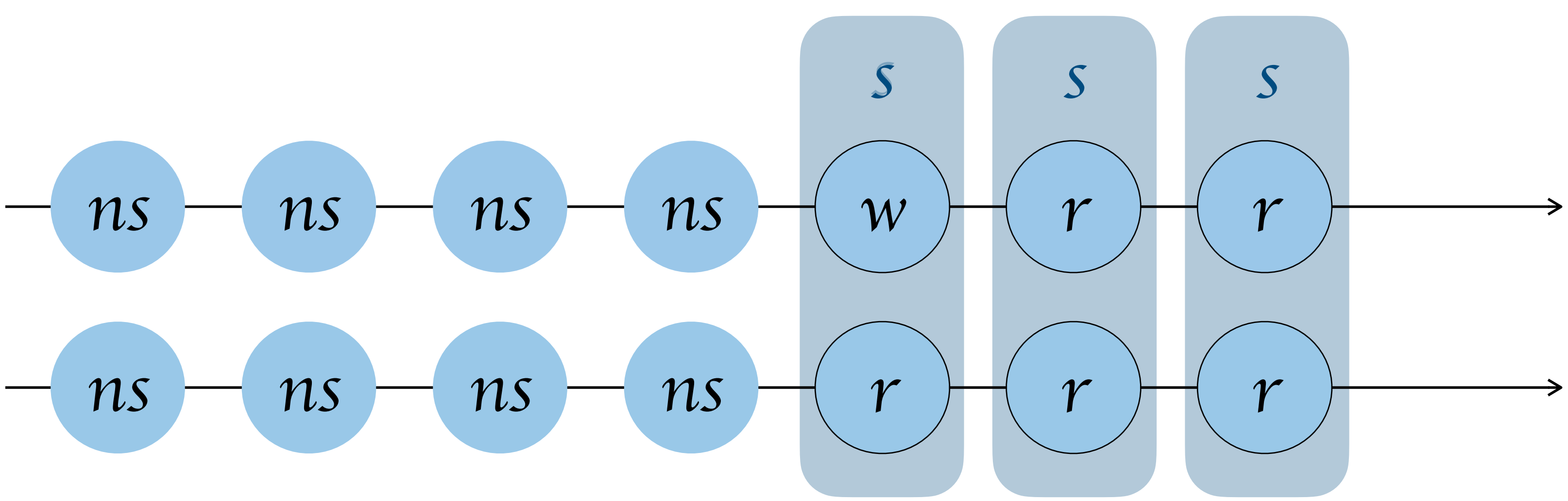
Causality

Hyper^{2}LTL

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

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

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



eventually knows r ?

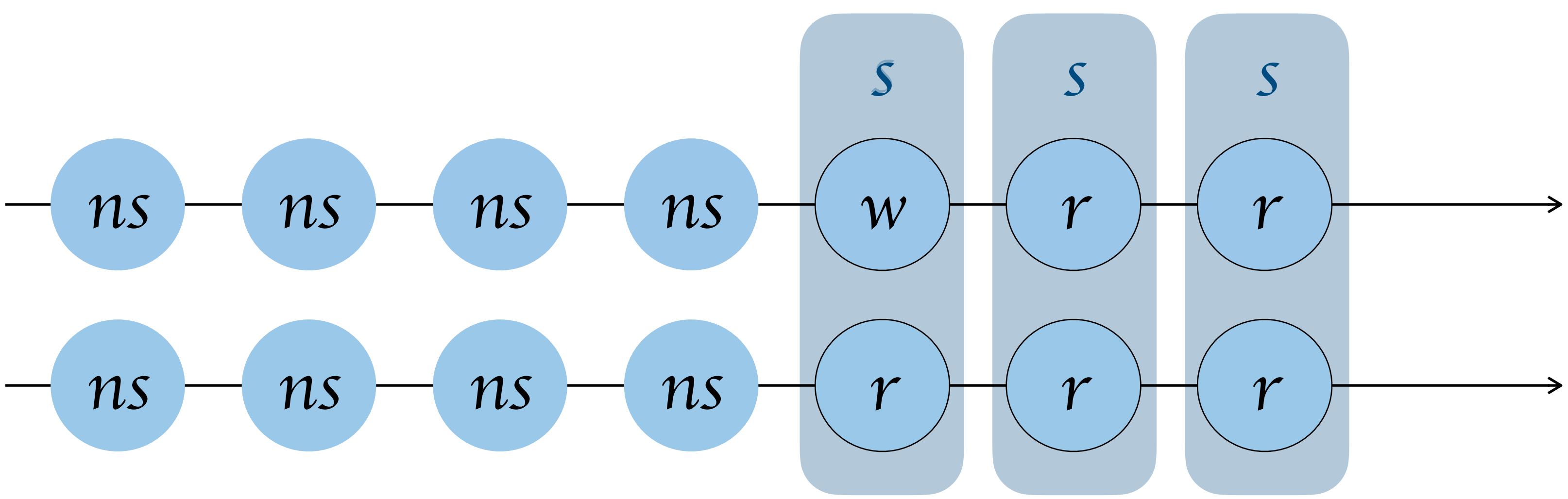
Hyper^{2}LTL

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

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

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

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



eventually knows r ?

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-set variable

$\mathcal{G}$ – system traces

$\mathcal{U}$ – Σ^ω

Hyper²LTL

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

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

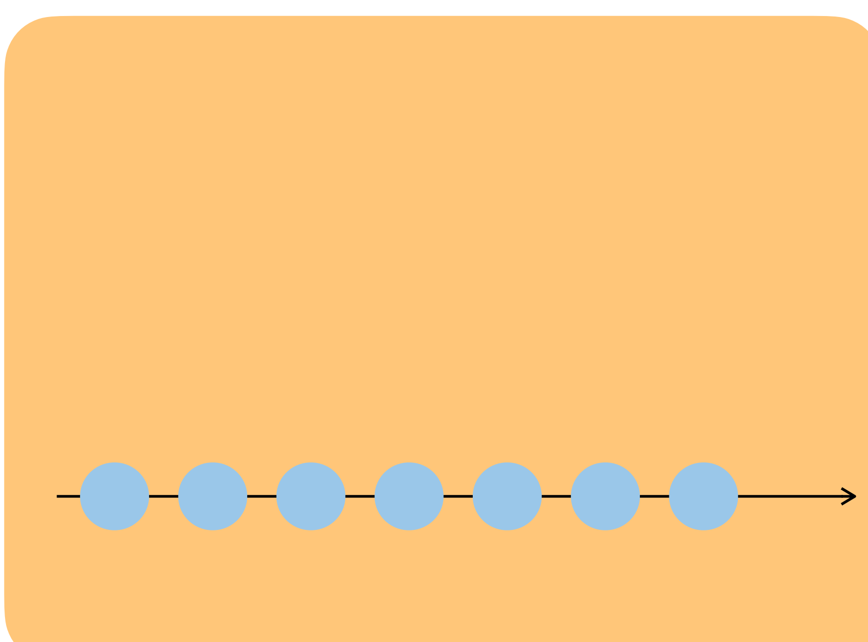
eventually common knowledge r ?

Hyper^{2}LTL

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

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

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



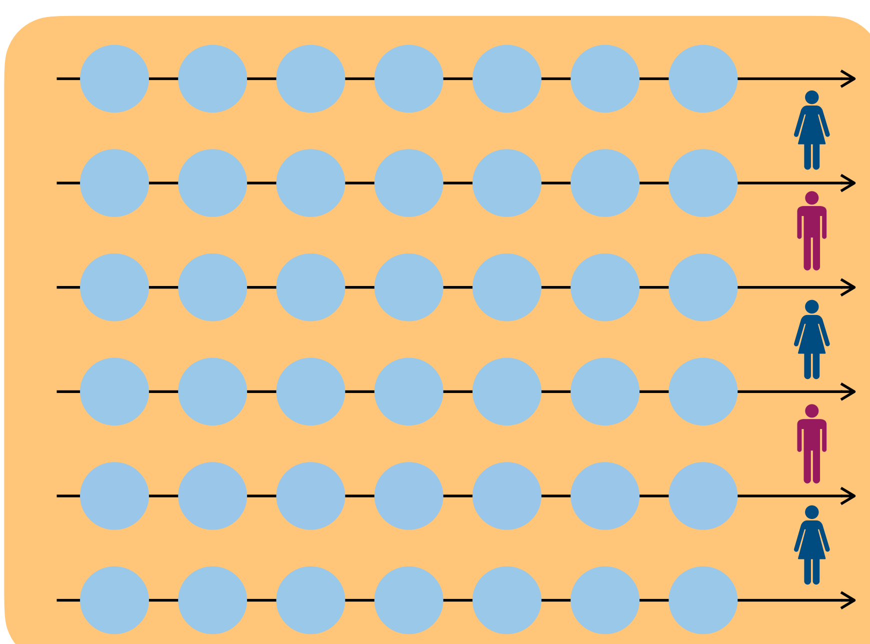
eventually common knowledge r ?

Hyper²LTL

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

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

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



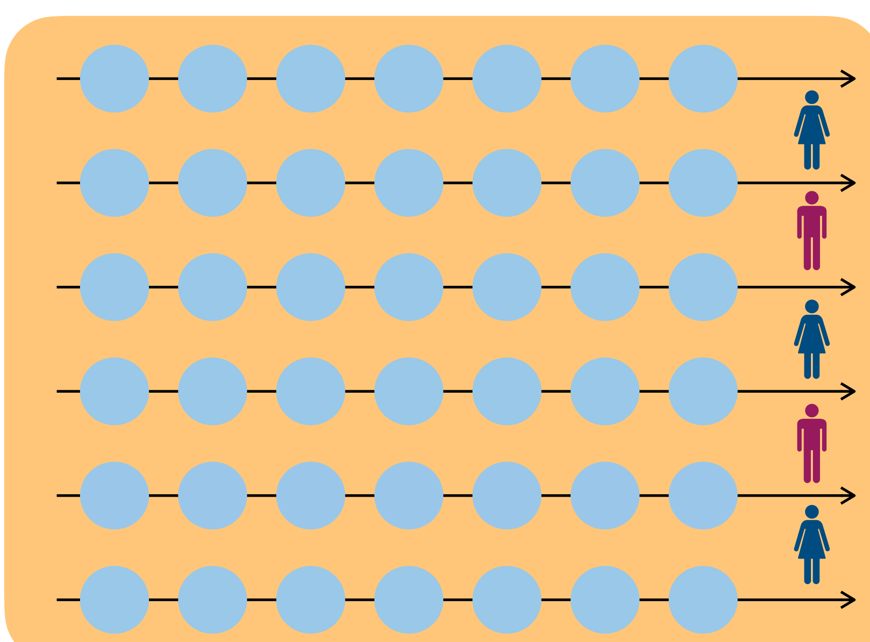
eventually common knowledge r ?

Hyper²LTL

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

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

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



eventually common knowledge r ?

Hyper²LTL

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality

Asynchronous Hyperproperties

Observational determinism

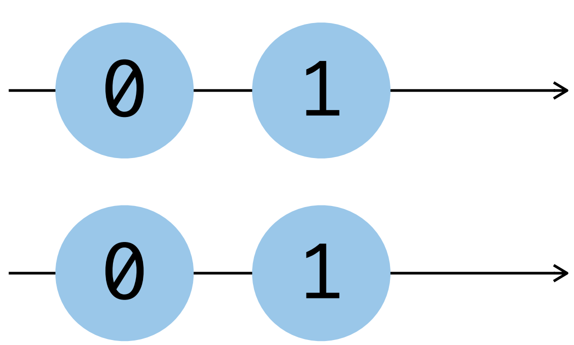
$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \square (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

Asynchronous Hyperproperties

Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \square (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
  l := 1
else
  l := l + 1
```



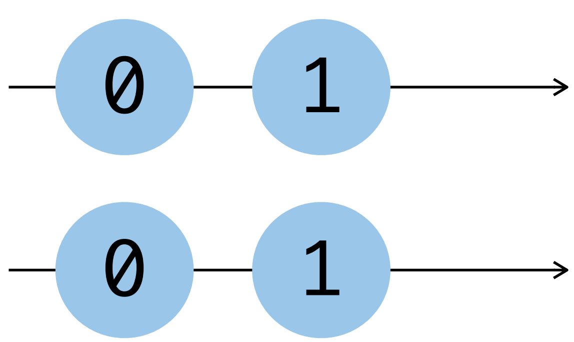
Asynchronous Hyperproperties

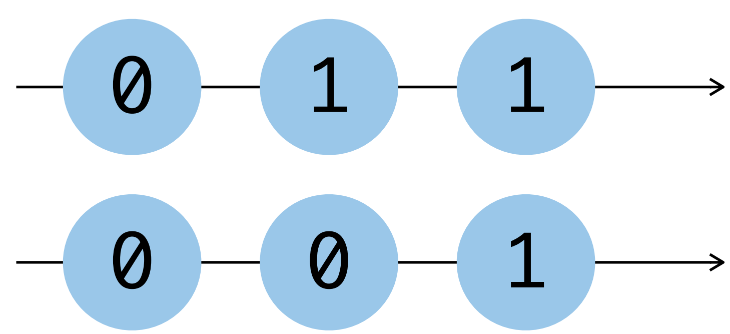
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \square (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
  l := 1
else
  l := l + 1
```

```
l := 0
if h then
  l := 1
else
  reg := l + 1
  l := reg
```



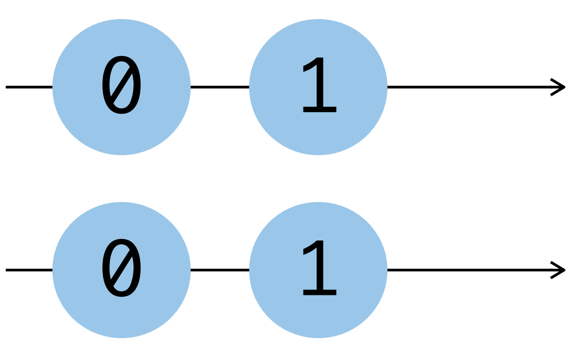


Asynchronous Hyperproperties

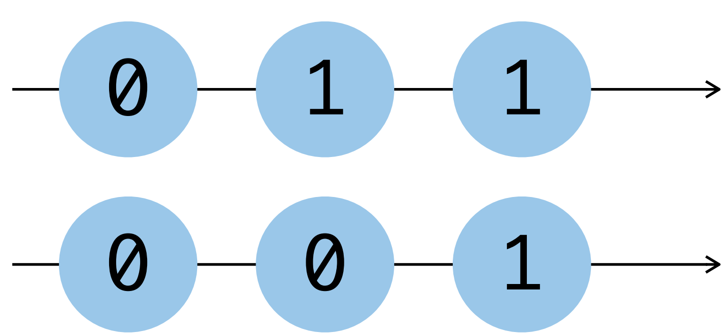
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
  l := 1
else
  l := l + 1
```




```
l := 0
if h then
  l := 1
else
  reg := l + 1
  l := reg
```



Access to shared resources

Scheduler decisions

Compiler optimizations

Asynchronous Hyperproperties

- HyperLTL$_S$
  HyperLTL + stuttering w.r.t a set of LTL formulas

- AHLTL
  HyperLTL + trajectories

- H_μ
  fixpoint-based logic

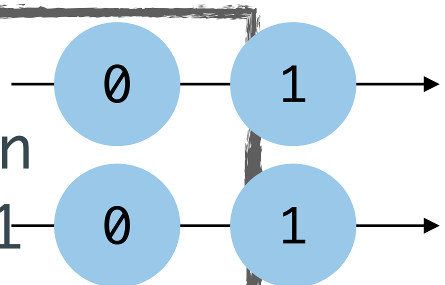
Asynchronous extensions of HyperLTL. Bozzelli, Peron, Sánchez (LICS 2021)
A temporal logic for asynchronous hyperproperties. Baumeister, Coenen, Bonakdarpour, Finkbeiner, Sánchez (CAV 2021)
Automata and fixpoints for asynchronous hyperproperties. Gutsfeld, Müller-Olm, Ohrem (POPL 2021)

Asynchronous Hyperproperties

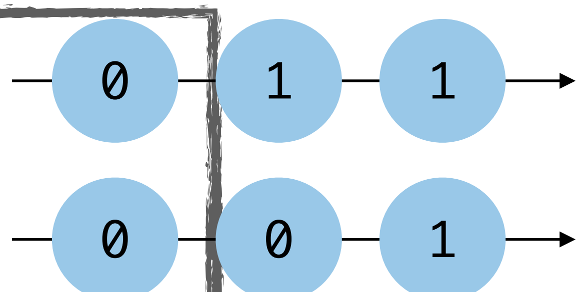
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
   l := 1
else
   l := l + 1
```




```
l := 0
if h then
   l := 1
else
   reg := l + 1
   l := reg
```

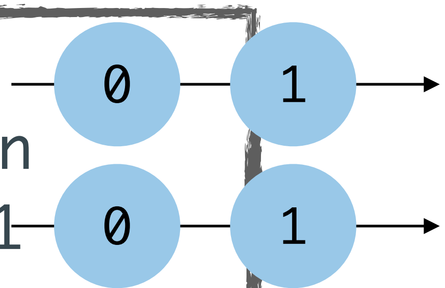


Asynchronous Hyperproperties

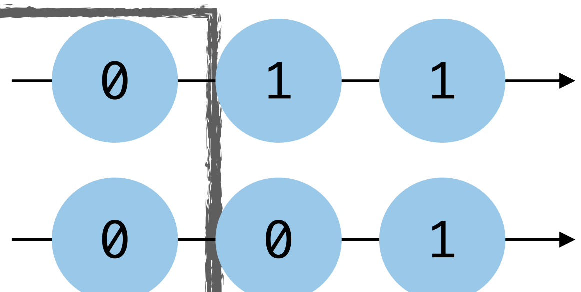
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
   l := 1
else
   l := l + 1
```




```
l := 0
if h then
   l := 1
else
   reg := l + 1
   l := reg
```



$\forall \pi_i . \exists X_i . \pi_i \in X_i$

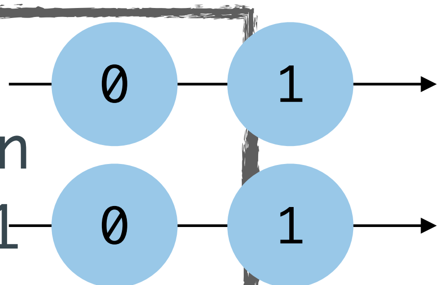
X_i — all stutter-equivalent traces to π_i

Asynchronous Hyperproperties

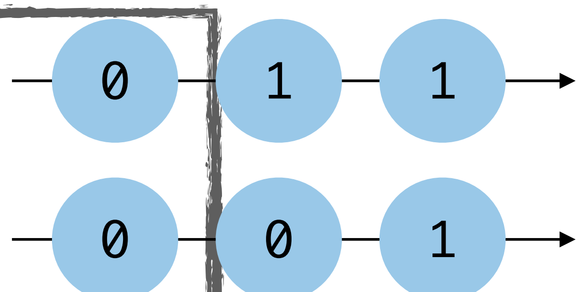
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
   l := 1
else
   l := l + 1
```




```
l := 0
if h then
   l := 1
else
   reg := l + 1
   l := reg
```



$$\forall \pi_i . \exists X_i . \pi_i \in X_i$$

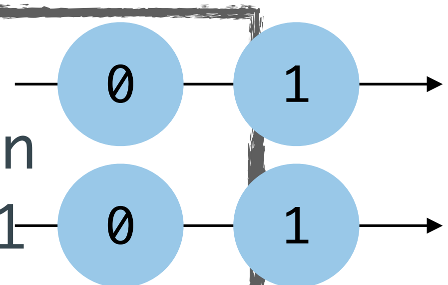
$$\forall \pi \in X_i . \forall \pi' \in \mathcal{U} . (\pi =_{AP} \pi') \, \mathcal{U}$$
$$(\pi =_{AP} \pi' \wedge \Box \bigwedge_{a \in AP} a_\pi \leftrightarrow \bigcirc a_{\pi'}) \rightarrow \pi' \in X$$

Asynchronous Hyperproperties

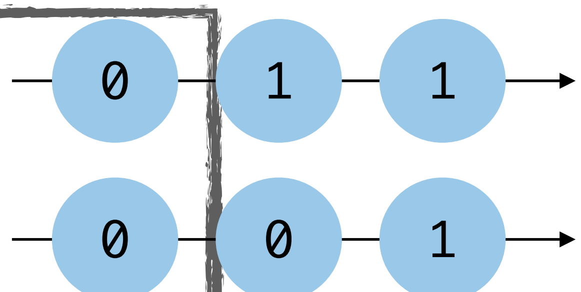
Observational determinism

$$\forall \pi_1 . \forall \pi_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

```
l := 0
if h then
   l := 1
else
   l := l + 1
```




```
l := 0
if h then
   l := 1
else
   reg := l + 1
   l := reg
```



$\forall \pi_i . \exists X_i . \pi_i \in X_i$

X_i — all stutter-equivalent traces to π_i

$$\exists \pi_1 \in X_1 . \exists \pi_2 \in X_2 . (l_{\pi_1} \leftrightarrow l_{\pi_2}) \rightarrow \Box (l_{\pi_1} \leftrightarrow l_{\pi_2})$$

Hyper^{2}LTL

Why?

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality

Generic reasoning

Hyper^{2}LTL

Why?

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

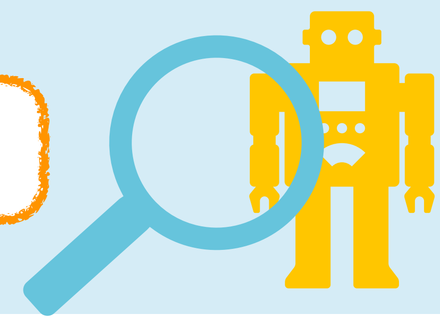
$$\varphi := \exists \pi \in X\,.\,\varphi \mid \forall \pi \in X\,.\,\varphi \mid \exists X\,.\,\varphi \mid \forall X\,.\,\varphi$$

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality



trace property = set of traces

Generic reasoning

Hyper²LTL

Why?

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

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

Common Knowledge

Asynchronous Hyperproperties

Trace Theory

Causality

Generic reasoning and algorithms

Model Checking Hyper^{2}LTL$_{fp}$

Friday afternoon @CAV

$$\varphi = \exists \pi_1 . \forall X_1 . \forall \pi_2 \in X_1 . \ldots . \exists X_k . \exists \pi_k \in X_k . \psi$$

Interpreted over general set assignments

Model Checking Hyper^{2}LTL$_{fp}$

Friday afternoon @CAV

$$\varphi = \exists \pi_1 . \forall X_1 . \forall \pi_2 \in X_1 \ldots . \exists X_k . \exists \pi_k \in X_k . \psi$$

under some conditions

under some conditions

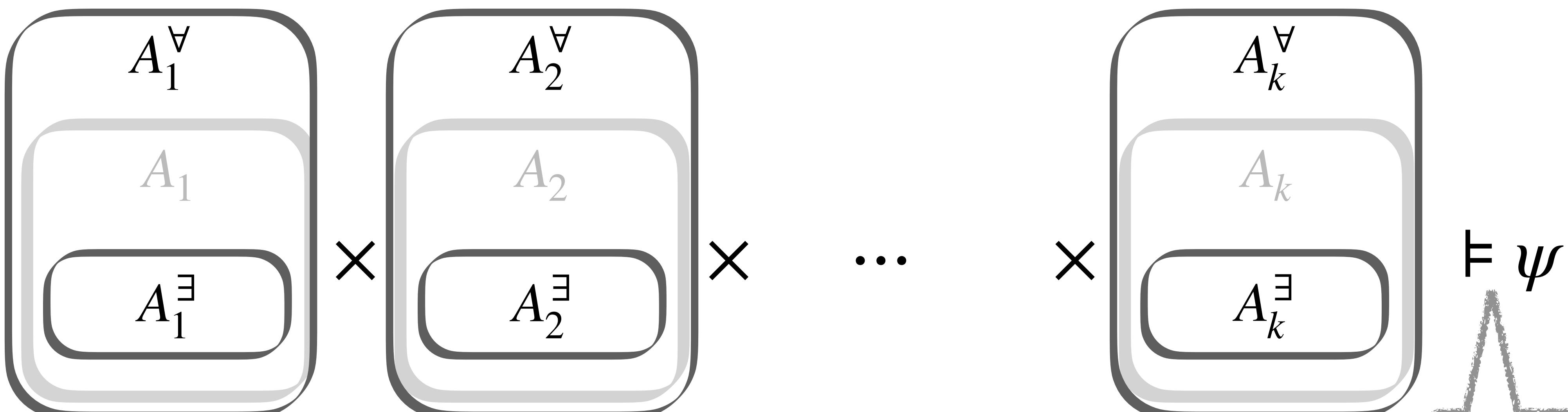
Model Checking Hyper²LTL$_{\mathrm{fp}}$

Friday afternoon @CAV

$$\varphi = \exists \pi_1 . \forall X_1 . \forall \pi_2 \in X_1 \ldots . \exists X_k . \exists \pi_k \in X_k . \psi$$

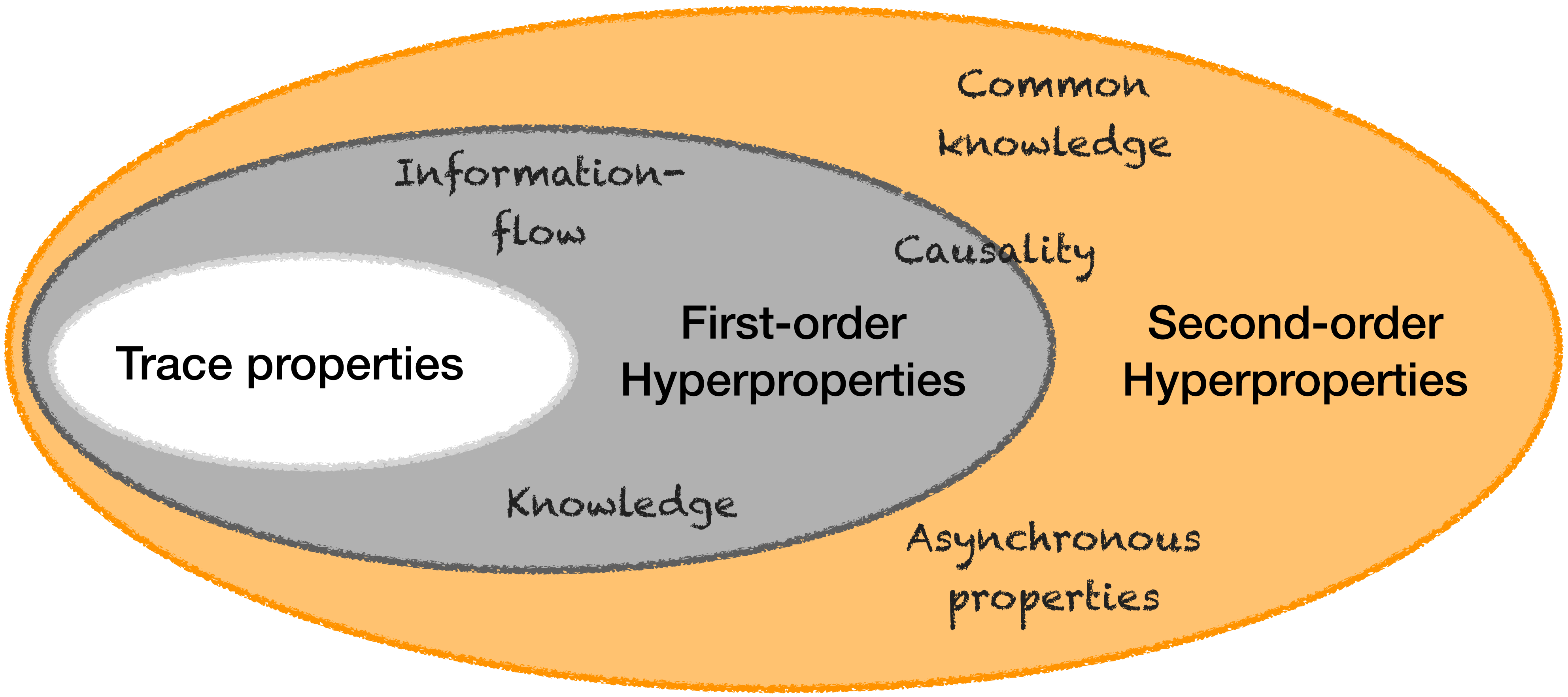
under some conditions

under some conditions



HyperLTL model checking

Why do we need **Second-Order Hyperlogics?**

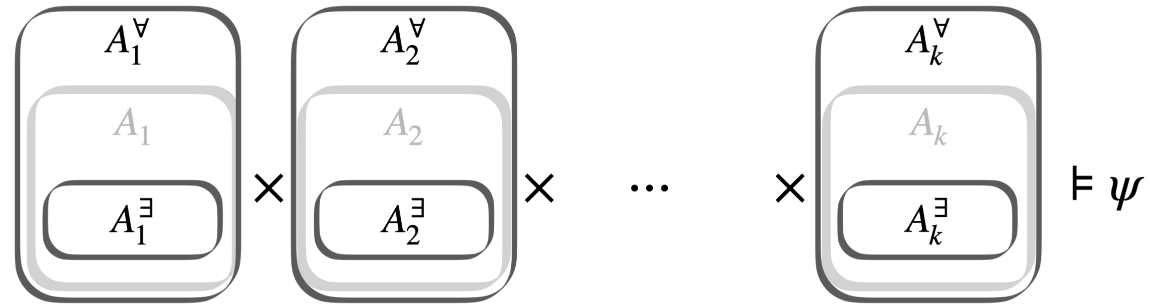


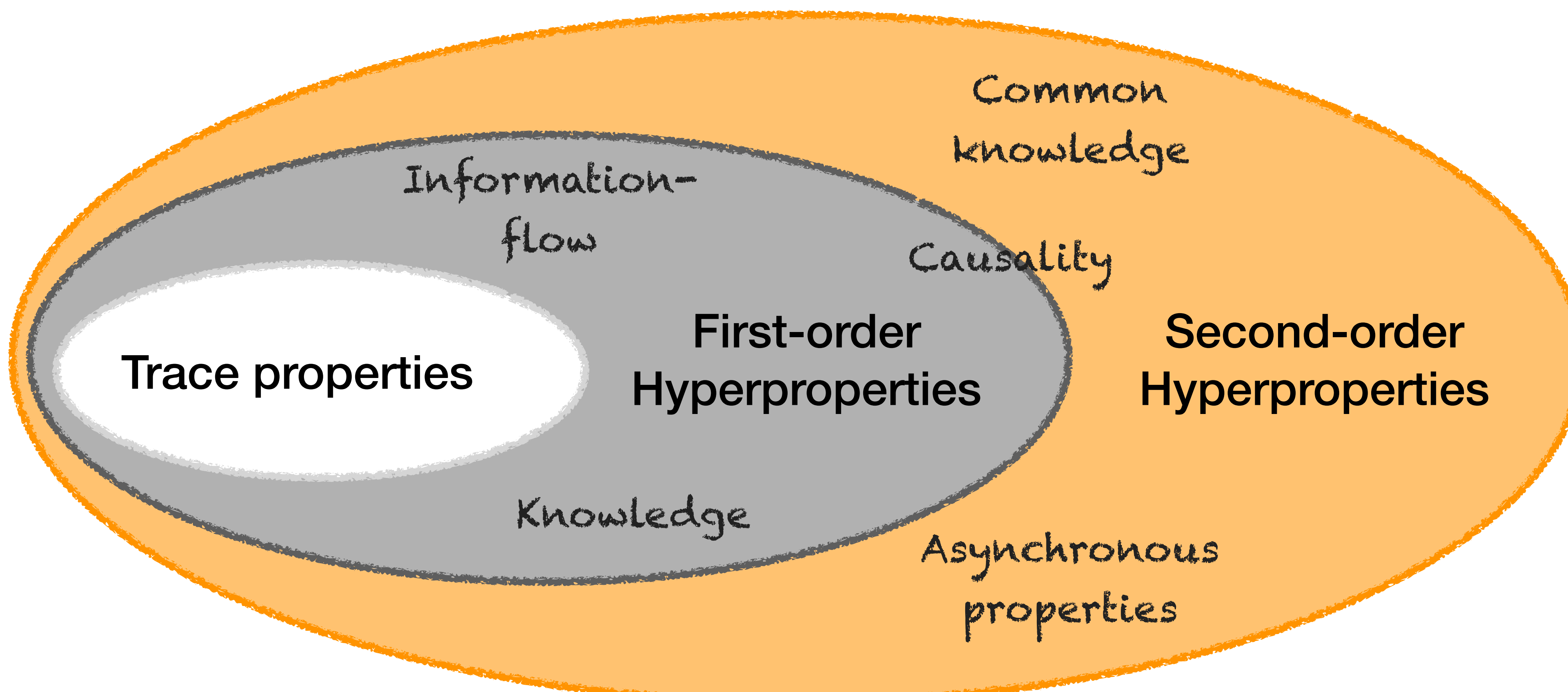
Why do we need Second-Order Hyperlogics?

Hyper²LTL

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

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



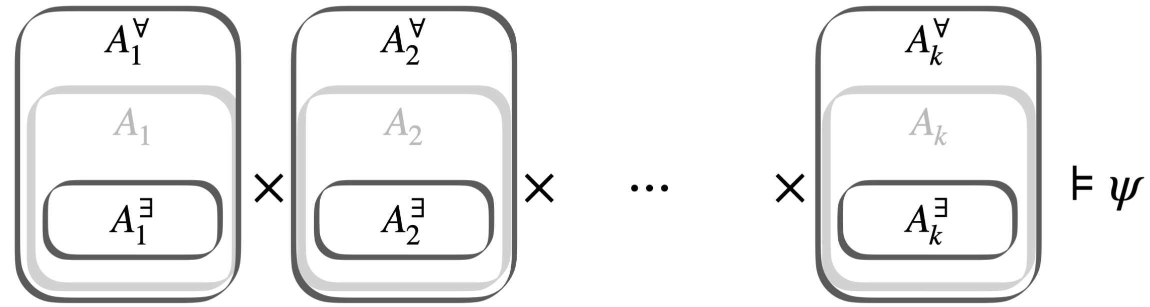


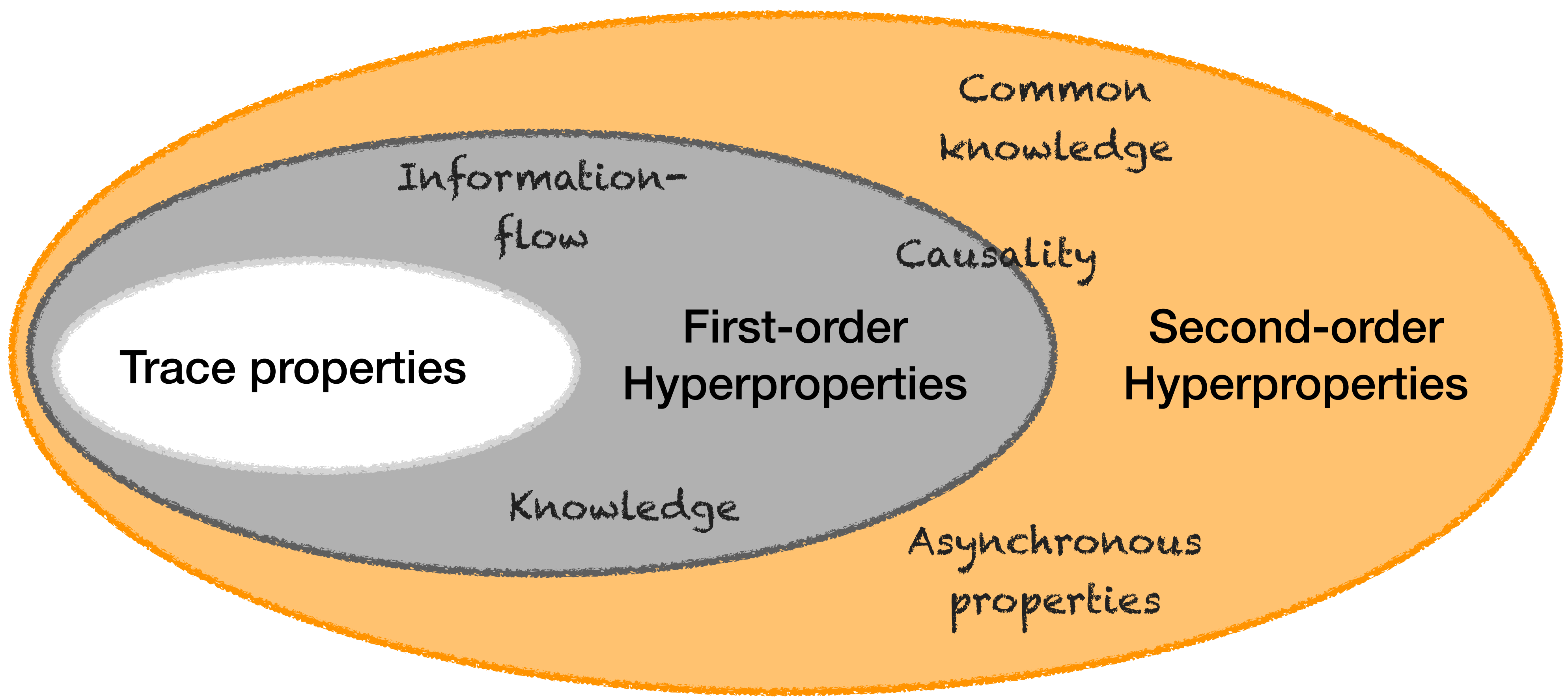
Why do we need **Second-Order Hyperlogics?**

Hyper²LTL

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

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





Thank you!