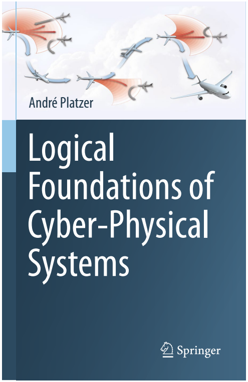
18: Axioms & Uniform Substitutions

Logical Foundations of Cyber-Physical Systems



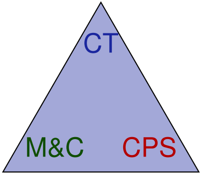
André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Outline

axiom vs. axiom schema
algorithmic impact of philosophical difference
local meaning of axioms
generic axioms like generic points
uniform substitution



meaning of differentials

parsimonious CPS reasoning impl.
modular impl. of logic $\|$ prover

Outline

Part I

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

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

$[\cup]\ [\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$

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

$[^*]\ [\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$

$\mathsf{K}\ [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

$\mathsf{I}\ [\alpha^*]\phi \leftrightarrow \phi \land [\alpha^*](\phi \rightarrow [\alpha]\phi)$

$\mathsf{V}\ \phi \rightarrow [\alpha]\phi$

$[']\ [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\,[x := y(t)]\phi$

Part I

$[{:=}]\ [x := \theta]\phi(x) \leftrightarrow \phi(\theta)$ (θ free for x in ϕ)

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

$[\cup]\ [\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$

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

$[^*]\ [\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$

$\text{K}\ [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

$\text{I}\ [\alpha^*]\phi \leftrightarrow \phi \land [\alpha^*](\phi \rightarrow [\alpha]\phi)$

$\text{V}\ \phi \rightarrow [\alpha]\phi$ ($FV(\phi) \cap BV(\alpha) = \emptyset$)

$[']\ [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi$ (t fresh and $y'(t) = \theta$)

Axiom Schema

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

V $\phi \rightarrow [\alpha]\phi$

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

Axiom Schema Matches Many Formulas

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$

- $[x := x+1 \cup x' = x^2]\, x \geq 0 \leftrightarrow [x := x+1]\, x \geq 0 \land [x' = x^2]\, x \geq 0$
- $[x' = 5 \cup x' = -x]\, x^2 \geq 5 \leftrightarrow [x' = 5]\, x^2 \geq 5 \land [x' = -x]\, x^2 \geq 5$
- $[v := v+1; x' = v \cup x' = 2]x \geq 5 \leftrightarrow [v := v+1; x' = v]x \geq 5 \land [x' = 2]x \geq 4$

V $\phi \rightarrow [\alpha]\phi$

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

Axiom Schema Matches Many Formulas

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

✓ $[x := x+1 \cup x' = x^2]\, x \geq 0 \leftrightarrow [x := x+1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

✓ $[x' = 5 \cup x' = -x]\, x^2 \geq 5 \leftrightarrow [x' = 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

× $[v := v+1; x' = v \cup x' = 2]x \geq 5 \leftrightarrow [v := v+1; x' = v]x \geq 5 \wedge [x' = 2]x \geq 4$

V $\phi \rightarrow [\alpha]\phi$

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

Axiom Schema Matches Many Formulas

[∪] $[\alpha\cup\beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

Match shape $\alpha\cup\beta$

Schema variable α match

Same ϕ everywhere

$\ldots = x \ldots x^2] x \ldots [x := x+1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$\ldots = 5 \ldots]\, x^2 \ldots = 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$\ldots = v + \ldots \cup x' \ldots \leftrightarrow [v := v+1; x' = v] x \geq 5 \wedge [x' = 2] x \geq 4$

V $\phi \rightarrow [\alpha]\phi$

- $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$
- $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$
- $y \geq z \rightarrow [x' = -5]\, y \geq z$

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

Axiom Schema Matches Many Formulas

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

Match shape $\alpha \cup \beta$

Schema variable α match

Same ϕ everywhere

$= x -$ $x^2] x$ $[x := x + 1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$= 5 \cup$ $] x^2 \geq$ $= 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$= v +$ $\cup\, x'$ $\leftrightarrow [v := v+1; x' = v] x \geq 5 \wedge [x' = 2] x \geq 4$

V $\phi \rightarrow [\alpha]\phi$

- ✓ $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$
- × $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$
- ✓ $y \geq z \rightarrow [x' = -5]\, y \geq z$

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

Axiom Schema Matches Many Formulas But Not All

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

Match shape $\alpha \cup \beta$

Schema variable α match

Same ϕ everywhere

✓ $\ldots = x \ldots x^2] x \ldots [x := x+1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$\ldots = 5 \cup \ldots]\, x^2 \geq \ldots = 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$\ldots = v + \ldots \cup x' \ldots \leftrightarrow [v := v+1; x' = v] x \geq 5 \wedge [x' = 2] x \geq 4$

V $\phi \rightarrow [\alpha]\phi$ $\qquad (FV(\phi) \cap BV(\alpha) = \emptyset)$

✓ $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$

× $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$

✓ $y \geq z \rightarrow [x' = -5]\, y \geq z$

rule out by side conditions

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

- $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$
- $[x := x + y][y := 5]\, x \geq 0 \leftrightarrow [y := 5]\, x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]\, x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]\, x \geq 2b$
- $[x := x + y][x := x + 1]\, x \geq 0 \leftrightarrow [x := x + y + 1]\, x \geq 0$

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

Match shape $\alpha \cup \beta$

Schema variable α match

Same ϕ everywhere

✓ $[\ldots = x - \ldots x^2]\, x \ldots [x := x + 1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$\ldots = 5 \cup \ldots]\, x^2 \geq \ldots = 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$\ldots = v + \ldots \cup x' \ldots] \geq \ldots \leftrightarrow [v := v+1;\, x' = v]x \geq 5 \wedge [x' = 2]x \geq 4$

V $\phi \rightarrow [\alpha]\phi$ $\quad (FV(\phi) \cap BV(\alpha) = \emptyset)$

✓ $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$

× $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$

✓ $y \geq z \rightarrow [x' = -5]\, y \geq z$

rule out by side conditions

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

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$

× $[x := x + y][y := 5]\, x \geq 0 \leftrightarrow [y := 5]\, x + y \geq 0$

✓ $[y := 2b][(x := x+y;\, x' = y)^*]\, x \geq y \leftrightarrow [(x := x+2b;\, x' = 2b)^*]\, x \geq 2b$

✓ $[x := x + y][x := x + 1]\, x \geq 0 \leftrightarrow [x := x + y + 1]\, x \geq 0$

Axiom Schema Matches Many Formulas But Not All

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

$= x$ … $x^2]$ … $[x := x+1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$= 5$ … $]\, x^2 \geq$ … $= 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$= v+$ … $\cup x'$ … $\leftrightarrow [v := v+1; x' = v] x \geq 5 \wedge [x' = 2] x \geq 4$

Match shape $\alpha \cup \beta$

Schema variable α match

Same ϕ everywhere

V $\phi \rightarrow [\alpha]\phi$ $(FV(\phi) \cap BV(\alpha) = \emptyset)$

✓ $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$

× $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$

✓ $y \geq z \rightarrow [x' = -5]\, y \geq z$

rule out by side conditions

$[:=]$ $[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$ (θ free for x in ϕ)

✓ … $y]\, x \leq y^2$ … $\leq y^2$

× … $y][y := 5]$ … $:= 5]\, x + y \geq 0$

✓ … $(x := x+y$ … $]\, x \geq y \leftrightarrow [(x := x+2b; x'$ … $\geq 2b$

✓ … $y][x := x$ … $\leftrightarrow [x := x+y+1]\, x \geq 0$

Match all free x occurrences

Replace by θ everywhere

no x occurrence where θ bound

Axiom Schema Matches Many Formulas But Not All

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi$

Algorithm

Match shape $\alpha \cup \beta$

Schema variable α match

Same ϕ everywhere

$= x$ ... $x^2]$ ... $x := x+1]\, x \geq 0 \wedge [x' = x^2]\, x \geq 0$

$= 5$ ... $]\, x^2 \geq$ ... $= 5]\, x^2 \geq 5 \wedge [x' = -x]\, x^2 \geq 5$

$= v+$ ... $\cup x'$ ... $\leftrightarrow [v := v+1; x' = v]x \geq 5 \wedge [x' = 2]x \geq 4$

V $\phi \rightarrow [\alpha]\phi$ $\quad (FV(\phi) \cap BV(\alpha) = \emptyset)$

✓ $y \geq 0 \rightarrow [x' = -5]\, y \geq 0$

× $x \geq 0 \rightarrow [x' = -5]\, x \geq 0$

✓ $y \geq z \rightarrow [x' = -5]\, y \geq z$

rule out by side conditions

[:=] $[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$ $\quad (\theta$ free for x in $\phi)$

Match all free x occurrences

Replace by θ everywhere

no x occurrence where θ bound

✓ ... $y]\, x \leq y^2$ ... $\leq y^2$

× ... $y][y := 5]$ ... $:= 5]\, x + y \geq 0$

✓ ... $(x := x+y$ ... $]\, x \geq y \leftrightarrow [(x := x+2b; x'$ ... $\geq 2b$

✓ ... $y][x := x$ ... $\leftrightarrow [x := x+y+1]\, x \geq 0$

Axiom Schema Side Conditions: ODE Solving

$[']\ [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi$

Axiom Schema Side Conditions: ODE Solving

$['] \; [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\,[x := y(t)]\phi$ $\qquad$ (t fresh and $y'(t) = \theta$)

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: $y(\cdot)$ solves the ODE $y'(t) = \theta$ with $y(\cdot)$ plugged in for x in term θ
3. Initial value check: $y(\cdot)$ solves the symbolic IVP $y(0) = x$

Axiom Schema Side Conditions: ODE Solving

$[']$ $[x' = \theta]\phi \leftrightarrow \forall t \geq 0\, [x := y(t)]\phi$ $\quad$ (t fresh and $y'(t) = \theta$)

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: $y(\cdot)$ solves the ODE $y'(t) = \theta$ with $y(\cdot)$ plugged in for x in term θ
3. Initial value check: $y(\cdot)$ solves the symbolic IVP $y(0) = x$
4. $y(\cdot)$ covers all solutions parametrically

Axiom Schema Side Conditions: ODE Solving

$[']$ $[x' = \theta]\phi \leftrightarrow \forall t \geq 0\, [x := y(t)]\phi$ $\quad$ (t fresh and $y'(t) = \theta$)

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: $y(\cdot)$ solves the ODE $y'(t) = \theta$ with $y(\cdot)$ plugged in for x in term θ
3. Initial value check: $y(\cdot)$ solves the symbolic IVP $y(0) = x$
4. $y(\cdot)$ covers all solutions parametrically
5. x' cannot occur free in ϕ

Axiom Schema Side Conditions: ODE Solving

$[']\ [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi$ $\qquad$ (t fresh and $y'(t) = \theta$)

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: $y(\cdot)$ solves the ODE $y'(t) = \theta$ with $y(\cdot)$ plugged in for x in term θ
3. Initial value check: $y(\cdot)$ solves the symbolic IVP $y(0) = x$
4. $y(\cdot)$ covers all solutions parametrically
5. x' cannot occur free in ϕ

Quite nontrivial soundness-critical side condition algorithms ...

What Axioms Want

V $\phi \rightarrow [\alpha]\phi$

What Axioms Want

V $\phi \rightarrow [\alpha]\phi$ V $p \rightarrow [a]p$

V predicate symbol p of arity 0 has no bound variable of HP a free
"Formula p has no explicit permission to depend on anything"
(except implicitly on what doesn't change in a anyhow)

V program constant symbol a could have arbitrary behavior

What Axioms Want

V $\phi \rightarrow [\alpha]\phi$

V $p \rightarrow [a]p$

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

V predicate symbol p of arity 0 has no bound variable of HP a free
"Formula p has no explicit permission to depend on anything"
(except implicitly on what doesn't change in a anyhow)

V program constant symbol a could have arbitrary behavior

What Axioms Want

V $\phi \to [\alpha]\phi$	V $p \to [a]p$
$[:=]$ $[x:=\theta]\phi(x) \leftrightarrow \phi(\theta)$	$[:=]$ $[x:=c]p(x) \leftrightarrow p(c)$

- V predicate symbol p of arity 0 has no bound variable of HP a free
  "Formula p has no explicit permission to depend on anything"
  (except implicitly on what doesn't change in a anyhow)
- $[:=]$ predicate symbol p of arity 1 has different arguments in different places
  "Formula $p(x)$ has explicit permission to depend on x"

- $[:=]$ function symbol c of arity 0 takes no arguments
- V program constant symbol a could have arbitrary behavior

[$\cup$] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

V $\phi \rightarrow [\alpha]\phi$

V $p \rightarrow [a]p$

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

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

V predicate symbol p of arity 0 has no bound variable of HP a free
"Formula p has no explicit permission to depend on anything"
(except implicitly on what doesn't change in a anyhow)

[:=] predicate symbol p of arity 1 has different arguments in different places
"Formula $p(x)$ has explicit permission to depend on x"

[:=] function symbol c of arity 0 takes no arguments

V program constant symbol a could have arbitrary behavior

What Axioms Want

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$ $[\cup]$ $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$

V $\phi \rightarrow [\alpha]\phi$ V $p \rightarrow [a]p$

$[:=]$ $[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$ $[:=]$ $[x := c]p(x) \leftrightarrow p(c)$

- V predicate symbol p of arity 0 has no bound variable of HP a free
  "Formula p has no explicit permission to depend on anything"
  (except implicitly on what doesn't change in a anyhow)
- $[:=]$ predicate symbol p of arity 1 has different arguments in different places
  "Formula $p(x)$ has explicit permission to depend on x"
- $[\cup]$ predicate symbol p of arity n takes all variables $\bar{x}$ as arguments
  "Formula $p(\bar{x})$ has explicit permission to depend on all variables $\bar{x}$"
- $[:=]$ function symbol c of arity 0 takes no arguments
- V program constant symbol a could have arbitrary behavior

Outline

Definition (Hybrid program α)

$$\alpha,\beta ::= a \mid x:=\theta \mid ?Q \mid x' = f(x)\,\&\,Q \mid \alpha\cup\beta \mid \alpha;\beta \mid \alpha^*$$

Definition (dL Formula ϕ)

$$\phi,\psi ::= p(\theta_1,\dots,\theta_k) \mid \theta\geq\eta \mid \neg\phi \mid \phi\wedge\psi \mid \forall x\,\phi \mid \exists x\,\phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Definition (Term θ)

$$\theta,\eta ::= f(\theta_1,\dots,\theta_k) \mid x \mid \theta+\eta \mid \theta\cdot\eta \mid (\theta)'$$

Differential Dynamic Logic with Interpretations: Syntax

Discrete Assign | Test Condition | Differential Equation | Nondet. Choice | Seq. Compose | Nondet. Repeat

Definition (Hybrid program α)

$$\alpha, \beta \ ::= \ a \mid x := \theta \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

Definition (dL Formula ϕ)

$$\phi, \psi \ ::= \ p(\theta_1, \ldots, \theta_k) \mid \theta \geq \eta \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Definition (Term θ)

$$\theta, \eta \ ::= \ f(\theta_1, \ldots, \theta_k) \mid x \mid \theta + \eta \mid \theta \cdot \eta \mid (\theta)'$$

All Reals | Some Reals | All Runs | Some Runs

Differential Dynamic Logic with Interpretations: Syntax

Program Symbol

Definition (Hybrid program α)

$$\alpha, \beta \ ::= \ a \mid x := \theta \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

Definition (dL Formula ϕ)

$$\phi, \psi \ ::= \ p(\theta_1, \ldots, \theta_k) \mid \theta \geq \eta \mid \neg \phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$$

Definition (Term θ)

$$\theta, \eta \ ::= \ f(\theta_1, \ldots, \theta_k) \mid x \mid \theta + \eta \mid \theta \cdot \eta \mid (\theta)'$$

Predicate Symbol

Function Symbol

Differential

Definition (Term semantics) $([\![\cdot]\!] : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R}))$

$$\begin{aligned} \omega[\![f(\theta_1,\dots,\theta_k)]\!] &= I(f)\big(\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]\big) \qquad I(f) : \mathbb{R}^k \to \mathbb{R} \text{ smooth} \\ \omega[\![(\theta)']\!] &= \sum_x \omega(x') \frac{\partial [\![\theta]\!]}{\partial x}(\omega) \end{aligned}$$

Definition (dL semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S}))$

$$\begin{aligned} [\![p(\theta_1,\dots,\theta_k)]\!] &= \{\omega : (\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]) \in I(p)\} \qquad I(p) \subseteq \mathbb{R}^k \\ [\![\langle\alpha\rangle\phi]\!] &= [\![\alpha]\!] \circ [\![\phi]\!] \end{aligned}$$

P valid iff $\omega \in [\![P]\!]$ for all states ω of all interpretations I

Definition (Program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$\begin{aligned} [\![a]\!] &= I(a) \qquad I(a) \subseteq \mathscr{S} \times \mathscr{S} \\ [\![x' = f(x) \,\&\, Q]\!] &= \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) : \varphi \models x' = f(x) \land Q\} \\ [\![\alpha \cup \beta]\!] &= [\![\alpha]\!] \cup [\![\beta]\!] \\ [\![\alpha;\beta]\!] &= [\![\alpha]\!] \circ [\![\beta]\!] \\ [\![\alpha^*]\!] &= \big([\![\alpha]\!]\big)^* = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!] \end{aligned}$$

Lemma (V vacuous axiom)

$$V \; p \rightarrow [a]p$$

Lemma ([:=] assignment axiom)

$$[:=] \;\; [x := c]p(x) \leftrightarrow p(c)$$

Lemma (V vacuous axiom)

$$V\ p \rightarrow [a]p$$

Proof.

Truth of an arity 0 predicate symbol p depends only on interpretation I.

1. I interprets p as *true*: $\omega \in [\![p]\!]$ for all ω, so $\omega \in [\![[a]p]\!]$ especially.
2. I interprets p as *false*: $\omega \notin [\![p]\!]$ for all ω, so $p \rightarrow [a]p$ vacuously. □

Lemma ([:=] assignment axiom)

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

Proof.

p is *true* of x after assigning the new value c to x ($\omega \in [\![[x := c]p(x)]\!]$) iff p is *true* of the new value c ($\omega \in [\![p(c)]\!]$). □

Outline

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$US \; \frac{\phi}{\sigma(\phi)}$$

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$

$$\text{US} \; \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$US\ \frac{\phi}{\sigma(\phi)}$$

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

Uniform Substitution: First-Order Examples

$$\frac{(\neg\neg p) \leftrightarrow p}{(\neg\neg[x' = x^2]\,x \geq 0) \leftrightarrow [x' = x^2]\,x \geq 0} \qquad \sigma = \{p \mapsto [x' = x^2]\,x \geq 0\}$$

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(x \geq 0) \leftrightarrow x \geq 0} \qquad \sigma = \{p \mapsto x \geq 0\}$$

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(y \geq 0) \leftrightarrow y \geq 0} \qquad \sigma = \{p \mapsto y \geq 0\}$$

Uniform Substitution: First-Order Examples

$$\frac{(\neg\neg p) \leftrightarrow p}{(\neg\neg[x' = x^2]\, x \geq 0) \leftrightarrow [x' = x^2]\, x \geq 0} \qquad \sigma = \{p \mapsto [x' = x^2]\, x \geq 0\}$$

Correct

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\, (x \geq 0) \leftrightarrow x \geq 0} \qquad \sigma = \{p \mapsto x \geq 0\}$$

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\, (y \geq 0) \leftrightarrow y \geq 0} \qquad \sigma = \{p \mapsto y \geq 0\}$$

$$\frac{(\neg\neg p) \leftrightarrow p}{(\neg\neg[x' = x^2]\,x \geq 0) \leftrightarrow [x' = x^2]\,x \geq 0} \qquad \sigma = \{p \mapsto [x' = x^2]\,x \geq 0\}$$

Correct

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(x \geq 0) \leftrightarrow x \geq 0} \qquad \sigma = \{p \mapsto x \geq 0\}$$

BV

Clash

FV

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(y \geq 0) \leftrightarrow y \geq 0} \qquad \sigma = \{p \mapsto y \geq 0\}$$

Uniform Substitution: First-Order Examples

$$\frac{(\neg\neg p) \leftrightarrow p}{(\neg\neg[x' = x^2]\,x \geq 0) \leftrightarrow [x' = x^2]\,x \geq 0}$$

Correct

$$\sigma = \{p \mapsto [x' = x^2]\,x \geq 0\}$$

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(x \geq 0) \leftrightarrow x \geq 0}$$

Clash

$$\sigma = \{p \mapsto x \geq 0\}$$

$$\frac{(\forall x\, p) \leftrightarrow p}{\forall x\,(y \geq 0) \leftrightarrow y \geq 0}$$

Correct

$$\sigma = \{p \mapsto y \geq 0\}$$

Uniform Substitution: Argument Examples

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2-1]x \geq x \leftrightarrow x^2-1 \geq x} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

Uniform Substitution: Argument Examples

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0}$$

Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]x \geq x \leftrightarrow x^2-1 \geq x}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

Uniform Substitution: Argument Examples

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0}$$

Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]x \geq x \leftrightarrow x^2-1 \geq x}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

Correct

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

BV Clash FV

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]x \geq x \leftrightarrow x^2-1 \geq x} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y} \qquad \sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

Uniform Substitution: Argument Examples

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0}$$

Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]x \geq x \leftrightarrow x^2-1 \geq x}$$

Clash

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1}$$

Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y}$$

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq 0 \leftrightarrow x^2-1 \geq 0}$$ Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq 0)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]x \geq x \leftrightarrow x^2-1 \geq x}$$ Clash

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq x \leftrightarrow x^2-1 \geq x^2-1}$$ Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq \cdot)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2-1]\,x \geq y \leftrightarrow x^2-1 \geq y}$$ Correct

$$\sigma = \{c \mapsto x^2-1, p(\cdot) \mapsto (\cdot \geq y)\}$$

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$US \frac{\phi}{\sigma(\phi)}$$

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \wedge [x' = v]x > 0}$$

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \text{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

If you bind a free variable, you go to logic jail!

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

$$
\begin{array}{rll}
\sigma(x) & = & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) & = & \text{for function symbol } f \in \sigma \\
 & \stackrel{\text{def}}{=} & \\
\sigma(\theta + \eta) & = & \\
\sigma((\theta)') & = & \\
\hline
\sigma(p(\theta)) & \equiv & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) & \equiv & \\
\sigma(\forall x\, \phi) & = & \\
\sigma([\alpha]\phi) & = & \\
\hline
\sigma(a) & \equiv & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) & \equiv & \\
\sigma(x' = \theta \,\&\, Q) & \equiv & \\
\sigma(?Q) & \equiv & \\
\sigma(\alpha \cup \beta) & \equiv & \\
\sigma(\alpha;\beta) & \equiv & \\
\sigma(\alpha^*) & \equiv &
\end{array}
$$

Uniform Substitution: Recursive Application

$\sigma(x) = x$		for variable $x \in \mathscr{V}$
$\sigma(f(\theta)) =$		for function symbol $f \in \sigma$
$\stackrel{\text{def}}{\equiv}$		
$\sigma(\theta + \eta) =$		
$\sigma((\theta)') =$		
$\sigma(p(\theta)) \equiv$		for predicate symbol $p \in \sigma$
$\sigma(\phi \wedge \psi) \equiv$		
$\sigma(\forall x\, \phi) =$		
$\sigma([\alpha]\phi) =$		
$\sigma(a) \equiv$		for program symbol $a \in \sigma$
$\sigma(x := \theta) \equiv$		
$\sigma(x' = \theta \,\&\, Q) \equiv$		
$\sigma(?Q) \equiv$		
$\sigma(\alpha \cup \beta) \equiv$		
$\sigma(\alpha;\beta) \equiv$		
$\sigma(\alpha^*) \equiv$		

$$
\begin{array}{rcll}
\sigma(x) & = & x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
 & \stackrel{\text{def}}{=} & \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) & = & & \\
\sigma((\theta)') & = & & \\
\hline
\sigma(p(\theta)) & \equiv & & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) & \equiv & & \\
\sigma(\forall x\, \phi) & = & & \\
\sigma([\alpha]\phi) & = & & \\
\hline
\sigma(a) & \equiv & & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) & \equiv & & \\
\sigma(x' = \theta \,\&\, Q) & \equiv & & \\
\sigma(?Q) & \equiv & & \\
\sigma(\alpha \cup \beta) & \equiv & & \\
\sigma(\alpha ; \beta) & \equiv & & \\
\sigma(\alpha^*) & \equiv & &
\end{array}
$$

Uniform Substitution: Recursive Application

$$
\begin{aligned}
\sigma(x) &= x && \text{for variable } x \in \mathcal{V}\\
\sigma(f(\theta)) &= (\sigma(f))(\sigma(\theta)) && \text{for function symbol } f \in \sigma\\
&\overset{\text{def}}{=} \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))\\
\sigma(\theta+\eta) &= \sigma(\theta)+\sigma(\eta)\\
\sigma((\theta)') &=
\end{aligned}
$$

$$
\begin{aligned}
\sigma(p(\theta)) &\equiv && \text{for predicate symbol } p \in \sigma\\
\sigma(\phi \land \psi) &\equiv\\
\sigma(\forall x\, \phi) &=\\
\sigma([\alpha]\phi) &=
\end{aligned}
$$

$$
\begin{aligned}
\sigma(a) &\equiv && \text{for program symbol } a \in \sigma\\
\sigma(x := \theta) &\equiv\\
\sigma(x' = \theta \,\&\, Q) &\equiv\\
\sigma(?Q) &\equiv\\
\sigma(\alpha \cup \beta) &\equiv\\
\sigma(\alpha;\beta) &\equiv\\
\sigma(\alpha^*) &\equiv
\end{aligned}
$$

$$
\begin{array}{rcll}
\sigma(x) & = & x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
 & \stackrel{\text{def}}{=} & \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) & = & \sigma(\theta) + \sigma(\eta) & \\
\sigma((\theta)') & = & (\sigma(\theta))' & \text{if } \sigma \ \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) & \equiv & & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \wedge \psi) & \equiv & & \\
\sigma(\forall x\, \phi) & = & & \\
\sigma([\alpha]\phi) & = & & \\
\hline
\sigma(a) & \equiv & & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) & \equiv & & \\
\sigma(x' = \theta \,\&\, Q) & \equiv & & \\
\sigma(?Q) & \equiv & & \\
\sigma(\alpha \cup \beta) & \equiv & & \\
\sigma(\alpha ; \beta) & \equiv & & \\
\sigma(\alpha^*) & \equiv & &
\end{array}
$$

Uniform Substitution: Recursive Application

$$
\begin{aligned}
\sigma(x) &= x && \text{for variable } x \in \mathscr{V}\\
\sigma(f(\theta)) &= (\sigma(f))(\sigma(\theta)) && \text{for function symbol } f \in \sigma\\
&\stackrel{\text{def}}{=} \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))\\
\sigma(\theta+\eta) &= \sigma(\theta)+\sigma(\eta)\\
\sigma((\theta)') &= (\sigma(\theta))' && \text{if } \sigma\ \mathscr{V}\text{-admissible for } \theta
\end{aligned}
$$

$$
\begin{aligned}
\sigma(p(\theta)) &\equiv (\sigma(p))(\sigma(\theta)) && \text{for predicate symbol } p \in \sigma\\
\sigma(\phi \land \psi) &\equiv\\
\sigma(\forall x\, \phi) &=\\
\sigma([\alpha]\phi) &=
\end{aligned}
$$

$$
\begin{aligned}
\sigma(a) &\equiv && \text{for program symbol } a \in \sigma\\
\sigma(x := \theta) &\equiv\\
\sigma(x' = \theta \,\&\, Q) &\equiv\\
\sigma(?Q) &\equiv\\
\sigma(\alpha \cup \beta) &\equiv\\
\sigma(\alpha;\beta) &\equiv\\
\sigma(\alpha^*) &\equiv
\end{aligned}
$$

Uniform Substitution: Recursive Application

$$
\begin{array}{rcll}
\sigma(x) & = & x & \text{for variable } x \in \mathcal{V} \\
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
 & \stackrel{\text{def}}{=} & \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta+\eta) & = & \sigma(\theta)+\sigma(\eta) & \\
\sigma((\theta)') & = & (\sigma(\theta))' & \text{if } \sigma\ \mathcal{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) & \equiv & (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) & \equiv & \sigma(\phi) \land \sigma(\psi) & \\
\sigma(\forall x\, \phi) & = & & \\
\sigma([\alpha]\phi) & = & & \\
\hline
\sigma(a) & \equiv & & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) & \equiv & & \\
\sigma(x' = \theta \,\&\, Q) & \equiv & & \\
\sigma(?Q) & \equiv & & \\
\sigma(\alpha \cup \beta) & \equiv & & \\
\sigma(\alpha;\beta) & \equiv & & \\
\sigma(\alpha^*) & \equiv & &
\end{array}
$$

Uniform Substitution: Recursive Application

$$
\begin{array}{rcll}
\sigma(x) &=& x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) &=& (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
&\stackrel{\text{def}}{=}& \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) &=& \sigma(\theta) + \sigma(\eta) & \\
\sigma((\theta)') &=& (\sigma(\theta))' & \text{if } \sigma \ \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) &\equiv& (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) &\equiv& \sigma(\phi) \land \sigma(\psi) & \\
\sigma(\forall x\, \phi) &=& \forall x\, \sigma(\phi) & \text{if } \sigma \ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) &=& & \\
\hline
\sigma(a) &\equiv& & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) &\equiv& & \\
\sigma(x' = \theta \,\&\, Q) &\equiv& & \\
\sigma(?Q) &\equiv& & \\
\sigma(\alpha \cup \beta) &\equiv& & \\
\sigma(\alpha ; \beta) &\equiv& & \\
\sigma(\alpha^*) &\equiv& &
\end{array}
$$

Uniform Substitution: Recursive Application

$$
\begin{array}{rcll}
\sigma(x) & = & x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
& \stackrel{\text{def}}{=} & \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) & = & \sigma(\theta) + \sigma(\eta) & \\
\sigma((\theta)') & = & (\sigma(\theta))' & \text{if } \sigma\ \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) & \equiv & (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) & \equiv & \sigma(\phi) \land \sigma(\psi) & \\
\sigma(\forall x\, \phi) & = & \forall x\, \sigma(\phi) & \text{if } \sigma\ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) & = & [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) & \equiv & & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) & \equiv & & \\
\sigma(x' = \theta \,\&\, Q) & \equiv & & \\
\sigma(?Q) & \equiv & & \\
\sigma(\alpha \cup \beta) & \equiv & & \\
\sigma(\alpha;\beta) & \equiv & & \\
\sigma(\alpha^*) & \equiv & &
\end{array}
$$

$$
\begin{array}{rcll}
\sigma(x) &=& x & \text{for variable } x \in \mathcal{V} \\
\sigma(f(\theta)) &=& (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
&\overset{\text{def}}{=}& \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta+\eta) &=& \sigma(\theta)+\sigma(\eta) & \\
\sigma((\theta)') &=& (\sigma(\theta))' & \text{if } \sigma\ \mathcal{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) &\equiv& (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \wedge \psi) &\equiv& \sigma(\phi) \wedge \sigma(\psi) & \\
\sigma(\forall x\, \phi) &=& \forall x\, \sigma(\phi) & \text{if } \sigma\ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) &=& [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma\ BV(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) &\equiv& \sigma a & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) &\equiv& & \\
\sigma(x' = \theta \,\&\, Q) &\equiv& & \\
\sigma(?Q) &\equiv& & \\
\sigma(\alpha \cup \beta) &\equiv& & \\
\sigma(\alpha;\beta) &\equiv& & \\
\sigma(\alpha^*) &\equiv& &
\end{array}
$$

Uniform Substitution: Recursive Application

$\sigma(x)$	$=$	x	for variable $x \in \mathscr{V}$
$\sigma(f(\theta))$	$=$	$(\sigma(f))(\sigma(\theta))$	for function symbol $f \in \sigma$
	$\stackrel{\text{def}}{=}$	$\{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$	
$\sigma(\theta + \eta)$	$=$	$\sigma(\theta) + \sigma(\eta)$	
$\sigma((\theta)')$	$=$	$(\sigma(\theta))'$	if σ $\mathscr{V}$-admissible for θ
$\sigma(p(\theta))$	$\equiv$	$(\sigma(p))(\sigma(\theta))$	for predicate symbol $p \in \sigma$
$\sigma(\phi \wedge \psi)$	$\equiv$	$\sigma(\phi) \wedge \sigma(\psi)$	
$\sigma(\forall x\, \phi)$	$=$	$\forall x\, \sigma(\phi)$	if σ $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi)$	$=$	$[\sigma(\alpha)]\sigma(\phi)$	if σ $BV(\sigma(\alpha))$-admissible for ϕ
$\sigma(a)$	$\equiv$	σa	for program symbol $a \in \sigma$
$\sigma(x := \theta)$	$\equiv$	$x := \sigma(\theta)$	
$\sigma(x' = \theta \,\&\, Q)$	$\equiv$		
$\sigma(?Q)$	$\equiv$		
$\sigma(\alpha \cup \beta)$	$\equiv$		
$\sigma(\alpha; \beta)$	$\equiv$		
$\sigma(\alpha^*)$	$\equiv$		

$$
\begin{array}{rcll}
\sigma(x) &=& x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) &=& (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
&\stackrel{\text{def}}{=}& \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) &=& \sigma(\theta) + \sigma(\eta) & \\
\sigma((\theta)') &=& (\sigma(\theta))' & \text{if } \sigma\ \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) &\equiv& (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \wedge \psi) &\equiv& \sigma(\phi) \wedge \sigma(\psi) & \\
\sigma(\forall x\, \phi) &=& \forall x\, \sigma(\phi) & \text{if } \sigma\ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) &=& [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma\ \text{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) &\equiv& \sigma a & \text{for program symbol } a \in \sigma \\
\sigma(x := \theta) &\equiv& x := \sigma(\theta) & \\
\sigma(x' = \theta \,\&\, Q) &\equiv& x' = \sigma(\theta) \,\&\, \sigma(Q) & \text{if } \sigma\ \{x, x'\}\text{-admissible for } \theta, Q \\
\sigma(?Q) &\equiv& & \\
\sigma(\alpha \cup \beta) &\equiv& & \\
\sigma(\alpha; \beta) &\equiv& & \\
\sigma(\alpha^*) &\equiv& &
\end{array}
$$

Uniform Substitution: Recursive Application

$\sigma(x)$	$=$	x	for variable $x \in \mathscr{V}$
$\sigma(f(\theta))$	$=$	$(\sigma(f))(\sigma(\theta))$	for function symbol $f \in \sigma$
	$\stackrel{\text{def}}{=}$	$\{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$	
$\sigma(\theta + \eta)$	$=$	$\sigma(\theta) + \sigma(\eta)$	
$\sigma((\theta)')$	$=$	$(\sigma(\theta))'$	if σ $\mathscr{V}$-admissible for θ
$\sigma(p(\theta))$	$\equiv$	$(\sigma(p))(\sigma(\theta))$	for predicate symbol $p \in \sigma$
$\sigma(\phi \land \psi)$	$\equiv$	$\sigma(\phi) \land \sigma(\psi)$	
$\sigma(\forall x\, \phi)$	$=$	$\forall x\, \sigma(\phi)$	if σ $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi)$	$=$	$[\sigma(\alpha)]\sigma(\phi)$	if σ BV$(\sigma(\alpha))$-admissible for ϕ
$\sigma(a)$	$\equiv$	σa	for program symbol $a \in \sigma$
$\sigma(x := \theta)$	$\equiv$	$x := \sigma(\theta)$	
$\sigma(x' = \theta \,\&\, Q)$	$\equiv$	$x' = \sigma(\theta) \,\&\, \sigma(Q)$	if σ $\{x, x'\}$-admissible for θ, Q
$\sigma(?Q)$	$\equiv$	$?\sigma(Q)$	
$\sigma(\alpha \cup \beta)$	$\equiv$		
$\sigma(\alpha;\beta)$	$\equiv$		
$\sigma(\alpha^*)$	$\equiv$		

Uniform Substitution: Recursive Application

$\sigma(x)$	$=$	x	for variable $x \in \mathscr{V}$
$\sigma(f(\theta))$	$=$	$(\sigma(f))(\sigma(\theta))$	for function symbol $f \in \sigma$
	$\stackrel{\text{def}}{=}$	$\{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$	
$\sigma(\theta + \eta)$	$=$	$\sigma(\theta) + \sigma(\eta)$	
$\sigma((\theta)')$	$=$	$(\sigma(\theta))'$	if σ $\mathscr{V}$-admissible for θ
$\sigma(p(\theta))$	$\equiv$	$(\sigma(p))(\sigma(\theta))$	for predicate symbol $p \in \sigma$
$\sigma(\phi \land \psi)$	$\equiv$	$\sigma(\phi) \land \sigma(\psi)$	
$\sigma(\forall x\, \phi)$	$=$	$\forall x\, \sigma(\phi)$	if σ $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi)$	$=$	$[\sigma(\alpha)]\sigma(\phi)$	if σ BV$(\sigma(\alpha))$-admissible for ϕ
$\sigma(a)$	$\equiv$	σa	for program symbol $a \in \sigma$
$\sigma(x := \theta)$	$\equiv$	$x := \sigma(\theta)$	
$\sigma(x' = \theta \,\&\, Q)$	$\equiv$	$x' = \sigma(\theta) \,\&\, \sigma(Q)$	if σ $\{x, x'\}$-admissible for θ, Q
$\sigma(?Q)$	$\equiv$	$?\sigma(Q)$	
$\sigma(\alpha \cup \beta)$	$\equiv$	$\sigma(\alpha) \cup \sigma(\beta)$	
$\sigma(\alpha;\beta)$	$\equiv$		
$\sigma(\alpha^*)$	$\equiv$		

$\sigma(x) = x$		for variable $x \in \mathcal{V}$
$\sigma(f(\theta)) = (\sigma(f))(\sigma(\theta))$		for function symbol $f \in \sigma$
$\stackrel{\text{def}}{=} \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$		
$\sigma(\theta + \eta) = \sigma(\theta) + \sigma(\eta)$		
$\sigma((\theta)') = (\sigma(\theta))'$		if σ $\mathcal{V}$-admissible for θ
$\sigma(p(\theta)) \equiv (\sigma(p))(\sigma(\theta))$		for predicate symbol $p \in \sigma$
$\sigma(\phi \wedge \psi) \equiv \sigma(\phi) \wedge \sigma(\psi)$		
$\sigma(\forall x\, \phi) = \forall x\, \sigma(\phi)$		if σ $\{x\}$-admissible for ϕ
$\sigma([\alpha]\phi) = [\sigma(\alpha)]\sigma(\phi)$		if σ BV$(\sigma(\alpha))$-admissible for ϕ
$\sigma(a) \equiv \sigma a$		for program symbol $a \in \sigma$
$\sigma(x := \theta) \equiv x := \sigma(\theta)$		
$\sigma(x' = \theta \,\&\, Q) \equiv x' = \sigma(\theta) \,\&\, \sigma(Q)$		if σ $\{x, x'\}$-admissible for θ, Q
$\sigma(?Q) \equiv ?\sigma(Q)$		
$\sigma(\alpha \cup \beta) \equiv \sigma(\alpha) \cup \sigma(\beta)$		
$\sigma(\alpha;\beta) \equiv \sigma(\alpha);\sigma(\beta)$		if σ BV$(\sigma(\alpha))$-admissible for β
$\sigma(\alpha^*) \equiv$		

$$
\begin{array}{rcll}
\sigma(x) &=& x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) &=& (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
&\stackrel{\text{def}}{=}& \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta+\eta) &=& \sigma(\theta)+\sigma(\eta) & \\
\sigma((\theta)') &=& (\sigma(\theta))' & \text{if } \sigma\ \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) &\equiv& (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(\phi \land \psi) &\equiv& \sigma(\phi) \land \sigma(\psi) & \\
\sigma(\forall x\, \phi) &=& \forall x\, \sigma(\phi) & \text{if } \sigma\ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) &=& [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) &\equiv& \sigma a & \text{for program symbol } a \in \sigma \\
\sigma(x:=\theta) &\equiv& x:=\sigma(\theta) & \\
\sigma(x'=\theta\,\&\,Q) &\equiv& x'=\sigma(\theta)\,\&\,\sigma(Q) & \text{if } \sigma\ \{x,x'\}\text{-admissible for } \theta, Q \\
\sigma(?Q) &\equiv& ?\sigma(Q) & \\
\sigma(\alpha \cup \beta) &\equiv& \sigma(\alpha) \cup \sigma(\beta) & \\
\sigma(\alpha;\beta) &\equiv& \sigma(\alpha);\sigma(\beta) & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \beta \\
\sigma(\alpha^*) &\equiv& (\sigma(\alpha))^* & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \alpha
\end{array}
$$

Uniform Substitution: Examples

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2][(y := x+y)^*]x \geq y \leftrightarrow [(y := x^2+y)^*]x^2 \geq y}$$

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y := \cdot + y)^*](\cdot \geq y)\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -5]x \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x' = -5]y \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2][(y:=x+y)^*]x \geq y \leftrightarrow [(y:=x^2+y)^*]x^2 \geq y}$$

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y:=\cdot+y)^*](\cdot \geq y)\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -5]x \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x' = -5]y \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

Uniform Substitution: Examples

BV Clash FV

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2][(y:=x+y)^*]x \geq y \leftrightarrow [(y:=x^2+y)^*]x^2 \geq y}$$
$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y:=\cdot+y)^*](\cdot \geq y)\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -5]x \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x' = -5]y \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Clash

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2][(y := x+y)^*]x \geq y \leftrightarrow [(y := x^2+y)^*]x^2 \geq y}$$

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y := \cdot + y)^*](\cdot \geq y)\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -5]x \geq 0} \qquad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x' = -5]y \geq 0} \qquad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Clash

$$\frac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x^2][(y:=x+y)^*]x \geq y \leftrightarrow [(y:=x^2+y)^*]x^2 \geq y}$$

Correct

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y:=\cdot+y)^*](\cdot \geq y)\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x'=-5]x \geq 0} \quad \sigma = \{a \mapsto x'=-5, p \mapsto x \geq 0\}$$

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x'=-5]y \geq 0} \quad \sigma = \{a \mapsto x'=-5, p \mapsto y \geq 0\}$$

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Clash

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2][(y := x+y)^*]x \geq y \leftrightarrow [(y := x^2+y)^*]x^2 \geq y}$$

Correct

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y := \cdot + y)^*](\cdot \geq y)\}$$

$$\frac{p \to [a]p}{x \geq 0 \to [x' = -5]x \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

BV Clash FV

$$\frac{p \to [a]p}{y \geq 0 \to [x' = -5]y \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

Uniform Substitution: Examples

Clash

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \quad \sigma = \{c \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Correct

$$\frac{[x := c]p(x) \leftrightarrow p(c)}{[x := x^2][(y := x+y)^*]x \geq y \leftrightarrow [(y := x^2+y)^*]x^2 \geq y}$$

$$\sigma = \{c \mapsto x^2, p(\cdot) \mapsto [(y := \cdot + y)^*](\cdot \geq y)\}$$

Clash

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -5]x \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto x \geq 0\}$$

Correct

$$\frac{p \rightarrow [a]p}{y \geq 0 \rightarrow [x' = -5]y \geq 0} \quad \sigma = \{a \mapsto x' = -5, p \mapsto y \geq 0\}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$US \ \frac{\phi}{\sigma(\phi)}$$

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

If you bind a free variable, you go to logic jail!

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \wedge [x' = v]x > 0}$$

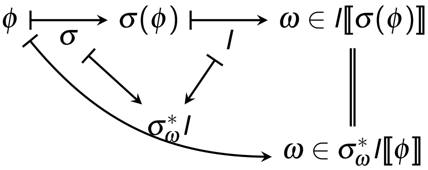
Correctness of Uniform Substitutions

"Syntactic uniform substitution = semantic replacement"

Lemma (Uniform substitution lemma)

Uniform substitution σ and its adjoint interpretation $\sigma^*_\omega I$ to σ for I, ω have the same semantics:

$$\omega \in I[\![\sigma(\phi)]\!] \text{ iff } \omega \in \sigma^*_\omega I[\![\phi]\!]$$



$$\sigma^*_\omega I(f) : \mathbb{R} \to \mathbb{R};\, d \mapsto I^d_\cdot \omega[\![\sigma f(\cdot)]\!]$$

$$\sigma^*_\omega I(p) = \{d \in \mathbb{R} \;:\; \omega \in I^d_\cdot[\![\sigma p(\cdot)]\!]\}$$

$$\sigma^*_\omega I(a) = I[\![\sigma a]\!]$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

Proof.

If premise ϕ valid, i.e. $\omega \in I[\![\phi]\!]$ in all I, ω

Then conclusion $\sigma(\phi)$ valid, because $\omega \in I[\![\sigma(\phi)]\!]$ iff $\omega \in \sigma^*_\omega I[\![\phi]\!]$ □

Outline

Part I

Part IV

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

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

$[\cup]\ [\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$

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

$[^*]\ [\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$

$\text{K}\ [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

$\text{I}\ [\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha^*](\phi \rightarrow [\alpha]\phi)$

$\text{V}\ \phi \rightarrow [\alpha]\phi$

$[']\ [x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi$

Part I		Part IV	
$[:=]$	$[x:=\theta]\phi(x) \leftrightarrow \phi(\theta)$	$[:=]$	$[x:=c]p(x) \leftrightarrow p(c)$
$[?]$	$[?\chi]\phi \leftrightarrow (\chi \to \phi)$	$[?]$	$[?q]p \leftrightarrow (q \to p)$
$[\cup]$	$[\alpha\cup\beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$	$[\cup]$	$[a\cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$
$[;]$	$[\alpha;\beta]\phi \leftrightarrow [\alpha][\beta]\phi$	$[;]$	$[a;b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$
$[^*]$	$[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$	$[^*]$	$[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$
K	$[\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$	K	$[a](p(\bar{x}) \to q(\bar{x})) \to ([a]p(\bar{x}) \to [a]q(\bar{x}))$
I	$[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha^*](\phi \to [\alpha]\phi)$	I	$[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a^*](p(\bar{x}) \to [a]p(\bar{x}))$
V	$\phi \to [\alpha]\phi$	V	$p \to [a]p$
$[']$	$[x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\,[x:=y(t)]\phi$		

Differential Dynamic Logic: Comparison

Infinite axiom schema

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

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

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$ — Schema

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

[*] $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$

K $[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

I $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha^*](\phi \rightarrow [\alpha]\phi)$

V $\phi \rightarrow [\alpha]\phi$ — Schema

['] $[x' = f(x)]\phi \leftrightarrow \forall t \geq 0\, [x := y(t)]\phi$

Axiom = one formula

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

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

[∪] $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$ — Axiom

[;] $[a;b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

[*] $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$

K $[a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$

I $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a^*](p(\bar{x}) \rightarrow [a]p(\bar{x}))$

V $p \rightarrow [a]p$ — Axiom

Example Proof

$$[;]\ \frac{}{j(x) \vdash [(v := 2 \cup v := x); x' = v]x > 0}$$

$$\sigma = \{a \mapsto (v := 2 \cup v := x), b \mapsto x' = v, p(\bar{x}) \mapsto x > 0\}$$

$$\text{US}\ \frac{[a;b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})}{[(v:=2 \cup v:=x); x'=v]x>0 \leftrightarrow [(v:=2 \cup v:=x)][x'=v]x>0}$$

$$\frac{\dfrac{}{j(x) \vdash [v:=2 \cup v:=x][x'=v]x>0}[\cup]}{j(x) \vdash [(v:=2 \cup v:=x); x'=v]x>0}[;]$$

$$\sigma = \{a \mapsto v := 2, b \mapsto v := x, p(\bar{x}) \mapsto [x' = v]x > 0\}$$

$$\text{US}\,\frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := 2 \cup v := x][x'=v]x>0 \leftrightarrow [v := 2][x' = v]x>0 \land [v := x][x'=v]x>0}$$

$$\dfrac{\dfrac{\dfrac{}{j(x) \vdash [v := 2][x' = v]x>0 \land [v := x][x' = v]x>0}[:=]}{j(x) \vdash [v := 2 \cup v := x][x' = v]x>0}[\cup]}{j(x) \vdash [(v := 2 \cup v := x); x' = v]x>0}[;]$$

$\sigma = \{c \mapsto 2, p(\cdot) \mapsto [x'=\cdot]x>0\}$

$$\frac{[v:=c]p(v) \leftrightarrow p(c)}{[v:=2][x'=v]x>0 \leftrightarrow [x'=2]x>0}$$

$\sigma = \{c \mapsto x, p(\cdot) \mapsto [x'=\cdot]x>0\}$

$$\frac{[v:=c]p(v) \leftrightarrow p(c)}{[v:=x][x'=v]x>0 \leftrightarrow [x'=x]x>0}$$

$$\dfrac{\dfrac{\dfrac{}{j(x) \vdash [v:=2][x'=v]x>0 \land [v:=x][x'=v]x>0}[:=]}{j(x) \vdash [v:=2 \cup v:=x][x'=v]x>0}[\cup]}{j(x) \vdash [(v:=2 \cup v:=x); x'=v]x>0}[;]$$

Example Proof

$\sigma = \{c \mapsto 2, p(\cdot) \mapsto [x'{=}\cdot]x{>}0\}$

$$\frac{[v:=c]p(v) \leftrightarrow p(c)}{[v:=2][x'{=}v]x{>}0 \leftrightarrow [x'{=}2]x{>}0}$$

$\sigma = \{c \mapsto x, p(\cdot) \mapsto [x'{=}\cdot]x{>}0\}$

$$\frac{[v:=c]p(v) \leftrightarrow p(c)}{[v:=x][x'{=}v]x{>}0 \leftrightarrow [x'{=}x]x{>}0} \;\lightning$$

$$\begin{array}{l}
{[']}\ \overline{j(x) \vdash [x' = 2]x{>}0 \wedge [v:=x][x' = v]x{>}0} \\
{[:=]}\ \overline{j(x) \vdash [v:=2][x' = v]x{>}0 \wedge [v:=x][x' = v]x{>}0} \\
{[\cup]}\ \overline{j(x) \vdash [v:=2 \cup v:=x][x' = v]x{>}0} \\
{[;]}\ \ j(x) \vdash [(v:=2 \cup v:=x); x' = v]x{>}0
\end{array}$$

Example Proof

$$\sigma = \{c \mapsto v, p(\cdot) \mapsto \cdot > 0\}$$

v can't have ODE

$$\text{US}\ \frac{[x' = c]p(x) \leftrightarrow \forall t \geq 0\, [x := x + ct]p(x)}{[x' = v]x > 0 \leftrightarrow \forall t \geq 0\, [x := x + vt]x > 0}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{j(x) \vdash \forall t \geq 0\, [x := x + 2t]x > 0 \land [v := x]\forall t \geq 0\, [x := x + vt]x > 0}[:=]}{j(x) \vdash [x' = 2]x > 0 \land [v := x][x' = v]x > 0}[']}{j(x) \vdash [v := 2][x' = v]x > 0 \land [v := x][x' = v]x > 0}[:=]}{j(x) \vdash [v := 2 \cup v := x][x' = v]x > 0}[\cup]}{j(x) \vdash [(v := 2 \cup v := x); x' = v]x > 0}[;]$$

Example Proof

$$\sigma = \{c \mapsto x, p(\cdot) \mapsto \forall t{\geq}0\, [x := x+(\cdot)t]x>0\}$$

$$\text{US}\ \frac{[v := c]p(v) \leftrightarrow p(c)}{[v := x]\forall t{\geq}0\, [x := x+vt]x>0 \leftrightarrow \forall t{\geq}0\, [x := x+xt]x>0}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{j(x) \vdash \forall t{\geq}0\, x+2t>0 \land \forall t{\geq}0\, [x := x+xt]x>0}[:=]}{j(x) \vdash \forall t{\geq}0\, [x := x+2t]x>0 \land [v := x]\forall t{\geq}0\, [x := x+vt]x>0}[:=]}{j(x) \vdash [x' = 2]x>0 \land [v := x][x' = v]x>0}[']}{j(x) \vdash [v := 2][x' = v]x>0 \land [v := x][x' = v]x>0}[:=]}{j(x) \vdash [v := 2 \cup v := x][x' = v]x>0}[\cup]}{j(x) \vdash [(v := 2 \cup v := x); x' = v]x>0}[;]$$

Example Proof

$$\sigma = \{c \mapsto x+xt, p(\cdot) \mapsto \cdot>0\}$$

$$\text{US}\dfrac{[x:=c]p(x) \leftrightarrow p(c)}{[x:=x+xt]x>0 \leftrightarrow x+xt>0}$$

$$
\cfrac{
  \cfrac{
    \cfrac{
      \cfrac{
        \cfrac{
          \cfrac{
            j(x) \vdash \forall t{\geq}0\, x+2t>0 \land \forall t{\geq}0\, x+xt>0
          }{j(x) \vdash \forall t{\geq}0\, x+2t>0 \land \forall t{\geq}0\, [x:=x+xt]x>0}[:=]
        }{j(x) \vdash \forall t{\geq}0\, [x:=x+2t]x>0 \land [v:=x]\forall t{\geq}0\, [x:=x+vt]x>0}[:=]
      }{j(x) \vdash [x'=2]x>0 \land [v:=x][x'=v]x>0}[']
    }{j(x) \vdash [v:=2][x'=v]x>0 \land [v:=x][x'=v]x>0}[:=]
  }{j(x) \vdash [v:=2 \cup v:=x][x'=v]x>0}[\cup]
}{j(x) \vdash [(v:=2 \cup v:=x); x'=v]x>0}[;]
$$

$$j(x) \vdash \forall t{\geq}0\, x{+}2t{>}0 \land \forall t{\geq}0\, x{+}xt{>}0$$

[:=]

$$j(x) \vdash \forall t{\geq}0\, x{+}2t{>}0 \land \forall t{\geq}0\, [x := x{+}xt]x{>}0$$

[:=]

$$j(x) \vdash \forall t{\geq}0\, [x := x{+}2t]x{>}0 \land [v := x]\forall t{\geq}0\, [x := x{+}vt]x{>}0$$

[′]

$$j(x) \vdash [x' = 2]x{>}0 \land [v := x][x' = v]x{>}0$$

[:=]

$$j(x) \vdash [v := 2][x' = v]x{>}0 \land [v := x][x' = v]x{>}0$$

[∪]

$$j(x) \vdash [v := 2 \cup v := x][x' = v]x{>}0$$

[;]

$$j(x) \vdash [(v := 2 \cup v := x); x' = v]x{>}0$$

Example Proof

Summarize:

$$\frac{j(x) \vdash \forall t{\geq}0\, x{+}2t{>}0 \land \forall t{\geq}0\, x{+}xt{>}0}{j(x) \vdash [(v:=2 \cup v:=x); x' = v]x > 0}$$

Summarize:

$$\frac{j(x) \vdash \forall t{\geq}0\, x{+}2t{>}0 \land \forall t{\geq}0\, x{+}xt{>}0}{j(x) \vdash [(v := 2 \cup v := x); x' = v]x > 0}$$

Using $\sigma = \{j(\cdot) \mapsto \cdot{>}0\}$ on above derived rule proves:

$$\text{USR}\ \dfrac{\mathbb{R}\ \dfrac{*}{x > 0 \vdash \forall t{\geq}0\, x + 2t > 0 \land \forall t{\geq}0\, x + xt > 0}}{x > 0 \vdash [(v := 2 \cup v := x); x' = v]x > 0}$$

Outline

Axiom vs. Axiom Schema: Philosophy Affects Provers

- ✓ Soundness easier: literal formula, not instantiation mechanism
- ✓ An axiom is one formula. Axiom schema is a decision algorithm.
- ✓ Generic formula, not some shape with characterization of exceptions
- ✓ No schema variable or meta variable algorithms
- ✓ No matching mechanisms / unification in prover kernel
- ✓ No side condition subtlety or occurrence pattern checks (per schema)
- × Need other means of instantiating axioms: uniform substitution (US)
- ✓ US + renaming: isolate static semantics
- ✓ US independent from axioms: modular logic vs. prover separation
- ✓ More flexible by syntactic contextual equivalence
- × Extra proofs branches since instantiation is explicit proof step

Axiom vs. Axiom Schema: Philosophy Affects Provers

- ✓ Soundness easier: literal formula, not instantiation mechanism
- ✓ An axiom is one formula. Axiom schema is a decision algorithm.
- ✓ Generic formula, not some shape with characterization of exceptions
- ✓ No schema variable or meta variable algorithms
- ✓ No matching mechanisms / unification in prover kernel
- ✓ No side condition subtlety or occurrence pattern checks (per schema)
- × Need other means of instantiating axioms: uniform substitution (US)
- ✓ US + renaming: isolate static semantics
- ✓ US independent from axioms: modular logic vs. prover separation
- ✓ More flexible by syntactic contextual equivalence
- × Extra proofs branches since instantiation is explicit proof step

---

∑ Net win for soundness since significantly simpler prover

Part I

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

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

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$

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

$[^*]$ $[\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$

K $[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

I $[\alpha^*]\phi \leftrightarrow \phi \land [\alpha^*](\phi \rightarrow [\alpha]\phi)$

V $\phi \rightarrow [\alpha]\phi$

$[']$ $[x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi$

Part IV

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

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

$[\cup]$ $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

$[;]$ $[a;b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

$[^*]$ $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \land [a][a^*]p(\bar{x})$

K $[a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$

I $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \land [a^*](p(\bar{x}) \rightarrow [a]p(\bar{x}))$

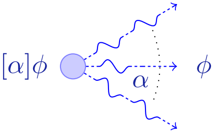
V $p \rightarrow [a]p$

Uniform Substitution for Differential Dynamic Logic

differential dynamic logic

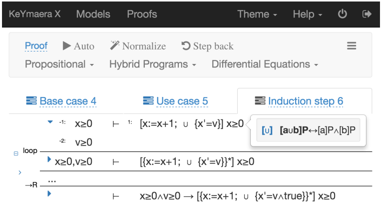
$\mathrm{dL} = \mathrm{DL} + \mathrm{HP}$

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



- Uniform substitution
  $\rightsquigarrow$ axioms not schemata
- Modular: Logic $\|$ Prover
- Straightforward to implement
- Prover microkernel
- Sound & complete / ODE
- Fast contextual equivalence

KeYmaera X



$$\text{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})}$$

Uniform Substitution of Rules and Proofs

$$\text{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})} \qquad \text{implies} \qquad \frac{x^2 \geq 0}{[x := x+1; (x' = x \cup x' = -2)]x^2 \geq 0}$$

Theorem (Soundness) $(\text{FV}(\sigma) = \emptyset)$

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi} \textit{ locally sound} \quad \textit{implies} \quad \frac{\sigma(\phi_1) \quad \dots \quad \sigma(\phi_n)}{\sigma(\psi)} \textit{ locally sound}$$

Uniform Substitution of Rules and Proofs

$$\text{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})} \qquad \text{implies} \qquad \frac{x^2 \geq 0}{[x := x+1; (x' = x \cup x' = -2)]x^2 \geq 0}$$

Theorem (Soundness) $(\text{FV}(\sigma) = \emptyset)$

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi} \textit{ locally sound} \quad \textit{implies} \quad \frac{\sigma(\phi_1) \quad \dots \quad \sigma(\phi_n)}{\sigma(\psi)} \textit{ locally sound}$$

Locally sound

The conclusion is valid in any interpretation I in which the premises are.

Uniform Substitution of Rules and Proofs

$$\text{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})} \qquad \text{implies} \qquad \frac{x^2 \geq 0}{[x := x+1; (x' = x \cup x' = -2)]x^2 \geq 0}$$

$$\text{CQ}\ \frac{f() = g()}{p(f()) \leftrightarrow p(g())}$$

Theorem (Soundness) $(\mathrm{FV}(\sigma) = \emptyset)$

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi}\ \textit{locally sound} \quad \textit{implies} \quad \frac{\sigma(\phi_1) \quad \dots \quad \sigma(\phi_n)}{\sigma(\psi)}\ \textit{locally sound}$$

Locally sound

The conclusion is valid in any interpretation I in which the premises are.

G $\dfrac{p(\bar{x})}{[a]p(\bar{x})}$ implies $\dfrac{x^2 \geq 0}{[x := x+1; (x' = x \cup x' = -2)]x^2 \geq 0}$

CQ $\dfrac{f() = g()}{p(f()) \leftrightarrow p(g())}$ implies $\dfrac{2x - x = x}{[x' = v]2x - x \geq 0 \leftrightarrow [x' = v]x \geq 0}$

Theorem (Soundness) ($\mathrm{FV}(\sigma) = \emptyset$)

$\dfrac{\phi_1 \quad \dots \quad \phi_n}{\psi}$ *locally sound* *implies* $\dfrac{\sigma(\phi_1) \quad \dots \quad \sigma(\phi_n)}{\sigma(\psi)}$ *locally sound*

Locally sound

The conclusion is valid in any interpretation I in which the premises are.

Outline

7 Differential Axioms
- Differential Equation and Differential Axioms
- Differential Substitution Lemmas
- Contextual Congruences
- Static Semantics
- Summary

Axiom Schema Side Conditions: ODE Solving

['] $[x' = \theta]\phi \leftrightarrow \forall t{\geq}0\,[x := y(t)]\phi$

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: $y(\cdot)$ solves the ODE $y'(t) = \theta$ with $y(\cdot)$ plugged in for x in term θ
3. Initial value check: $y(\cdot)$ solves the symbolic IVP $y(0) = x$
4. $y(\cdot)$ covers all solutions parametrically
5. x' cannot occur free in ϕ

Quite nontrivial soundness-critical side condition algorithms . . .

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$

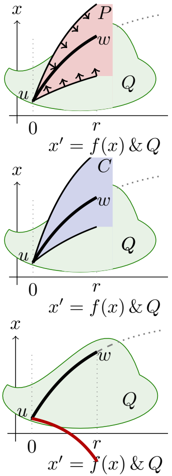
Differential Cut

$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$

Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

if new $y' = g(x,y)$ has long enough solution



DW $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)]\big(q(x) \rightarrow p(x)\big)$

DI $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [?q(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)](p(x))'$

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$

DE $[x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$

DG $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$

DS $[x' = c\,\&\,q(x)]p(x) \leftrightarrow \forall t{\ge}0\,\big((\forall 0{\le}s{\le}t\; q(x+cs)) \rightarrow [x := x+ct]p(x)\big)$

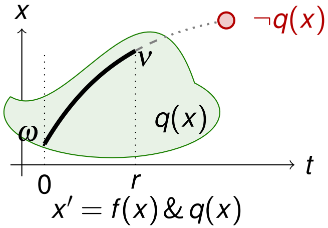
$+'$ $(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$

$\cdot'$ $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

c' $(c)' = 0$

Axiom (Differential Weakening) (JAR'17)

$$\text{DW}\quad [x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x)]\big(q(x) \rightarrow p(x)\big)$$

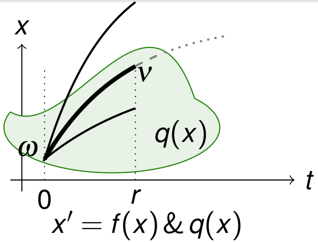


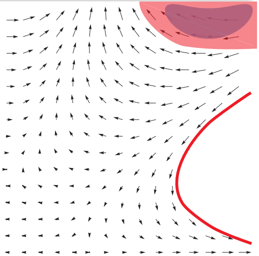
Differential equations cannot leave their evolution domains. Derives from:

$$\text{DW}\quad [x' = f(x) \,\&\, q(x)]q(x)$$

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$



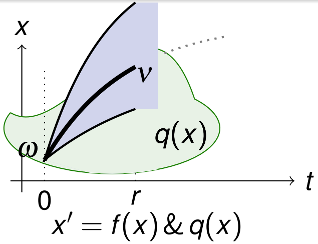


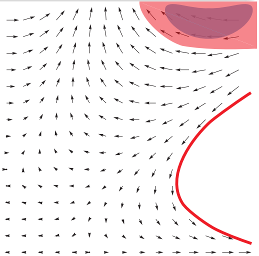
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$



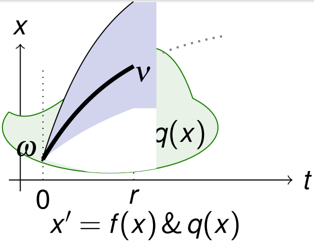


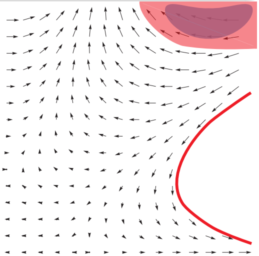
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

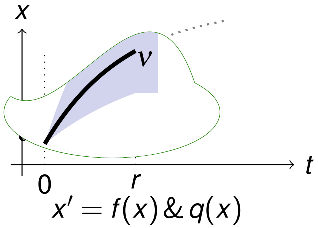


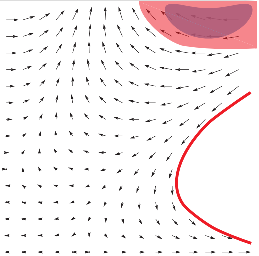


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$

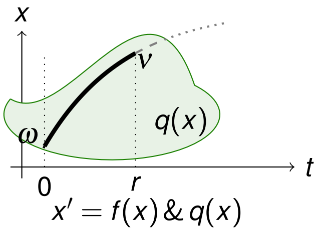


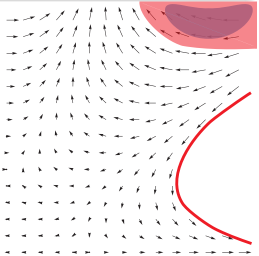


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \wedge r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$

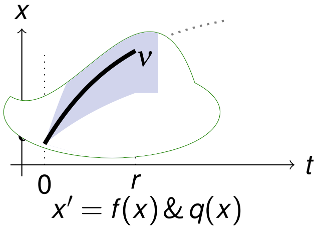


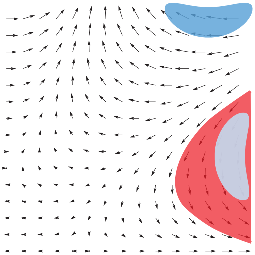


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

$$\text{DC} \quad ([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)) \leftarrow [x' = f(x) \,\&\, q(x)]r(x)$$





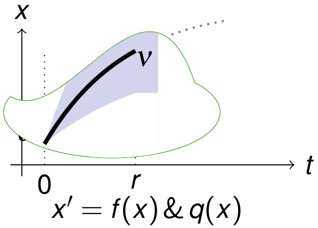
DC is a cut for differential equations.

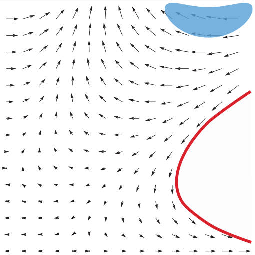
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$





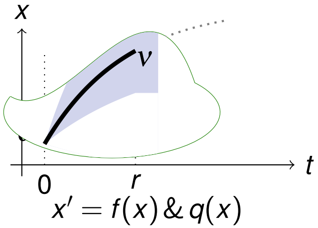
DC is a cut for differential equations.

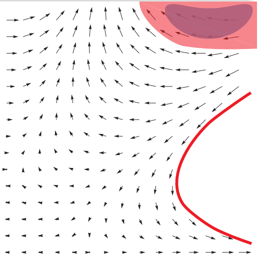
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

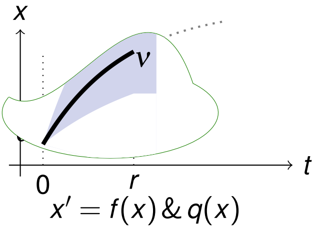


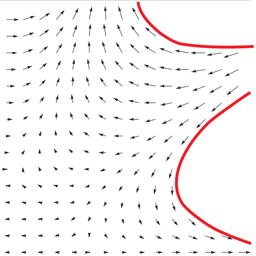


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (JAR'17)

DC $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

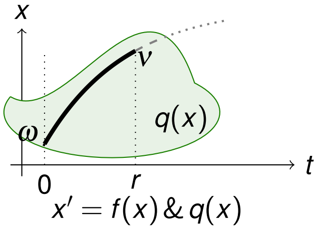


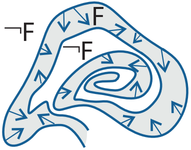


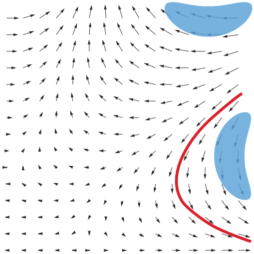
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Invariant) (JAR'17)

DI $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [?q(x)]p(x)\big) \leftarrow [x' = f(x) \,\&\, q(x)](p(x))'$







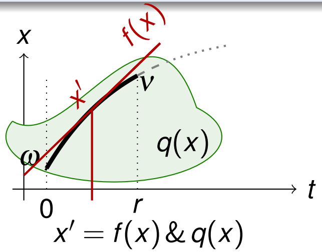
Differential invariant: if $p(x)$ true now and if differential $(p(x))'$ true always

What's the differential of a formula???

What's the meaning of a differential term . . . in a state???

Axiom (Differential Effect) (JAR'17)

DE $[x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$



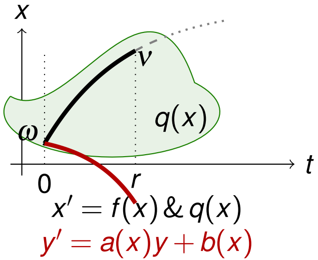
Effect of differential equation on differential symbol x'

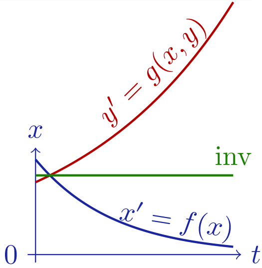
$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on x'

$[x' := f(x)]$ selects vector field $x' = f(x)$ for subsequent differentials

Axiom (Differential Ghost) (JAR'17)

DG $[x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, q(x)]p(x)$

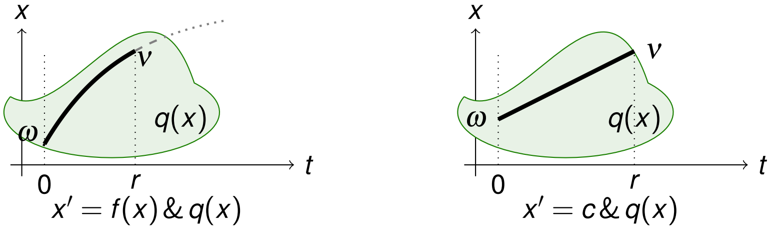




Differential ghost/auxiliaries: extra differential equations that exist
Can cause new invariants
"Dark matter" counterweight to balance conserved quantities

Axiom (Differential Solution) (JAR'17)

$$\text{DS}\ [x' = c\,\&\,q(x)]p(x) \leftrightarrow \forall t{\geq}0\,\big((\forall 0{\leq}s{\leq}t\,q(x{+}cs)) \rightarrow [x := x{+}ct]p(x)\big)$$



Differential solutions: solve differential equations
with DG,DC and inverse companions

Example: Differential Invariants — Don't Solve. Prove!

1. DI proves a property of an ODE inductively by its differentials
2. DE exports vector field, possibly after DW exports evolution domain
3. CE+CQ reason efficiently in Equivalence or eQuational context
4. G isolates postcondition
5. $[:=]$ differential assignment uses vector field
6. $\cdot'$ differential computations are axiomatic (US)

Left branch:

$$\ast$$
$$\mathbb{R}\quad \vdash x^3\cdot x + x\cdot x^3 \geq 0$$
$$[:=]\quad \vdash [x' := x^3]x'\cdot x + x\cdot x' \geq 0$$
$$\mathrm{G}\quad \vdash [x' = x^3][x' := x^3]x'\cdot x + x\cdot x' \geq 0$$

Right branch:

$$\ast$$
$$\cdot'\quad (f(\bar{x})\cdot g(\bar{x}))' = (f(\bar{x}))'\cdot g(\bar{x}) + f(\bar{x})\cdot(g(\bar{x}))'$$
$$\mathrm{US}\quad (x\cdot x)' = (x)'\cdot x + x\cdot(x)'$$
$$(x\cdot x)' = x'\cdot x + x\cdot x'$$
$$\mathrm{CQ}\quad (x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$
$$(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$

Combined:

$$\mathrm{CE}\quad \vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'$$
$$\mathrm{DE}\quad \vdash [x' = x^3](x\cdot x \geq 1)'$$
$$\mathrm{DI}\quad x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1$$

Differential Substitution Lemmas

Lemma (Differential lemma)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$*, then for all* $0 \le \zeta \le r$*:*

Syntactic $\qquad \varphi(\zeta)[\![(\theta)']\!] = \dfrac{\mathrm{d}\varphi(t)[\![\theta]\!]}{\mathrm{d}t}(\zeta) \qquad$ Analytic

Lemma (Differential assignment)

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models \phi \leftrightarrow [x' := f(x)]\phi$

Lemma (Derivations)

$$(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$$

$$(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$$

$$(c)' = 0 \qquad \text{for arity 0 functions } c$$

Differential Substitution Lemmas

Lemma (Differential lemma)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$*, then for all* $0 \le \zeta \le r$*:*

Syntactic $\quad \varphi(\zeta)[\![(\theta)']\!] = \dfrac{\mathrm{d}\varphi(t)[\![\theta]\!]}{\mathrm{d}t}(\zeta) \quad$ Analytic

Lemma (Differential assignment)

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models \phi \leftrightarrow [x' := f(x)]\phi$

Lemma (Derivations)

$$(\theta + \eta)' = (\theta)' + (\eta)'$$

$$(\theta \cdot \eta)' = (\theta)' \cdot \eta + \theta \cdot (\eta)'$$

$$(c)' = 0 \qquad \textit{for arity 0 functions } c$$

DW $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)]\big(q(x) \rightarrow p(x)\big)$

DI $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [?q(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)](p(x))'$

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$

DE $[x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$

DG $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$

DS $[x' = c\,\&\,q(x)]p(x) \leftrightarrow \forall t {\geq} 0\,\big((\forall 0 {\leq} s {\leq} t\; q(x+cs)) \rightarrow [x := x+ct]p(x)\big)$

$+'$ $(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$

$\cdot'$ $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

c' $(c)' = 0$

1. DI proves a property of an ODE inductively by its differentials
2. DE exports vector field, possibly after DW exports evolution domain
3. CE+CQ reason efficiently in Equivalence or eQuational context
4. G isolates postcondition
5. $[:=]$ differential assignment uses vector field

$$
\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash x^3 \cdot x + x \cdot x^3 \geq 0}\ \mathbb{R}}{\vdash [x' := x^3] x' \cdot x + x \cdot x' \geq 0}\ [:=]}{\vdash [x' = x^3][x' := x^3] x' \cdot x + x \cdot x' \geq 0}\ \mathrm{G} \qquad \dfrac{\dfrac{\overline{(x \cdot x)' = x' \cdot x + x \cdot x'}}{(x \cdot x)' \geq 0 \leftrightarrow x' \cdot x + x \cdot x' \geq 0}\ \mathrm{CQ}}{(x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}}{\dfrac{\dfrac{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}{\vdash [x' = x^3](x \cdot x \geq 1)'}\ \mathrm{DE}}{x \cdot x \geq 1 \vdash [x' = x^3] x \cdot x \geq 1}\ \mathrm{DI}}\ \mathrm{CE}
$$

Example: Contextual Congruence Reasoning by US

$$\text{CQ}\ \frac{f() = g()}{p(f()) \leftrightarrow p(g())}$$

$$\text{CQ}\ \frac{(x \cdot x)' = x' \cdot x + x \cdot x'}{(x \cdot x)' \geq 0 \leftrightarrow x' \cdot x + x \cdot x' \geq 0}$$

$$\text{CE}\ \frac{P \leftrightarrow Q}{C(P) \leftrightarrow C(Q)}$$

$$\text{CE}\ \frac{(x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}{[x' = x^3][x' := x^3](x \cdot x \geq 1)' \leftrightarrow [x' = x^3][x' := x^3]x' \cdot x + x \cdot x' \geq 0}$$

Example: Contextual Congruence Reasoning by US

$$\text{CQ}\ \frac{f() = g()}{p(f()) \leftrightarrow p(g())}$$

$$\text{CQ}\ \frac{(x \cdot x)' = x' \cdot x + x \cdot x'}{(x \cdot x)' \geq 0 \leftrightarrow x' \cdot x + x \cdot x' \geq 0}$$

with $\sigma \approx \{p(\cdot) \mapsto \cdot \geq 0, f() \mapsto (x \cdot x)', g() \mapsto x' \cdot x + x \cdot x'\}$

$$\text{CE}\ \frac{P \leftrightarrow Q}{C(P) \leftrightarrow C(Q)}$$

$$\text{CE}\ \frac{(x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}{[x' = x^3][x' := x^3](x \cdot x \geq 1)' \leftrightarrow [x' = x^3][x' := x^3]x' \cdot x + x \cdot x' \geq 0}$$

with $\sigma \approx \{C(\_) \mapsto [x'=x^3][x' := x^3]\_, P \mapsto (x \cdot x \geq 1)', Q \mapsto x' \cdot x + x \cdot x' \geq 0\}$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}\text{CE}}{\vdash [x' = x^3](x \cdot x \geq 1)'}\text{DE}}{x \cdot x \geq 1 \vdash [x' = x^3]x \cdot x \geq 1}\text{DI}$$

1. Free function $j(x,x')$ for parametric differential computation

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash [x'=x^3][x':=x^3]j(x,x')\geq 0}\text{G} \qquad \dfrac{}{(x\cdot x\geq 1)' \leftrightarrow j(x,x')\geq 0}}{\vdash [x'=x^3][x':=x^3](x\cdot x\geq 1)'}\text{CE}}{\vdash [x'=x^3](x\cdot x\geq 1)'}\text{DE}}{x\cdot x\geq 1 \vdash [x'=x^3]x\cdot x\geq 1}\text{DI}
$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash [x':=x^3]j(x,x')\geq 0}\,[:=]}{\vdash [x'=x^3][x':=x^3]j(x,x')\geq 0}\,\text{G} \qquad \dfrac{}{(x\cdot x\geq 1)' \leftrightarrow j(x,x')\geq 0}}{\vdash [x'=x^3][x':=x^3](x\cdot x\geq 1)'}\,\text{CE}}{\dfrac{\vdash [x'=x^3](x\cdot x\geq 1)'}{x\cdot x\geq 1 \vdash [x'=x^3]x\cdot x\geq 1}\,\text{DI}}\,\text{DE}
$$

Example: Differential Invariants

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition

$$
\dfrac{\dfrac{\dfrac{\vdash j(x,x^3)\geq 0}{\vdash [x':=x^3]j(x,x')\geq 0}\;[:=]}{\vdash [x'=x^3][x':=x^3]j(x,x')\geq 0}\;\mathrm{G} \qquad \overline{(x\cdot x\geq 1)'\leftrightarrow j(x,x')\geq 0}}{\dfrac{\dfrac{\vdash [x'=x^3][x':=x^3](x\cdot x\geq 1)'}{\vdash [x'=x^3](x\cdot x\geq 1)'}\;\mathrm{DE}}{x\cdot x\geq 1\vdash [x'=x^3]x\cdot x\geq 1}\;\mathrm{DI}}\;\mathrm{CE}
$$

Example: Differential Invariants — Parametric

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,$[:=]$ to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation

$$\vdash j(x,x^3) \geq 0$$
$$[:=]\quad \vdash [x' := x^3] j(x,x') \geq 0$$
$$\text{G}\quad \vdash [x' = x^3][x' := x^3] j(x,x') \geq 0$$

$$(x\cdot x)' \geq 0 \leftrightarrow j(x,x') \geq 0$$
$$\text{CQ}\quad (x\cdot x \geq 1)' \leftrightarrow j(x,x') \geq 0$$

$$\text{CE}\quad \vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'$$
$$\text{DE}\quad \vdash [x' = x^3](x\cdot x \geq 1)'$$
$$\text{DI}\quad x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash j(x,x^3)\geq 0}{\vdash [x':=x^3]j(x,x')\geq 0}\,[:=]}{\vdash [x'=x^3][x':=x^3]j(x,x')\geq 0}\,\text{G} \qquad \dfrac{\dfrac{(x\cdot x)'=j(x,x')}{(x\cdot x)'\geq 0 \leftrightarrow j(x,x')\geq 0}\,\text{CQ}}{(x\cdot x\geq 1)'\leftrightarrow j(x,x')\geq 0}}{\vdash [x'=x^3][x':=x^3](x\cdot x\geq 1)'}\,\text{CE}}{\dfrac{\vdash [x'=x^3](x\cdot x\geq 1)'}{x\cdot x\geq 1\vdash [x'=x^3]x\cdot x\geq 1}\,\text{DI}}\,\text{DE}$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation
4. USR instantiates proof by $\{j(x,x') \mapsto x' \cdot x + x \cdot x'\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash j(x,x^3) \geq 0}{\vdash [x' := x^3] j(x,x') \geq 0}\,[:=]}{\vdash [x' = x^3][x' := x^3] j(x,x') \geq 0}\,\mathrm{G} \qquad \dfrac{\dfrac{(x \cdot x)' = j(x,x')}{(x \cdot x)' \geq 0 \leftrightarrow j(x,x') \geq 0}\,\mathrm{CQ}}{(x \cdot x \geq 1)' \leftrightarrow j(x,x') \geq 0}}{\dfrac{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}{\vdash [x' = x^3](x \cdot x \geq 1)'}\,\mathrm{DE}}\,\mathrm{CE}}{x \cdot x \geq 1 \vdash [x' = x^3] x \cdot x \geq 1}\,\mathrm{DI}$$

$$\dfrac{\dfrac{}{\vdash x^3 \cdot x + x \cdot x^3 \geq 0}\,\mathbb{R} \qquad \dfrac{}{(x \cdot x)' = x' \cdot x + x \cdot x'}\,x'}{x \cdot x \geq 1 \vdash [x' = x^3] x \cdot x \geq 1}\,\mathrm{USR}$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation
4. USR instantiates proof by $\{j(x,x') \mapsto x' \cdot x + x \cdot x'\}$

$$
\dfrac{
\dfrac{\dfrac{\vdash j(x,x^3) \geq 0}{\vdash [x' := x^3] j(x,x') \geq 0}\ [:=]}{\vdash [x' = x^3][x' := x^3] j(x,x') \geq 0}\ \mathrm{G}
\qquad
\dfrac{\dfrac{(x\cdot x)' = j(x,x')}{(x\cdot x)' \geq 0 \leftrightarrow j(x,x') \geq 0}\ \mathrm{CQ}}{(x\cdot x \geq 1)' \leftrightarrow j(x,x') \geq 0}
}{
\dfrac{\dfrac{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}{\vdash [x' = x^3](x\cdot x \geq 1)'}\ \mathrm{DE}}{x\cdot x \geq 1 \vdash [x' = x^3] x\cdot x \geq 1}\ \mathrm{DI}
}\ \mathrm{CE}
$$

$$
\dfrac{\dfrac{*}{\vdash x^3\cdot x + x\cdot x^3 \geq 0}\ \mathbb{R} \qquad \dfrac{}{(x\cdot x)' = x'\cdot x + x\cdot x'}\ x'}{x\cdot x \geq 1 \vdash [x' = x^3] x\cdot x \geq 1}\ \mathrm{USR}
$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation
4. USR instantiates proof by $\{j(x,x') \mapsto x' \cdot x + x \cdot x'\}$

$$\dfrac{\dfrac{\dfrac{\vdash j(x,x^3) \geq 0}{\vdash [x' := x^3] j(x,x') \geq 0}\,[:=]}{\vdash [x' = x^3][x' := x^3] j(x,x') \geq 0}\,\mathrm{G} \qquad \dfrac{\dfrac{(x \cdot x)' = j(x,x')}{(x \cdot x)' \geq 0 \leftrightarrow j(x,x') \geq 0}\,\mathrm{CQ}}{(x \cdot x \geq 1)' \leftrightarrow j(x,x') \geq 0}}{\dfrac{\dfrac{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}{\vdash [x' = x^3](x \cdot x \geq 1)'}\,\mathrm{DE}}{x \cdot x \geq 1 \vdash [x' = x^3] x \cdot x \geq 1}\,\mathrm{DI}}\,\mathrm{CE}$$

$$\dfrac{\dfrac{*}{\vdash x^3 \cdot x + x \cdot x^3 \geq 0}\,\mathbb{R} \qquad \dfrac{\dfrac{}{(x \cdot x)' = (x)' \cdot x + x \cdot (x)'}\,\mathrm{US}}{(x \cdot x)' = x' \cdot x + x \cdot x'}\,x'}{x \cdot x \geq 1 \vdash [x' = x^3] x \cdot x \geq 1}\,\mathrm{USR}$$

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation
4. USR instantiates proof by $\{j(x,x') \mapsto x'\cdot x + x\cdot x'\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash j(x,x^3) \geq 0}{\vdash [x' := x^3] j(x,x') \geq 0}\,[:=]}{\vdash [x' = x^3][x' := x^3] j(x,x') \geq 0}\,\mathrm{G} \qquad \dfrac{\dfrac{(x\cdot x)' = j(x,x')}{(x\cdot x)' \geq 0 \leftrightarrow j(x,x') \geq 0}\,\mathrm{CQ}}{(x\cdot x \geq 1)' \leftrightarrow j(x,x') \geq 0}}{\dfrac{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}{\vdash [x' = x^3](x\cdot x \geq 1)'}\,\mathrm{DE}}\,\mathrm{CE}}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\,\mathrm{DI}$$

$$\dfrac{\dfrac{*}{\vdash x^3\cdot x + x\cdot x^3 \geq 0}\,\mathbb{R} \qquad \dfrac{\dfrac{\dfrac{}{(f(\bar{x})\cdot g(\bar{x}))' = (f(\bar{x}))'\cdot g(\bar{x}) + f(\bar{x})\cdot (g(\bar{x}))'}\,\cdot'}{(x\cdot x)' = (x)'\cdot x + x\cdot (x)'}\,\mathrm{US}}{(x\cdot x)' = x'\cdot x + x\cdot x'}\,x'}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\,\mathrm{USR}$$

Example: Differential Invariants

1. Free function $j(x,x')$ for parametric differential computation
2. Again G,[:=] to isolate differentially substituted postcondition
3. Construct parametric $j(x,x')$ by axiomatic differential computation
4. USR instantiates proof by $\{j(x,x') \mapsto x'\cdot x + x\cdot x'\}$

$$\dfrac{\dfrac{\dfrac{\vdash j(x,x^3)\geq 0}{\vdash [x':=x^3]j(x,x')\geq 0}[:=]}{\vdash [x'=x^3][x':=x^3]j(x,x')\geq 0}\text{G} \qquad \dfrac{\dfrac{(x\cdot x)'=j(x,x')}{(x\cdot x)'\geq 0 \leftrightarrow j(x,x')\geq 0}\text{CQ}}{(x\cdot x\geq 1)' \leftrightarrow j(x,x')\geq 0}}{\dfrac{\dfrac{\vdash [x'=x^3][x':=x^3](x\cdot x\geq 1)'}{\vdash [x'=x^3](x\cdot x\geq 1)'}\text{DE}}{x\cdot x\geq 1 \vdash [x'=x^3]x\cdot x\geq 1}\text{DI}}\text{CE}$$

$$\dfrac{\dfrac{*}{\vdash x^3\cdot x + x\cdot x^3 \geq 0}\mathbb{R} \qquad \dfrac{\dfrac{\dfrac{*}{(f(\bar{x})\cdot g(\bar{x}))' = (f(\bar{x}))'\cdot g(\bar{x}) + f(\bar{x})\cdot (g(\bar{x}))'}\cdot'}{(x\cdot x)' = (x)'\cdot x + x\cdot (x)'}\text{US}}{(x\cdot x)' = x'\cdot x + x\cdot x'}x'}{x\cdot x\geq 1 \vdash [x'=x^3]x\cdot x\geq 1}\text{USR}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}\text{CE}}{\vdash [x' = x^3](x \cdot x \geq 1)'}\text{DE}}{x \cdot x \geq 1 \vdash [x' = x^3]x \cdot x \geq 1}\text{DI}$$

1. Start with identity differential computation result

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{(x\cdot x)' = (x\cdot x)'}\ \mathbb{R}}{}\ .'}{}\ x'}{}\ \mathrm{CT}}{}}{}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}\ \mathrm{CE}}{\vdash [x' = x^3](x\cdot x \geq 1)'}\ \mathrm{DE}}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\ \mathrm{DI}$$

1. Start with identity differential computation result which proves

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(x\cdot x)' = (x\cdot x)'}\ \mathbb{R}}{}\ .'}{}\ x'}{}\ \mathrm{CT}}{}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}\ \mathrm{CE}}{\vdash [x' = x^3](x\cdot x \geq 1)'}\ \mathrm{DE}}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\ \mathrm{DI}$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(x\cdot x)' = (x\cdot x)'}\ \mathbb{R}}{(x\cdot x)' = (x)'\cdot x + x\cdot(x)'}\ \cdot'}{}\ x'}{}\ \text{CT}}{}}{}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}\ \text{CE}}{\vdash [x' = x^3](x\cdot x \geq 1)'}\ \text{DE}}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\ \text{DI}$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{(x \cdot x)' = (x \cdot x)'}\,\mathbb{R}}{(x \cdot x)' = (x)' \cdot x + x \cdot (x)'}\,\cdot'}{(x \cdot x)' = x' \cdot x + x \cdot x'}\,x'}{\quad}\,\text{CT}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}\,\text{CE}}{\vdash [x' = x^3](x \cdot x \geq 1)'}\,\text{DE}}{x \cdot x \geq 1 \vdash [x' = x^3]x \cdot x \geq 1}\,\text{DI}$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(x\cdot x)' = (x\cdot x)'}\mathbb{R}}{(x\cdot x)' = (x)'\cdot x + x\cdot(x)'}\cdot'}{(x\cdot x)' = x'\cdot x + x\cdot x'}x'}{(x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0}\text{CT}}{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}\text{CE}}{\vdash [x' = x^3](x\cdot x \geq 1)'}\text{DE}}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\text{DI}$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT
4. Construct differential invariant computation result forward accordingly

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(x\cdot x)' = (x\cdot x)'}\,\mathbb{R}}{(x\cdot x)' = (x)'\cdot x + x\cdot(x)'}\,\cdot'}{(x\cdot x)' = x'\cdot x + x\cdot x'}\,x'}{(x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0}\,\mathrm{CT}}{(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0}}{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}\,\mathrm{CE}}{\dfrac{\vdash [x' = x^3](x\cdot x \geq 1)'}{x\cdot x \geq 1 \vdash [x' = x^3]\,x\cdot x \geq 1}\,\mathrm{DI}}\,\mathrm{DE}
$$

Example: Differential Invariants

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT
4. Construct differential invariant computation result forward accordingly
5. Resume backward proof with result computed by forward proof right

$$
\dfrac{
  \dfrac{
    \dfrac{}{\vdash [x' = x^3][x' := x^3]x'\cdot x + x\cdot x' \geq 0}\,\mathrm{G}
    \quad
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{
            \dfrac{*}{(x\cdot x)' = (x\cdot x)'}\,\mathbb{R}
          }{(x\cdot x)' = (x)'\cdot x + x\cdot (x)'}\,\cdot'
        }{(x\cdot x)' = x'\cdot x + x\cdot x'}\,x'
      }{(x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0}\,\mathrm{CT}
    }{(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0}
  }{
    \dfrac{\vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'}{\vdash [x' = x^3](x\cdot x \geq 1)'}\,\mathrm{DE}
  }\,\mathrm{CE}
}{x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1}\,\mathrm{DI}
$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT
4. Construct differential invariant computation result forward accordingly
5. Resume backward proof with result computed by forward proof right

$$
\dfrac{\dfrac{[:=]\dfrac{}{\vdash [x' := x^3]x' \cdot x + x \cdot x' \geq 0}}{\vdash [x' = x^3][x' := x^3]x' \cdot x + x \cdot x' \geq 0}\text{G} \quad \dfrac{\text{CT}\dfrac{x'\dfrac{\cdot'\dfrac{\mathbb{R}\dfrac{*}{(x \cdot x)' = (x \cdot x)'}}{(x \cdot x)' = (x)' \cdot x + x \cdot (x)'}}{(x \cdot x)' = x' \cdot x + x \cdot x'}}{(x \cdot x)' \geq 0 \leftrightarrow x' \cdot x + x \cdot x' \geq 0}}{(x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}}{\dfrac{\vdash [x' = x^3][x' := x^3](x \cdot x \geq 1)'}{\dfrac{\vdash [x' = x^3](x \cdot x \geq 1)'}{x \cdot x \geq 1 \vdash [x' = x^3]x \cdot x \geq 1}\text{DI}}\text{DE}}\text{CE}
$$

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT
4. Construct differential invariant computation result forward accordingly
5. Resume backward proof with result computed by forward proof right

Left branch:

$$\mathbb{R}\quad \vdash x^3\cdot x + x\cdot x^3 \geq 0$$

$$[:=]\quad \vdash [x' := x^3]\,x'\cdot x + x\cdot x' \geq 0$$

$$\text{G}\quad \vdash [x' = x^3][x' := x^3]\,x'\cdot x + x\cdot x' \geq 0$$

Right branch:

$$*$$

$$\mathbb{R}\quad (x\cdot x)' = (x\cdot x)'$$

$$\cdot'\quad (x\cdot x)' = (x)'\cdot x + x\cdot (x)'$$

$$x'\quad (x\cdot x)' = x'\cdot x + x\cdot x'$$

$$\text{CT}\quad (x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$

$$(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$

Conclusion:

$$\text{CE}\quad \vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'$$

$$\text{DE}\quad \vdash [x' = x^3](x\cdot x \geq 1)'$$

$$\text{DI}\quad x\cdot x \geq 1 \vdash [x' = x^3]\,x\cdot x \geq 1$$

Example: Differential Invariants — Computation

1. Start with identity differential computation result which proves
2. Construct differential computation result forward by $\cdot'$ x'
3. Embed differential computation result forward by CT
4. Construct differential invariant computation result forward accordingly
5. Resume backward proof with result computed by forward proof right

Left branch (read bottom-up):

$$*$$
$$\mathbb{R}\quad \vdash x^3\cdot x + x\cdot x^3 \geq 0$$
$$[:=]\quad \vdash [x' := x^3]x'\cdot x + x\cdot x' \geq 0$$
$$G\quad \vdash [x' = x^3][x' := x^3]x'\cdot x + x\cdot x' \geq 0$$

Right branch (read bottom-up):

$$*$$
$$\mathbb{R}\quad (x\cdot x)' = (x\cdot x)'$$
$$\cdot'\quad (x\cdot x)' = (x)'\cdot x + x\cdot (x)'$$
$$x'\quad (x\cdot x)' = x'\cdot x + x\cdot x'$$
$$CT\quad (x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$
$$(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0$$

Conclusion:

$$CE\quad \vdash [x' = x^3][x' := x^3](x\cdot x \geq 1)'$$
$$DE\quad \vdash [x' = x^3](x\cdot x \geq 1)'$$
$$DI\quad x\cdot x \geq 1 \vdash [x' = x^3]x\cdot x \geq 1$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

If you bind a free variable, you go to logic jail!

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \wedge [x' = v]x > 0}$$

Theorem (Soundness) replace all occurrences of $p(\cdot)$

Modular interface: Prover vs. Logic

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

If you bind a free variable, you go to logic jail!

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \land [x' = v]x > 0}$$

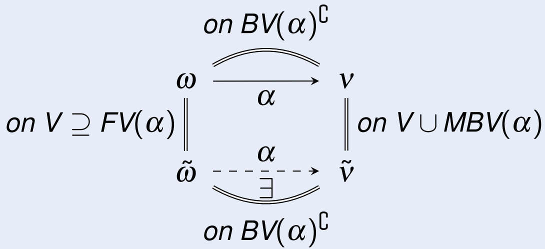
Lemma (Bound effect lemma) (Only BV(·) change)

If $(\omega, \nu) \in [\![\alpha]\!]$, *then* $\omega = \nu$ *on* $BV(\alpha)^\complement$.

Lemma (Coincidence lemma) (Only FV(·) determine truth)

If $\omega = \tilde{\omega}$ *on* $FV(\theta)$ *and* $I = J$ *on* $\Sigma(\theta)$, *then* $\omega[\![\theta]\!] = \tilde{\omega}[\![\theta]\!]$

If $\omega = \tilde{\omega}$ *on* $FV(\phi)$ $\omega \in [\![\phi]\!]$ *iff* $\tilde{\omega} \in J[\![\phi]\!]$



Correctness of Static Semantics

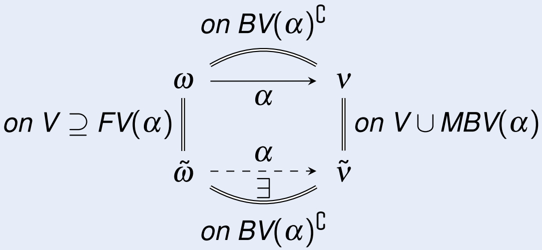
Lemma (Bound effect lemma) (Only BV(·) change)

If $(\omega, \nu) \in [\![\alpha]\!]$, *then* $\omega = \nu$ *on* $BV(\alpha)^\complement$.

Lemma (Coincidence lemma) (Only FV(·) determine truth)

If $\omega = \tilde{\omega}$ *on* $FV(\theta)$ *and* $I = J$ *on* $\Sigma(\theta)$, *then* $\omega[\![\theta]\!] = \tilde{\omega}[\![\theta]\!]$

If $\omega = \tilde{\omega}$ *on* $FV(\phi)$ $\omega \in [\![\phi]\!]$ *iff* $\tilde{\omega} \in J[\![\phi]\!]$



Differential Dynamic Logic dL: Static Semantics

$$
\begin{aligned}
\mathrm{FV}((\theta)') &= \\
\mathrm{FV}(p(\theta_1, \ldots, \theta_k)) &= \\
\mathrm{FV}(\phi \land \psi) &= \\
\mathrm{FV}(\forall x\, \phi) = \mathrm{FV}(\exists x\, \phi) &= \\
\mathrm{FV}([\alpha]\phi) = \mathrm{FV}(\langle\alpha\rangle\phi) &= \\
\mathrm{FV}(a) &= \\
\mathrm{FV}(x := \theta) &= \\
\mathrm{FV}(?Q) &= \\
\mathrm{FV}(x' = \theta \,\&\, Q) &= \\
\mathrm{FV}(\alpha \cup \beta) &= \\
\mathrm{FV}(\alpha; \beta) &= \\
\mathrm{FV}(\alpha^*) &=
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{FV}((\theta)') &= \mathsf{FV}(\theta) \\
\hline
\mathsf{FV}(p(\theta_1,\dots,\theta_k)) &= \mathsf{FV}(\theta_1)\cup\dots\cup\mathsf{FV}(\theta_k) \\
\mathsf{FV}(\phi\land\psi) &= \mathsf{FV}(\phi)\cup\mathsf{FV}(\psi) \\
\mathsf{FV}(\forall x\,\phi) = \mathsf{FV}(\exists x\,\phi) &= \mathsf{FV}(\phi)\setminus\{x\} \\
\mathsf{FV}([\alpha]\phi) = \mathsf{FV}(\langle\alpha\rangle\phi) &= \mathsf{FV}(\alpha)\cup(\mathsf{FV}(\phi)\setminus\mathsf{BV}(\alpha)) \\
\hline
\mathsf{FV}(a) &= \mathscr{V} \qquad \text{for program symbol } a \\
\mathsf{FV}(x:=\theta) &= \mathsf{FV}(\theta) \\
\mathsf{FV}(?Q) &= \mathsf{FV}(Q) \\
\mathsf{FV}(x'=\theta\,\&\,Q) &= \{x\}\cup\mathsf{FV}(\theta)\cup\mathsf{FV}(Q) \\
\mathsf{FV}(\alpha\cup\beta) &= \mathsf{FV}(\alpha)\cup\mathsf{FV}(\beta) \\
\mathsf{FV}(\alpha;\beta) &= \mathsf{FV}(\alpha)\cup(\mathsf{FV}(\beta)\setminus\mathsf{BV}(\alpha)) \\
\mathsf{FV}(\alpha^*) &= \mathsf{FV}(\alpha)
\end{aligned}
$$

$$\mathrm{FV}((\theta)') = \mathrm{FV}(\theta) \cup \mathrm{FV}(\theta)' \qquad \text{caution}$$

$$\mathrm{FV}(p(\theta_1,\dots,\theta_k)) = \mathrm{FV}(\theta_1) \cup \dots \cup \mathrm{FV}(\theta_k)$$

$$\mathrm{FV}(\phi \wedge \psi) = \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi)$$

$$\mathrm{FV}(\forall x\, \phi) = \mathrm{FV}(\exists x\, \phi) = \mathrm{FV}(\phi) \setminus \{x\}$$

$$\mathrm{FV}([\alpha]\phi) = \mathrm{FV}(\langle\alpha\rangle\phi) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha)) \qquad \text{caution}$$

$$\mathrm{FV}(a) = \mathscr{V} \qquad \text{for program symbol } a$$

$$\mathrm{FV}(x := \theta) = \mathrm{FV}(\theta)$$

$$\mathrm{FV}(?Q) = \mathrm{FV}(Q)$$

$$\mathrm{FV}(x' = \theta \,\&\, Q) = \{x\} \cup \mathrm{FV}(\theta) \cup \mathrm{FV}(Q)$$

$$\mathrm{FV}(\alpha \cup \beta) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta)$$

$$\mathrm{FV}(\alpha;\beta) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) \qquad \text{caution}$$

$$\mathrm{FV}(\alpha^*) = \mathrm{FV}(\alpha)$$

$$
\begin{aligned}
\mathrm{BV}(\theta \geq \eta) = \mathrm{BV}(p(\theta_1, \ldots, \theta_k)) &= \\
\mathrm{BV}(\phi \wedge \psi) &= \\
\mathrm{BV}(\forall x\, \phi) = \mathrm{BV}(\exists x\, \phi) &= \\
\mathrm{BV}([\alpha]\phi) = \mathrm{BV}(\langle\alpha\rangle\phi) &= \\
\mathrm{BV}(a) &= \\
\mathrm{BV}(x := \theta) &= \\
\mathrm{BV}(?Q) &= \\
\mathrm{BV}(x' = \theta \,\&\, Q) &= \\
\mathrm{BV}(\alpha \cup \beta) = \mathrm{BV}(\alpha; \beta) &= \\
\mathrm{BV}(\alpha^*) &=
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{BV}(\theta \geq \eta) = \mathrm{BV}(p(\theta_1,\dots,\theta_k)) &= \emptyset \\
\mathrm{BV}(\phi \land \psi) &= \mathrm{BV}(\phi) \cup \mathrm{BV}(\psi) \\
\mathrm{BV}(\forall x\, \phi) = \mathrm{BV}(\exists x\, \phi) &= \{x\} \cup \mathrm{BV}(\phi) \\
\mathrm{BV}([\alpha]\phi) = \mathrm{BV}(\langle\alpha\rangle\phi) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\phi) \\
\hline
\mathrm{BV}(a) &= \mathscr{V} \qquad \text{for program symbol } a \\
\mathrm{BV}(x := \theta) &= \{x\} \\
\mathrm{BV}(?Q) &= \emptyset \\
\mathrm{BV}(x' = \theta \,\&\, Q) &= \{x, x'\} \\
\mathrm{BV}(\alpha \cup \beta) = \mathrm{BV}(\alpha;\beta) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta) \\
\mathrm{BV}(\alpha^*) &= \mathrm{BV}(\alpha)
\end{aligned}
$$

$$\begin{aligned}
\mathsf{BV}(\theta \geq \eta) = \mathsf{BV}(p(\theta_1,\dots,\theta_k)) &= \emptyset \\
\mathsf{BV}(\phi \land \psi) &= \mathsf{BV}(\phi) \cup \mathsf{BV}(\psi) \\
\mathsf{BV}(\forall x\,\phi) = \mathsf{BV}(\exists x\,\phi) &= \{x\} \cup \mathsf{BV}(\phi) \\
\mathsf{BV}([\alpha]\phi) = \mathsf{BV}(\langle\alpha\rangle\phi) &= \mathsf{BV}(\alpha) \cup \mathsf{BV}(\phi)
\end{aligned}$$

$$\begin{aligned}
\mathsf{BV}(a) &= \mathscr{V} && \text{for program symbol } a \\
\mathsf{BV}(x := \theta) &= \{x\} \\
\mathsf{BV}(?Q) &= \emptyset \\
\mathsf{BV}(x' = \theta \,\&\, Q) &= \{x, x'\} \\
\mathsf{BV}(\alpha \cup \beta) = \mathsf{BV}(\alpha;\beta) &= \mathsf{BV}(\alpha) \cup \mathsf{BV}(\beta) \\
\mathsf{BV}(\alpha^*) &= \mathsf{BV}(\alpha)
\end{aligned}$$

$$\begin{aligned}
\mathsf{MBV}(a) &= \\
\mathsf{MBV}(\alpha) &= \\
\mathsf{MBV}(\alpha \cup \beta) &= \\
\mathsf{MBV}(\alpha;\beta) &= \\
\mathsf{MBV}(\alpha^*) &=
\end{aligned}$$

$$
\begin{aligned}
\mathrm{BV}(\theta \geq \eta) = \mathrm{BV}(p(\theta_1,\dots,\theta_k)) &= \emptyset \\
\mathrm{BV}(\phi \land \psi) &= \mathrm{BV}(\phi) \cup \mathrm{BV}(\psi) \\
\mathrm{BV}(\forall x\, \phi) = \mathrm{BV}(\exists x\, \phi) &= \{x\} \cup \mathrm{BV}(\phi) \\
\mathrm{BV}([\alpha]\phi) = \mathrm{BV}(\langle\alpha\rangle\phi) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\phi)
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{BV}(a) &= \mathscr{V} && \text{for program symbol } a \\
\mathrm{BV}(x := \theta) &= \{x\} \\
\mathrm{BV}(?Q) &= \emptyset \\
\mathrm{BV}(x' = \theta \,\&\, Q) &= \{x, x'\} \\
\mathrm{BV}(\alpha \cup \beta) = \mathrm{BV}(\alpha;\beta) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta) \\
\mathrm{BV}(\alpha^*) &= \mathrm{BV}(\alpha)
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{MBV}(a) &= \emptyset && \text{program symbol } a \\
\mathrm{MBV}(\alpha) &= \mathrm{BV}(\alpha) && \text{other atomic HPs } \alpha \\
\mathrm{MBV}(\alpha \cup \beta) &= \mathrm{MBV}(\alpha) \cap \mathrm{MBV}(\beta) \\
\mathrm{MBV}(\alpha;\beta) &= \mathrm{MBV}(\alpha) \cup \mathrm{MBV}(\beta) \\
\mathrm{MBV}(\alpha^*) &= \emptyset
\end{aligned}
$$

Correctness of Static Semantics

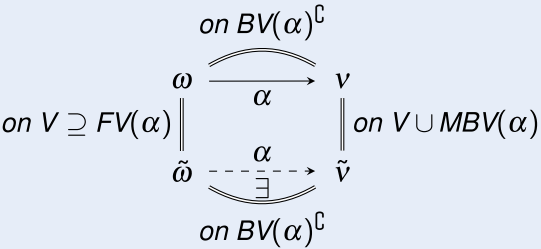
Lemma (Bound effect lemma) (Only BV(·) change)

If $(\omega, \nu) \in [\![\alpha]\!]$, *then* $\omega = \nu$ *on* $BV(\alpha)^{\complement}$.

Lemma (Coincidence lemma) (Only FV(·) determine truth)

If $\omega = \tilde{\omega}$ *on* $FV(\theta)$ *and* $I = J$ *on* $\Sigma(\theta)$, *then* $\omega[\![\theta]\!] = \tilde{\omega}[\![\theta]\!]$

If $\omega = \tilde{\omega}$ *on* $FV(\phi)$ $\omega \in [\![\phi]\!]$ *iff* $\tilde{\omega} \in J[\![\phi]\!]$



Theorem (Soundness) replace all occurrences of $p(\cdot)$

Modular interface: Prover vs. Logic

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

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \text{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

If you bind a free variable, you go to logic jail!

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function sym. $f(\theta)$ for any θ by $\eta(\theta)$
program sym. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[v := v+1 \cup x' = v]x > 0 \leftrightarrow [v := v+1]x > 0 \wedge [x' = v]x > 0}$$

Differential Equation Axioms & Differential Axioms

DW $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)]\big(q(x) \rightarrow p(x)\big)$

DI $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [?q(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)](p(x))'$

DC $\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \wedge r(x)]p(x)\big)$
$\leftarrow [x' = f(x)\,\&\,q(x)]r(x)$

DE $[x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$

DG $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$

DS $[x' = c\,\&\,q(x)]p(x) \leftrightarrow \forall t{\geq}0\,\big((\forall 0{\leq}s{\leq}t\; q(x+cs)) \rightarrow [x := x+ct]p(x)\big)$

$+'$ $(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$

$\cdot'$ $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

c' $(c)' = 0$

André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Cham, 2018.
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
J. Autom. Reas., 59(2):219–265, 2017.
doi:10.1007/s10817-016-9385-1.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481, Berlin, 2015. Springer.
doi:10.1007/978-3-319-21401-6_32.

André Platzer.
The complete proof theory of hybrid systems.
In LICS [7], pages 541–550.
doi:10.1109/LICS.2012.64.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.
doi:10.1145/2817824.

André Platzer.
Logics of dynamical systems.
In LICS [7], pages 13–24.
doi:10.1109/LICS.2012.13.

Logic in Computer Science (LICS), 2012 27th Annual IEEE Symposium on, Los Alamitos, 2012. IEEE.

Definition (Term semantics) $([\![\cdot]\!] : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R}))$

$$
\begin{aligned}
\omega[\![f(\theta_1,\dots,\theta_k)]\!] &= I(f)\big(\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]\big) \qquad I(f) : \mathbb{R}^k \to \mathbb{R} \text{ smooth}\\
\omega[\![(\theta)']\!] &= \sum_x \omega(x')\frac{\partial[\![\theta]\!]}{\partial x}(\omega)
\end{aligned}
$$

Definition (dL semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S}))$

$$
\begin{aligned}
[\![p(\theta_1,\dots,\theta_k)]\!] &= \{\omega : (\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]) \in I(p)\} \qquad I(p) \subseteq \mathbb{R}^k\\
[\![\langle\alpha\rangle\phi]\!] &= [\![\alpha]\!] \circ [\![\phi]\!]
\end{aligned}
$$

P valid iff $\omega \in [\![P]\!]$ for all states ω of all interpretations I

Definition (Program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$
\begin{aligned}
[\![a]\!] &= I(a) \qquad I(a) \subseteq \mathscr{S} \times \mathscr{S}\\
[\![x' = f(x)\,\&\,Q]\!] &= \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) : \varphi \models x' = f(x) \land Q\}\\
[\![\alpha \cup \beta]\!] &= [\![\alpha]\!] \cup [\![\beta]\!]\\
[\![\alpha;\beta]\!] &= [\![\alpha]\!] \circ [\![\beta]\!]\\
[\![\alpha^*]\!] &= \big([\![\alpha]\!]\big)^* = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]
\end{aligned}
$$

Definition (Term semantics) $(\llbracket\cdot\rrbracket : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R}))$

$$
\begin{aligned}
\omega\llbracket x\rrbracket &= \omega(x) && \text{for variable } x \in \mathscr{V}\\
\omega\llbracket \theta+\eta\rrbracket &= \omega\llbracket\theta\rrbracket + \omega\llbracket\eta\rrbracket\\
\omega\llbracket \theta\cdot\eta\rrbracket &= \omega\llbracket\theta\rrbracket \cdot \omega\llbracket\eta\rrbracket\\
\omega\llbracket f(\theta_1,\dots,\theta_k)\rrbracket &= I(f)\big(\omega\llbracket\theta_1\rrbracket,\dots,\omega\llbracket\theta_k\rrbracket\big) && I(f) : \mathbb{R}^k \to \mathbb{R} \text{ smooth}\\
\omega\llbracket(\theta)'\rrbracket &= \sum_x \omega(x')\frac{\partial\llbracket\theta\rrbracket}{\partial x}(\omega)
\end{aligned}
$$

Definition (dL semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathscr{S}))$

$$
\begin{aligned}
\llbracket p(\theta_1,\dots,\theta_k)\rrbracket &= \{\omega : (\omega\llbracket\theta_1\rrbracket,\dots,\omega\llbracket\theta_k\rrbracket) \in I(p)\} && I(p) \subseteq \mathbb{R}^k\\
\llbracket\langle\alpha\rangle\phi\rrbracket &= \llbracket\alpha\rrbracket \circ \llbracket\phi\rrbracket\\
\llbracket[\alpha]\phi\rrbracket &= \llbracket\neg\langle\alpha\rangle\neg\phi\rrbracket
\end{aligned}
$$

Definition (Program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathscr{S}\times\mathscr{S}))$

$$
\begin{aligned}
\llbracket a\rrbracket &= I(a) && I(a) \subseteq \mathscr{S}\times\mathscr{S}\\
\llbracket x' = f(x) \,\&\, Q\rrbracket &= \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) : \varphi \models x' = f(x) \land Q\}\\
\llbracket\alpha\cup\beta\rrbracket &= \llbracket\alpha\rrbracket \cup \llbracket\beta\rrbracket\\
\llbracket\alpha;\beta\rrbracket &= \llbracket\alpha\rrbracket \circ \llbracket\beta\rrbracket
\end{aligned}
$$

Differential Dynamic Logic with Interpretations: Semantics

Definition (Term semantics) ($[\![\cdot]\!] : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R})$)

$$\omega[\![f(\theta_1,\dots,\theta_k)]\!] = I(f)\big(\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]\big) \qquad I(f) : \mathbb{R}^k \to \mathbb{R} \text{ smooth}$$

$$\omega[\![(\theta)']\!] = \sum_x \omega(x')\frac{\partial[\![\theta]\!]}{\partial x}(\omega)$$

Definition (dL semantics) ($[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S})$)

$$[\![\theta \geq \eta]\!] = \{\omega : \omega[\![\theta]\!] \geq \omega[\![\eta]\!]\}$$

$$[\![p(\theta_1,\dots,\theta_k)]\!] = \{\omega : (\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]) \in I(p)\} \qquad I(p) \subseteq \mathbb{R}^k$$

$$[\![\neg\phi]\!] = ([\![\phi]\!])^{\complement}$$

$$[\![\phi \land \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$$

$$[\![\exists x\, \phi]\!] = \{\omega \in \mathscr{S} : \omega_x^r \in [\![\phi]\!] \text{ for some } r \in \mathbb{R}\}$$

$$[\![\langle\alpha\rangle\phi]\!] = [\![\alpha]\!] \circ [\![\phi]\!] = \{\omega : \nu \in [\![\phi]\!] \text{ for some } \nu\ (\omega,\nu) \in [\![\alpha]\!]\}$$

$$[\![[\alpha]\phi]\!] = [\![\neg\langle\alpha\rangle\neg\phi]\!] = \{\omega : \nu \in [\![\phi]\!] \text{ for all } \nu\ (\omega,\nu) \in [\![\alpha]\!]\}$$

Definition (Program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S})$)

$$[\![a]\!] = I(a) \qquad I(a) \subseteq \mathscr{S} \times \mathscr{S}$$

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0)|_{\{x'\}^{\complement}}, \varphi(r)) : \varphi \models x' = f(x) \land Q\}$$

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

Definition (Term semantics) $([\![\cdot]\!] : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R}))$

$$\omega[\![f(\theta_1,\dots,\theta_k)]\!] = I(f)\big(\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]\big) \qquad I(f) : \mathbb{R}^k \to \mathbb{R} \text{ smooth}$$

$$\omega[\![(\theta)']\!] = \sum_x \omega(x')\frac{\partial[\![\theta]\!]}{\partial x}(\omega)$$

Definition (dL semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S}))$

$$[\![p(\theta_1,\dots,\theta_k)]\!] = \{\omega : (\omega[\![\theta_1]\!],\dots,\omega[\![\theta_k]\!]) \in I(p)\} \qquad I(p) \subseteq \mathbb{R}^k$$

$$[\![\langle\alpha\rangle\phi]\!] = [\![\alpha]\!] \circ [\![\phi]\!]$$

$$[\![[\alpha]\phi]\!] = [\![\neg\langle\alpha\rangle\neg\phi]\!]$$

Definition (Program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$[\![a]\!] = I(a) \qquad I(a) \subseteq \mathscr{S} \times \mathscr{S}$$

$$[\![x := \theta]\!] = \{(\omega,\nu) : \nu = \omega \text{ except } \nu[\![x]\!] = \omega[\![\theta]\!]\}$$

$$[\![?Q]\!] = \{(\omega,\omega) : \omega \in [\![Q]\!]\}$$

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) : \varphi \models x' = f(x) \wedge Q\}$$

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

$$[\![\alpha;\beta]\!] = [\![\alpha]\!] \circ [\![\beta]\!]$$

$$[\![\alpha^*]\!] = \big([\![\alpha]\!]\big)^* = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]$$