

# Uniform Substitution for Dynamic Logic with Communicating Hybrid Programs

Marvin Brieger<sup>1</sup>, Stefan Mitsch<sup>2</sup>, and André Platzer<sup>3,4</sup>

<sup>1</sup> LMU Munich, Germany

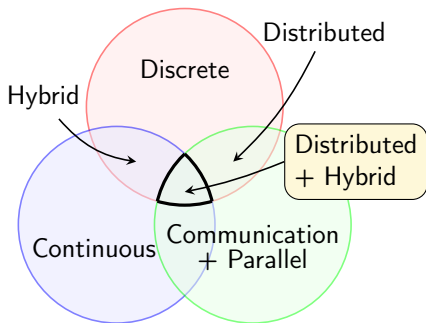
<sup>2</sup> DePaul University, Chicago, USA

<sup>4</sup> Karlsruhe Institute of Technology, Germany

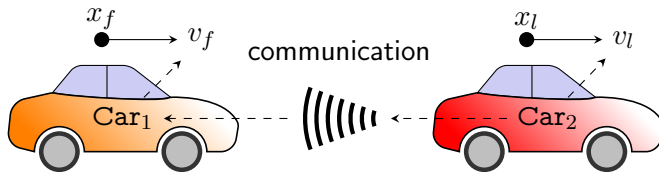
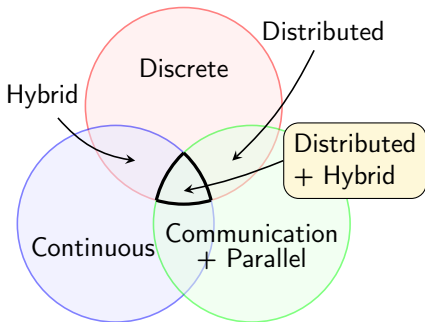
<sup>3</sup> Carnegie Mellon University, Pittsburgh, USA

6th April 2024

# Challenge: Distributed Cyber-physical Systems

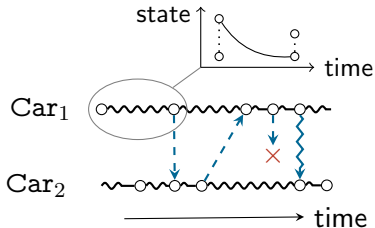
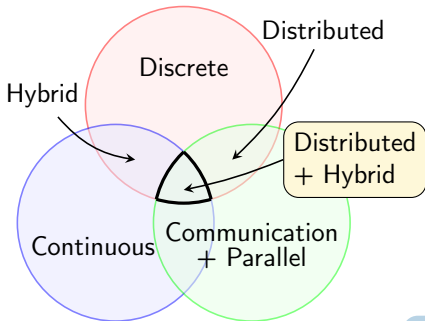


# Challenge: Distributed Cyber-physical Systems



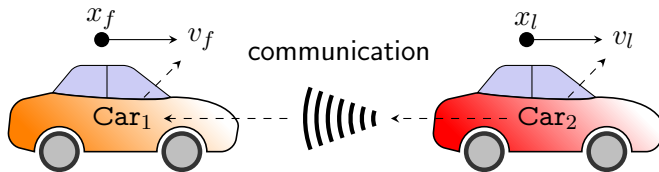
Many real-world systems are distributed hybrid systems

# Challenge: Distributed Cyber-physical Systems



Challenge: Capture the truly simultaneous continuous dynamics of physics

Requires: Reflection in semantics and reasoning



Many real-world systems are distributed hybrid systems

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side conditions (\*\*\*) are extensive and subtle

$$\mathbf{FV}(\phi) \cap \mathbf{BV}(\beta) \subseteq \emptyset$$

$$\mathbf{CN}(\phi) \cap \mathbf{CN}(\beta) \subseteq \emptyset$$

$$\mathbf{FV}(\psi) \cap \mathbf{BV}(\alpha) \subseteq \emptyset$$

$$\mathbf{CN}(\psi) \cap \mathbf{CN}(\alpha) \subseteq \emptyset$$

Free variables  $\mathbf{FV}(\cdot)$ , bound variables  $\mathbf{BV}(\cdot)$ , read or written channels  $\mathbf{CN}(\cdot)$ , and globally synchronized variables  $V_G$

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side conditions (\*\*\*) are extensive and subtle

$$\text{FV}(\phi) \cap \text{BV}(\beta) \subseteq \emptyset$$

$$\text{CN}(\phi) \cap \text{CN}(\beta) \subseteq \emptyset$$

$$\text{FV}(\psi) \cap \text{BV}(\alpha) \subseteq \emptyset$$

$$\text{CN}(\psi) \cap \text{CN}(\alpha) \subseteq \emptyset$$

Free variables  $\text{FV}(\cdot)$ , bound variables  $\text{BV}(\cdot)$ , read or written channels  $\text{CN}(\cdot)$ , and globally synchronized variables  $V_G$

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side conditions (\*\*\*) are extensive and subtle

$$\mathbf{FV}(\phi) \cap \mathbf{BV}(\beta) \subseteq \emptyset$$

$$\mathbf{CN}(\phi) \cap \mathbf{CN}(\beta) \subseteq \emptyset$$

$$\mathbf{FV}(\psi) \cap \mathbf{BV}(\alpha) \subseteq \emptyset$$

$$\mathbf{CN}(\psi) \cap \mathbf{CN}(\alpha) \subseteq \emptyset$$

Free variables  $\mathbf{FV}(\cdot)$ , bound variables  $\mathbf{BV}(\cdot)$ , read or written channels  $\mathbf{CN}(\cdot)$ , and globally synchronized variables  $V_G$



# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side conditions (\*\*\*) are extensive and subtle

$$\mathbf{FV}(\phi) \cap \mathbf{BV}(\beta) \subseteq V_G$$

$$\mathbf{CN}(\phi) \cap \mathbf{CN}(\beta) \subseteq \mathbf{CN}(\alpha) \quad V_G = \text{globally synchronized behavior}$$

$$\mathbf{FV}(\psi) \cap \mathbf{BV}(\alpha) \subseteq V_G$$

$$\mathbf{CN}(\psi) \cap \mathbf{CN}(\alpha) \subseteq \mathbf{CN}(\beta)$$

Free variables  $\mathbf{FV}(\cdot)$ , bound variables  $\mathbf{BV}(\cdot)$ , read or written channels  $\mathbf{CN}(\cdot)$ , and globally synchronized variables  $V_G$

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side conditions (\*\*\*) are extensive and subtle

$$\mathbf{FV}(\phi) \cap \mathbf{BV}(\beta) \subseteq V_G$$

$$\mathbf{CN}(\phi) \cap \mathbf{CN}(\beta) \subseteq \mathbf{CN}(\alpha) \quad V_G = \text{globally synchronized behavior}$$

$$\mathbf{FV}(\psi) \cap \mathbf{BV}(\alpha) \subseteq V_G \quad + \text{incl. global time}$$

$$\mathbf{CN}(\psi) \cap \mathbf{CN}(\alpha) \subseteq \mathbf{CN}(\beta)$$

Free variables  $\mathbf{FV}(\cdot)$ , bound variables  $\mathbf{BV}(\cdot)$ , read or written channels  $\mathbf{CN}(\cdot)$ , and globally synchronized variables  $V_G$

# The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks

- In case of parallel (hybrid) systems, side

Schematic proof rules with side conditions are subtle and cause large soundness-critical prover kernels

$$FV(\phi) \cap BV(\beta) \subseteq V_G$$

$$CN(\phi) \cap CN(\beta) = \emptyset$$

Uniform substitution is to the rescue

isolated behavior

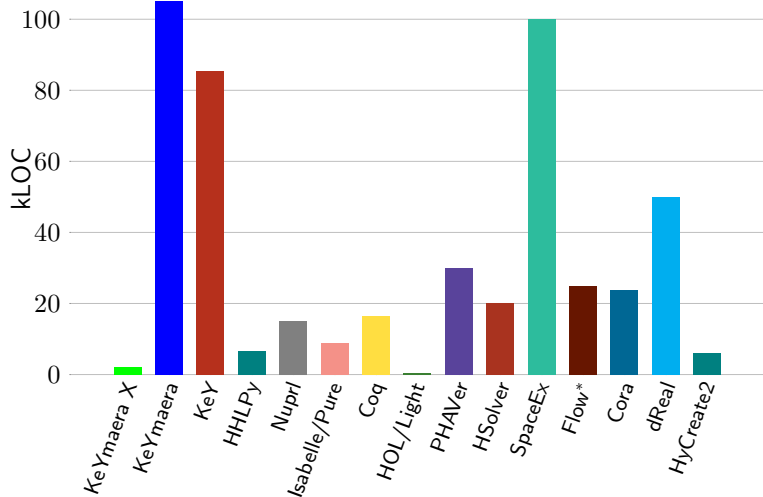
$$FV(\psi) \cap BV(\alpha) \subseteq V_G$$

isolation guarantee

$$CN(\psi) \cap CN(\alpha) \subseteq CN(\beta)$$

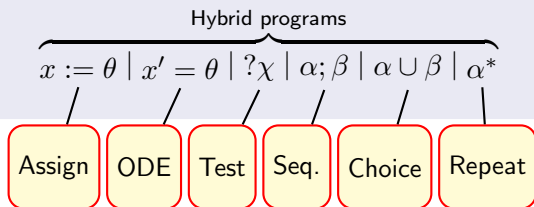
Free variables  $FV(\cdot)$ , bound variables  $BV(\cdot)$ , read or written channels  $CN(\cdot)$ , and globally synchronized variables  $V_G$

# Sound Microkernels for Theorem Provers

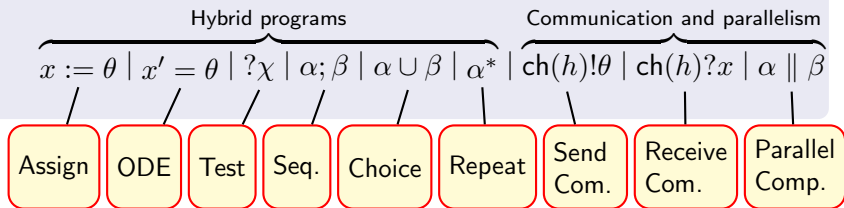


Disclaimer: self-reported estimates

## Definition: Communicating hybrid programs



## Definition: Communicating hybrid programs



## Definition: Communicating hybrid programs

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

Prog.  
Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send  
Com.

Receive  
Com.

Parallel  
Comp.

## Definition: Communicating hybrid programs

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

Prog.  
Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send  
Com.

Receive  
Com.

Parallel  
Comp.

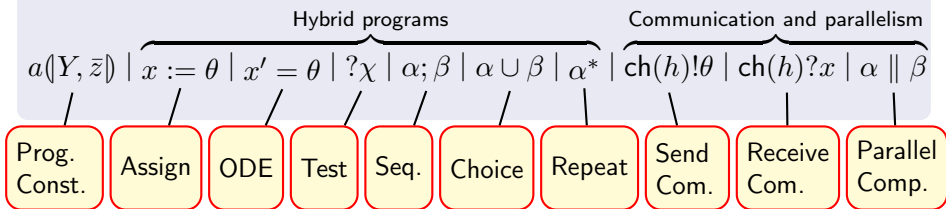
## Definition: Dynamic assumption-commitment logic

$\overbrace{e_1 \sim e_2 \mid \neg \varphi \mid \varphi \wedge \psi \mid \forall x \varphi}^{\text{First-order logic}}$

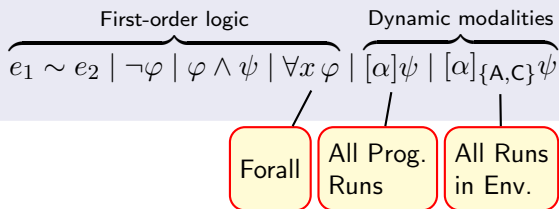
Forall



## Definition: Communicating hybrid programs



## Definition: Dynamic assumption-commitment logic



# Dynamic Logic of Communicating Hybrid Programs $d\mathcal{L}_{\text{CHP}}$

## Definition: Communicating hybrid programs

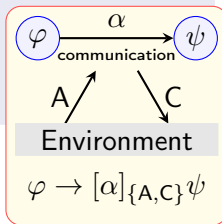
$a(Y, \bar{z}) \mid \overbrace{x := \theta \mid x' = \theta \mid ?\chi \mid \alpha; \beta \mid \alpha \cup \beta \mid \alpha^*}^{\text{Hybrid programs}} \mid \overbrace{\text{ch}(h)! \theta \mid \text{ch}(h)?x \mid \alpha \parallel \beta}^{\text{Communication and parallelism}}$

Prog. Const.   Assign   ODE   Test   Seq.   Choice   Repeat   Send Com.   Receive Com.   Parallel Comp.

## Definition: Dynamic assumption-commitment logic

$\overbrace{e_1 \sim e_2 \mid \neg \varphi \mid \varphi \wedge \psi \mid \forall x \varphi}^{\text{First-order logic}} \mid \overbrace{[\alpha]\psi \mid [\alpha]\{A,C\}\psi}^{\text{Dynamic modalities}}$

Forall   All Prog. Runs   All Runs in Env.



# Dynamic Logic of Communicating Hybrid Programs $d\mathcal{L}_{\text{CHP}}$

## Definition: Communicating hybrid programs

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

Prog.  
Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send  
Com.

Receive  
Com.

Parallel  
Comp.

## Definition: Dynamic assumption-commitment logic

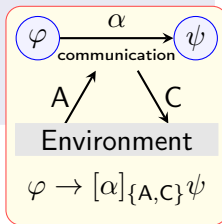
$p(Y, \bar{e}) \mid \overbrace{e_1 \sim e_2 \mid \neg \varphi \mid \varphi \wedge \psi \mid \forall x \varphi}^{\text{First-order logic}} \mid \overbrace{[\alpha]\psi \mid [\alpha]\{A,C\}\psi}^{\text{Dynamic modalities}}$

Pred.  
Symb.

Forall

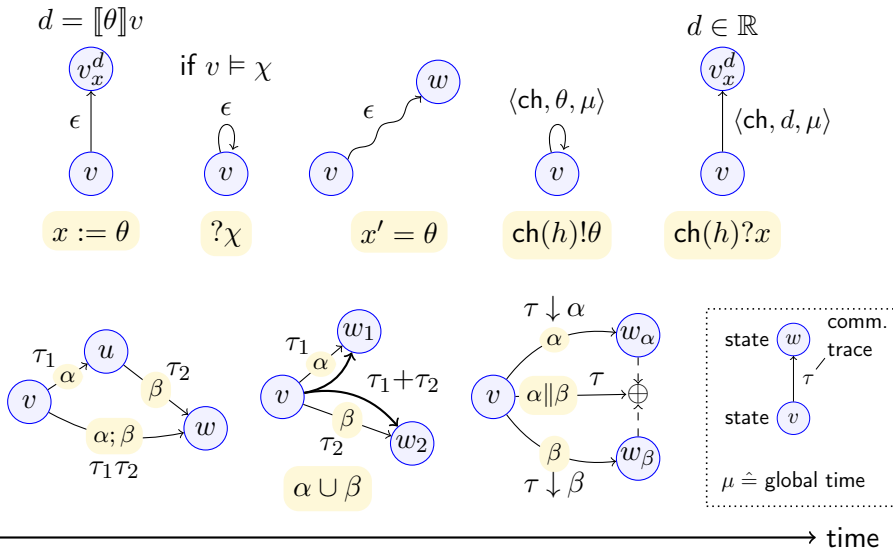
All Prog.  
Runs

All Runs  
in Env.



# Semantics of Communicating Hybrid Programs

state



# Semantics of Communicating Hybrid Programs

state

$$d = \llbracket \theta \rrbracket v$$

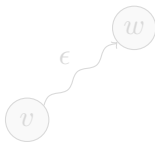


$x := \theta$

if  $v \models \chi$



$? \chi$



$x' = \theta$

$\langle \text{ch}, \theta, \mu \rangle$

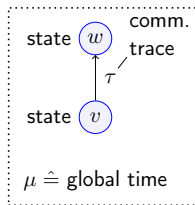
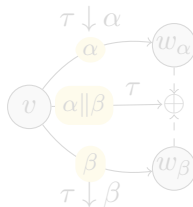
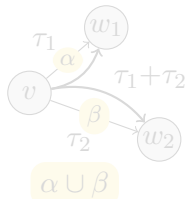
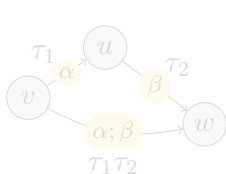


$\text{ch}(h)! \theta$

$d \in \mathbb{R}$



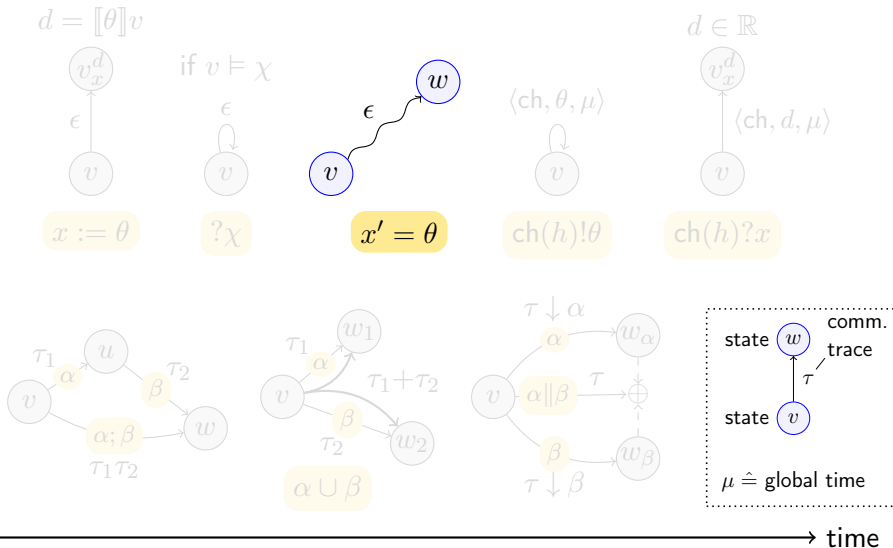
$\text{ch}(h)? x$



time

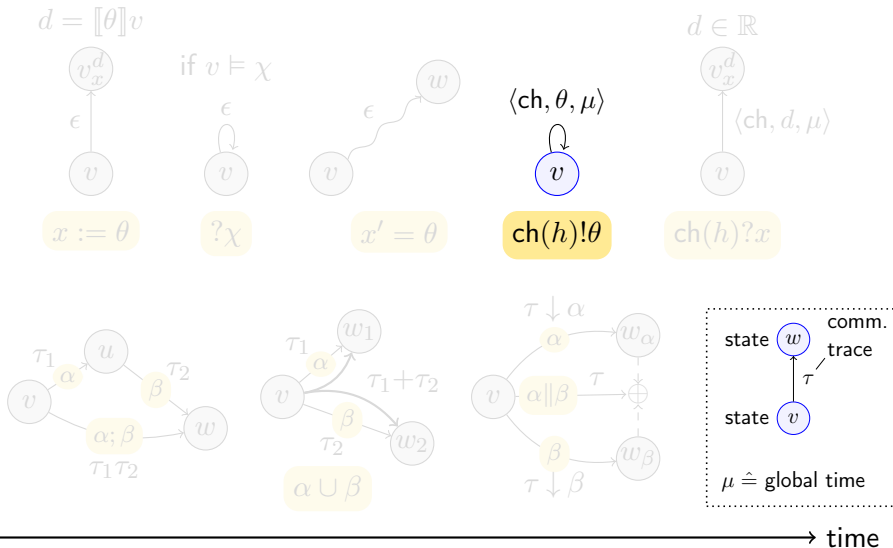
# Semantics of Communicating Hybrid Programs

state



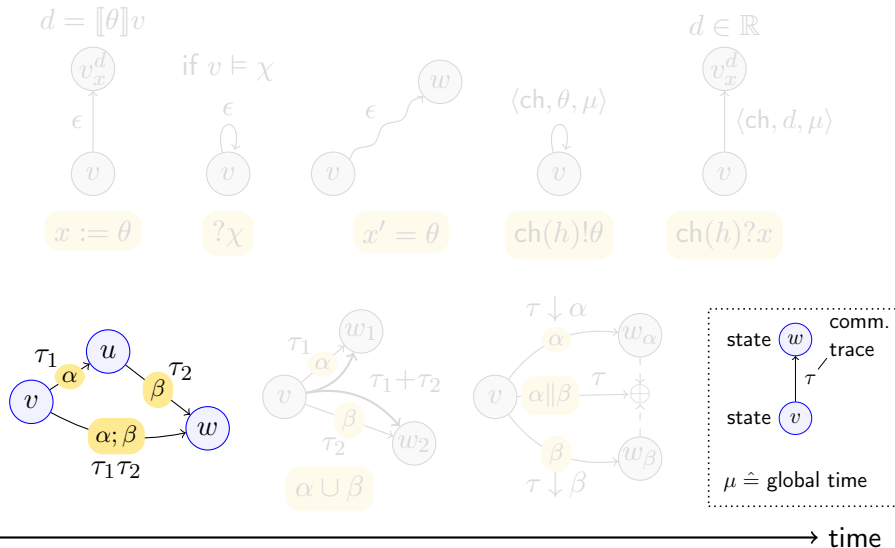
# Semantics of Communicating Hybrid Programs

state



# Semantics of Communicating Hybrid Programs

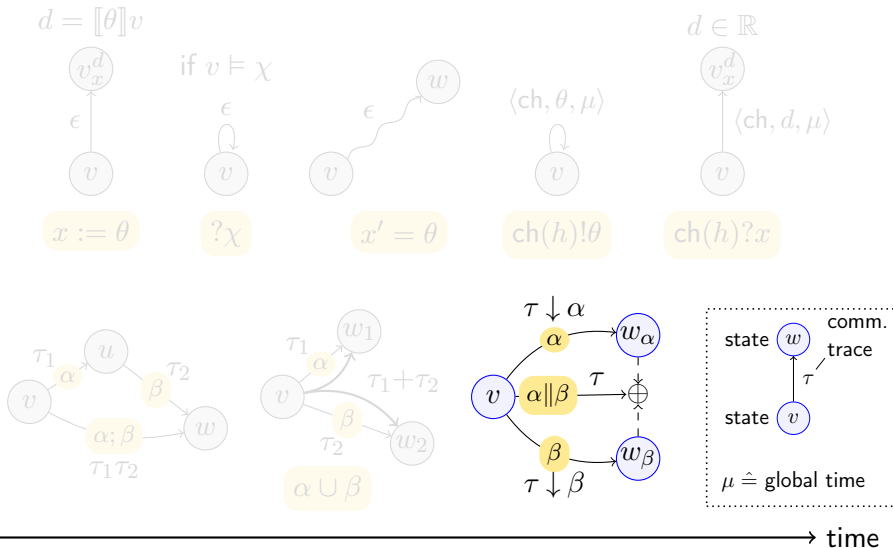
state





# Semantics of Communicating Hybrid Programs

state



# Axiomatization of $d\mathcal{L}_{\text{CHP}}$

## Axiom (one formula)

modulo symbolic (co)finite sets

$$[x := f]p(x) \leftrightarrow p(f)$$

$$[?q]p \leftrightarrow (q \rightarrow p)$$

$$[\text{ch}(h)!\theta]p(\text{ch}, h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch}(h)?x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})$$

## Axiom schema ( $\infty$ formulas)

for all  $x, \theta, \psi, \chi, \alpha, \beta$

$$[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$$

$$[?\chi]\psi \leftrightarrow (\chi \rightarrow \psi)$$

$$[\text{ch}(h)!\theta]\psi(h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow \psi(h_0))$$

(where  $h_0$  is fresh)

$$[\text{ch}(h)?x]_{\{A, C\}}\psi$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}\psi$$

$$[\alpha; \beta]\psi \leftrightarrow [\alpha][\beta]\psi$$

# Axiomatization of $d\mathcal{L}_{\text{CHP}}$

## Axiom (one formula)

modulo symbolic (co)finite sets

$$[x := f]p(x) \leftrightarrow p(f)$$

$$[?q]p \leftrightarrow (q \rightarrow p)$$

$$[\text{ch}(h)!\theta]p(\text{ch}, h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch}(h)?x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})$$

## Axiom schema ( $\infty$ formulas)

for all  $x, \theta, \psi, \chi, \alpha, \beta$

$$[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$$

$$[?\chi]\psi \leftrightarrow (\chi \rightarrow \psi)$$

$$[\text{ch}(h)!\theta]\psi(h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow \psi(h_0))$$

(where  $h_0$  is fresh)

$$[\text{ch}(h)?x]_{\{A, C\}}\psi$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}\psi$$

$$[\alpha; \beta]\psi \leftrightarrow [\alpha][\beta]\psi$$

# Axiomatization of $d\mathcal{L}_{\text{CHP}}$

## Axiom (one formula)

modulo symbolic (co)finite sets

$$[x := f]p(x) \leftrightarrow p(f)$$

uniform  
substitution

$$[?q]p \leftrightarrow (q \rightarrow p)$$

$$[\text{ch}(h)!\theta]p(\text{ch}, h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch}(h)?x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})$$

## Axiom schema ( $\infty$ formulas)

for all  $x, \theta, \psi, \chi, \alpha, \beta$

$$[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$$

$$[?\chi]\psi \leftrightarrow (\chi \rightarrow \psi)$$

$$[\text{ch}(h)!\theta]\psi(h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow \psi(h_0))$$

(where  $h_0$  is fresh)

$$[\text{ch}(h)?x]_{\{A, C\}}\psi$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}\psi$$

$$[\alpha; \beta]\psi \leftrightarrow [\alpha][\beta]\psi$$

# Axiomatization of $d\mathcal{L}_{\text{CHP}}$

## Axiom (one formula)

modulo symbolic (co)finite sets

$$[x := f]p(x) \leftrightarrow p(f) \quad \begin{array}{c} \text{uniform} \\ \text{substitution} \end{array}$$

$$[?q]p \leftrightarrow (q \rightarrow p)$$

$$[\text{ch}(h)!\theta]p(\text{ch}, h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch}(h)?x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}p(\text{ch}, h, x)$$

$$[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})$$

## Axiom schema ( $\infty$ formulas)

for all  $x, \theta, \psi, \chi, \alpha, \beta$

$$[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$$

$$[?\chi]\psi \leftrightarrow (\chi \rightarrow \psi)$$

$$[\text{ch}(h)!\theta]\psi(h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow \psi(h_0))$$

(where  $h_0$  is fresh)

$$[\text{ch}(h)?x]_{\{A, C\}}\psi$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}}\psi$$

$$[\alpha; \beta]\psi \leftrightarrow [\alpha][\beta]\psi$$

# Axiomatization of $d\mathcal{L}_{\text{CHP}}$

## Axiom (one formula)

modulo symbolic (co)finite sets

$$[x := f]p(x) \leftrightarrow p(f) \quad \begin{array}{c} \text{uniform} \\ \text{substitution} \end{array}$$

$$[?q]p \leftrightarrow (q \rightarrow p)$$

$$[\text{ch}(h)!\theta]p(\text{ch}, h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch}(h)?x]_{\{A, C\}} p(\text{ch}, h, x)$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}} p(\text{ch}, h, x)$$

$$[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})$$

implementation by  
object instances

## Axiom schema ( $\infty$ formulas)

for all  $x, \theta, \psi, \chi, \alpha, \beta$

$$[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$$

$$[?\chi]\psi \leftrightarrow (\chi \rightarrow \psi)$$

$$[\text{ch}(h)!\theta]\psi(h)$$

$$\leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, \theta, \mu \rangle \rightarrow \psi(h_0))$$

(where  $h_0$  is fresh)

$$[\text{ch}(h)?x]_{\{A, C\}} \psi$$

$$\leftrightarrow [x := *][\text{ch}(h)!x]_{\{A, C\}} \psi$$

$$[\alpha; \beta]\psi \leftrightarrow [\alpha][\beta]\psi$$

  
kLOC

algorithmic  
implementation

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

(B I)       $\text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset$  and  $\text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$

(B II)       $\text{BV}(\sigma a) \subseteq \text{BV}(a(\!|Y, \bar{z}|))$  and  $\text{CN}(\sigma a) = \text{CN}(a(\!|Y, \bar{z}|))$

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

$$(B \text{ I}) \quad \text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \text{ and } \text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$$

$$(B \text{ II}) \quad \text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z})) \text{ and } \text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$$

Uniform substitution is sound if

[FOL: Church,  $d\mathcal{L}$ : Platzer]

(B I) it never introduces **free variables** or **channel access** into a **context** where the variable or channel is **written**

(B II) it never extends **bound variables** or **writes channels** beyond the **original scope**



# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

(B I)  $\text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset$  and  $\text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$

(B II)  $\text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z}))$  and  $\text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$

Uniform substitution is sound if

(B I) it never releases **variables** or **channel access** into a context where a **variable** or channel is **written** for synchronization!

(B II) it never extends **bound variables** or **writes channels** beyond the **original** scope

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

(B I)       $\text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset$  and  $\text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$

(B II)       $\text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z}))$  and  $\text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$

$$\frac{[a; b]p(Y, \bar{z}) \leftrightarrow [a][b]p(Y, \bar{z})}{[\text{ch}(h)?v; \{x' = v\}]x > 0 \leftrightarrow [\text{ch}(h)?v][\{x' = v\}]x > 0} \text{ US}$$

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

$$(B \text{ I}) \quad \text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \text{ and } \text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$$

$$(B \text{ II}) \quad \text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z})) \text{ and } \text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$$

Uniform substitution is sound if

- (B I) it never introduces **free variables** or **channel access** into a **context** where the variable or channel is **written**

$$\frac{p(h) \rightarrow [a]p(h)}{|h \downarrow \text{ch}| = 0 \rightarrow [\text{ch}(h)!\theta]|h \downarrow \text{ch}| = 0} \quad \text{⚡ clash}$$

↑  
free in a context  
where it is bound

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

$$(B \text{ I}) \quad \text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \text{ and } \text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$$

$$(B \text{ II}) \quad \text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z})) \text{ and } \text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$$

Uniform substitution is sound if

- (B I) it never introduces **free variables** or **channel access** into a **context** where the variable or channel is **written**

$$\frac{p(h) \rightarrow [a]p(h)}{|h \downarrow dh| = 0 \rightarrow [\text{ch}(h)!\theta]|h \downarrow dh| = 0} \text{ US}$$

# Parallel Injection Axiom

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

replace by  
~~~~~  
per branch

$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi (*)$$

(\*)  $\beta$  does not affect  $\psi$

# Parallel Injection Axiom

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

replace by  
~~~~~  
per branch

$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \quad (*)$$

## Theorem

(\*)  $\beta$  does not affect  $\psi$

*The parallel injection axiom is sound:*

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

where  $a(Y_a, \bar{z}_a) \parallel_{wf} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^c) \cup \{\mu, \mu'\} \cup V_T)$

# Parallel Injection Axiom

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

## Theorem

(\*)  $\beta$  does not affect  $\psi$

The parallel injection axiom is sound:

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

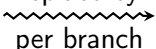
where  $a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^{\text{C}}) \cup \{\mu, \mu'\} \cup V_{\mathcal{T}})$

$$[a(\{\text{ch}\}, h)]p(\text{gh}, h) \rightarrow [a(\{\text{ch}\}, h) \parallel_{\text{wf}} b(\{\text{gh}\} \cap (\{\text{gh}\}^{\text{C}} \cup \{\text{ch}\}), \{h\}^{\text{C}})]p(\text{gh}, h)$$

$$[\text{ch}(h)!1] |h \downarrow \text{gh}| = 1 \rightarrow [\text{ch}(h)!1 \parallel \text{gh}(h)!2] |h \downarrow \text{gh}| = 1$$

# Parallel Injection Axiom

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



$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \quad (*)$$

## Theorem

(\*)  $\beta$  does not affect  $\psi$


The parallel injection axiom is sound:

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

where  $a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^{\text{C}}) \cup \{\mu, \mu'\} \cup V_{\mathcal{T}})$

$$[a(\{\text{ch}\}, h)]p(\text{gh}, h) \rightarrow [a(\{\text{ch}\}, h) \parallel_{\text{wf}} b(\{\text{gh}\} \cap (\{\text{gh}\}^{\text{C}} \cup \{\text{ch}\}), \{h\}^{\text{C}})]p(\text{gh}, h)$$


$$[\text{ch}(h)!1] |h \downarrow \text{gh}| = 1 \rightarrow [\text{ch}(h)!1 \parallel \text{gh}(h)!2] |h \downarrow \text{gh}| = 1$$


  
 ⚡ clash due to (B II)



# Parallel Injection Axiom

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


 replace by  
per branch

$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \quad (*)$$

Theorem

(\*)  $\beta$  does not affect  $\psi$

The parallel injection axiom is sound:

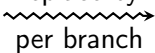
$$[a(Y_a, \bar{z}_a)]p(Y, \bar{z}) \rightarrow [a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b \cap (Y^{\text{C}} \cup Y_a), \bar{z}^{\text{C}})]p(Y, \bar{z})$$

where  $a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^{\text{C}}) \cup \{\mu, \mu'\} \cup V_{\mathcal{T}})$

$$\frac{[a(\{\text{ch}\}, h)]p(\text{ch}, h) \rightarrow [a(\{\text{ch}\}, h) \parallel_{\text{wf}} b(\{\text{ch}\} \cap (\{\text{ch}\}^{\text{C}} \cup \{\text{ch}\}), \{h\}^{\text{C}})]p(\text{ch}, h)}{[\text{ch}(h)!] |h \downarrow \text{ch}| = 1 \rightarrow [\text{ch}(h)! \parallel \text{ch}(h)?x] |h \downarrow \text{ch}| = 1}$$

# Parallel Injection Axiom

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



$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \quad (*)$$

## Theorem

(\*)  $\beta$  does not affect  $\psi$

The parallel injection axiom is sound:

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

where  $a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^{\text{C}}) \cup \{\mu, \mu'\} \cup V_{\mathcal{T}})$

$$\frac{[a(\{\text{ch}\}, h)]p(\text{ch}, h) \rightarrow [a(\{\text{ch}\}, h) \parallel_{\text{wf}} b(\{\text{ch}\} \cap (\{\text{ch}\}^{\text{C}} \cup \{\text{ch}\}), \{h\}^{\text{C}})]p(\text{ch}, h)}{[\text{ch}(h)!] |h \downarrow \text{ch}| = 1 \rightarrow [\text{ch}(h)! \parallel \text{ch}(h)?x] |h \downarrow \text{ch}| = 1}$$

# Parallel Injection Axiom

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

replace by  
~~~~~  
per branch

$$[\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \quad (*)$$

## Theorem

(\*)  $\beta$  does not affect  $\psi$

The parallel injection axiom is sound:

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

where  $a(Y_a, \bar{z}_a) \parallel_{\text{wf}} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^c) \cup \{\mu, \mu'\} \cup V_T)$

$$[a(\{\text{ch}\}, h)]p(\text{ch}, h) \rightarrow [a(\{\text{ch}\}, h) \parallel_{\text{wf}} b(\{\text{ch}\} \cap (\{\text{ch}\}^c \cup \{\text{ch}\}), \{h\}^c)]p(\text{ch}, h)$$

$$[\text{true}]|h \downarrow \text{ch}| = 1 \rightarrow [\text{true} \parallel \text{ch}(h)?x]|h \downarrow \text{ch}| = 1$$

⚡ clash due to (B II)

# Parallel Injection Axiom

Say goodbye to schematic parallel proof rules with subtle side conditions!

**All** parallel systems reasoning reduces to flat **axioms** + **uniform substitution**!

Theorem

( $\star$ )  $\beta$  does not affect  $\psi$

*The parallel injection axiom is sound:*

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

where  $a(Y_a, \bar{z}_a) \parallel_{wf} b(Y_b, \bar{z}_b) \equiv a(Y_a, \bar{z}_a) \parallel b(Y_b, (\bar{z}_b \cap \bar{z}_a^c) \cup \{\mu, \mu'\} \cup V_T)$

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

(B I)  $\text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset$  and  $\text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$

(B II)  $\text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z}))$  and  $\text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$

Uniform substitution is sound if

(B I) it never introduces **free variables** into a **context** where they are not **access**

(B II) it never introduces **free parameters** or **writes channels** into a **scope** where they are not **written**

Binding free parameters sentences you to logic jail!

# Application of Uniform Substitution

substitution  $\sigma$

$U \subseteq V \cup \Omega$  tabooed variables and channels

$$\sigma^U(e_1 \sim e_2) \equiv \sigma^U(e_1) \sim \sigma^U(e_2)$$

$$\sigma^U(p(Y, e)) \equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset(\sigma p(\cdot)) \quad \text{if } (\text{FV}(\sigma p(\cdot)) \cup \text{CN}(\sigma p(\cdot))) \cap U = \emptyset$$

$$\sigma^U(\neg\varphi) \equiv \neg\sigma^U(\varphi)$$

$$\sigma^U(\varphi \wedge \psi) \equiv \sigma^U(\varphi) \wedge \sigma^U(\psi)$$

$$\sigma^U(\forall z \varphi) \equiv \forall z \sigma^{U \cup \{z\}}(\varphi)$$

$$\sigma^U([\alpha]_{\{A, C\}} \psi) \equiv [\sigma_Z^{U, \emptyset}(\alpha)]_{\{\sigma^Z(A), \sigma^Z(C)\}} \sigma^Z(\psi)$$

---

$$\sigma_{U \cup \text{BV}(\sigma a) \cup \text{CN}(\sigma a)}^U(a \Downarrow Y, \bar{z}) \equiv \sigma a$$

if  $\text{BV}(\sigma a) \subseteq \bar{z}$  and  $\text{CN}(\sigma a) = Y$

$$\sigma_{U \cup \{x\}}^U(x := \theta) \equiv x := \sigma^U(\theta)$$

$$\sigma_Z^U(\{x' = \theta\}) \equiv \{x' = \sigma^U(\theta)\}$$

with  $Z = U \cup \{x, x', \mu, \mu'\}$

$$\sigma_{U \cup \{\text{ch}, h\}}^U(\text{ch}(h)! \theta) \equiv \text{ch}(h)! \sigma^U(\theta)$$

$$\sigma_{U \cup \{\text{ch}, h, x\}}^U(\text{ch}(h)? x) \equiv \text{ch}(h)? x$$

$$\sigma_{B \cup Z}^U(\alpha \cup \beta) \equiv \sigma_B^U(\alpha) \cup \sigma_Z^U(\beta)$$

$$\sigma_Z^U(\alpha; \beta) \equiv \sigma_B^U(\alpha); \sigma_Z^U(\beta)$$

$$\sigma_{B \cup Z}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \parallel \sigma_Z^U(\beta)$$

Implementation of

$$\frac{\phi}{\sigma\phi} \text{ US} \quad (\text{B I}) + (\text{B II})$$

by a canonical recursion

# Application of Uniform Substitution

substitution  $\sigma$

$U \subseteq V \cup \Omega$  tabooed variables and channels

$$\sigma^U(e_1 \sim e_2) \equiv \sigma^U(e_1) \sim \sigma^U(e_2)$$

$$\sigma^U(\tau, e) \equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset(\sigma p(\cdot)) \quad \text{if } (\text{FV}(\sigma p(\cdot)) \cup \text{CN}(\sigma p(\cdot))) \cap U = \emptyset$$

$$\sigma^U(\neg \varphi) \equiv \neg \sigma^U(\varphi)$$

$$\sigma^U(\varphi \wedge \psi) \equiv \sigma^U(\varphi) \wedge \sigma^U(\psi) \quad \text{homomorphic application}$$

$$\sigma^U(\forall z \varphi) \equiv \forall z \sigma^{U \cup \{z\}}(\varphi)$$

$$\sigma^U([\alpha]_{\{A,C\}} \psi) \equiv [\sigma_Z^{U,\emptyset}(\alpha)]_{\{\sigma^Z(A), \sigma^Z(C)\}} \sigma^Z(\psi)$$

$$\sigma_{U \cup \text{BV}(\sigma a) \cup \text{CN}(\sigma a)}^U(a(Y, \bar{z})) \equiv \sigma a \quad \text{if } \text{BV}(\sigma a) \subseteq \bar{z} \text{ and } \text{CN}(\sigma a) = Y$$

$$\sigma_{U \cup \{x\}}^U(x := \theta) \equiv x := \sigma^U(\theta)$$

$$\sigma_Z^U(\{x' = \theta\}) \equiv \{x' = \sigma^U(\theta)\} \quad \text{with } Z = U \cup \{x, x', \mu, \mu'\}$$

$$\sigma_{U \cup \{\text{ch}, h\}}^U(\text{ch}(h)! \theta) \equiv \text{ch}(h)! \sigma^U(\theta)$$

$$\sigma_{U \cup \{\text{ch}, h, x\}}^U(\text{ch}(h)? x) \equiv \text{ch}(h)? x$$

$$\sigma_{B \cup Z}^U(\alpha \cup \beta) \equiv \sigma_B^U(\alpha) \cup \sigma_Z^U(\beta)$$

$$\sigma_Z^U(\alpha; \beta) \equiv \sigma_B^U(\alpha); \sigma_Z^U(\beta)$$

$$\sigma_{B \cup Z}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \parallel \sigma_Z^U(\beta)$$

Implementation of

$$\frac{\phi}{\sigma \phi} \text{ US} \quad (\text{B I}) + (\text{B II})$$

by a canonical recursion

# Application of Uniform Substitution

substitution  $\sigma$

$U \subseteq V \cup \Omega$  tabooed variables and channels

$$\sigma^U(e_1 \sim e_2) \equiv \sigma^U(e_1) \sim \sigma^U(e_2)$$

$$\sigma^U(p(Y, e)) \equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset(\sigma p(\cdot)) \quad \text{if } (\text{FV}(\sigma p(\cdot)) \cup \text{CN}(\sigma p(\cdot))) \cap U = \emptyset$$

$$\sigma^U(\neg\varphi) \equiv \neg\sigma^U(\varphi)$$

$$\sigma^U(\varphi \wedge \psi) \equiv \sigma^U(\varphi) \wedge \sigma^U(\psi)$$

$$\sigma^U(\forall z \varphi) \equiv \forall z \sigma^{U \cup \{z\}}(\varphi)$$

$$\sigma^U([\alpha]_{\{A, C\}} \psi) \equiv [\sigma_Z^{U, \emptyset}(\alpha)]_{\{\sigma^Z(A), \sigma^Z(C)\}} \sigma^Z(\psi)$$

bound

$$\sigma_{U \cup \text{BV}(\sigma a) \cup \text{CN}(\sigma a)}^U(a(Y, \bar{z})) \equiv \sigma a$$

if  $\text{BV}(\sigma a) \subseteq \bar{z}$  and  $\text{CN}(\sigma a) = Y$

$$\sigma_{U \cup \{x\}}^U(x := \theta) \equiv x := \sigma^U(\theta)$$

$$\sigma_Z^U(\{x' = \theta\}) \equiv \{x' = \sigma^U(\theta)\}$$

with  $Z = U \cup \{x, x', \mu, \mu'\}$

$$\sigma_{U \cup \{\text{ch}, h\}}^U(\text{ch}(h)! \theta) \equiv \text{ch}(h)! \sigma^U(\theta)$$

$$\sigma_{U \cup \{\text{ch}, h, x\}}^U(\text{ch}(h)? x) \equiv \text{ch}(h)? x$$

$$\sigma_{B \cup Z}^U(\alpha \cup \beta) \equiv \sigma_B^U(\alpha) \cup \sigma_Z^U(\beta)$$

$$\sigma_Z^U(\alpha; \beta) \equiv \sigma_B^U(\alpha); \sigma_Z^U(\beta)$$

$$\sigma_{B \cup Z}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \parallel \sigma_Z^U(\beta)$$

Implementation of

$$\frac{\phi}{\sigma\phi} \text{ US} \quad (\text{B I}) + (\text{B II})$$

by a canonical recursion



# Application of Uniform Substitution

substitution  $\sigma$

$U \subseteq V \cup \Omega$  tabooed variables and channels

$$\sigma^U(e_1 \sim e_2) \equiv \sigma^U(e_1) \sim \sigma^U(e_2)$$

$$\sigma^U(p(Y, e)) \equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset(\sigma p(\cdot)) \quad \text{if } (\text{FV}(\sigma p(\cdot)) \cup \text{CN}(\sigma p(\cdot))) \cap U = \emptyset$$

$$\sigma^U(\neg \varphi) \equiv \neg \sigma^U(\varphi)$$

$$\sigma^U(\varphi \wedge \psi) \equiv \sigma^U(\varphi) \wedge \sigma^U(\psi) \quad \text{recursive substitution}$$

does  $\sigma p(\cdot)$  respect taboo  $U$ ?

$$\sigma^U(\forall z \varphi) \equiv \forall z \sigma^{U \cup \{z\}}(\varphi)$$

$$\sigma^U([\alpha]_{\{A, C\}} \psi) \equiv [\sigma_Z^{U, \emptyset}(\alpha)]_{\{\sigma^Z(A), \sigma^Z(C)\}} \sigma^Z(\psi)$$

$$\sigma_{U \cup \text{BV}(\sigma a) \cup \text{CN}(\sigma a)}^U(a(Y, \bar{z})) \equiv \sigma a$$

if  $\text{BV}(\sigma a) \subseteq \bar{z}$  and  $\text{CN}(\sigma a) = Y$

$$\sigma_{U \cup \{x\}}^U(x := \theta) \equiv x := \sigma^U(\theta)$$

$$\sigma_Z^U(\{x' = \theta\}) \equiv \{x' = \sigma^U(\theta)\}$$

with  $Z = U \cup \{x, x', \mu, \mu'\}$

$$\sigma_{U \cup \{\text{ch}, h\}}^U(\text{ch}(h)! \theta) \equiv \text{ch}(h)! \sigma^U(\theta)$$

$$\sigma_{U \cup \{\text{ch}, h, x\}}^U(\text{ch}(h)? x) \equiv \text{ch}(h)? x$$

$$\sigma_{B \cup Z}^U(\alpha \cup \beta) \equiv \sigma_B^U(\alpha) \cup \sigma_Z^U(\beta)$$

$$\sigma_Z^U(\alpha; \beta) \equiv \sigma_B^U(\alpha); \sigma_Z^U(\beta)$$

$$\sigma_{B \cup Z}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \parallel \sigma_Z^U(\beta)$$

Implementation of

$$\frac{\phi}{\sigma \phi} \text{ US} \quad (\text{B I}) + (\text{B II})$$

by a canonical recursion

# Application of Uniform Substitution

substitution  $\sigma$

$U \subseteq V \cup \Omega$  tabooed variables and channels

$$\sigma^U(e_1 \sim e_2) \equiv \sigma^U(e_1) \sim \sigma^U(e_2)$$

$$\sigma^U(p(Y, e)) \equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset(\sigma p(\cdot)) \quad \text{if } (\text{FV}(\sigma p(\cdot)) \cup \text{CN}(\sigma p(\cdot))) \cap U = \emptyset$$

$$\sigma^U(\neg\varphi) \equiv \neg\sigma^U(\varphi)$$

$$\sigma^U(\varphi \wedge \psi) \equiv \sigma^U(\varphi) \wedge \sigma^U(\psi)$$

$$\sigma^U(\forall z \varphi) \equiv \forall z \sigma^{U \cup \{z\}}(\varphi)$$

$$\sigma^U([\alpha]_{\{A, C\}} \psi) \equiv [\sigma_Z^{U, \emptyset}(\alpha)]_{\{\sigma^Z(A), \sigma^Z(C)\}} \sigma^Z(\psi)$$

$$\sigma_{U \cup \text{BV}(\sigma a) \cup \text{CN}(\sigma a)}^U(a(Y, \bar{z})) \equiv \sigma a$$

if  $\text{BV}(\sigma a) \subseteq \bar{z}$  and  $\text{CN}(\sigma a) = Y$

$$\sigma_{U \cup \{x\}}^U(x := \theta) \equiv x := \sigma^U(\theta)$$

$$\sigma_Z^U(\{x' = \theta\}) \equiv \{x' = \sigma^U(\theta)\}$$

with  $Z = U \cup \{x, x', \mu, \mu'\}$

$$\sigma_{U \cup \{\text{ch}, h\}}^U(\text{ch}(h)! \theta) \equiv \text{ch}(h)! \sigma^U(\theta)$$

$$\sigma_{U \cup \{\text{ch}, h, x\}}^U(\text{ch}(h)? x) \equiv \text{ch}(h)? x$$

$$\sigma_{BUZ}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \cup \sigma_Z^U(\beta)$$

$$\sigma_{BUZ}^U(\alpha; \beta) \equiv \sigma_B^U(\alpha); \sigma_Z^U(\beta)$$

$$\sigma_{BUZ}^U(\alpha \parallel \beta) \equiv \sigma_B^U(\alpha) \parallel \sigma_Z^U(\beta)$$

input

output

Implementation of

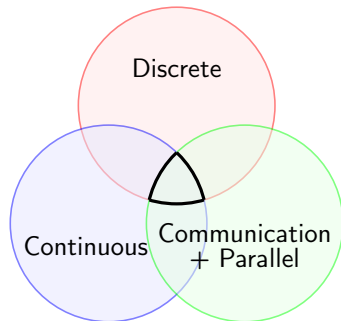
$$\frac{\phi}{\sigma\phi} \text{ US} \quad (\text{B I}) + (\text{B II})$$

by a canonical recursion

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Dynamic logic of CHPs

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

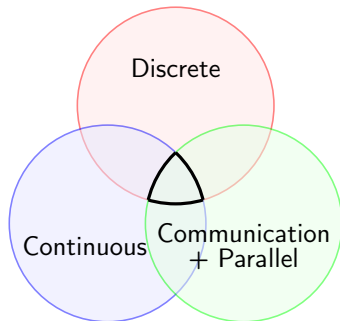


# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

## Dynamic logic of CHPs

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

- Uniform substitution for  $d\mathcal{L}_{\text{CHP}}$  that operates linearly in the formulas
- Modular soundness argument
- **Modular, thus smaller, prover implementation**

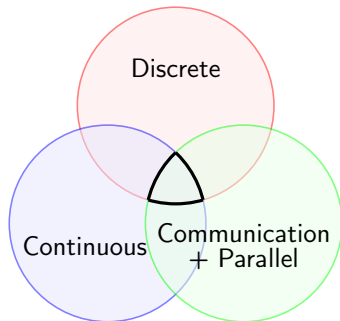


# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

## Dynamic logic of CHPs

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

- Uniform substitution for  $d\mathcal{L}_{\text{CHP}}$  that operates linearly in the formulas
- Modular soundness argument
- **Modular, thus smaller, prover implementation**
- Uniform substitution for the subtle parallel case paves the way to a general framework

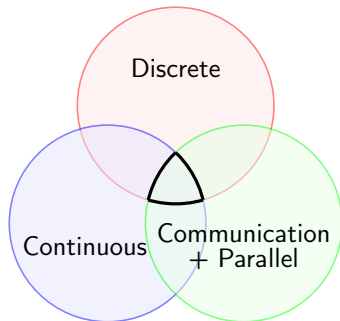






# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

## Dynamic logic of CHPs

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

- Uniform substitution for  $d\mathcal{L}_{\text{CHP}}$  that operates linearly in the formulas
- Modular soundness argument
- **Modular, thus smaller, prover implementation**
- Uniform substitution for the subtle parallel case paves the way to a general framework
- **All parallel reasoning reduces to multiple uses of the simple parallel injection axiom**
- Discrete parallelism benefits as well



-  Marvin Brieger, Stefan Mitsch, and André Platzer.  
Dynamic logic of communicating hybrid programs.  
*CoRR*, abs/2302.14546, 2023.
-  André Platzer.  
A complete uniform substitution calculus for differential dynamic logic.  
*J. Autom. Reas.*, 59(2):219–265, 2017.
-  André Platzer.  
Uniform substitution at one fell swoop.  
In *CADE*, pages 425–441, 2019.
-  Job Zwiers, Willem P. de Roever, and Peter van Emde Boas.  
Compositionality and concurrent networks: Soundness and completeness of a proofs system.  
In *ICALP*, pages 509–519, 1985.

# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

$$(B \text{ I}) \quad \text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \quad \textit{and} \quad \text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$$

$$(B \text{ II}) \quad \text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z})) \quad \textit{and} \quad \text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$$

Uniform substitution is sound if

- (B I) it never introduces **free variables** or **channel access** into a **context** where the variable or channel is **written**

$$\frac{[t_0 := f]p(t_0) \leftrightarrow p(f)}{[t_0 := \mu][x' = \theta][\text{ch}(h)!\theta]\varphi(t_0) \leftrightarrow [x' = \theta][\text{ch}(h)!\theta]\varphi(\mu)} \quad \text{clash}$$

$\varphi(t) \equiv \text{time}(h \downarrow \text{ch}) = t$

free in a context  
 where it is bound



# Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

Theorem (substitution  $\sigma$  maps symbols to terms, formulas, or programs)

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

$$(B I) \quad \text{FV}(\sigma|_{\Sigma(e)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \textit{ and } \text{CN}(\sigma|_{\Sigma(e)}) \cap \text{CN}(\otimes(\cdot)) = \emptyset$$

$$(B II) \quad \text{BV}(\sigma a) \subseteq \text{BV}(a(\downarrow Y, \bar{z})) \textit{ and } \text{CN}(\sigma a) = \text{CN}(a(\downarrow Y, \bar{z}))$$

Uniform substitution is sound if

(B II) it never extends **bound variables** or **writes channels** beyond the **original** scope

$$[a(\downarrow \emptyset, V_{\mathbb{R}})]_{\{A, C\}} P \leftrightarrow C \wedge (A \rightarrow [a(\downarrow \emptyset, V_{\mathbb{R}})] P)$$

$$[\text{ch}(h)!\theta]_{\{\text{true}, |h \downarrow \text{ch}| = 0\}} x = 0 \leftrightarrow |h \downarrow \text{ch}| = 0 \wedge (\text{true} \rightarrow [\text{ch}(h)!\theta] x = 0)$$

↑  
free in a context  
where it is bound

A, C, and P may mention channels

⚡ clash

# Program Semantics - Part I

Semantics  $I[\alpha] \subseteq \mathcal{S} \times \mathcal{T}_{\text{rec}} \times \mathcal{S}_{\perp}$  consists of state-trace-state triples

$$I[a(Y, \bar{z})] = I(a(Y, \bar{z}))$$

$$I[x := \theta] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, w) \mid w = v_x^d \text{ where } d = Iv[\theta]\}$$

$$I[x := *] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, w) \mid w = v_x^d \text{ where } d \in \mathbb{R}\}$$

$$I[?\chi] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, v) \mid Iv \models \chi\}$$

$$I[\{x' = \theta \ \& \ \chi\}] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, \varphi(s)) \mid v = \varphi(0) \text{ on } \{\mu', x'\}^{\mathbb{G}},$$

and  $\varphi(\zeta) = \varphi(0)$  on  $\{x, x', \mu, \mu'\}^{\mathbb{G}}$ , and  $I\varphi(\zeta) \models \mu' = 1 \wedge x' = \theta \wedge \chi$

for all  $\zeta \in [0, s]$  and a solution  $\varphi : [0, s] \rightarrow \mathcal{S}$  with  $\varphi(\zeta)(z') = \frac{d\varphi(t)(z)}{dt}(\zeta)$

for  $z \in \{x, \mu\}$

where  $\perp_{\mathcal{D}} = \mathcal{S} \times \{\epsilon\} \times \{\perp\}$  and  $\mathcal{T}_{\text{rec}} = (V_{\mathcal{T}} \times \Omega \times \mathbb{R} \times \mathbb{R})^*$

$$I[\text{ch}(h)!\theta] = \{(v, \tau, w) \mid (\tau, w) \preceq (\langle h, \text{ch}, d, v(\mu) \rangle, v) \text{ where } d = Iv[\theta]\}$$

$$I[\text{ch}(h)?x] = \{(v, \tau, w) \mid (\tau, w) \preceq (\langle h, \text{ch}, d, v(\mu) \rangle, v_x^d) \text{ where } d \in \mathbb{R}\}$$

$$I[\alpha \cup \beta] = I[\alpha] \cup I[\beta]$$

$$I[\alpha; \beta] = I[\alpha] \hat{\circ} I[\beta] \stackrel{\text{def}}{=} (I[\alpha])_{\perp} \cup (I[\alpha] \triangleright I[\beta])$$

$$I[\alpha^*] = \bigcup_{n \in \mathbb{N}} (I[\alpha])^n = \bigcup_{n \in \mathbb{N}} I[\alpha^n] \quad \text{where } \alpha^0 \equiv ?\top \text{ and } \alpha^{n+1} = \alpha; \alpha^n$$

$$I[\alpha_1 \parallel \alpha_2] = \left\{ (v, \tau, w_{\alpha_1} \oplus w_{\alpha_2}) \mid \begin{array}{l} (v, \tau \downarrow \alpha_j, w_{\alpha_j}) \in I[\alpha_j] \text{ for } j = 1, 2, \text{ and} \\ w_{\alpha_1}(\mu) = w_{\alpha_2}(\mu), \text{ and } \tau = \tau \downarrow (\alpha_1 \parallel \alpha_2) \end{array} \right\}$$

## Definition (Static semantics)

For term or formula  $e$ , and program  $\alpha$ , free variables  $\text{FV}(e)$  and  $\text{FV}(\alpha)$ , bound variables  $\text{BV}(\alpha)$ , accessed channels  $\text{CN}(e)$ , and written channels  $\text{CN}(\alpha)$  form the static semantics.

$$\text{FV}(e) = \{z \in V \mid \exists I, v, \tilde{v} : v = \tilde{v} \text{ on } \{z\}^G \text{ and } Iv[e] \neq I\tilde{v}[e]\}$$

$$\text{CN}(e) = \{\text{ch} \in \Omega \mid \exists I, v, \tilde{v} : v \downarrow \{\text{ch}\}^G = \tilde{v} \downarrow \{\text{ch}\}^G \text{ and } Iv[e] \neq I\tilde{v}[e]\}$$

$$\text{FV}(\alpha) = \{z \in V \mid \exists I, v, \tilde{v}, \tau, w : v = \tilde{v} \text{ on } \{z\}^G \text{ and } (v, \tau, w) \in I[\alpha], \\ \text{and there is no } (\tilde{v}, \tilde{\tau}, \tilde{w}) \in I[\alpha] : \tilde{\tau} = \tau \text{ and } w = \tilde{w} \text{ on } \{z\}^G\}$$

$$\text{BV}(\alpha) = \{z \in V \mid \exists I, (v, \tau, w) \in I[\alpha] : w \neq \perp \text{ and } (w \cdot \tau)(z) \neq v(z)\}$$

$$\text{CN}(\alpha) = \{\text{ch} \in \Omega \mid \exists I, (v, \tau, w) \in I[\alpha] : \tau \downarrow \{\text{ch}\} \neq \epsilon\}$$

# Communication-aware Coincidence

## Lemma (Bound effect property)

$BV(\alpha)$  and  $CN(\alpha)$  are the smallest sets with the bound effect property for program  $\alpha$ . That is,  $v = w$  on  $V_{\mathcal{T}}$  and  $v = w \cdot \tau$  on  $BV(\alpha)^{\mathbb{C}}$  if  $w \neq \perp$ , and  $\tau \downarrow CN(\alpha)^{\mathbb{C}} = \epsilon$  for all  $(v, \tau, w) \in I[\alpha]$ .

## Lemma (Coincidence for terms and formulas)

$FV(e)$  and  $CN(e)$  are the smallest sets with the communication-aware coincidence property for term or formula  $e$ : If  $v \downarrow CN(e) = \tilde{v} \downarrow CN(e)$  on  $FV(e)$  and  $I = J$  on  $\Sigma(e)$ , then  $Iv[e] = J\tilde{v}[e]$ .

## Lemma (Coincidence for programs)

$FV(\alpha)$  is the smallest set with the coincidence property for program  $\alpha$ : If  $v = \tilde{v}$  on  $X \supseteq FV(\alpha)$ , and  $I = J$  on  $\Sigma(\alpha)$ , and  $(v, \tau, w) \in I[\alpha]$ , then  $\exists(\tilde{v}, \tilde{\tau}, \tilde{w}) \in J[\alpha] : w = \tilde{w}$  on  $X$ , and  $\tau = \tilde{\tau}$ , and  $(w = \perp \text{ iff } \tilde{w} = \perp)$ .

# Soundness argument

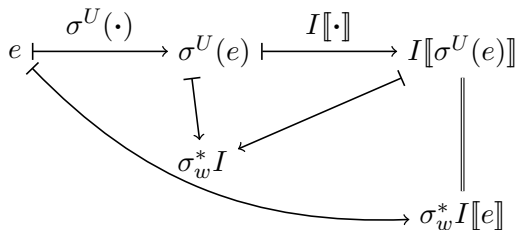
## Lemma (Semantic uniform substitution)

Terms  $e$ , and formulas  $\phi$ , and programs  $\alpha$  evaluate equally under substitution  $\sigma^U$  and adjoint interpretation  $\sigma_w^* I$  for all  $U$ -variations  $v$  of  $w$ :

$$I[\sigma^U(e)] = \sigma_w^* I[e]$$

$$Iv \models \sigma^U(\phi) \text{ iff } \sigma_w^* Iv \models \phi$$

$$(v, \tau, o) \in I[\sigma_Z^U(\alpha)] \text{ iff } (v, \tau, o) \in \alpha[\phi]$$



# Axiomatization - Part I

$$[:=] \quad [x := g^{\mathbb{R}}]p(x) \leftrightarrow p(g^{\mathbb{R}})$$

$$[*] \quad [x := *]p(x) \leftrightarrow \forall x p(x)$$

$$[?] \quad [?q_{\mathbb{R}}]p \leftrightarrow (q_{\mathbb{R}} \rightarrow p)$$

$$[\mu] \quad [\{\bar{x}' = g^{\mathbb{R}}(\bar{x}, \mu) \ \& \ q_{\mathbb{R}}(\bar{x}, \mu)\}]p(\bar{x}, \mu) \leftrightarrow [\{\mu' = 1, \bar{x}' = g^{\mathbb{R}}(\bar{x}, \mu) \ \& \ q_{\mathbb{R}}(\bar{x}, \mu)\}]p(\bar{x}, \mu)$$

$$[\text{ch!}] \quad [\text{ch}(h)!g^{\mathbb{R}}]p(\text{ch}, h) \leftrightarrow \forall h_0 (h_0 = h \cdot \langle \text{ch}, g^{\mathbb{R}}, \mu \rangle \rightarrow p(\text{ch}, h_0))$$

$$[\text{ch!}]_{\mathcal{AC}} \quad [\text{ch}(h)!g^{\mathbb{R}}]_{\{\hat{r}, \hat{q}\}}\hat{p} \leftrightarrow \hat{q} \wedge (\hat{r} \rightarrow [\text{ch}(h)!g^{\mathbb{R}}](\hat{q} \wedge (\hat{r} \rightarrow \hat{p})))$$

$$[\text{ch?}]_{\mathcal{AC}} \quad [\text{ch}(h)?x]_{\{\hat{r}, \hat{q}\}}p(\text{ch}, h, x) \leftrightarrow [x := *][\text{ch}(h)!x]_{\{\hat{r}, \hat{q}\}}p(\text{ch}, h, x)$$

$P_j \equiv p_j(Y, \bar{z})$ , and  $R_j \equiv r_j(Y, \bar{h})$ , and  $Q_j \equiv q_j(Y, \bar{h})$ , and  $\hat{\chi} \equiv \chi(\text{ch}, h)$ , where  $j$  may be blank, and  $Y \subseteq \Omega$ ,  $\bar{z} \subseteq V_{\mathbb{R}} \cup V_{\mathcal{T}}$ , and  $\bar{h} \subseteq V_{\mathcal{T}}$  are (co)finite.

$$[;]_{AC} \quad [a; b]_{\{R,Q\}} P \leftrightarrow [a]_{\{R,Q\}} [b]_{\{R,Q\}} P$$

$$[\cup]_{AC} \quad [a \cup b]_{\{R,Q\}} P \leftrightarrow [a]_{\{R,Q\}} P \wedge [b]_{\{R,Q\}} P$$

$$[*]_{AC} \quad [a^*]_{\{R,Q\}} P \leftrightarrow [a^0]_{\{R,Q\}} P \wedge [a]_{\{R,Q\}} [a^*]_{\{R,Q\}} P$$

$$I_{AC} \quad [a^*]_{\{R,Q\}} P \leftrightarrow [a^0]_{\{R,Q\}} P \wedge [a^*]_{\{R, \text{true}\}} (P \rightarrow [a]_{\{R,Q\}} P)$$

$P_j \equiv p_j(Y, \bar{z})$ , and  $R_j \equiv r_j(Y, \bar{h})$ , and  $Q_j \equiv q_j(Y, \bar{h})$ , and  $\hat{\chi} \equiv \chi(\text{ch}, h)$ , where  $j$  may be blank, and  $Y \subseteq \Omega$ ,  $\bar{z} \subseteq V_{\mathbb{R}} \cup V_{\mathcal{T}}$ , and  $\bar{h} \subseteq V_{\mathcal{T}}$  are (co)finite.



$$\boxed{\top, \top} \quad [a]P \leftrightarrow [a]_{\{\text{true}, \text{true}\}}P$$

$$\boxed{\epsilon} \mathbf{AC} \quad [a(\emptyset, V_{\mathbb{R}})]_{\{R, Q\}}P \leftrightarrow Q \wedge (R \rightarrow [a(\emptyset, V_{\mathbb{R}})]P)$$

$$\boxed{\text{WA}} \quad [a]_{\{\text{true}, W_A\}}\text{true} \wedge [a]_{\{R_1 \wedge R_2, Q_1 \wedge Q_2\}}P \rightarrow [a]_{\{R, Q_1 \wedge Q_2\}}P$$

$$\mathbf{W} \boxed{\text{AC}} \quad [a]_{\{R, Q\}}P \leftrightarrow Q \wedge [a]_{\{R, Q\}}(Q \wedge (R \rightarrow P))$$

$$\mathbf{KAC} \quad [a]_{\{R, Q_1 \rightarrow Q_2\}}(P_1 \rightarrow P_2) \rightarrow ([a]_{\{R, Q_1\}}P_1 \rightarrow [a]_{\{R, Q_2\}}P_2)$$

$P_j \equiv p_j(Y, \bar{z})$ , and  $R_j \equiv r_j(Y, \bar{h})$ , and  $Q_j \equiv q_j(Y, \bar{h})$ , and  $\hat{\chi} \equiv \chi(\text{ch}, h)$ , where  $j$  may be blank, and  $Y \subseteq \Omega$ ,  $\bar{z} \subseteq V_{\mathbb{R}} \cup V_{\mathcal{T}}$ , and  $\bar{h} \subseteq V_{\mathcal{T}}$  are (co)finite.

$$\text{MP} \quad \frac{p \rightarrow q \quad p}{q}$$

$$\text{GAC} \quad \frac{Q \wedge P}{[a]_{\{R, Q\}} P}$$

$$\forall \quad \frac{p(x)}{\forall x p(x)}$$

$$\text{CE} \quad \frac{P_1 \leftrightarrow P_2}{C(P_1) \leftrightarrow C(P_2)}$$

$P_j \equiv p_j(Y, \bar{z})$ , and  $R_j \equiv r_j(Y, \bar{h})$ , and  $Q_j \equiv q_j(Y, \bar{h})$ , and  $\hat{\chi} \equiv \chi(\text{ch}, h)$ , where  $j$  may be blank, and  $Y \subseteq \Omega$ ,  $\bar{z} \subseteq V_{\mathbb{R}} \cup V_{\mathcal{T}}$ , and  $\bar{h} \subseteq V_{\mathcal{T}}$  are (co)finite.

# Don't Release the Synchronization Dragon!

This instantiation is unsound as it releases  $dh$  from synchronization!

$$\frac{[a(\text{ch}) \cup (?false; c(\text{dh}))]p(\text{dh}) \rightarrow [a(\text{ch}) \cup (?false; c(\text{dh}))] \parallel \text{dh?x}]p(\text{dh})}{[\text{ch}(h)!\theta \cup (?false; ?true)]\varphi(\text{dh}) \rightarrow [\text{ch}(h)!\theta \cup (?false; ?true)] \parallel \text{dh?x}]\varphi(\text{dh})}$$

↑                      ↑  
free in a context  
where it is bound

Luckily uniform substitution sorts it out by a ⚡ clash.

$$\begin{array}{c}
 \vdots \\
 \frac{\Gamma \vdash [\alpha]_{\{A_1, C_1\}} \psi_1}{\Gamma \vdash [\alpha \parallel \beta]_{\{A_1, C_1\}} \psi_1} \llbracket \_ \rrbracket_{AC} \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{A_1, C_1\}} \psi_1}{\Gamma \vdash [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1\}} \psi_1} M[\cdot]_{AC} \quad \vdots \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1\}} \psi_1 \quad \Gamma \vdash [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)}{\Gamma \vdash [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)} \llbracket \_ \rrbracket_{AC \wedge} \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{true, W_A\}} true \quad \Gamma \vdash [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)}{\Gamma \vdash [\alpha \parallel \beta]_{\{true, W_A\}} true \wedge [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)} \wedge R \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{true, W_A\}} true \wedge [\alpha \parallel \beta]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)}{\Gamma \vdash [\alpha \parallel \beta]_{\{true, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)} \llbracket \_ \rrbracket_{W_A} \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{true, C_1 \wedge C_2\}} (\psi_1 \wedge \psi_2)}{\Gamma \vdash [\alpha \parallel \beta]_{\{true, true\}} \psi} M[\cdot]_{AC} \\
 \frac{\Gamma \vdash [\alpha \parallel \beta]_{\{true, true\}} \psi}{\Gamma \vdash [\alpha \parallel \beta] \psi} \llbracket \_ \rrbracket_{T, T}
 \end{array}$$

$$W_A \equiv (A_2 \rightarrow C_1) \wedge (A_1 \rightarrow C_2)$$