

# Logical Safety Analysis of Concurrent Cyber-physical Systems

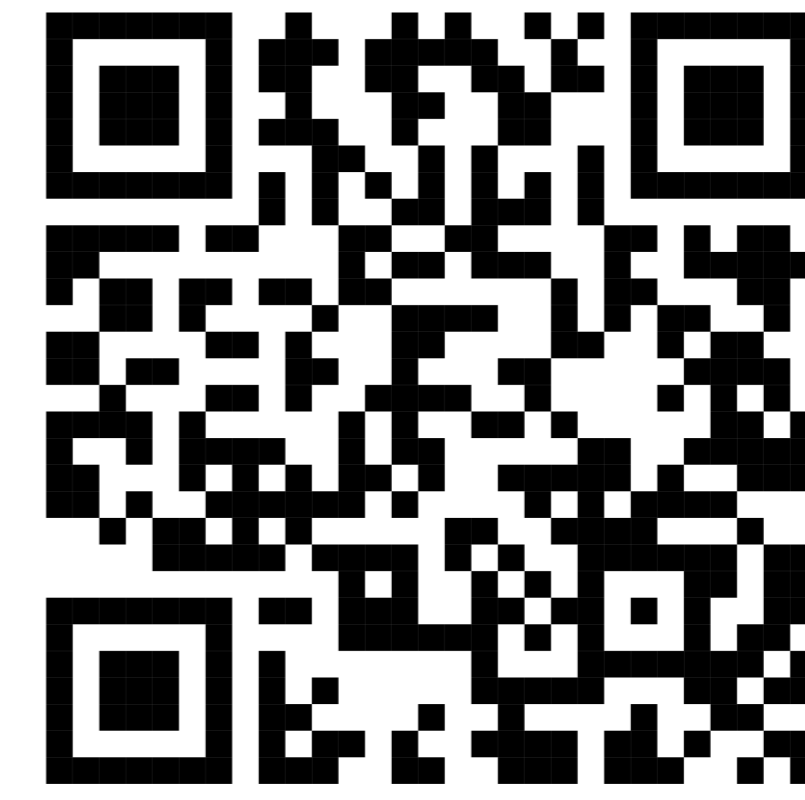


**Marvin Brieger**

marvin.brieger@sosy.ifi.lmu.de

**Supervisors:** André Platzer (KIT) & Dirk Beyer (LMU)

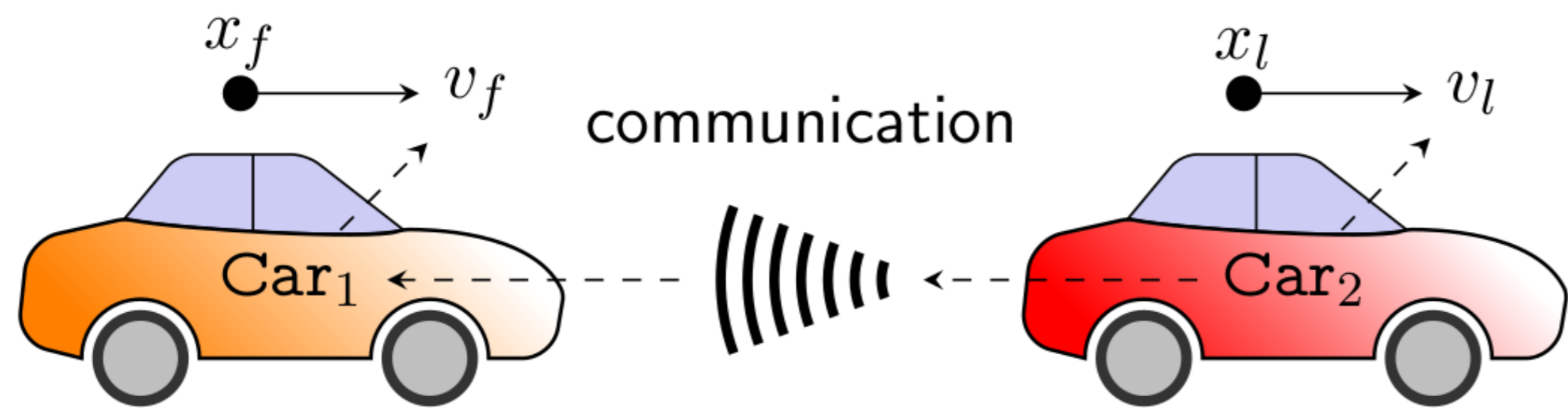
**Collaborators:** Stefan Mitsch (CMU)



CONVEY

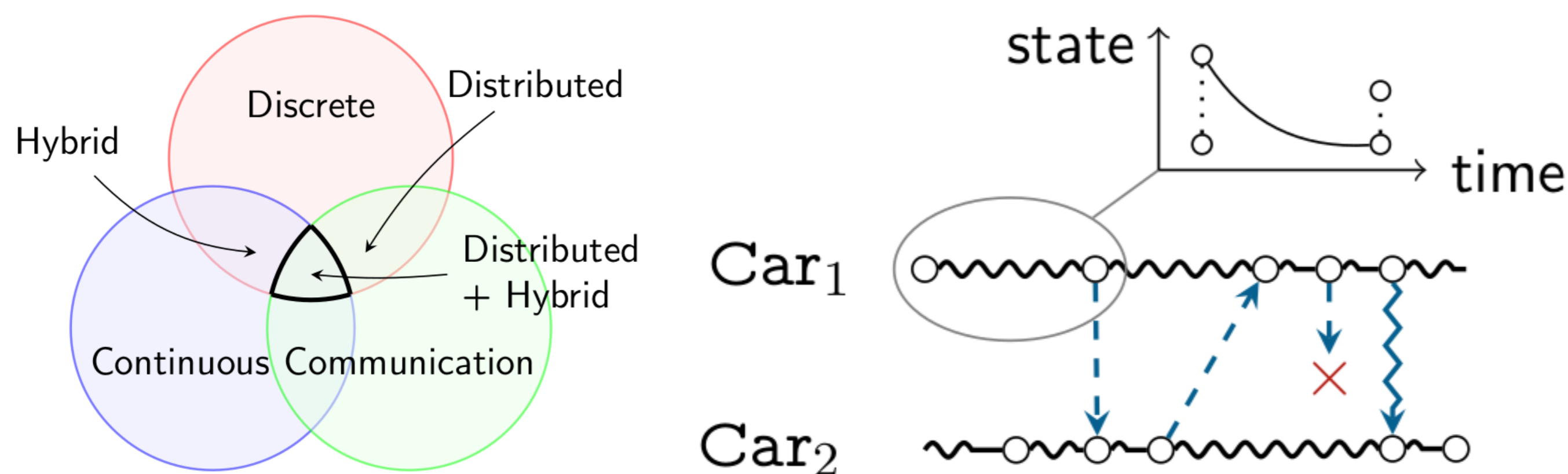


## Distributed Cyber-physical Systems



**Distributed CPS = Discrete + Continuous + Parallel**

**But more complex than: Parallelism + Hybrid!**



## Dynamic Logic of Communicating Hybrid Programs

$$d\mathcal{L}_{\text{CHP}} = d\mathcal{L} + \text{CSP} + \text{AC-reasoning} + \text{symbols}$$

### Definition 1: Communicating Hybrid Programs

$$a(|Y, \bar{z}|) \mid x := \theta \mid \{x' = \theta\} \mid ?\chi \mid \alpha; \beta \mid \alpha \cup \beta \mid \alpha^* \mid \text{ch}(h)! \theta \mid \text{ch}(h)?x \mid \alpha \parallel \beta$$

↑  
at most binds channels  $Y$  and variables  $\bar{z}$

hybrid programs      communication and parallelism

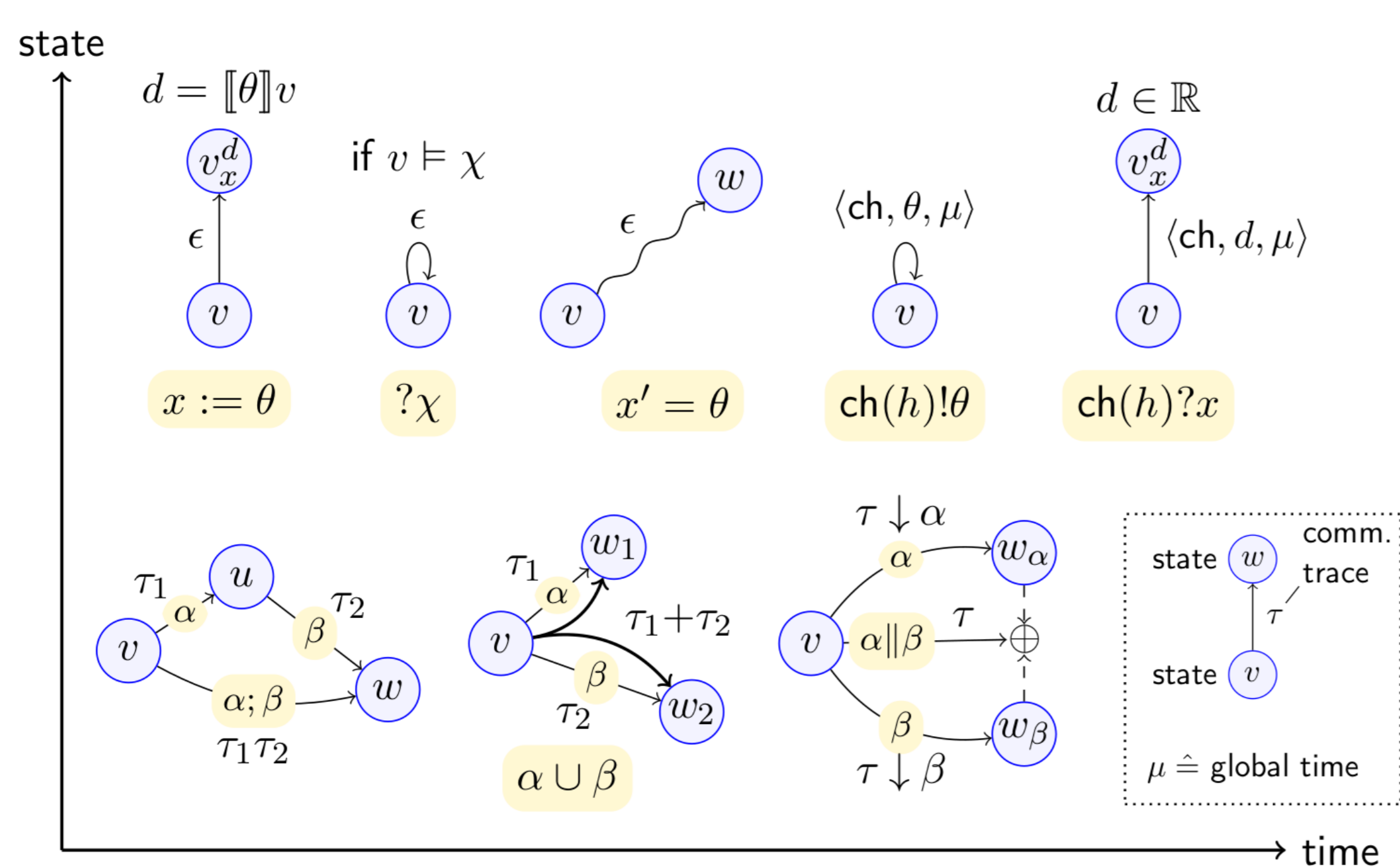
### Definition 2: Dynamic assumption-commitment logic

$$p(Y, \bar{e}) \mid e_1 \sim e_2 \mid \neg \varphi \mid \varphi \wedge \psi \mid \forall x \varphi \mid [\alpha] \psi \mid [\alpha]_{\{A, C\}} \psi$$

↑  
at most depends on channels  $Y$  and variables  $\bar{z}$

first-order dynamic logic      assumption-commitment modality

## Semantics of Communicating Hybrid Programs



## References

- [1] M. Brieger et al. "Dynamic Logic of Communicating Hybrid Programs". In: *arXiv/CoRR* (2023).
- [2] M. Brieger et al. "Uniform Substitution for Dynamic Logic with Communicating Hybrid Programs". In: *CADE (preprint in arXiv/CoRR)*. 2023.

## Uniform Substitution

The proof rule **US** is the **single point of truth** for axiom instantiation!

### Theorem 1: Uniform substitution is sound

A substitution  $\sigma$  maps symbols to terms, formulas, or programs.

$$\frac{\phi}{\sigma\phi} \text{US} \quad \text{if for each operation } \otimes(e) \text{ and program constant } a(|Y, \bar{z}|) \text{ in } \phi:$$

- $\text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset$  and  $\text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$
- $\text{BV}(\sigma a) \subseteq \text{BV}(a(|Y, \bar{z}|))$  and  $\text{CN}(\sigma a) = \text{CN}(a(|Y, \bar{z}|))$

Uniform substitution is **sound** if (parameters = variables + channels)

- it **never** puts a **free** parameter **into** a **context** where it is bound
- it **never** binds parameters **beyond** the **original** sets

**If you bind a free parameter, you go to logic jail!**

## Axiomatization by Example

$$\begin{aligned} [:=] \quad [x := g^{\mathbb{R}}]p(x) &\leftrightarrow p(g^{\mathbb{R}}) & [;]_{\text{AC}} \quad [a; b]_{\{R, Q\}}P &\leftrightarrow [a]_{\{R, Q\}}[b]_{\{R, Q\}}P \\ [?] \quad [?q_{\mathbb{R}}]p &\leftrightarrow (q_{\mathbb{R}} \rightarrow p) & [ ]_{\text{T}, \text{T}} \quad [a]P &\leftrightarrow [a]_{\{T, T\}}P \\ [\mu] \quad [\{\bar{x}' = g^{\mathbb{R}}(\bar{x}, \mu)\}]p(\bar{x}, \mu) &\leftrightarrow [\{\mu' = 1, \bar{x}' = g^{\mathbb{R}}(\bar{x}, \mu)\}]p(\bar{x}, \mu) \\ [\text{ch}!] \quad [\text{ch}(h)!g^{\mathbb{R}}]p(\text{ch}, h) &\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, g^{\mathbb{R}}, \mu \rangle \rightarrow p(\text{ch}, h_0)) \\ [e]_{\text{AC}} \quad [a(|\emptyset, V_{\mathbb{R}}|)]_{\{R, Q\}}P &\leftrightarrow Q \wedge (R \rightarrow [a(|\emptyset, V_{\mathbb{R}}|)]P) \end{aligned}$$

$$P \equiv p(Y, \bar{z}) \mid R \equiv r(Y, \bar{h}) \mid Q \equiv q(Y, \bar{h}) \mid \sigma g^{\mathbb{R}} \in \mathbb{Q}[V_{\mathbb{R}}] \mid \sigma q_{\mathbb{R}} \in \text{FOL}_{\mathbb{R}}$$

## Non-schematic Parallel Injection Axiom $[| |]_{\text{AC}}$

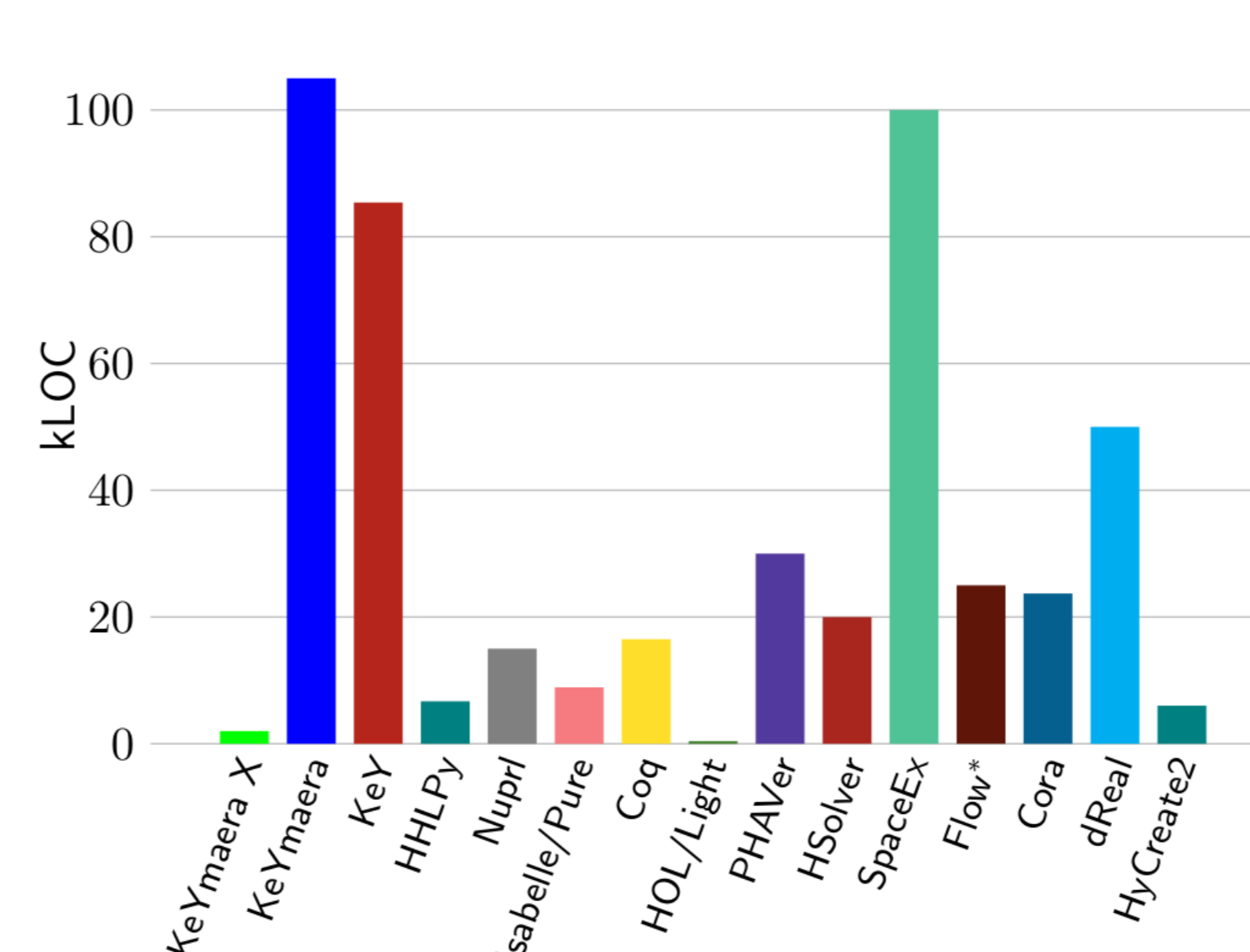
$$\frac{[\alpha]\varphi \quad [\beta]\psi}{[\alpha \parallel \beta](\varphi \wedge \psi)} (**)$$

Everyone's favorite parallel proof rule      Requires algorithmic implementation :(

Instead, the parallel injection axiom drops a parallel subprogram if it **does not interfere** with the surrounding contract :

$$[a(|Y_a, \bar{z}_a|)]p(Y, \bar{z}) \rightarrow [a(|Y_a, \bar{z}_a|) \parallel_{\text{wf}} b(|Y_b \cap (Y^c \cup Y_a), \bar{z}^c|)]p(Y, \bar{z})$$

## Schematic vs. Flat Axioms



Schematic proof calculus  
↓  
Algorithmic implementation  
↓  
Large soundness-critical prover kernel

vs.

**KeYmaera X**