Logics for Hyperproperties

Jana Hofmann
CISPA Helmholtz Center for Information Security

joint work with
Norine Coenen, Bernd Finkbeiner, Christopher Hahn and Leander Tentrup

"The Hierarchy of Hyperlogics", LICS 2019
"Realizing ω-regular Hyperproperties", CAV 2020

IST Austria, 28 July 2020

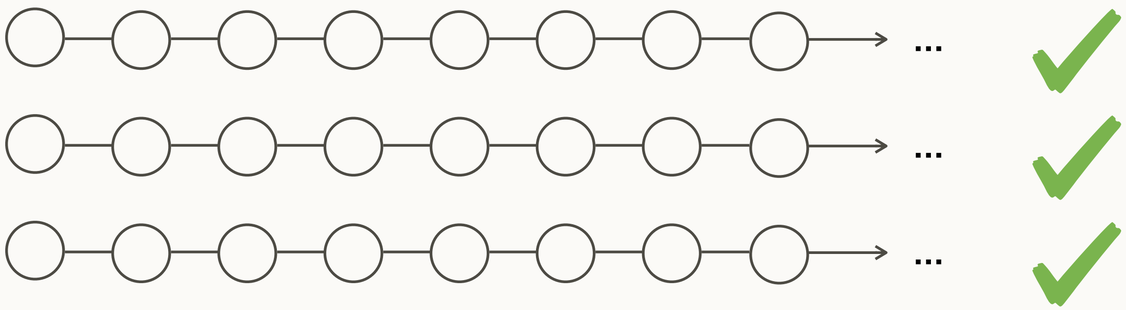
UNIVERSITÄT
DES
SAARLANDES

CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

Trace Properties vs Hyperproperties

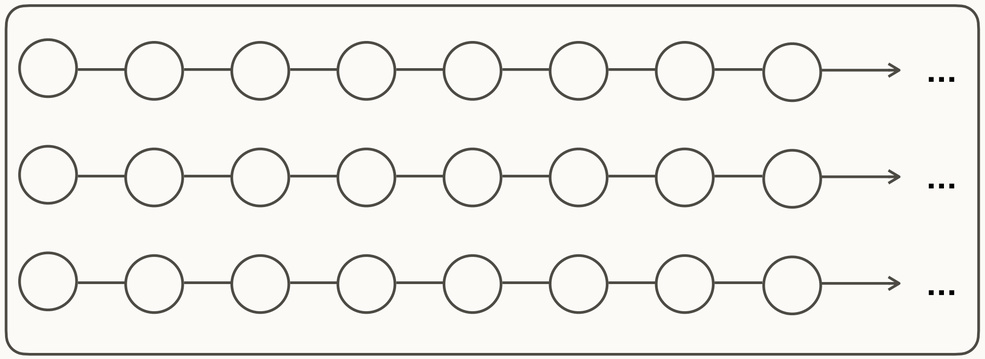
System:

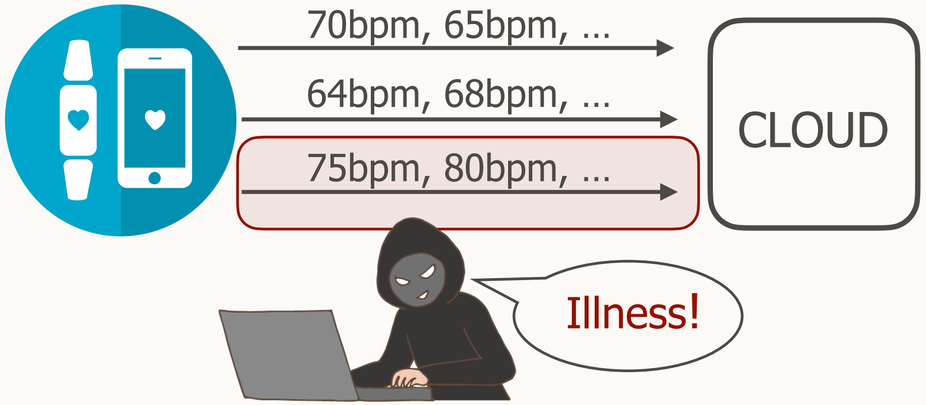
Trace property P?



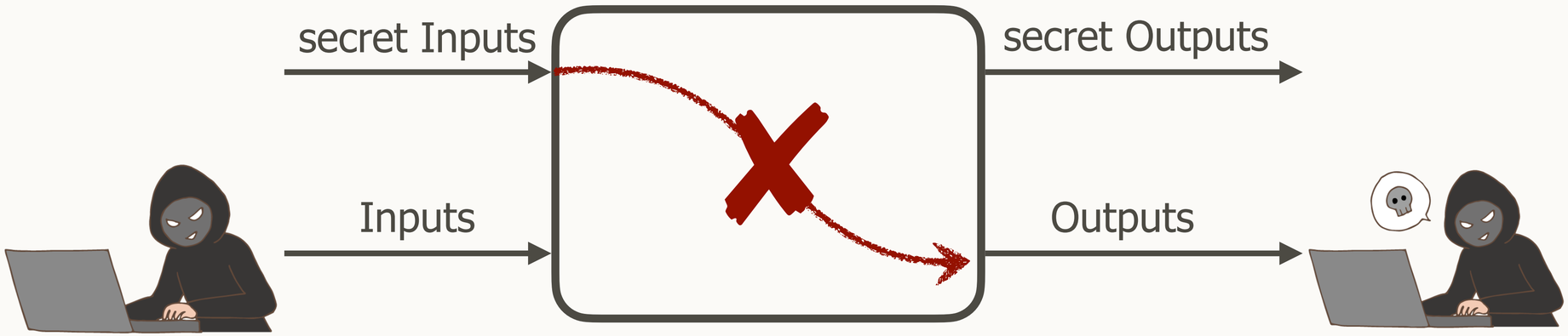
System:

Hyperproperty H?





Information Flow Security

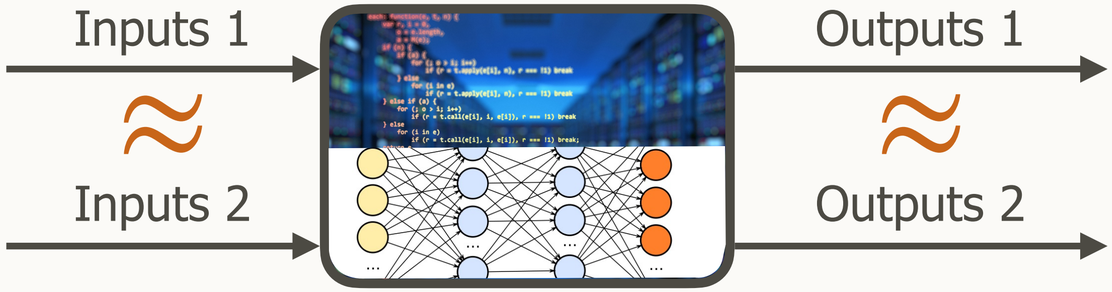


Noninterference: "For any two traces, if they agree on the inputs, they must agree on the outputs."

$$\forall t, t' \in T\,.\; sameInputs(t, t') \rightarrow sameOutputs(t, t')$$

Beyond Information Flow Control

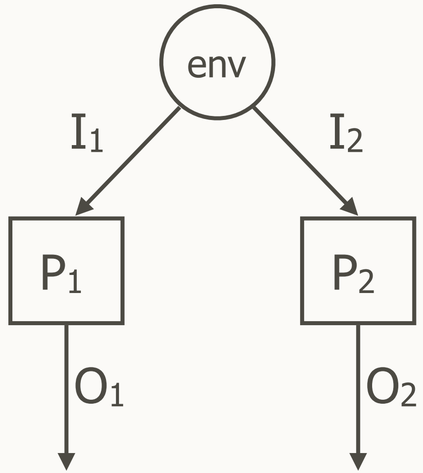
Robustness properties: “similar inputs lead to similar outputs”



System properties:

- partial observation
- distributivity
- fault tolerance

… are expressible as hyperproperties



Distributivity:

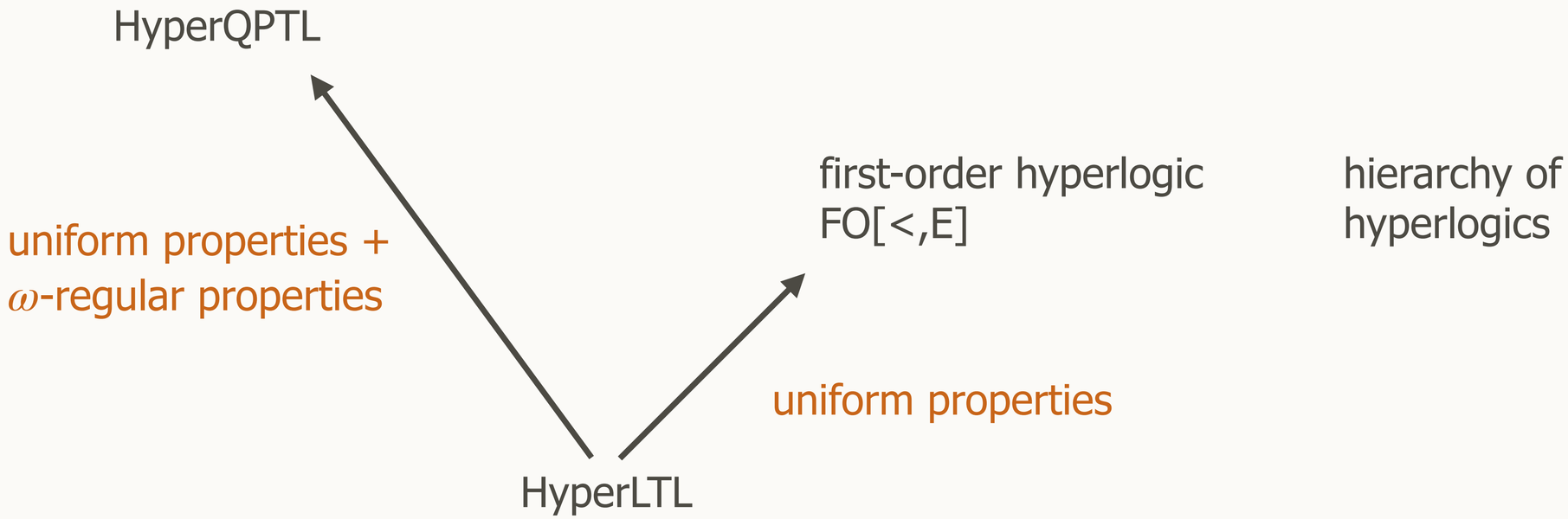
“on all two traces, if P_1 receives the same inputs, it produces the same outputs”

Finkbeiner, Hahn, Lukert, Stenger, Tentrup

Acta Informatica, 2019

Outline

model checking
satisfiability
synthesis



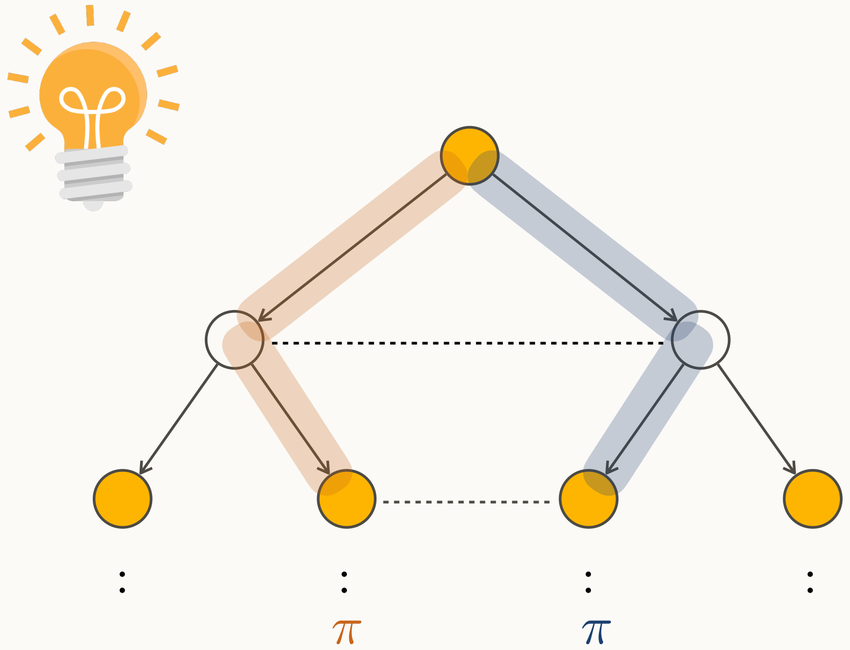
hierarchy of
hyperlogics

HyperLTL

$$\varphi \;::=\; \exists \pi.\ \varphi \mid \forall \pi.\ \varphi \mid \psi$$
$$\psi \;::=\; a_\pi \mid \bigcirc \psi \mid \psi \,\mathcal{U}\, \psi \mid \neg\psi \mid \psi \vee \psi$$

"All traces have the light on at the same time":

$$\forall \pi . \forall \pi' .\ \square(on_\pi \leftrightarrow on_{\pi'})$$



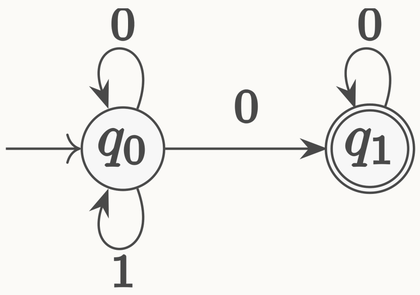
Noninterference:

$$\forall \pi . \forall \pi' . \square\Big(\bigwedge_{i \in inputs} i_\pi \leftrightarrow i_{\pi'}\Big) \rightarrow \square\Big(\bigwedge_{o \in outputs} o_\pi \leftrightarrow o_{\pi'}\Big)$$

HyperLTL Expressiveness

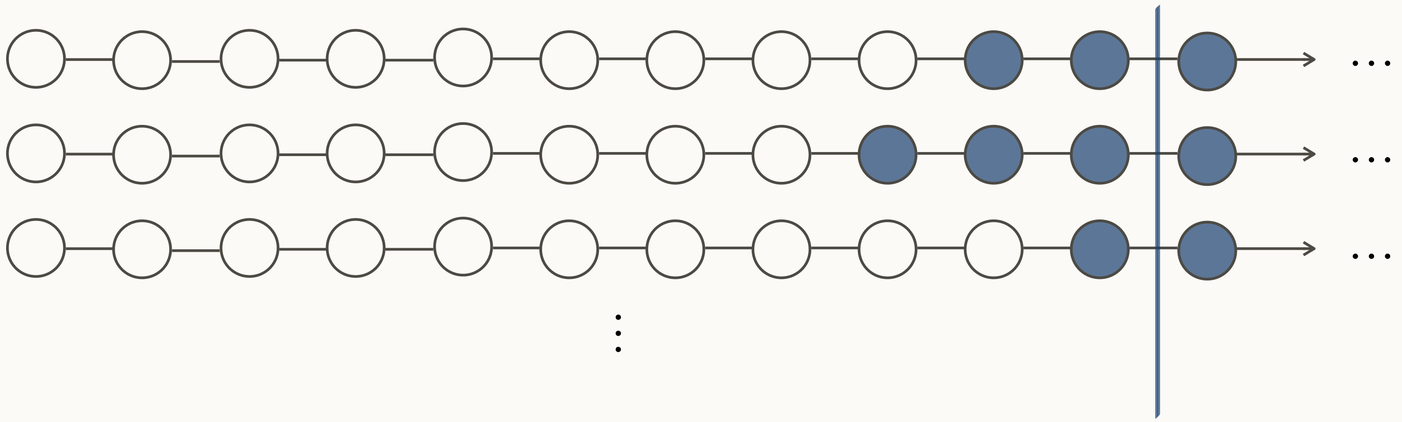
No ω-regular properties

No uniform properties



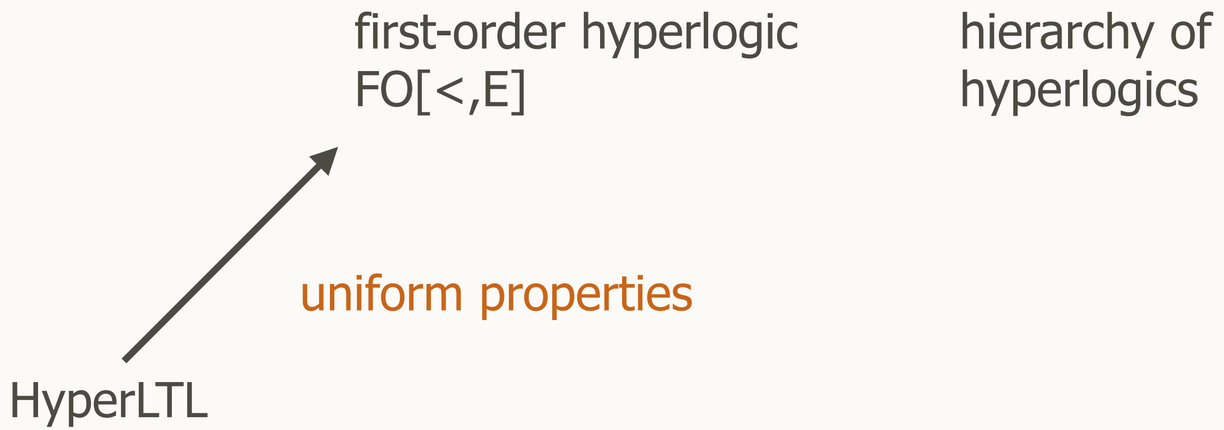
Bozzelli, Maubert, Pinchinat
FoSSaCS, 2015

Uniform Termination: "There is a global bound up to which the system terminates on all traces."



Hyperlogics beyond HyperLTL?

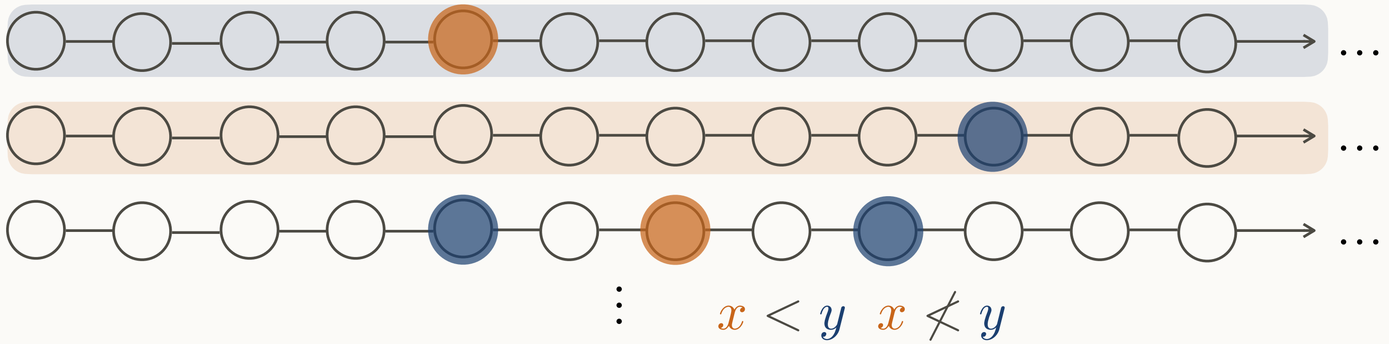
Outline


first-order hyperlogic
FO[<,E]
hierarchy of
hyperlogics
uniform properties
HyperLTL

First-Order Hyperlogics

FO[<,E]: First-Order Monadic Logic of Order with Equal-Level Predicate:

$$atom ::= P(x) \mid x < y \mid E(x,y)$$
$$\varphi ::= atom \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \exists x.\varphi \mid \forall x.\varphi$$



Kamp's Theorem:

LTL ≡ FO[<]

HyperLTL < FO[<,E]

Finkbeiner, Zimmermann
STACS, 2017

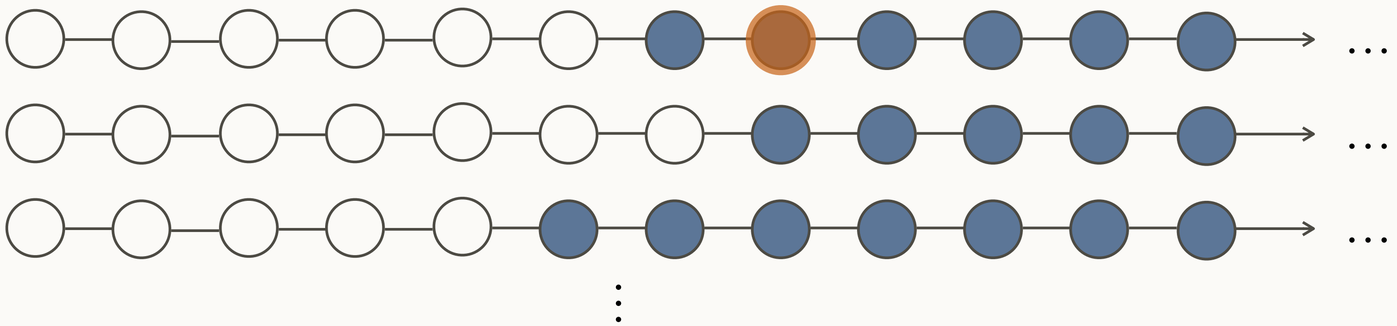
"All traces globally agree on a":

$$\forall\pi.\forall\pi'.\ \square(a_\pi \leftrightarrow a_{\pi'})$$

$$\forall x.\forall y.\ E(x,y) \rightarrow (P_a(x) \leftrightarrow P_a(y))$$

HyperLTL < FO[<,E]

FO[<,E] can express uniform properties:

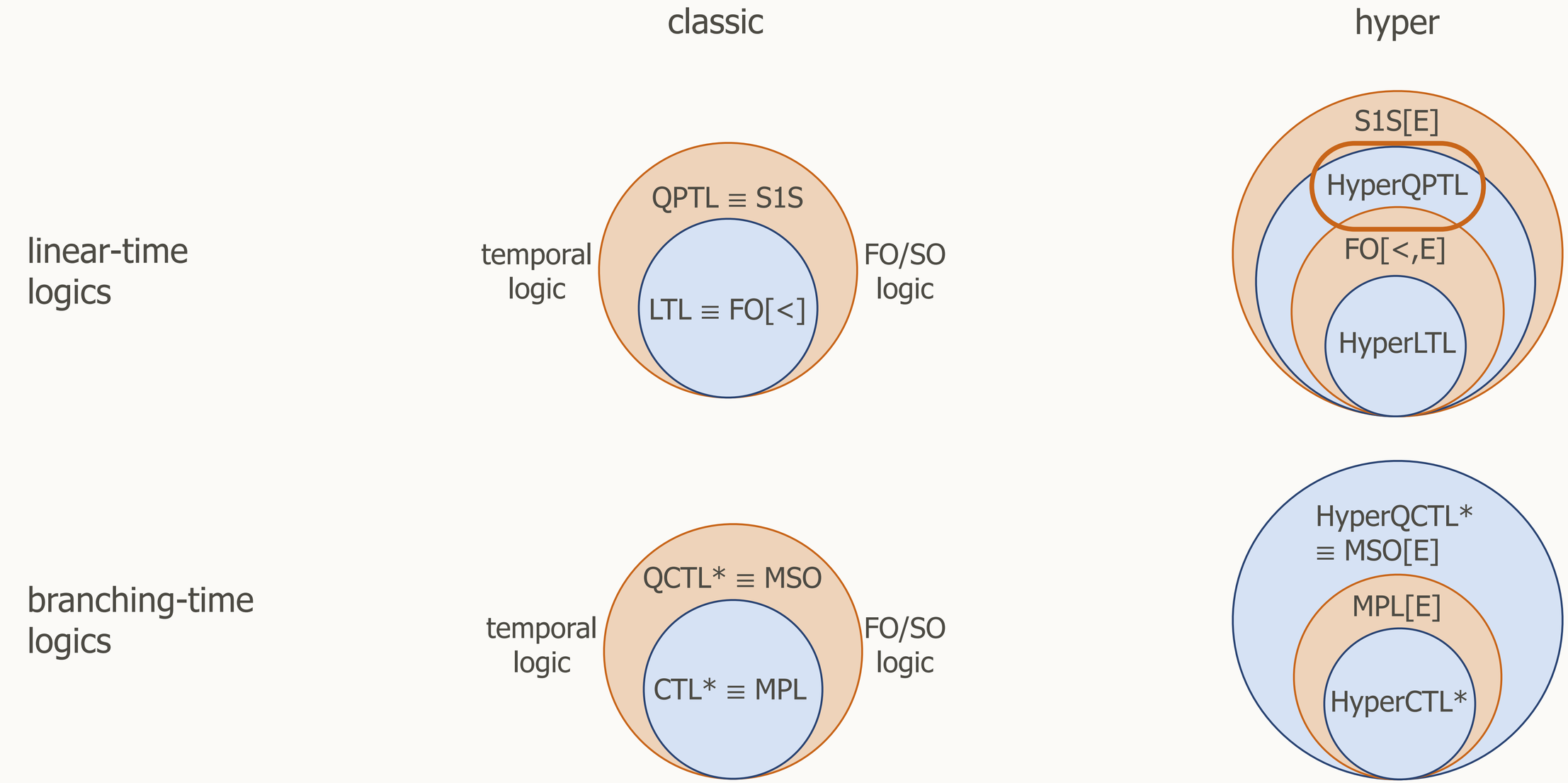


Uniform Termination: “There is a global bound up to which the system terminates on all traces.”

$$\exists b. \forall x.\ E(x, b) \rightarrow P_{halt}(x)$$

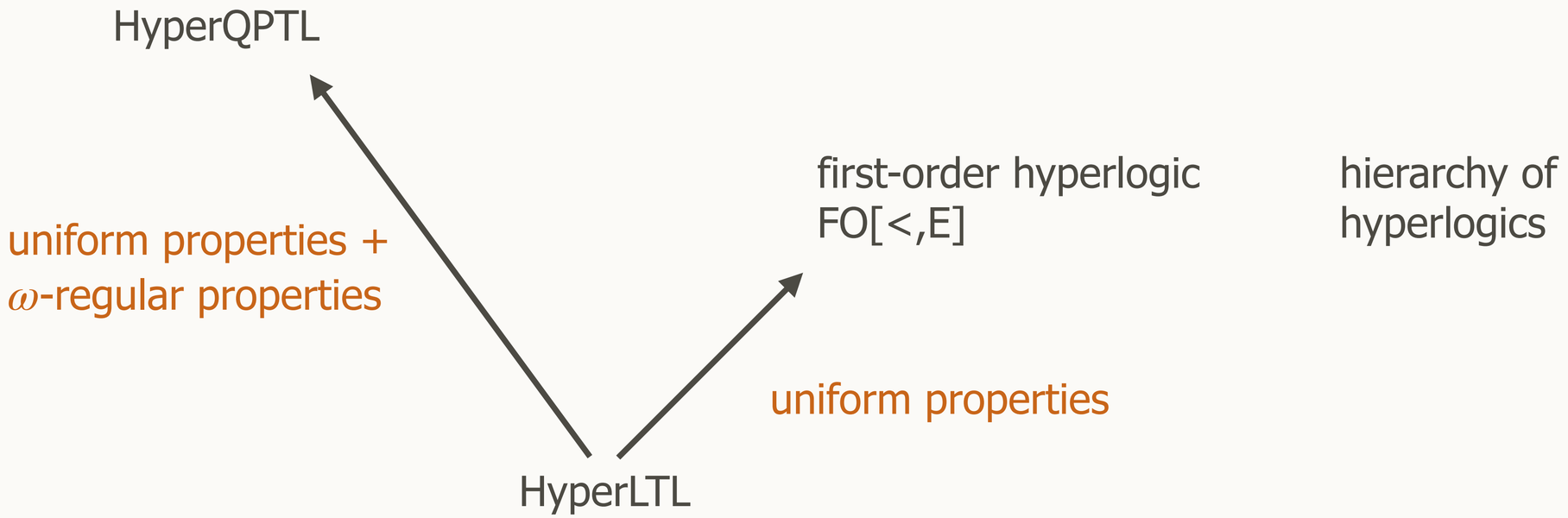
$$\forall x. \forall y.\ x < y \wedge P_{halt}(x) \rightarrow P_{halt}(y)$$

The Hierarchy of Hyperlogics



Outline

model checking
satisfiability
synthesis



hierarchy of
hyperlogics

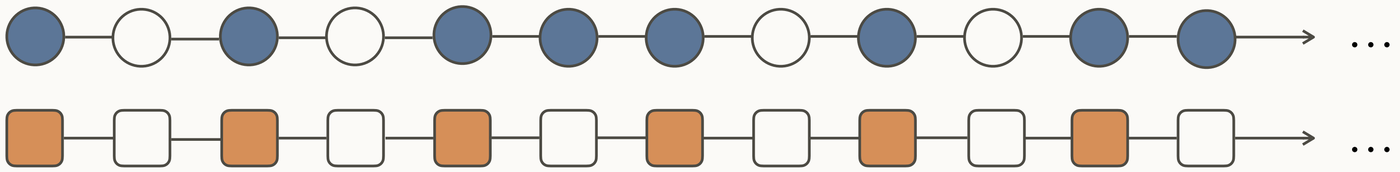
Omega-regularity

LTL cannot express ω-regular properties

QPTL = LTL + propositional quantification

Counting properties: “On all even positions, a holds.”

$$\exists q.\ q \wedge \square(q \leftrightarrow \bigcirc \neg q) \wedge \square(q \rightarrow a)$$



HyperQPTL => QPTL instead of LTL?

$$\forall \pi \forall \pi'. \square(on_\pi \leftrightarrow on'_\pi)$$

$$\exists q.\ \square\ \ldots$$

ω-regular properties over n-tuples

We can do better!

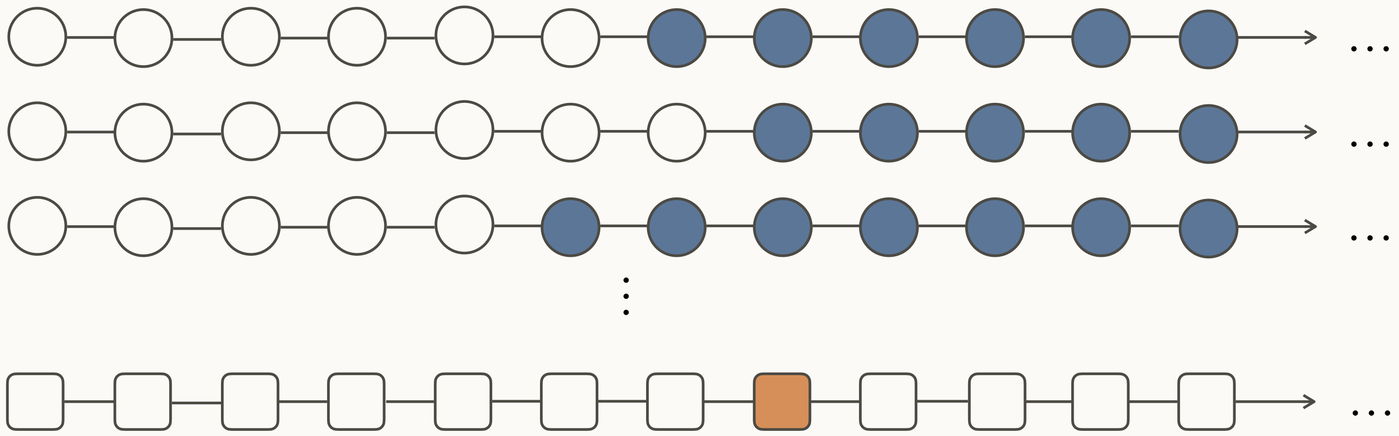
HyperQPTL

HyperQPTL = HyperLTL + Propositional Quantification

$$\varphi \;::=\; \exists \pi.\, \varphi \mid \forall \pi.\, \varphi \mid \psi \mid \exists q.\, \varphi \mid \forall q.\, \varphi$$
$$\psi \;::=\; a_\pi \mid \bigcirc \psi \mid \psi \,\mathcal{U}\, \psi \mid \neg \psi \mid \psi \vee \psi \mid q$$

Rabe
Ph.D. Thesis, 2016

Uniform Termination: "There is a global bound up to which the system terminates on all traces."

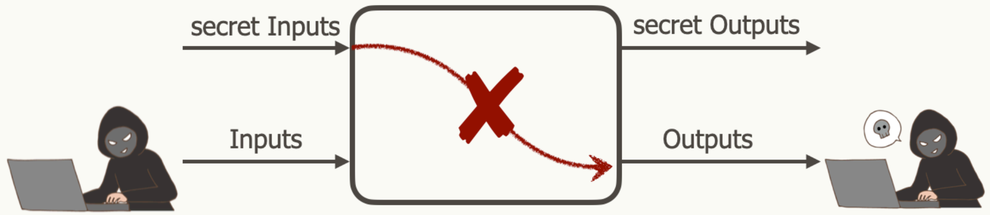


$$\exists q. \forall \pi.\; once(q) \wedge \Diamond(halt_\pi \wedge \Diamond\, q)$$

HyperQPTL Expressiveness

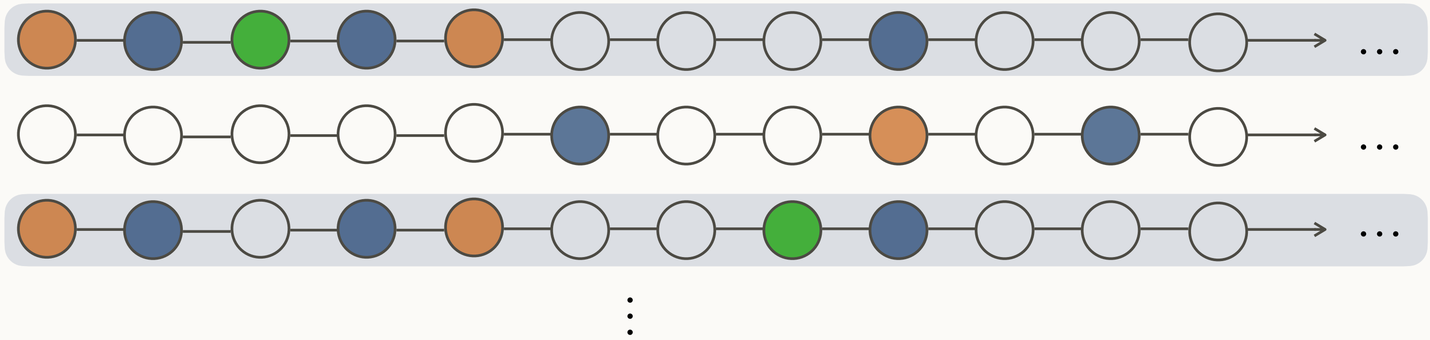
ω-regular properties over n-tuples

Uniform hyperproperties: Uniform termination, promptness



Epistemic properties: HyperQPTL subsumes LTL$_{\mathcal{K}}$

"An agent that can only observe low security variables can never infer the value of the secret"



$$\square \neg((\mathcal{K}_{\{low\}}\ sec) \leftrightarrow sec)$$

HyperQPTL Model Checking

HyperQPTL Model Checking is decidable.

Rabe
Ph.D. Thesis, 2016

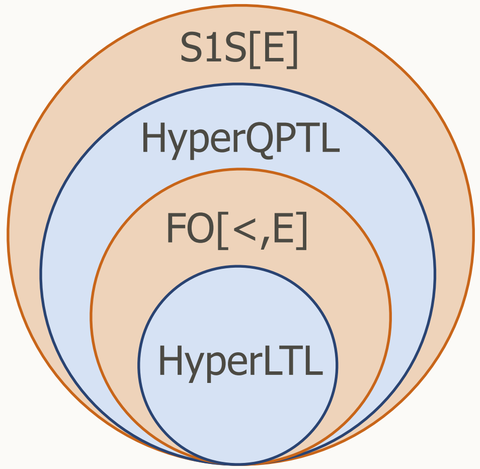
Idea: propositional sequences can be treated as normal traces by modifying the system

Space complexity: $2^{2^{\cdot^{\cdot^{\cdot^{2^{\varphi}}}}}}$ number of quantifier alternations $\exists \Rightarrow \forall$ / $\forall \Rightarrow \exists$

Uniform termination: 1 quantifier alternation

$$\exists q. \forall \pi.\ once(q) \wedge \Diamond(halt_\pi \wedge \Diamond q)$$

S1S[E]: model checking undecidable

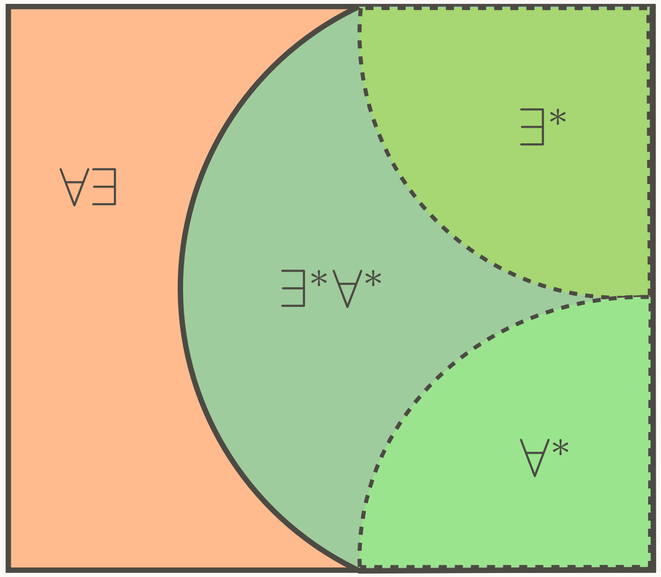


HyperQPTL Satisfiability

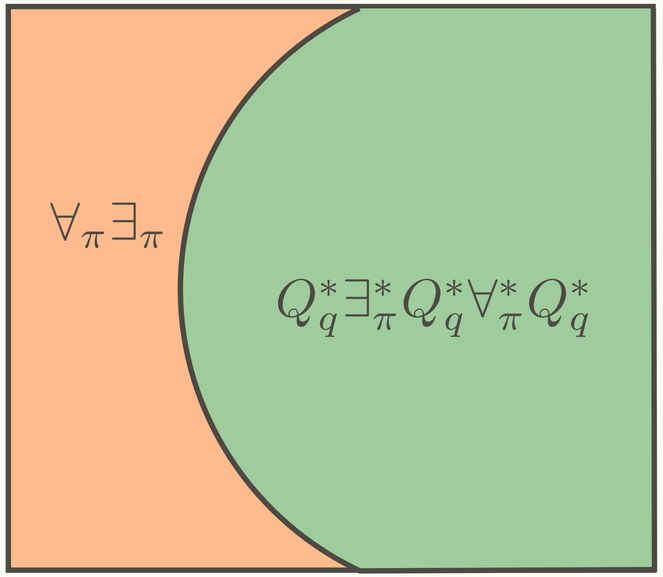
Finkbeiner, Hahn
CONCUR, 2016

$\forall\exists$ enough to encode
Post's correspondence problem

HyperLTL



HyperQPTL



Propositional quantifiers do not change decidability of the fragments

Uniform termination in decidable fragment

HyperQPTL Synthesis

No $\forall_\pi$: decidable

Propositional quantifiers **do** change decidability of the fragments

Uniform termination in decidable fragment

One $\forall_\pi$: $\exists^*_{q/\pi}\forall^*_q\forall_\pi Q^*_q$ decidable

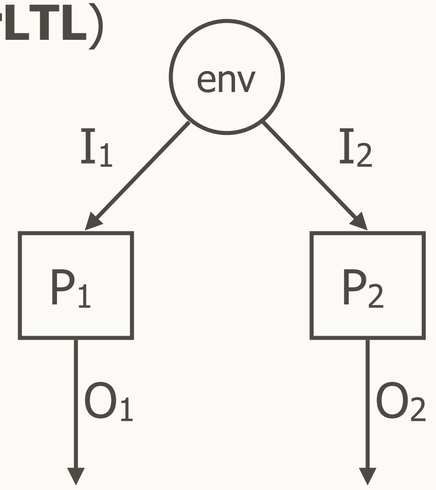
leading to undecidablity:

- $\forall_\pi\exists_\pi$ inherited from HyperLTL
- $\forall^*_q\exists^*_q\forall_\pi$ can encode PCP (even though **decidable in HyperLTL**)

Two $\forall_\pi$: linear fragment decidable

leading to undecidablity:

- information forks in distributed architectures (non-linear)

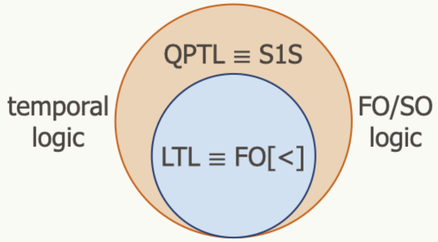


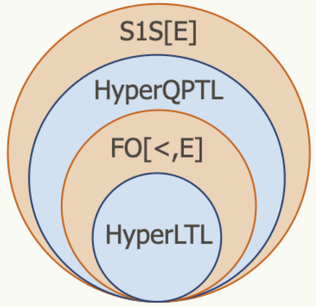
$I_1 \subset I_2$

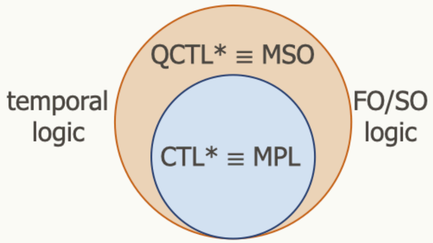
Finkbeiner, Hahn, Lukert, Stenger, Tentrup

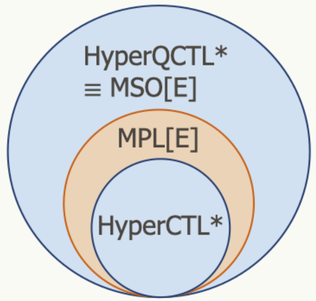
Acta Informatica, 2019

Conclusion

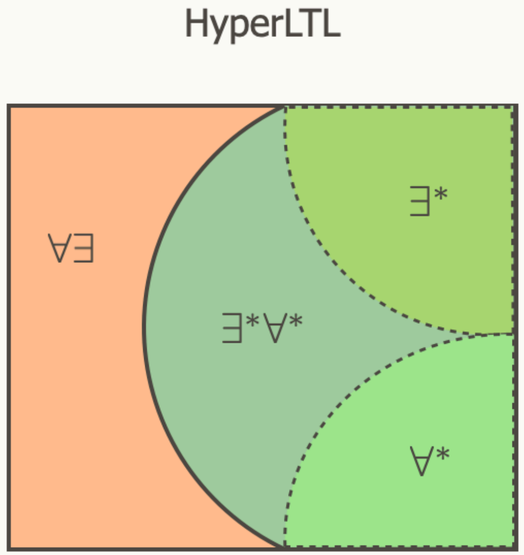


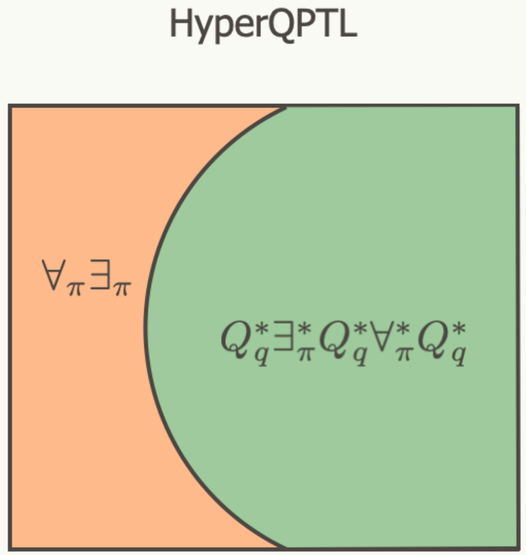






First/second-order hyperlogics are more expressive than their temporal counterparts





HyperQPTL can express ω-regular, uniform, and epistemic properties

Decidable (MC/SAT/SYNT) fragments are expressive

Other FO/SO hyperlogics? Model Checking, SAT, …?

More expressiveness?