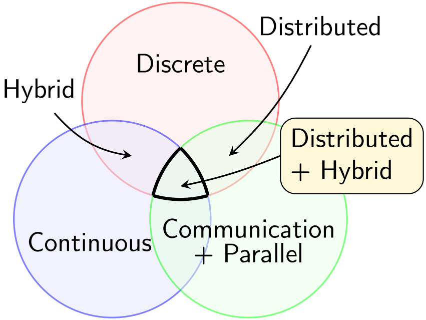
Uniform Substitution for Dynamic Logic with Communicating Hybrid Programs

Marvin Brieger[1], Stefan Mitsch[2], and André Platzer[2,3]

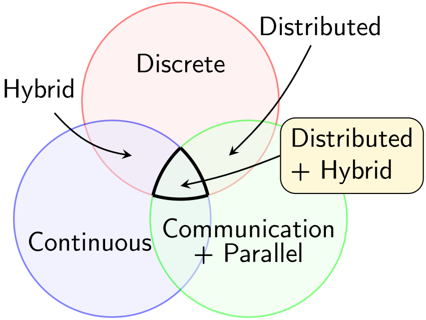
[1] LMU Munich, Germany
[2] Carnegie Mellon University, Pittsburgh, USA
[3] Karlsruhe Institute of Technology, Germany

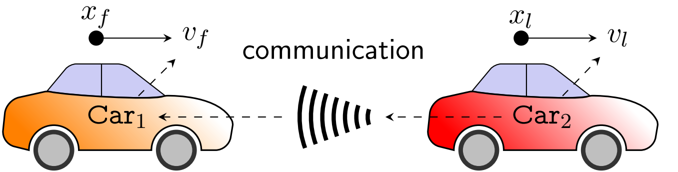
3rd June 2023

Challenge: Distributed Cyber-physical Systems



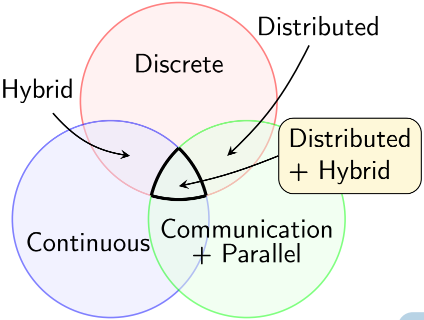
Challenge: Distributed Cyber-physical Systems

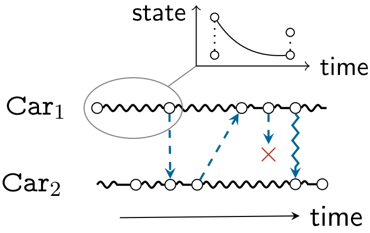




Many real-world systems are distributed hybrid systems

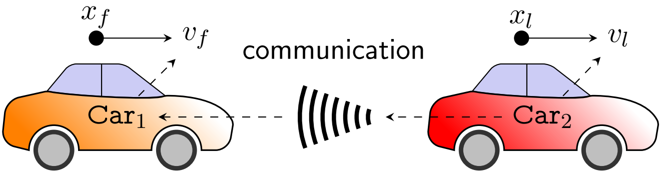
Challenge: Distributed Cyber-physical Systems





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

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \land \psi)}$$

- Compositional reasoning reduces complex systems to their building blocks

The Downside of Schematic Proof Calculi

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

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

$$\begin{aligned} \mathsf{FV}(\phi) \cap \mathsf{BV}(\beta) &\subseteq \emptyset \\ \mathsf{CN}(\phi) \cap \mathsf{CN}(\beta) &\subseteq \emptyset \\ \mathsf{FV}(\psi) \cap \mathsf{BV}(\alpha) &\subseteq \emptyset \\ \mathsf{CN}(\psi) \cap \mathsf{CN}(\alpha) &\subseteq \emptyset \end{aligned}$$

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

The Downside of Schematic Proof Calculi

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\,(\star\star)$$

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

$$\begin{gathered}
\mathsf{FV}(\phi) \cap \mathsf{BV}(\beta) \subseteq \emptyset \\
\mathsf{CN}(\phi) \cap \mathsf{CN}(\beta) \subseteq \emptyset \\
\mathsf{FV}(\psi) \cap \mathsf{BV}(\alpha) \subseteq \emptyset \\
\mathsf{CN}(\psi) \cap \mathsf{CN}(\alpha) \subseteq \emptyset
\end{gathered}$$

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

The Downside of Schematic Proof Calculi

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)} \; (\star\star)$$

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

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

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

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

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

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

The Downside of Schematic Proof Calculi

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

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

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

$\mathsf{CN}(\phi) \cap \mathsf{CN}(\beta) \subseteq \mathsf{CN}(\alpha)$

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

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

$V_G =$ globally synchronized behavior

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

The Downside of Schematic Proof Calculi

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)} \; (\star\star)$$

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

$$\mathsf{FV}(\phi) \cap \mathsf{BV}(\beta) \subseteq V_G$$
$$\mathsf{CN}(\phi) \cap \mathsf{CN}(\beta) \subseteq \mathsf{CN}(\alpha)$$
$$\mathsf{FV}(\psi) \cap \mathsf{BV}(\alpha) \subseteq V_G$$
$$\mathsf{CN}(\psi) \cap \mathsf{CN}(\alpha) \subseteq \mathsf{CN}(\beta)$$

$V_G =$ globally synchronized behavior

$+$ incl. global time

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

The Downside of Schematic Proof Calculi

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

- Compositional reasoning reduces complex systems to their building blocks
- In case of parallel (hybrid) systems, side ... e and subtle

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

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

$\mathsf{CN}(\phi) \cap \mathsf{CN}($ ... ized behavior

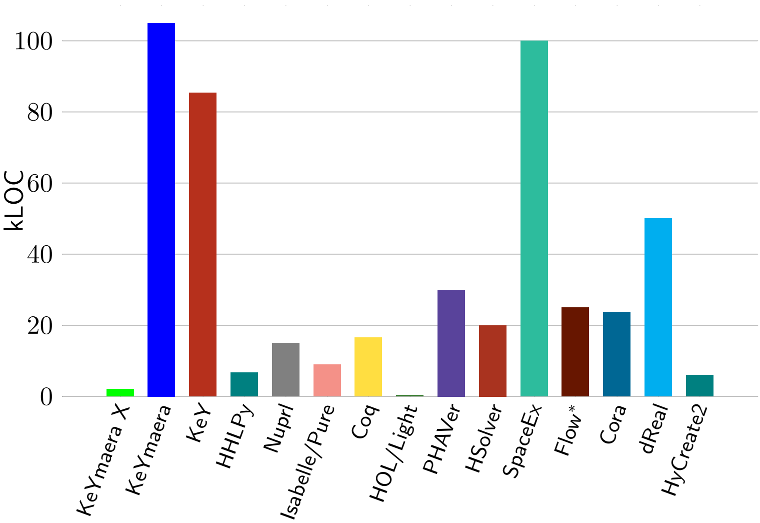
$\mathsf{FV}(\psi) \cap \mathsf{BV}(\alpha) \subseteq V_G$ ... e

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

Uniform substitution is to the rescue

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

Sound Microkernels for Theorem Provers

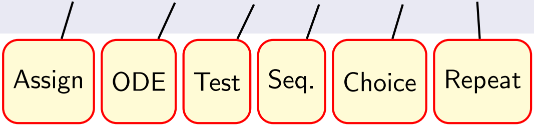


Disclaimer: self-reported estimates

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

Definition: Communicating hybrid programs

$$\overbrace{x := \theta \mid x' = \theta \mid ?\chi \mid \alpha ; \beta \mid \alpha \cup \beta \mid \alpha^*}^{\text{Hybrid programs}}$$



Assign ODE Test Seq. Choice Repeat

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

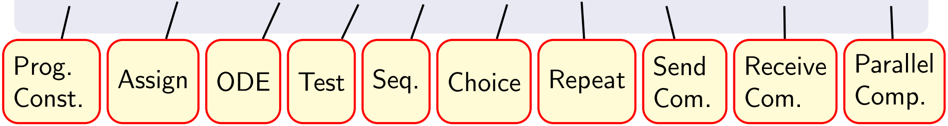
Definition: Communicating hybrid programs

$$\overbrace{\underbrace{x := \theta}_{\text{Assign}} \mid \underbrace{x' = \theta}_{\text{ODE}} \mid \underbrace{?\chi}_{\text{Test}} \mid \underbrace{\alpha;\beta}_{\text{Seq.}} \mid \underbrace{\alpha \cup \beta}_{\text{Choice}} \mid \underbrace{\alpha^*}_{\text{Repeat}}}^{\text{Hybrid programs}} \mid \overbrace{\underbrace{\mathsf{ch}(h)!\theta}_{\text{Send Com.}} \mid \underbrace{\mathsf{ch}(h)?x}_{\text{Receive Com.}} \mid \underbrace{\alpha \parallel \beta}_{\text{Parallel Comp.}}}^{\text{Communication and parallelism}}$$

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

Definition: Communicating hybrid programs

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



Prog. Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send Com.

Receive Com.

Parallel Comp.

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

Definition: Communicating hybrid programs

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

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

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

Definition: Communicating hybrid programs

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

Prog. Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send Com.

Receive Com.

Parallel Comp.

Definition: Dynamic assumption-commitment logic

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

Forall

All Prog. Runs

All Runs in Env.

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

Definition: Communicating hybrid programs

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

Prog. Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send Com.

Receive Com.

Parallel Comp.

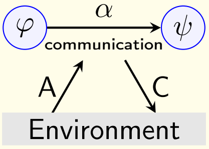
Definition: Dynamic assumption-commitment logic

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

Forall

All Prog. Runs

All Runs in Env.



$$\varphi \rightarrow [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$$

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

Definition: Communicating hybrid programs

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

Prog. Const.

Assign

ODE

Test

Seq.

Choice

Repeat

Send Com.

Receive Com.

Parallel Comp.

Definition: Dynamic assumption-commitment logic

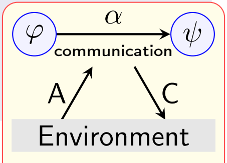
$$p(Y,\bar{e}) \mid \overbrace{e_1 \sim e_2 \mid \neg\varphi \mid \varphi \land \psi \mid \forall x\, \varphi}^{\text{First-order logic}} \mid \overbrace{[\alpha]\psi \mid [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi}^{\text{Dynamic modalities}}$$

Pred. Symb.

Forall

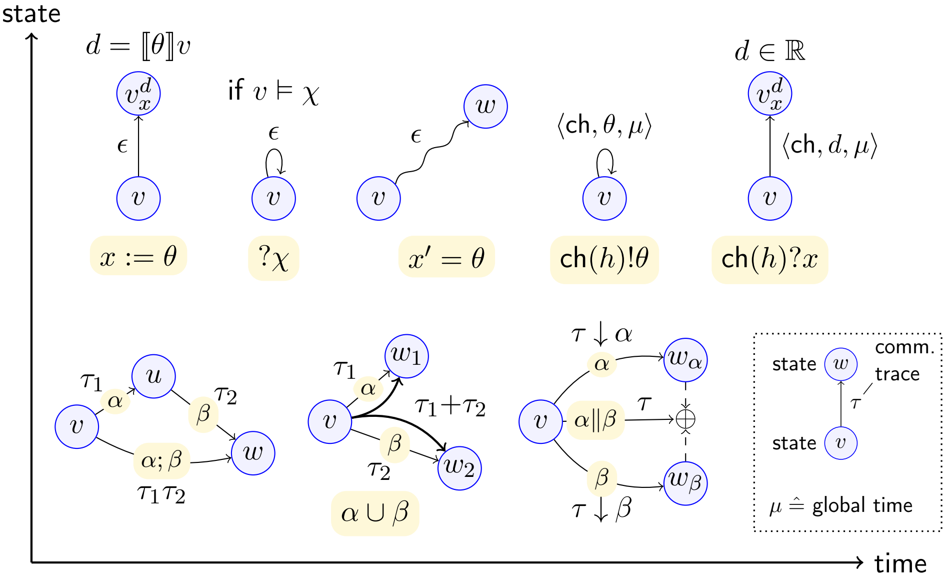
All Prog. Runs

All Runs in Env.

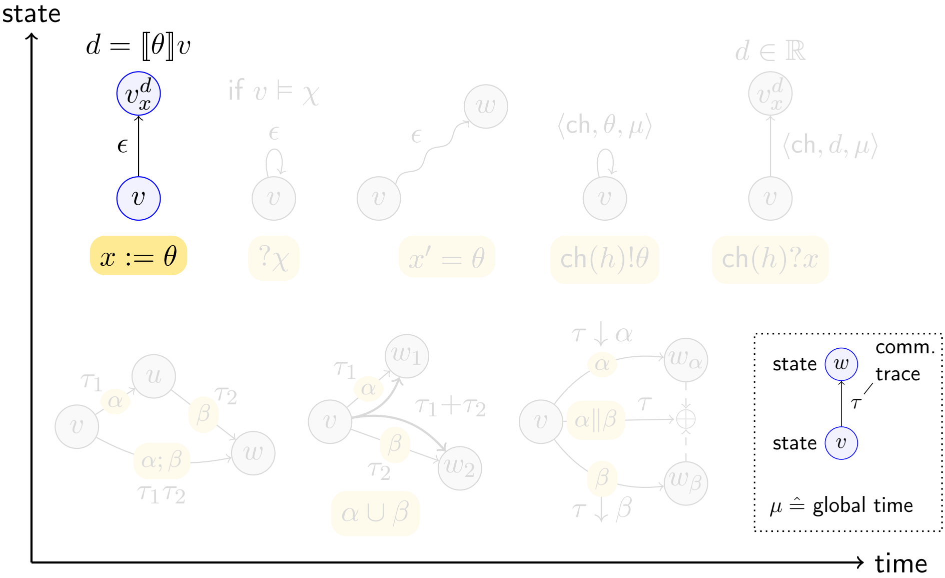


$$\varphi \to [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$$

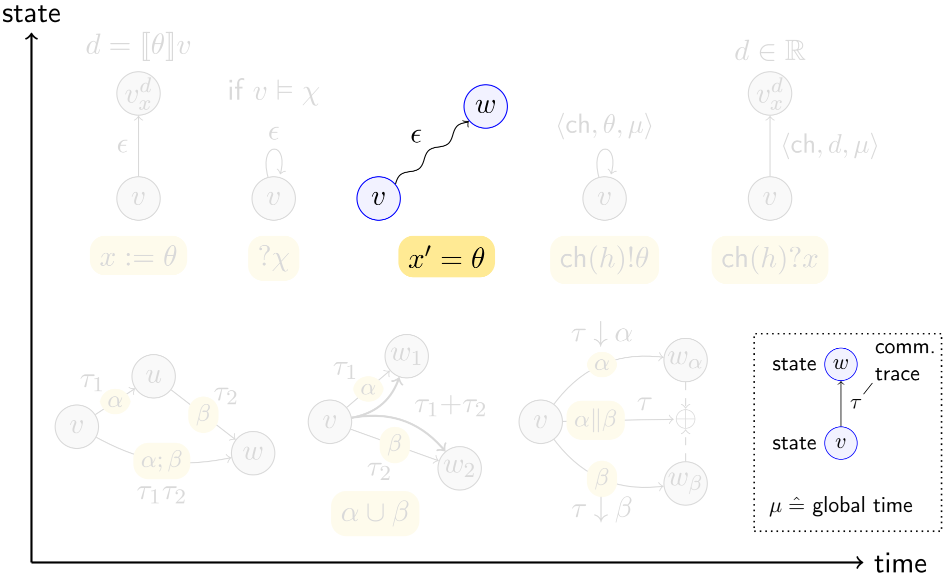
Semantics of Communicating Hybrid Programs



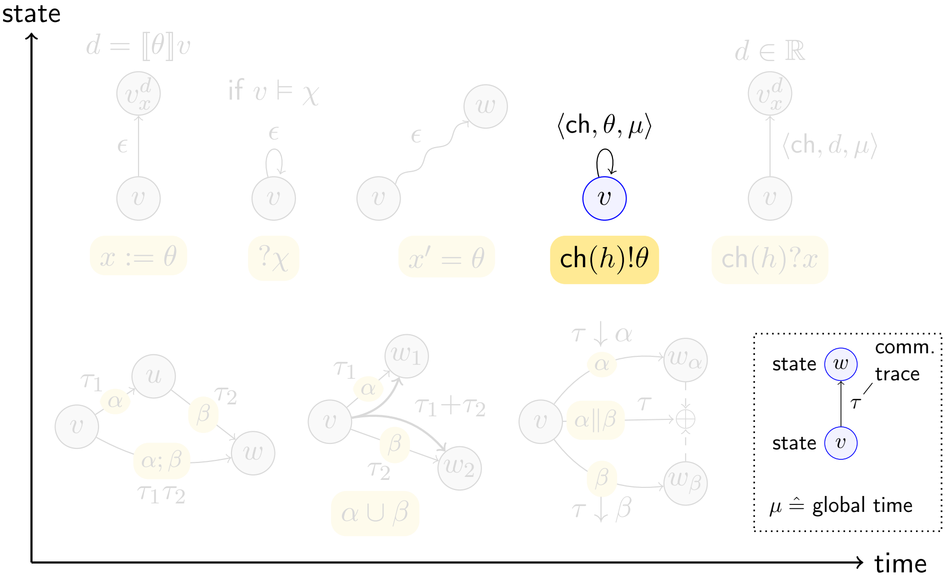
Semantics of Communicating Hybrid Programs



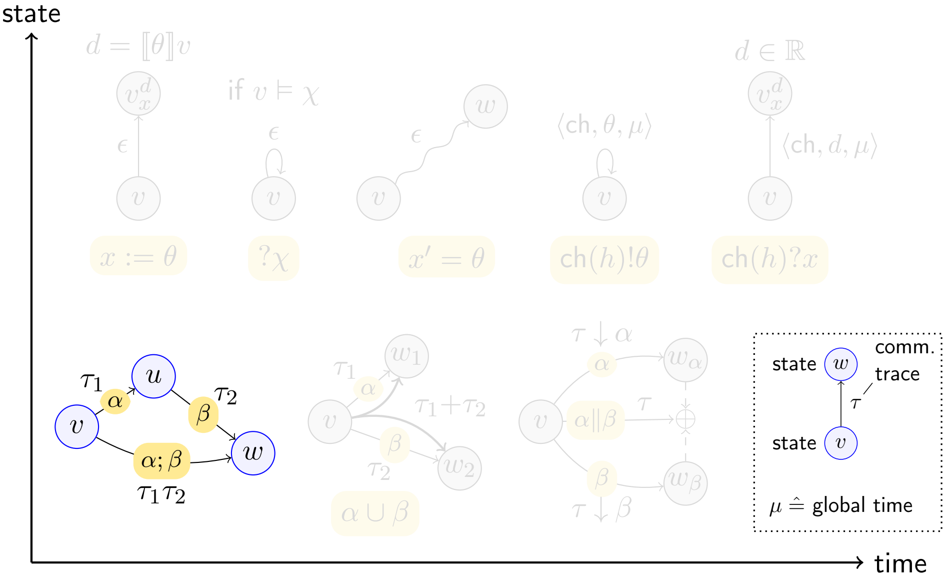
Semantics of Communicating Hybrid Programs



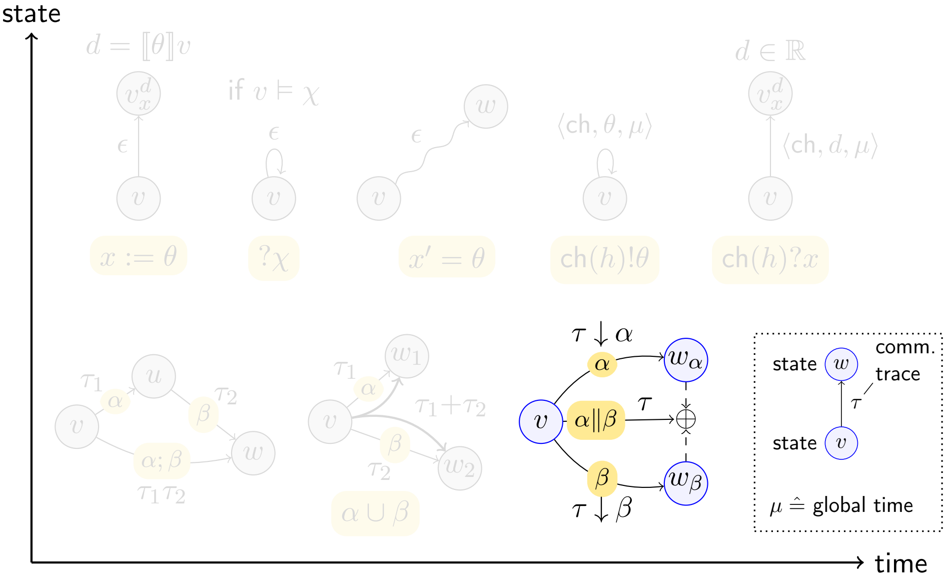
Semantics of Communicating Hybrid Programs



Semantics of Communicating Hybrid Programs



Semantics of Communicating Hybrid Programs



Axiomatization of $d\mathcal{L}_{\mathsf{CHP}}$

Axiom (one formula)

modulo symbolic (co)finite sets

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

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

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

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

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

Axiom schema (∞ formulas)

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

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

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

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

(where h_0 is fresh)

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

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

Axiomatization of $d\mathcal{L}_{\mathsf{CHP}}$

Axiom (one formula)

modulo symbolic (co)finite sets

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

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

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

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

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

Axiom schema (∞ formulas)

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

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

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

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

(where h_0 is fresh)

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

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

Axiomatization of $d\mathcal{L}_{\mathsf{CHP}}$

Axiom (one formula)

modulo symbolic (co)finite sets

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

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

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

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

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

$\xrightarrow[\text{substitution}]{\text{uniform}}$

Axiom schema (∞ formulas)

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

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

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

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

(where h_0 is fresh)

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

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

Axiomatization of $d\mathcal{L}_{\mathsf{CHP}}$

Axiom (one formula)

modulo symbolic (co)finite sets

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

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

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

$\quad \leftrightarrow \forall h_0\,(h_0 = h \cdot \langle \mathsf{ch}, \theta, \mu\rangle \to p(\mathsf{ch}, h_0))$

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

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

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

$\xrightarrow[\text{substitution}]{\text{uniform}}$

Axiom schema (∞ formulas)

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

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

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

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

$\quad \leftrightarrow \forall h_0\,(h_0 = h \cdot \langle \mathsf{ch}, \theta, \mu\rangle \to \psi(h_0))$

(where h_0 is fresh)

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

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

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

Axiomatization of $d\mathcal{L}_{\mathsf{CHP}}$

Axiom (one formula)

modulo symbolic (co)finite sets

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

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

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

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

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

implementation by object instances

$$\xrightarrow[\text{substitution}]{\text{uniform}}$$

Axiom schema (∞ formulas)

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

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

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

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

(where h_0 is fresh)

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

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

$\searrow$ kLOC

algorithmic implementation

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

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

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

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

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

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

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

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

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

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**

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

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \mathsf{US}$$

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

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

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

Uniform substitution is sound if

(B I) it never ariables or **channel access** into a c riable or channel is **written**

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

Don't release the context from synchronization!

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\,\text{US}$$

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

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

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

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

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

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

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

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

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**

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

free in a context where it is bound

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

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

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

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

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**

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

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\,(\star\star) \qquad \underset{\text{per branch}}{\overset{\text{replace by}}{\rightsquigarrow}} \qquad [\alpha]\psi \to [\alpha \parallel \beta]\psi \ (\star)$$

$\boxed{(\star)\ \beta \text{ does not affect } \psi}$

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\,(\star\star) \quad \overset{\text{replace by}}{\underset{\text{per branch}}{\rightsquigarrow}} \quad [\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \ (\star)$$

Theorem

$(\star)$ β does not affect ψ

The parallel injection axiom is sound:

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

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

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\ (\star\star) \quad \underset{\text{per branch}}{\overset{\text{replace by}}{\rightsquigarrow}} \quad [\alpha]\psi \to [\alpha \parallel \beta]\psi\ (\star)$$

Theorem

$(\star)$ β does not affect ψ

The parallel injection axiom is sound:

$$[a(\!|Y_a, \bar{z}_a|\!)]p(Y, \bar{z}) \to [a(\!|Y_a, \bar{z}_a|\!) \parallel_{\mathit{wf}} \boxed{b(\!|Y_b \cap (Y^\complement \cup Y_a), \bar{z}^\complement|\!)}]p(Y, \bar{z})$$

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

$$\frac{[a(\!|\{\mathsf{ch}\}, h|\!)]p(\mathsf{gh}, h) \to [a(\!|\{\mathsf{ch}\}, h|\!) \parallel_{\mathsf{wf}} b(\!|\{\mathsf{gh}\} \cap (\{\mathsf{gh}\}^\complement \cup \{\mathsf{ch}\}), \{h\}^\complement|\!)]p(\mathsf{gh}, h)}{[\mathsf{ch}(h)!1]|h \downarrow \mathsf{gh}| = 1 \to [\mathsf{ch}(h)!1 \parallel \mathsf{gh}(h)!2]|h \downarrow \mathsf{gh}| = 1}$$

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\ (\star\star) \quad \underset{\text{per branch}}{\overset{\text{replace by}}{\rightsquigarrow}} \quad [\alpha]\psi \to [\alpha \parallel \beta]\psi\ (\star)$$

Theorem

$(\star)$ β does not affect ψ

The parallel injection axiom is sound:

$$[a(\!|Y_a, \bar{z}_a|\!)]p(Y, \bar{z}) \to [a(\!|Y_a, \bar{z}_a|\!) \parallel_{\mathit{wf}} \boxed{b(\!|Y_b \cap (Y^{\complement} \cup Y_a), \bar{z}^{\complement}|\!)}]p(Y, \bar{z})$$

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

$$\frac{[a(\!|\{\mathsf{ch}\}, h|\!)]p(\mathsf{gh}, h) \to [a(\!|\{\mathsf{ch}\}, h|\!) \parallel_{\mathsf{wf}} b(\!|\{\mathsf{gh}\} \cap (\{\mathsf{gh}\}^{\complement} \cup \{\mathsf{ch}\}), \{h\}^{\complement}|\!)]p(\mathsf{gh}, h)}{[\mathsf{ch}(h)!1]|h \downarrow \mathsf{gh}| = 1 \to [\mathsf{ch}(h)!1 \parallel \mathsf{gh}(h)!2]|h \downarrow \mathsf{gh}| = 1}$$

↯ clash due to (B II)

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\ (\star\star) \quad \underset{\text{per branch}}{\overset{\text{replace by}}{\rightsquigarrow}} \quad [\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi\ (\star)$$

Theorem

$(\star)$ β does not affect ψ

The parallel injection axiom is sound:

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

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

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

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\;(\star\star) \quad \xrightarrow[\text{per branch}]{\text{replace by}} \quad [\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi \;(\star)$$

Theorem

(⋆) β does not affect ψ

The parallel injection axiom is sound:

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

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

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

Parallel Injection Axiom

$$\frac{[\alpha]\phi \qquad [\beta]\psi}{[\alpha \parallel \beta](\phi \wedge \psi)}\ (\star\star) \qquad \overset{\text{replace by}}{\underset{\text{per branch}}{\rightsquigarrow}} \qquad [\alpha]\psi \rightarrow [\alpha \parallel \beta]\psi\ (\star)$$

($\star$) β does not affect ψ

Theorem

The parallel injection axiom is sound:

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

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

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

↯ 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 **axiom + uniform substitution**!

Theorem

($\star$) β does not affect ψ

The parallel injection axiom is sound:

$$[a(\!|Y_a, \bar{z}_a|\!)]p(Y, \bar{z}) \to [a(\!|Y_a, \bar{z}_a|\!) \parallel_{\mathit{wf}} \boxed{b(\!|Y_b \cap (Y^{\complement} \cup Y_a), \bar{z}^{\complement}|\!)}]p(Y, \bar{z})$$

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

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

provided for each operation $\otimes(e)$ and program constant $a\llparenthesis Y, \bar{z}\rrparenthesis$ in ϕ:

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

(B II) $\mathsf{BV}(\sigma a) \subseteq \mathsf{BV}(a\llparenthesis Y, \bar{z}\rrparenthesis)$ *and* $\mathsf{CN}(\sigma a) = \mathsf{CN}(a\llparenthesis Y, \bar{z}\rrparenthesis)$

Uniform substitution is sound if

(B I) it never introduces **free vari** **cess** into a **context** wh s **written**

(B II) it nev les or **writes channels** scope

Binding free parameters sentences you to logic jail!

Application of Uniform Substitution

substitution σ

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

$$\begin{aligned}
\sigma^U(e_1 \sim e_2) &\equiv \sigma^U(e_1) \sim \sigma^U(e_2) \\
\sigma^U(p(Y, e)) &\equiv \{\cdot \mapsto \sigma^U(e \downarrow Y)\}^{\emptyset}(\sigma p(\cdot)) && \text{if } (\mathsf{FV}(\sigma p(\cdot)) \cup \mathsf{CN}(\sigma p(\cdot))) \cap U = \emptyset \\
\sigma^U(\neg\varphi) &\equiv \neg\sigma^U(\varphi) \\
\sigma^U(\varphi \wedge \psi) &\equiv \sigma^U(\varphi) \wedge \sigma^U(\psi) \\
\sigma^U(\forall z\, \varphi) &\equiv \forall z\, \sigma^{U \cup \{z\}}(\varphi) \\
\sigma^U([\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi) &\equiv [\sigma_Z^{U,\emptyset}(\alpha)]_{\{\sigma^Z(\mathsf{A}),\sigma^Z(\mathsf{C})\}}\sigma^Z(\psi)
\end{aligned}$$

$$\begin{aligned}
\sigma^U_{U \cup \mathsf{BV}(\sigma a) \cup \mathsf{CN}(\sigma a)}(a\llparenthesis Y, \bar{z}\rrparenthesis) &\equiv \sigma a && \text{if } \mathsf{BV}(\sigma a) \subseteq \bar{z} \text{ and } \mathsf{CN}(\sigma a) = Y \\
\sigma^U_{U \cup \{x\}}(x := \theta) &\equiv x := \sigma^U(\theta) \\
\sigma^U_Z(\{x' = \theta\}) &\equiv \{x' = \sigma^U(\theta)\} && \text{with } Z = U \cup \{x, x', \mu, \mu'\} \\
\sigma^U_{U \cup \{\mathsf{ch}, h\}}(\mathsf{ch}(h)!\theta) &\equiv \mathsf{ch}(h)!\sigma^U(\theta) \\
\sigma^U_{U \cup \{\mathsf{ch}, h, x\}}(\mathsf{ch}(h)?x) &\equiv \mathsf{ch}(h)?x \\
\sigma^U_{B \cup Z}(\alpha \cup \beta) &\equiv \sigma^U_B(\alpha) \cup \sigma^U_Z(\beta) \\
\sigma^U_Z(\alpha; \beta) &\equiv \sigma^U_B(\alpha); \sigma^B_Z(\beta) \\
\sigma^U_{B \cup Z}(\alpha \parallel \beta) &\equiv \sigma^U_B(\alpha) \parallel \sigma^U_Z(\beta)
\end{aligned}$$

Implementation of

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

by a canonical recursion

Application of Uniform Substitution

substitution σ

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

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

taboo

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

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

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

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

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

$\sigma^U_{U \cup \mathsf{BV}(\sigma a) \cup \mathsf{CN}(\sigma a)}(a\llparenthesis Y, \bar{z}\rrparenthesis) \equiv \sigma a$ if $\mathsf{BV}(\sigma a) \subseteq \bar{z}$ and $\mathsf{CN}(\sigma a) = Y$

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

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

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

$$\sigma^U_{U \cup \{\mathsf{ch}, h, x\}}(\mathsf{ch}(h)?x) \equiv \mathsf{ch}(h)?x$$

$$\sigma^U_{B \cup Z}(\alpha \cup \beta) \equiv \sigma^U_B(\alpha) \cup \sigma^U_Z(\beta)$$

$$\sigma^U_Z(\alpha; \beta) \equiv \sigma^U_B(\alpha); \sigma^B_Z(\beta)$$

$$\sigma^U_{B \cup Z}(\alpha \parallel \beta) \equiv \sigma^U_B(\alpha) \parallel \sigma^U_Z(\beta)$$

Implementation of $\dfrac{\phi}{\sigma\phi}$ US (B I) + (B II)

by a canonical recursion

Application of Uniform Substitution

substitution σ

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

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

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

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

bound

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

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

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

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

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

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

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

$$\sigma^U_{U \cup \{\mathsf{ch}, h, x\}}(\mathsf{ch}(h)?x) \equiv \mathsf{ch}(h)?x$$

$$\sigma^U_{B \cup Z}(\alpha \cup \beta) \equiv \sigma^U_B(\alpha) \cup \sigma^U_Z(\beta)$$

$$\sigma^U_Z(\alpha; \beta) \equiv \sigma^U_B(\alpha); \sigma^B_Z(\beta)$$

$$\sigma^U_{B \cup Z}(\alpha \parallel \beta) \equiv \sigma^U_B(\alpha) \parallel \sigma^U_Z(\beta)$$

Implementation of

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

by a canonical recursion

Application of Uniform Substitution

substitution σ

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

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

$$\sigma^U(p(Y,e)) \equiv \underbrace{\{\cdot \mapsto \sigma^U(e \downarrow Y)\}^\emptyset}_{\text{recursive substitution}}(\sigma p(\cdot)) \quad \underbrace{\text{if } (\mathsf{FV}(\sigma p(\cdot)) \cup \mathsf{CN}(\sigma p(\cdot))) \cap U = \emptyset}_{\text{does } \sigma p(\cdot) \text{ respect taboo } U\text{?}}$$

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

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

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

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

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

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

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

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

$$\sigma^U_{U \cup \{\mathsf{ch}, h, x\}}(\mathsf{ch}(h)?x) \equiv \mathsf{ch}(h)?x$$

$$\sigma^U_{B \cup Z}(\alpha \cup \beta) \equiv \sigma^U_B(\alpha) \cup \sigma^U_Z(\beta)$$

$$\sigma^U_Z(\alpha;\beta) \equiv \sigma^U_B(\alpha); \sigma^B_Z(\beta)$$

$$\sigma^U_{B \cup Z}(\alpha \parallel \beta) \equiv \sigma^U_B(\alpha) \parallel \sigma^U_Z(\beta)$$

Implementation of

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

by a canonical recursion

Application of Uniform Substitution

substitution σ

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

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

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

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

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

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

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

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

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

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

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

$$\sigma^U_{U \cup \{\mathsf{ch},h,x\}}(\mathsf{ch}(h)?x) \equiv \mathsf{ch}(h)?x$$

$$\sigma^U_{B \cup Z}(\alpha \cup \beta) \equiv \sigma^U_B(\alpha) \cup \sigma^U_Z(\beta)$$

$$\sigma^U_Z(\alpha; \beta) \equiv \sigma^U_B(\alpha); \sigma^B_Z(\beta)$$

input

output

$$\sigma^U_{B \cup Z}(\alpha \parallel \beta) \equiv \sigma^U_B(\alpha) \parallel \sigma^U_Z(\beta)$$

Implementation of

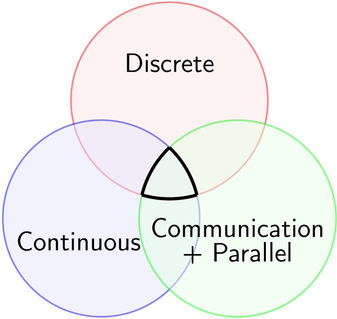
$$\frac{\phi}{\sigma\phi}\ \text{US} \qquad \text{(B I) + (B II)}$$

by a canonical recursion

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

Dynamic logic of CHPs

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

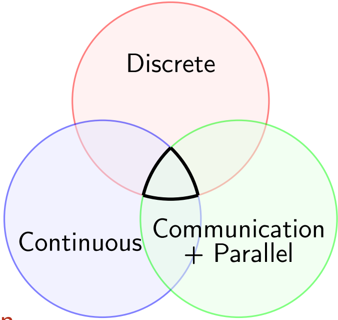


Uniform Substitution for $d\mathcal{L}_{\text{CHP}}$

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

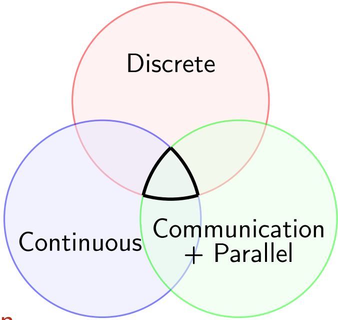


Uniform Substitution for $d\mathcal{L}_{\mathsf{CHP}}$

Dynamic logic of CHPs

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

- Uniform substitution for $d\mathcal{L}_{\mathsf{CHP}}$ that operates linearly in the formulas
- Modular soundness argument
- Modular, thus smaller, prover implementation
- Implementation in KeYmaera X:
  Ongoing effort shows promising progress

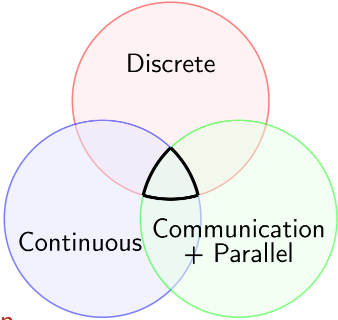


Uniform Substitution for $d\mathcal{L}_{\mathsf{CHP}}$

Dynamic logic of CHPs

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

- Uniform substitution for $d\mathcal{L}_{\mathsf{CHP}}$ that operates linearly in the formulas
- Modular soundness argument
- Modular, thus smaller, prover implementation
- Implementation in KeYmaera X: Ongoing effort shows promising progress
- All parallel reasoning reduces to multiple uses of the simple parallel injection axiom
- Discrete parallelism benefits as well



References

📄 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 proofsystem.
In *ICALP*, pages 509–519, 1985.

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \text{US}$$

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

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

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

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**

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

free in a context where it is bound

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

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

Theorem (substitution σ maps symbols to terms, formulas, or programs)

$$\frac{\phi}{\sigma\phi}\ \mathsf{US}$$

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

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

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

Uniform substitution is sound if

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

$$\frac{[a(\!|\emptyset, V_{\mathbb{R}}|\!)]_{\{\mathsf{A},\mathsf{C}\}}\mathsf{P} \leftrightarrow \mathsf{C} \land (\mathsf{A} \rightarrow [a(\!|\emptyset, V_{\mathbb{R}}|\!)]\mathsf{P})}{[\mathsf{ch}(h)!\theta]_{\{\mathsf{true}, |h \downarrow \mathsf{ch}| = 0\}}\, x = 0 \leftrightarrow |h \downarrow \mathsf{ch}| = 0 \land (\mathsf{true} \rightarrow [\mathsf{ch}(h)!\theta]x = 0)}\ ↯\,\text{clash}$$

free in a context
where it is bound

A, C, and P may mention channels

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

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

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

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

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

$$I[\![\{x' = \theta \,\&\, \chi\}]\!] = \perp_\mathcal{D} \cup \big\{(v, \epsilon, \varphi(s)) \mid v = \varphi(0) \text{ on } \{\mu', x'\}^\complement,$$
$$\text{and } \varphi(\zeta) = \varphi(0) \text{ on } \{x, x', \mu, \mu'\}^\complement, \text{ and } I\varphi(\zeta) \vDash \mu' = 1 \wedge x' = \theta \wedge \chi$$
$$\text{for all } \zeta \in [0, s] \text{ anda solution } \varphi : [0, s] \to \mathcal{S} \text{ with } \varphi(\zeta)(z') = \frac{d\varphi(t)(z)}{dt}(\zeta)$$
$$\text{for } z \in \{x, \mu\}\big\}$$

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

Program Semantics - Part II

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

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

$$I\llbracket \alpha \cup \beta \rrbracket = I\llbracket\alpha\rrbracket \cup I\llbracket\beta\rrbracket$$

$$I\llbracket \alpha;\beta \rrbracket = I\llbracket\alpha\rrbracket \mathbin{\hat{\circ}} I\llbracket\beta\rrbracket \overset{\mathsf{def}}{=} (I\llbracket\alpha\rrbracket)_\perp \cup (I\llbracket\alpha\rrbracket \triangleright I\llbracket\beta\rrbracket)$$

$$I\llbracket \alpha^* \rrbracket = \bigcup_{n\in\mathbb{N}} (I\llbracket\alpha\rrbracket)^n = \bigcup_{n\in\mathbb{N}} I\llbracket\alpha^n\rrbracket \quad \text{where } \alpha^0 \equiv ?\mathrm{T} \text{ and } \alpha^{n+1} = \alpha;\alpha^n$$

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

Static Semantics

Definition (Static semantics)

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

$$\begin{aligned}
\mathsf{FV}(e) &= \{z \in V \mid \exists I, v, \tilde{v} : v = \tilde{v} \text{ on } \{z\}^{\complement} \text{ and } Iv[\![e]\!] \neq I\tilde{v}[\![e]\!]\} \\
\mathsf{CN}(e) &= \{\mathsf{ch} \in \Omega \mid \exists I, v, \tilde{v} : v \downarrow \{\mathsf{ch}\}^{\complement} = \tilde{v} \downarrow \{\mathsf{ch}\}^{\complement} \text{ and } Iv[\![e]\!] \neq I\tilde{v}[\![e]\!]\} \\
\mathsf{FV}(\alpha) &= \{z \in V \mid \exists I, v, \tilde{v}, \tau, w : v = \tilde{v} \text{ on } \{z\}^{\complement} \text{ and } (v, \tau, w) \in I[\![\alpha]\!], \\
&\qquad \text{and there is no } (\tilde{v}, \tilde{\tau}, \tilde{w}) \in I[\![\alpha]\!] : \tilde{\tau} = \tau \text{ and } w = \tilde{w} \text{ on } \{z\}^{\complement}\} \\
\mathsf{BV}(\alpha) &= \{z \in V \mid \exists I, (v, \tau, w) \in I[\![\alpha]\!] : w \neq \bot \text{ and } (w \cdot \tau)(z) \neq v(z)\} \\
\mathsf{CN}(\alpha) &= \{\mathsf{ch} \in \Omega \mid \exists I, (v, \tau, w) \in I[\![\alpha]\!] : \tau \downarrow \{\mathsf{ch}\} \neq \epsilon\}
\end{aligned}$$

Communication-aware Coincidence

Lemma (Bound effect property)

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

Lemma (Coincidence for terms and formulas)

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

Lemma (Coincidence for programs)

$\mathsf{FV}(\alpha)$ *is the smallest set with the coincidence property for program* α*: If* $v = \tilde{v}$ *on* $X \supseteq \mathsf{FV}(\alpha)$*, 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 (*$w = \bot$ *iff* $\tilde{w} = \bot$*).*

Soundness argument

Lemma (Semantic uniform substitution)

Terms e, and formulas ϕ, and programs α evaluate equally under substitution σ^U and adjoint interpretation $\sigma^*_w I$ for all U-variations v of w:

$$I\llbracket\sigma^U(e)\rrbracket = \sigma^*_w I\llbracket e\rrbracket$$

$$Iv \vDash \sigma^U(\phi) \text{ iff } \sigma^*_w Iv \vDash \phi$$

$$(v, \tau, o) \in I\llbracket\sigma^U_Z(\alpha)\rrbracket \text{ iff } (v, \tau, o) \in \alpha\llbracket\phi\rrbracket$$

$$\begin{tikzcd}
e \arrow[r, mapsto, "\sigma^U(\cdot)"] \arrow[rrdd, mapsto, bend right] & \sigma^U(e) \arrow[r, mapsto, "I\llbracket\cdot\rrbracket"] \arrow[d, mapsto] & I\llbracket\sigma^U(e)\rrbracket \arrow[ld, mapsto] \arrow[dd, equal] \\
 & \sigma^*_w I & \\
 & & \sigma^*_w I\llbracket e\rrbracket
\end{tikzcd}$$

Axiomatization - Part I

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

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

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

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

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

$[\mathsf{ch}!]_{\mathsf{AC}}$ $\quad [\mathsf{ch}(h)!g^{\mathbb{R}}]_{\{\widehat{r},\widehat{q}\}}\widehat{p} \leftrightarrow \widehat{q} \land \Big(\widehat{r} \to [\mathsf{ch}(h)!g^{\mathbb{R}}]\big(\widehat{q} \land (\widehat{r} \to \widehat{p})\big)\Big)$

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

$\mathsf{P}_j \equiv p_j(Y, \bar{z})$, and $\mathsf{R}_j \equiv r_j(Y, \bar{h})$, and $\mathsf{Q}_j \equiv q_j(Y, \bar{h})$, and $\widehat{\chi} \equiv \chi(\mathsf{ch}, h)$, 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.

Axiomatization - Part II

$[;]_{\mathsf{AC}}$	$[a;b]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow [a]_{\{\mathsf{R},\mathsf{Q}\}}[b]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P}$
$[\cup]_{\mathsf{AC}}$	$[a \cup b]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow [a]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \land [b]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P}$
$[^*]_{\mathsf{AC}}$	$[a^*]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow [a^0]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \land [a]_{\{\mathsf{R},\mathsf{Q}\}}[a^*]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P}$
I_{AC}	$[a^*]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow [a^0]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \land [a^*]_{\{\mathsf{R},\mathsf{true}\}}(\mathsf{P} \rightarrow [a]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P})$

$\mathsf{P}_j \equiv p_j(Y, \bar{z})$, and $\mathsf{R}_j \equiv r_j(Y, \bar{h})$, and $\mathsf{Q}_j \equiv q_j(Y, \bar{h})$, and $\widehat{\chi} \equiv \chi(\mathsf{ch}, h)$, 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.

Axiomatization - Part III

$[]_{\top,\top}$	$[a]\mathsf{P} \leftrightarrow [a]_{\{\mathsf{true},\mathsf{true}\}}\mathsf{P}$
$[\epsilon]_{\mathsf{AC}}$	$[a(\!\vert\emptyset, V_{\mathbb{R}}\vert\!)]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow \mathsf{Q} \wedge (\mathsf{R} \rightarrow [a(\!\vert\emptyset, V_{\mathbb{R}}\vert\!)]\mathsf{P})$
$[]_{\mathsf{WA}}$	$[a]_{\{\mathsf{true},\mathsf{W_A}\}}\mathsf{true} \wedge [a]_{\{\mathsf{R}_1\wedge\mathsf{R}_2,\mathsf{Q}_1\wedge\mathsf{Q}_2\}}\mathsf{P} \rightarrow [a]_{\{\mathsf{R},\mathsf{Q}_1\wedge\mathsf{Q}_2\}}\mathsf{P}$
$\mathsf{W}[]_{\mathsf{AC}}$	$[a]_{\{\mathsf{R},\mathsf{Q}\}}\mathsf{P} \leftrightarrow \mathsf{Q} \wedge [a]_{\{\mathsf{R},\mathsf{Q}\}}(\mathsf{Q} \wedge (\mathsf{R} \rightarrow \mathsf{P}))$
K_{AC}	$[a]_{\{\mathsf{R},\mathsf{Q}_1\rightarrow\mathsf{Q}_2\}}(\mathsf{P}_1 \rightarrow \mathsf{P}_2) \rightarrow ([a]_{\{\mathsf{R},\mathsf{Q}_1\}}\mathsf{P}_1 \rightarrow [a]_{\{\mathsf{R},\mathsf{Q}_2\}}\mathsf{P}_2)$

$\mathsf{P}_j \equiv p_j(Y, \bar{z})$, and $\mathsf{R}_j \equiv r_j(Y, \bar{h})$, and $\mathsf{Q}_j \equiv q_j(Y, \bar{h})$, and $\widehat{\chi} \equiv \chi(\mathsf{ch}, h)$, 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.

Axiomatization - Part IV

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

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

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

$$\text{CE}\quad \frac{\mathsf{P}_1 \leftrightarrow \mathsf{P}_2}{C(\mathsf{P}_1)\leftrightarrow C(\mathsf{P}_2)}$$

$\mathsf{P}_j \equiv p_j(Y, \bar{z})$, and $\mathsf{R}_j \equiv r_j(Y, \bar{h})$, and $\mathsf{Q}_j \equiv q_j(Y, \bar{h})$, and $\widehat{\chi} \equiv \chi(\mathsf{ch}, h)$, 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 realeses dh from synchronization!

$$\frac{[a\llparenthesis \mathsf{ch} \rrparenthesis \cup (?\mathsf{false}; c\llparenthesis \mathsf{dh} \rrparenthesis)]p(\mathsf{dh}) \rightarrow [a\llparenthesis \mathsf{ch} \rrparenthesis \cup (?\mathsf{false}; c\llparenthesis \mathsf{dh} \rrparenthesis) \parallel \mathsf{dh}?x]p(\mathsf{dh})}{[\mathsf{ch}(h)!\theta \cup (?\mathsf{false}; ?\mathsf{true})]\varphi(\mathsf{dh}) \rightarrow [\mathsf{ch}(h)!\theta \cup (?\mathsf{false}; ?\mathsf{true}) \parallel \underbrace{\mathsf{dh}?x]\varphi(\mathsf{dh}}_{\text{free in a context where it is bound}})}$$

Luckily uniform substitution sorts it out by a ↯ clash.

Parallel Decomposition

$$
\dfrac{
  \mathsf{G_{AC}}\ \dfrac{\vdash \mathsf{W_A} \land \mathsf{true}}{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{true},\mathsf{W_A}\}}\mathsf{true}}
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{\vdots}{\Gamma \vdash [\alpha]_{\{\mathsf{A_1},\mathsf{C_1}\}}\psi_1}
      }{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{A_1},\mathsf{C_1}\}}\psi_1}\ [\parallel\_]_{\mathsf{AC}}
    }{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{A_1}\land\mathsf{A_2},\mathsf{C_1}\}}\psi_1}\ \mathsf{M}[\cdot]_{\mathsf{AC}}
    \qquad \vdots
  }{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{A_1}\land\mathsf{A_2},\mathsf{C_1}\land\mathsf{C_2}\}}(\psi_1 \land \psi_2)}\ []_{\mathsf{AC}}\land
}{
  \dfrac{
    \dfrac{
      \dfrac{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{true},\mathsf{W_A}\}}\mathsf{true} \land [\alpha \parallel \beta]_{\{\mathsf{A_1}\land\mathsf{A_2},\mathsf{C_1}\land\mathsf{C_2}\}}(\psi_1 \land \psi_2)}{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{true},\mathsf{C_1}\land\mathsf{C_2}\}}(\psi_1 \land \psi_2)}\ []\mathsf{WA}
    }{\Gamma \vdash [\alpha \parallel \beta]_{\{\mathsf{true},\mathsf{true}\}}\psi}\ \mathsf{M}[\cdot]_{\mathsf{AC}}
  }{\Gamma \vdash [\alpha \parallel \beta]\psi}\ []_{\top,\top}
}\ \land\mathsf{R}
$$

$$\mathsf{W_A} \equiv (\mathsf{A_2} \to \mathsf{C_1}) \land (\mathsf{A_1} \to \mathsf{C_2})$$