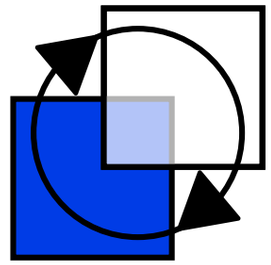
UNIVERSITÄT
DES
SAARLANDES



Reactive
Systems
Group

Causality and Hyperproperties

Norine Coenen

Shonan Meeting No. 139
Causal Reasoning in Systems

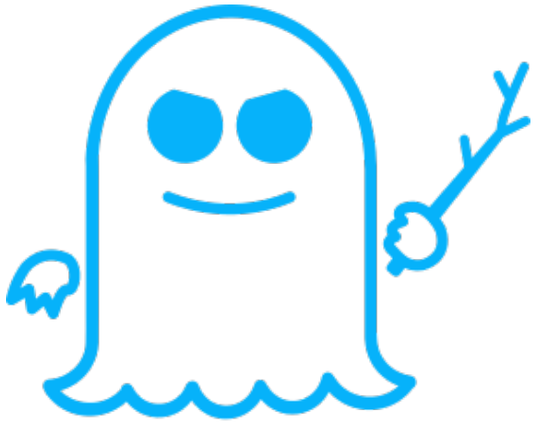
Meltdown and Spectre

Many processors (Intel, Arm, …) are

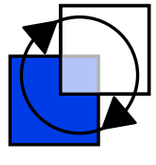
vulnerable although **proven correct**

Trace properties

Side channel attacks



Attacks **compare multiple executions**



Reactive Systems Group

Hyperproperties and Properties

Hyperproperty (Clarkson and Schneider)

Set of sets of traces $H \subseteq 2^{\Sigma^\omega}$

$T \vDash H \Leftrightarrow T \in H$

Compare multiple traces

Ex: Require at least two different traces:

$$\{T \subseteq \Sigma^\omega \mid \exists t, t' \in T.\ t \neq t'\}$$

Trace property

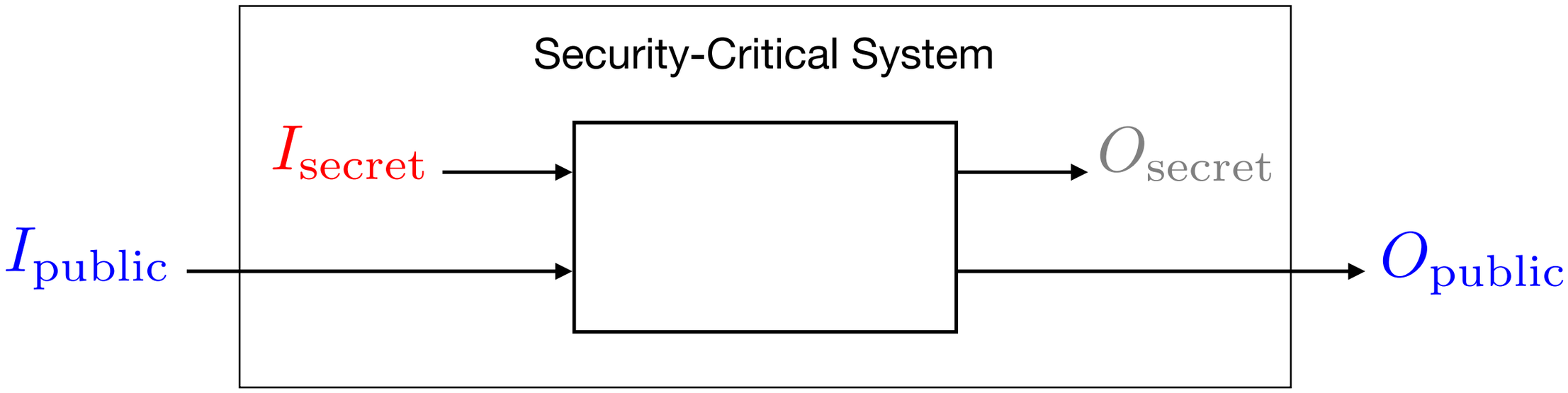
Set of traces $P \subseteq \Sigma^\omega$

$T \vDash P \Leftrightarrow T \subseteq P$

No trace comparison possible

Ex: Cannot require two different traces

Information-Flow Control



Public output should only depend on public input

Typical information-flow property: Noninterference

$$\{T \subseteq \Sigma^\omega \mid \forall t, t' \in T : t =_{I_{\text{public}}} t' \;\Rightarrow\; t =_{O_{\text{public}}} t'\}$$

Other Hyperproperties

Cleanliness (software doping)

Do traces with similar inputs also have similar outputs?

Symmetry in protocols

Are clients treated symmetrically?

Error-resistant codes

Do codes for distinct inputs have at least Hamming distance *d*?

Promptness

Is there a common bound on the number of steps until a requirement is satisfied?

Causality

Counterfactual dependence

Hume: “We may define a cause to be an object followed by another **...**

where, <u>if the first object had not been, the second never had existed</u>.”

Compare **actual world** with a **different possible world**

Cause and effect both occur

Cause and effect both do **not** occur

Causality

Contingencies

Halpern and Pearl:

Restrict possible alternate worlds to those **satisfying the contingencies**

Transition systems

Leitner-Fischer and Leue:

Restrict possible alternate worlds to the **traces of a transition system**

Causality Definition

Let ψ range over Z and $\mathcal{A} \setminus Z = W$.
ψ causes φ iff

AC1: $\exists t.\ t \vDash \psi \wedge t \vDash \varphi$

AC2(1): $\exists t'.\ t' \nvDash \psi \wedge t' \nvDash \varphi \wedge$
$(val_Z(t) \neq val_Z(t') \vee$
$val_W(t) \neq val_W(t'))$

AC2(2): $\forall t''.\ t'' \vDash \psi \wedge val_Z(t) = val_Z(t'')$
$\wedge\, val_{W'}(t) \neq val_{W'}(t'') \rightarrow t'' \vDash \varphi$

AC3: Minimality of ψ

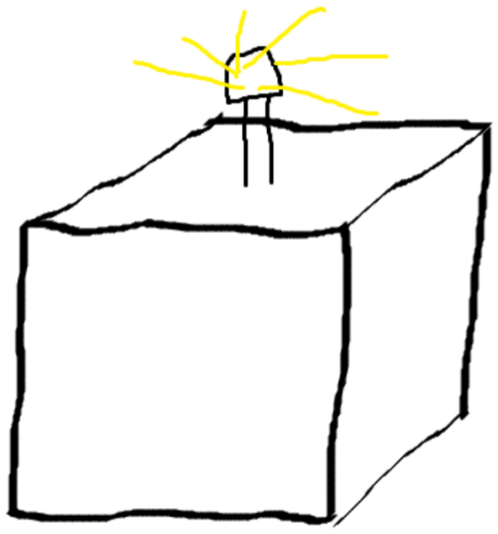
Reactive Systems Group

Temporal Logics for Hyperproperties

Noninterference

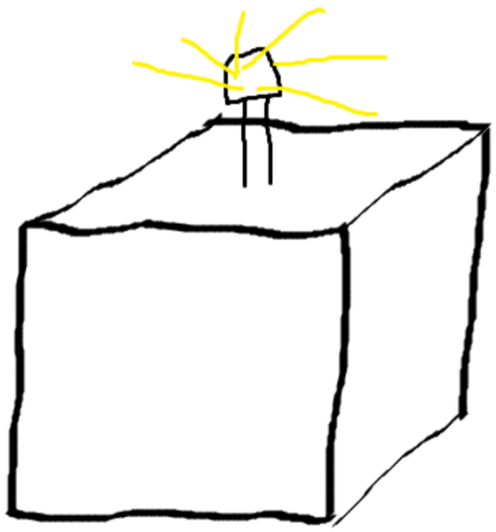
$$\{T \subseteq \Sigma^\omega \mid \forall t, t' \in T : t =_{I_{\text{public}}} t' \;\Rightarrow\; t =_{O_{\text{public}}} t'\}$$

Is there an **appropriate logic** for the expression of hyperproperties?



“All executions have the light on at the same time.”

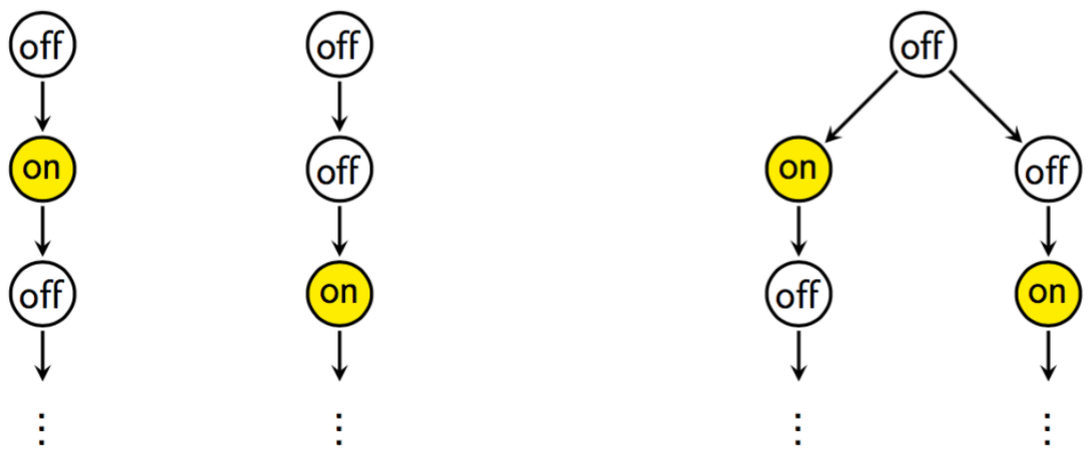
LTL



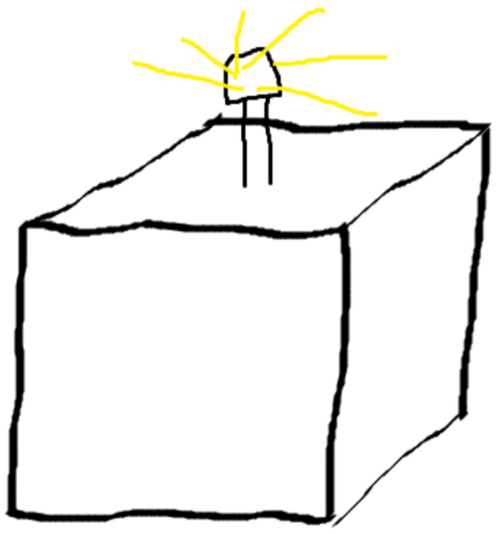
“All executions have the light on at the same time.”

LTL: Specifies computations

Syntax: $\varphi ::= a \mid \bigcirc\psi \mid \Box\psi \mid \Diamond\psi \mid \psi\,\mathcal{U}\,\psi \mid \ldots$



CTL*

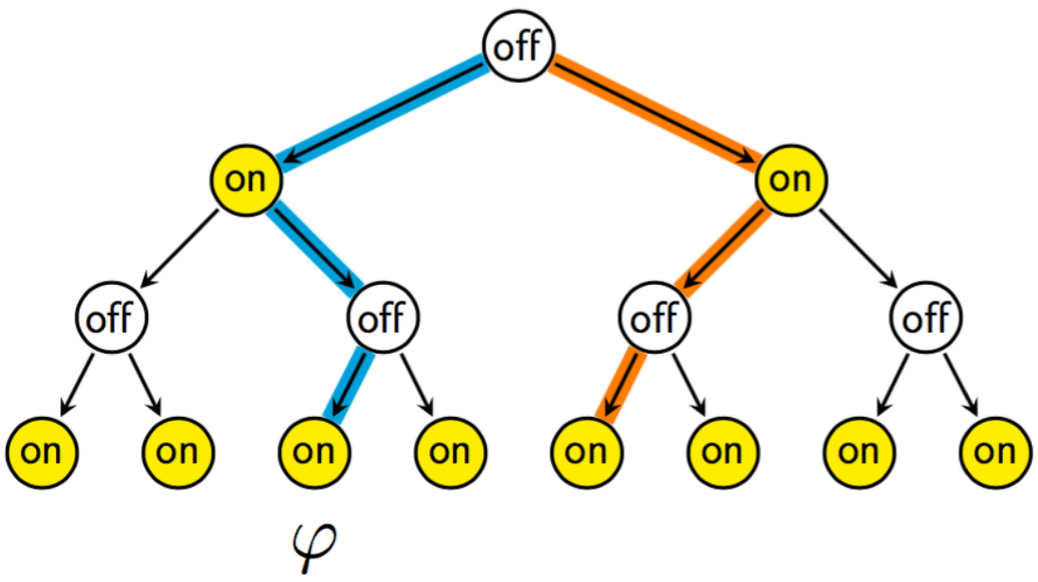


“All executions have the light on at the same time.”

AA φ **?**

CTL*: Specifies computation trees

Syntax: $\varphi ::= a \mid \mathsf{A}\varphi \mid \mathsf{E}\varphi \mid \bigcirc\varphi \mid \Box\varphi \mid \varphi\,\mathcal{U}\,\varphi \mid \ldots$



HyperLTL

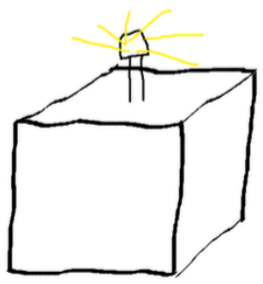
Add **trace quantifiers**: $\forall \pi . \varphi \quad \exists \pi . \varphi$

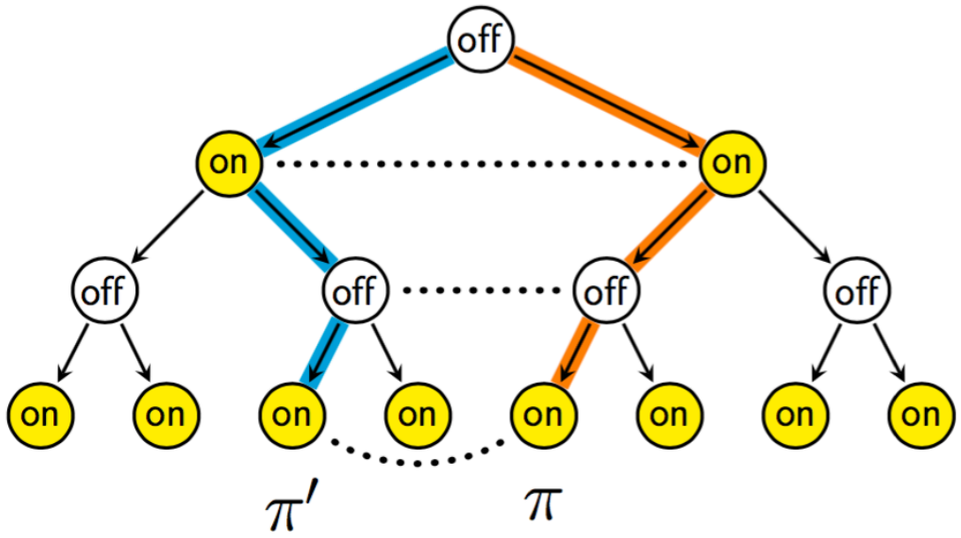
Syntax: $\varphi ::= \forall \pi . \varphi \mid \exists \pi . \varphi \mid \psi$

$\psi ::= a_\pi \mid \bigcirc \psi \mid \square \psi \mid \Diamond \psi \mid \psi \, \mathcal{U} \, \psi \mid \ldots$

“All executions have the light on at the same time.”

$\forall \pi . \forall \pi' . \; \square (\text{on}_\pi \leftrightarrow \text{on}_{\pi'})$





HyperLTL

Require at least two different traces in a system:

$$\{T \subseteq \Sigma^\omega \mid \exists t, t' \in T.\ t \neq t'\}$$

In HyperLTL: $\exists \pi . \exists \pi' .\ \pi \neq \pi'$

$$\pi = \pi' := \square\Big(\bigwedge_{a \in AP} a_\pi \leftrightarrow a_{\pi'}\Big)$$

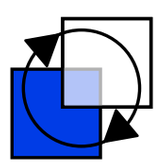
Semantics:

trace assignment $\Pi : Vars \to T$

$$\Pi \models_T a_\pi \quad \text{iff} \quad a \in \Pi(\pi)(0)$$

$$\Pi \models_T \square\varphi \quad \text{iff} \quad \forall i \geq 0 :\ \Pi[i, \infty] \models_T \varphi$$

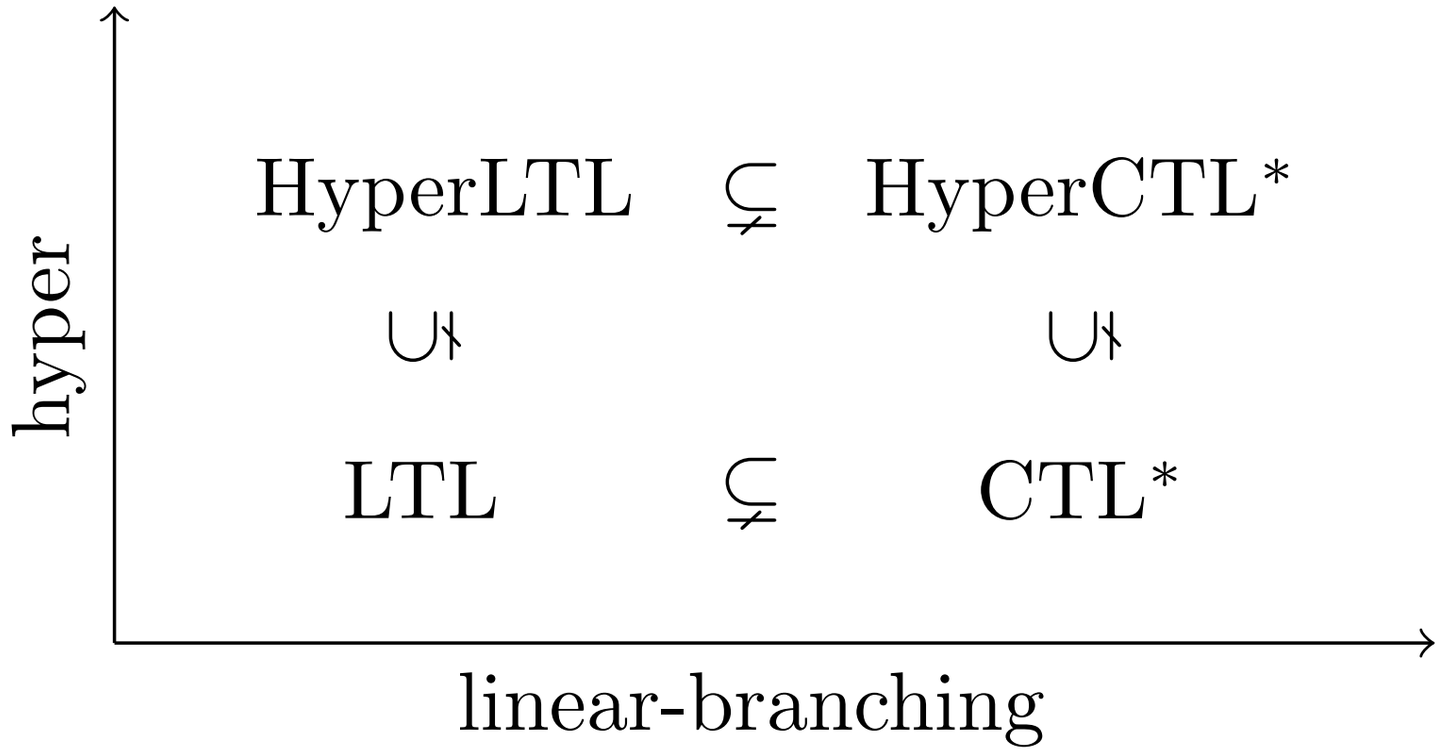
$$\Pi \models_T \forall \pi .\ \varphi \quad \text{iff} \quad \forall t \in T :\ \Pi[\pi \mapsto t] \models_T \varphi$$



HyperCTL*

Add **path variables** to path quantifiers:

Syntax: $\varphi ::= a_\pi \mid \forall \pi.\varphi \mid \exists \pi.\varphi \mid \bigcirc \varphi \mid \square \varphi \mid \varphi \mathcal{U} \varphi \mid \ldots$



Causality in HyperLTL

Let ψ range over Z and $\mathcal{A} \setminus Z = W$.
ψ causes φ iff

AC1: $\exists t.\ t \vDash \psi \wedge t \vDash \varphi$

AC2(1): $\exists t'.\ t' \nvDash \psi \wedge t' \nvDash \varphi \wedge$
$(val_Z(t) \neq val_Z(t') \vee$
$val_W(t) \neq val_W(t'))$

AC2(2): $\forall t''.\ t'' \vDash \psi \wedge val_Z(t) = val_Z(t'')$
$\wedge\ val_{W'}(t) \neq val_{W'}(t'') \rightarrow t'' \vDash \varphi$

$\exists \pi.\exists \pi'.\forall \pi''.$
$\psi_\pi \wedge \varphi_\pi \wedge$
$\neg\psi_{\pi'} \wedge \neg\varphi_{\pi'} \wedge \pi \neq \pi' \wedge$
$\psi_{\pi''} \wedge \pi =_Z \pi'' \rightarrow \varphi_{\pi''}$

$\pi =_Z \pi' := \square(\bigwedge_{z \in Z} z_\pi \leftrightarrow z_{\pi'})$

Results and Tools

Satisfiability

- Decidability results for HyperLTL, HyperCTL*, HyperQPTL
- EAHyper
- MGHyper

Model Checking

- Automata-based algorithm for HyperCTL*
- MCHyper: Alternation-free fragment of HyperLTL

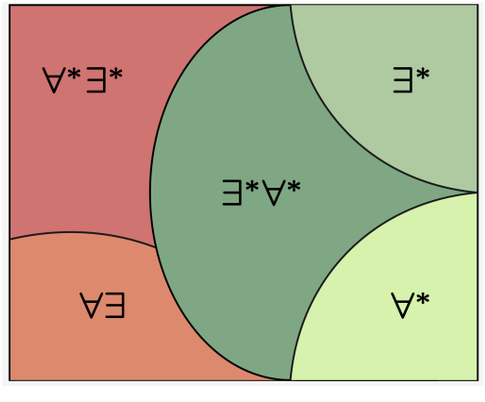
  Recently extended to one quantifier alternation
- MCQHyper: Model checking of quantitative hyperproperties → Responsibility

Synthesis

- Decidability results
- BoSyHyper

Runtime Monitoring

- RVHyper



How can we use hyperproperties for causality checking?

Further information: https://www.react.uni-saarland.de