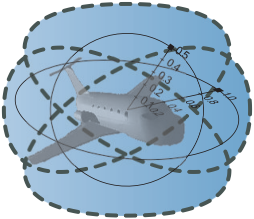
Uniform Substitution for Differential Game Logic

André Platzer

Carnegie Mellon University



Outline

Uniform Substitution is Fundamental but Crucial

Q: How to build a prover with a small soundness-critical core?

A: Uniform substitution [Church]

Q: Impact on hybrid systems prover core?

A: 65 989 $\searrow$ 1 651 LOC (2.5%) [KeYmaera X]

Q: Impact on hybrid games prover core?

A: months $\searrow$ minutes (+10 LOC) [KeYmaera X]

Q: How to prove soundness?

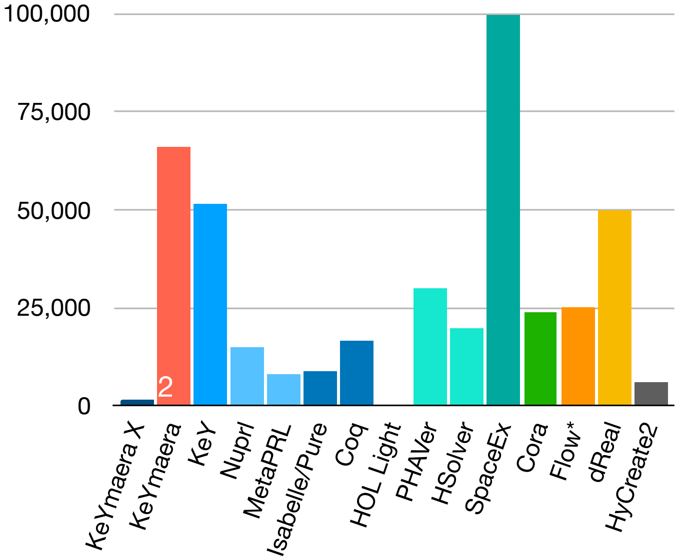
A: Uniform substitution enables modular soundness [Modularity]

Q: Biggest challenges for uniform substitution on games?

A: State transition relation impossible for games [Complications]

A: Transfinite induction for least fixpoint of loops $>\omega^\omega$

A: Conservative extension of formulas, not of axioms

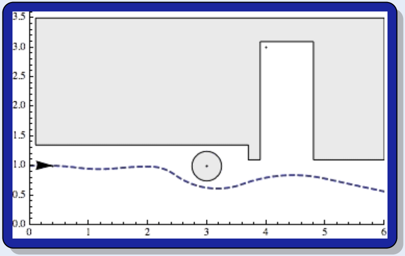


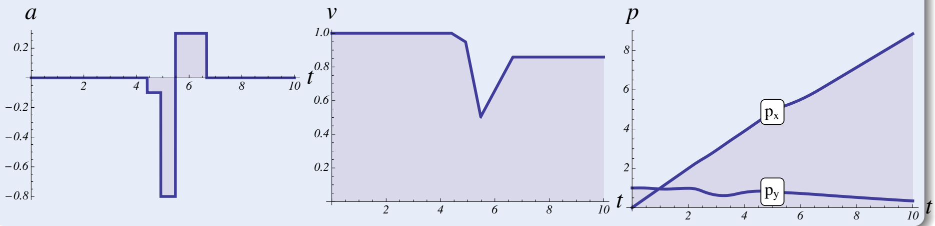
Disclaimer: Self-reported estimates of the soundness-critical lines of code + rules

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

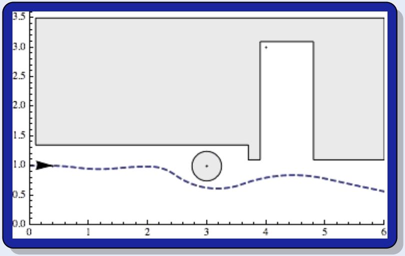


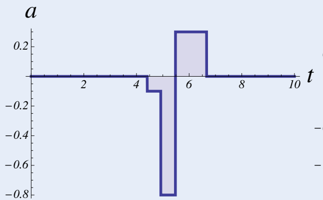


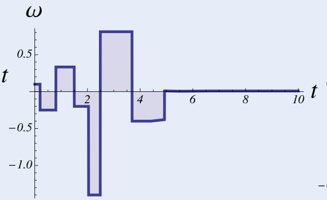
Challenge (Hybrid Systems)

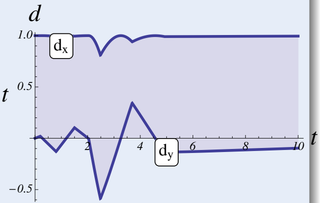
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







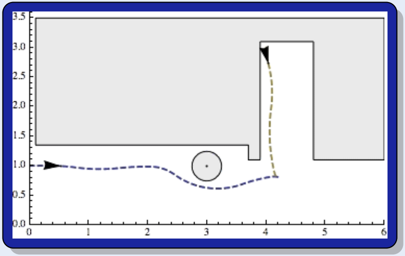


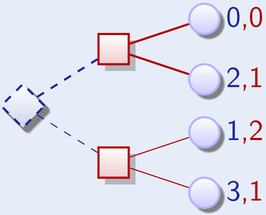
CPS Analysis: Robot Control

Challenge (Games)

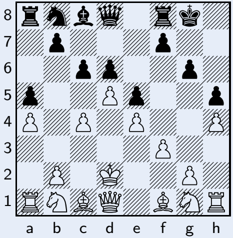
Game rules describing play evolution with both

- Angelic choices (player ◇ Angel)
- Demonic choices (player □ Demon)





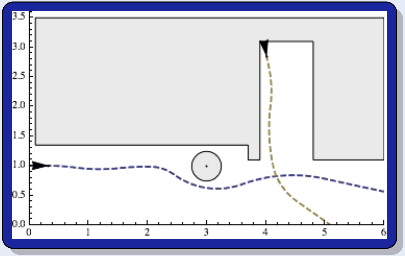
◇\□	Tr	Pl
Trash	1,2	0,0
Plant	0,0	2,1

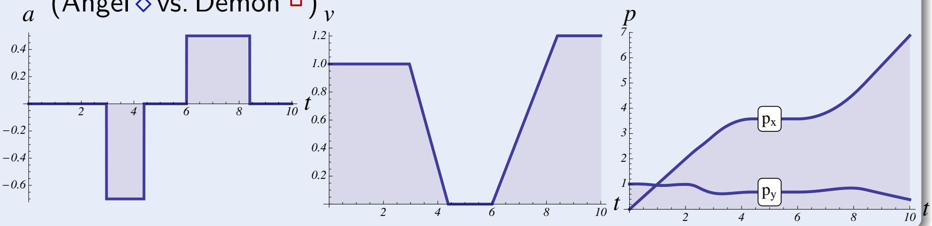


Challenge (Hybrid Games)

Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel ◇ vs. Demon □)



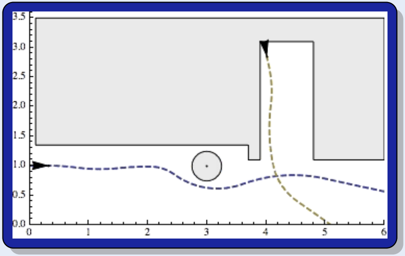


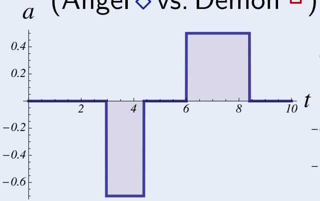
CPS Analysis: Robot Control

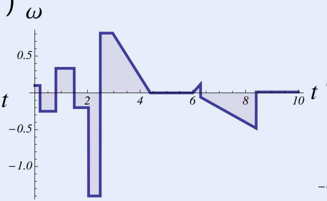
Challenge (Hybrid Games)

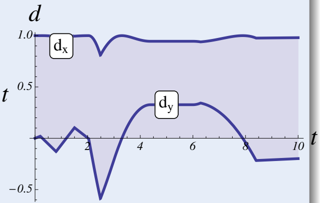
Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel ◇ vs. Demon □)





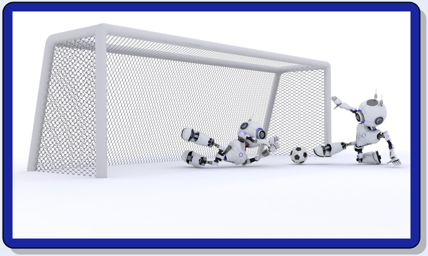


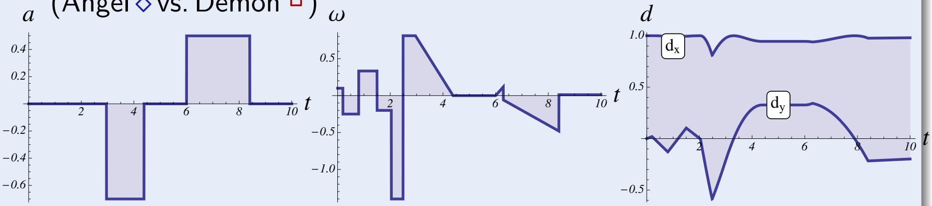


Challenge (Hybrid Games)

Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel ◇ vs. Demon □)





Differential Game Logic: Syntax

Definition (Hybrid game α)

$$a \mid x := \theta \mid ?q \mid x' = \theta \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula ϕ)

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

TOCL'15

Differential Game Logic: Syntax

Discrete Assign | Test Game | Differential Equation | Choice Game | Seq. Game | Repeat Game

Definition (Hybrid game α)

$$a \mid x := \theta \mid ?q \mid x' = \theta \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula ϕ)

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

All Reals | Some Reals

TOCL'15

Differential Game Logic: Syntax

Game Symb. | Discrete Assign | Test Game | Differential Equation | Choice Game | Seq. Game | Repeat Game | Dual Game

Definition (Hybrid game α)

$$a \mid x := \theta \mid ?q \mid x' = \theta \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula ϕ)

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

All Reals | Some Reals

TOCL'15

Differential Game Logic: Syntax

Game Symb. | Discrete Assign | Test Game | Differential Equation | Choice Game | Seq. Game | Repeat Game | Dual Game

Definition (Hybrid game α)

$$a \mid x := \theta \mid ?q \mid x' = \theta \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

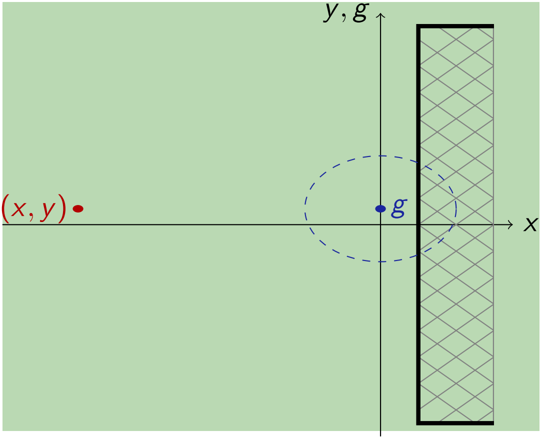
Definition (dGL Formula ϕ)

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

All Reals | Some Reals | Angel Wins | Demon Wins

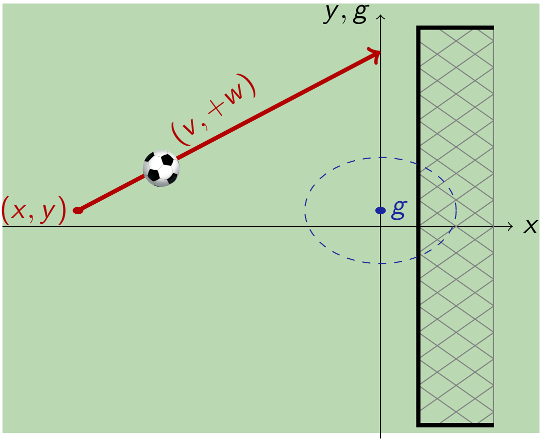
TOCL'15

Example: Goalie in Robot Soccer



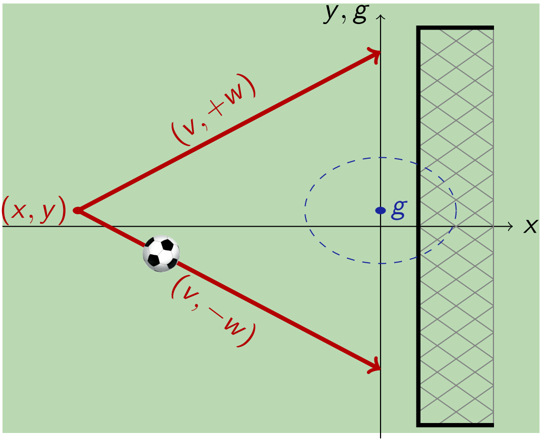
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\Big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \Big\rangle\, x^2 + (y-g)^2 \le 1$$

Example: Goalie in Robot Soccer



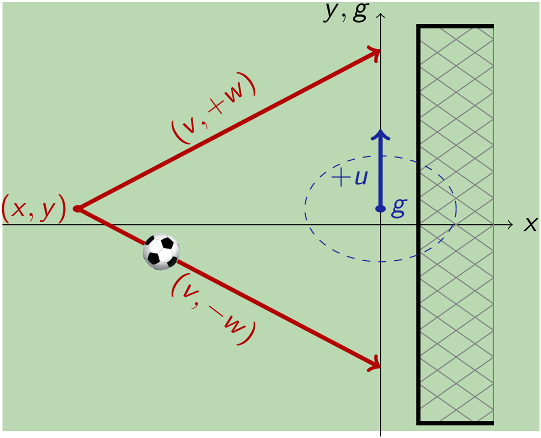
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\langle (w := +w \cap w := -w);$$
$$((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\})^* \rangle\, x^2 + (y - g)^2 \le 1$$

Example: Goalie in Robot Soccer



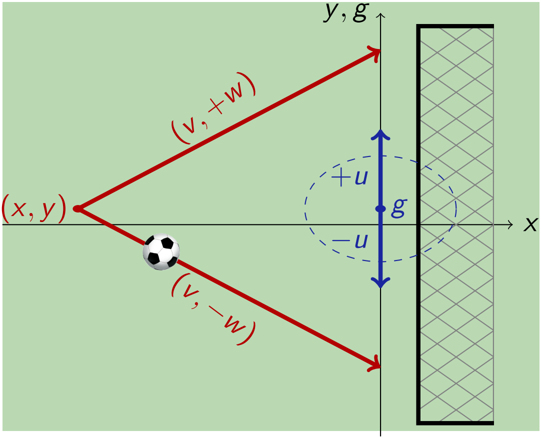
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\Big\langle (w := +w \cap w := -w); \big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \Big\rangle\, x^2 + (y - g)^2 \le 1$$

Example: Goalie in Robot Soccer



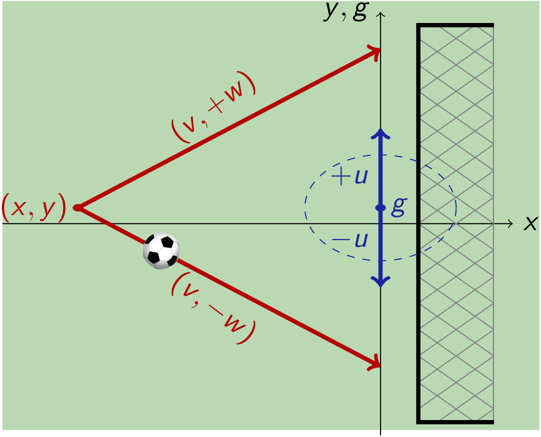
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \big\rangle\, x^2 + (y - g)^2 \le 1$$

Example: Goalie in Robot Soccer



$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \big\rangle\, x^2 + (y-g)^2 \le 1$$

Example: Goalie in Robot Soccer



Goalie's Secret

$$\left(\frac{x}{v}\right)^2 (u-w)^2 \leq 1 \land$$
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \big\rangle\, x^2 + (y-g)^2 \leq 1$$

Differential Game Logic: Denotational Semantics

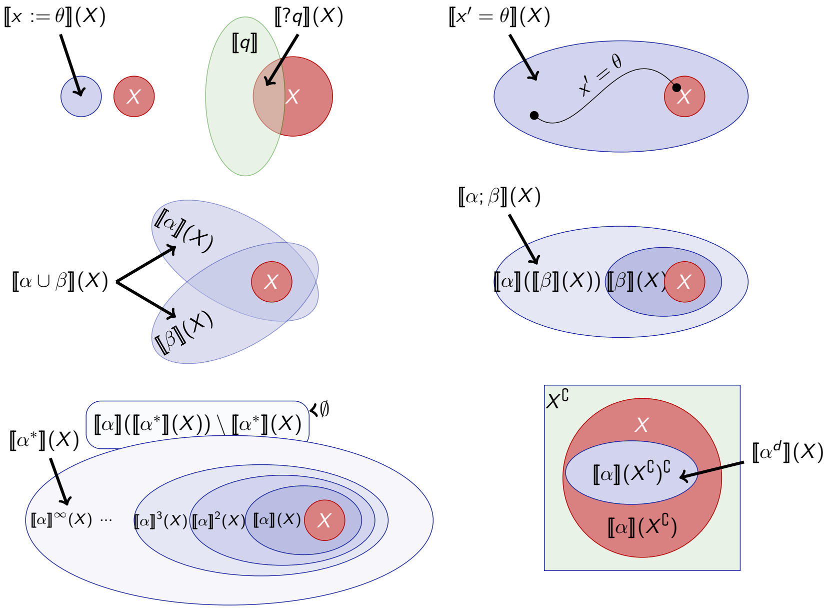
Definition (Hybrid game α) $[\![\cdot]\!] : \mathrm{HG} \to (\wp(\mathcal{S}) \to \wp(\mathcal{S}))$

$$
\begin{aligned}
[\![x := \theta]\!](X) &= \{\omega \in \mathcal{S} : \omega_x^{\omega[\![\theta]\!]} \in X\} \\
[\![x' = \theta]\!](X) &= \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X, \frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = \varphi(\zeta)[\![\theta]\!] \text{ for all } \zeta\} \\
[\![?q]\!](X) &= [\![q]\!] \cap X \\
[\![\alpha \cup \beta]\!](X) &= [\![\alpha]\!](X) \cup [\![\beta]\!](X) \\
[\![\alpha; \beta]\!](X) &= [\![\alpha]\!]([\![\beta]\!](X)) \\
[\![\alpha^*]\!](X) &= \bigcap\{Z \subseteq \mathcal{S} : X \cup [\![\alpha]\!](Z) \subseteq Z\} \\
[\![\alpha^d]\!](X) &= ([\![\alpha]\!](X^{\complement}))^{\complement}
\end{aligned}
$$

Definition (dGL Formula ϕ) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S})$

$$
\begin{aligned}
[\![\theta \geq \eta]\!] &= \{\omega \in \mathcal{S} : \omega[\![\theta]\!] \geq \omega[\![\eta]\!]\} \\
[\![\neg\phi]\!] &= ([\![\phi]\!])^{\complement} \\
[\![\phi \wedge \psi]\!] &= [\![\phi]\!] \cap [\![\psi]\!] \\
[\![\langle\alpha\rangle\phi]\!] &= [\![\alpha]\!]([\![\phi]\!]) \\
[\![[\alpha]\phi]\!] &= [\![\alpha]\!]([\![\phi]\!]^{\complement})^{\complement}
\end{aligned}
$$

Differential Game Logic: Denotational Semantics



Uniform Substitution

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

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

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 operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)
"If you bind a free variable, you go to logic jail!"

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

Uniform Substitution

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

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

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 operator $\otimes$
are not 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 symb. $f(\theta)$ for any θ by $\eta(\theta)$
game symbol a by α

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

Uniform Substitution

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

Modular interface: Prover vs. Logic

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

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 operator $\otimes$
are not 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 symb. $f(\theta)$ for any θ by $\eta(\theta)$
game symbol a by α

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

Axiom = one formula		Infinite axiom schema
$[a]p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$	$[\cdot]$	$[\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$
$\langle x := f\rangle p(x) \leftrightarrow p(f)$	$\langle:=\rangle$	$\langle x := \theta\rangle\phi \leftrightarrow \phi(\theta)$
$\langle x' = f\rangle p(x) \leftrightarrow \exists t{\geq}0\, \langle x := x + ft\rangle p(x)$	$\langle'\rangle$	$\langle x' = \theta\rangle\phi \leftrightarrow \exists t{\geq}0\, \langle x := y(t)\rangle\phi$
$\langle ?q\rangle p \leftrightarrow (q \land p)$	$\langle ?\rangle$	$\langle ?\psi\rangle\phi \leftrightarrow (\psi \land \phi)$
$\langle a \cup b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle p(\bar{x}) \lor \langle b\rangle p(\bar{x})$	$\langle\cup\rangle$	$\langle\alpha \cup \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi \lor \langle\beta\rangle\phi$
$\langle a; b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle\langle b\rangle p(\bar{x})$	$\langle;\rangle$	$\langle\alpha; \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$
$\langle a^*\rangle p(\bar{x}) \leftrightarrow p(\bar{x}) \lor \langle a\rangle\langle a^*\rangle p(\bar{x})$	$\langle^*\rangle$	$\langle\alpha^*\rangle\phi \leftrightarrow \phi \lor \langle\alpha\rangle\langle\alpha^*\rangle\phi$
$\langle a^d\rangle p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$	$\langle^d\rangle$	$\langle\alpha^d\rangle\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$

IJCAR'18 TOCL'15

Example Proof

$$\langle;\rangle \frac{}{j(x) \vdash \langle (v := 2 \cup v := x)^d; x' = v \rangle x>0}$$

Example Proof

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

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

$$\langle ;\rangle\frac{\langle^d\rangle\dfrac{}{j(x) \vdash \langle(v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x{>}0}}{j(x) \vdash \langle(v := 2 \cup v := x)^d; x' = v\rangle x{>}0}$$

Example Proof

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

$$\text{US}\ \dfrac{\langle a^d\rangle p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})}{\langle (v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x>0 \leftrightarrow \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x>0}$$

$$\langle\cup\rangle\ \dfrac{}{j(x) \vdash \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x>0}$$

$$\langle{}^d\rangle\ \dfrac{}{j(x) \vdash \langle (v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x>0}$$

$$\langle;\rangle\ \dfrac{}{j(x) \vdash \langle (v := 2 \cup v := x)^d ; x' = v\rangle x>0}$$

Example Proof

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

$$\text{US}\frac{\langle a \cup b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle p(\bar{x}) \lor \langle b\rangle p(\bar{x})}{\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x>0 \leftrightarrow \langle v := 2\rangle\neg\langle x' = v\rangle x>0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x>0}$$

$$\langle{:=}\rangle\frac{}{j(x) \vdash \neg(\langle v := 2\rangle\neg\langle x' = v\rangle x>0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x>0)}$$
$$\langle\cup\rangle\frac{}{j(x) \vdash \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x>0}$$
$$\langle^d\rangle\frac{}{j(x) \vdash \langle(v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x>0}$$
$$\langle;\rangle\frac{}{j(x) \vdash \langle(v := 2 \cup v := x)^d; x' = v\rangle x>0}$$

Example Proof

$$\sigma = \{f \mapsto 2, p(\cdot) \mapsto \neg\langle x'{=}\cdot\rangle x{>}0\} \qquad \sigma = \{f \mapsto x, p(\cdot) \mapsto \neg\langle x'{=}\cdot\rangle x{>}0\}$$

$$\frac{\langle v := f\rangle p(v) \leftrightarrow p(f)}{\langle v := 2\rangle\neg\langle x'{=}v\rangle x{>}0 \leftrightarrow \neg\langle x'{=}2\rangle x{>}0} \qquad \frac{\langle v := f\rangle p(v) \leftrightarrow p(f) \quad ↯}{\langle v := x\rangle\neg\langle x'{=}v\rangle x{>}0 \leftrightarrow \neg\langle x'{=}x\rangle x{>}0}$$

$$\langle ' \rangle \frac{}{j(x) \vdash \neg(\neg\langle x' = 2\rangle x{>}0 \vee \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)}$$

$$\langle := \rangle \frac{}{j(x) \vdash \neg(\langle v := 2\rangle\neg\langle x' = v\rangle x{>}0 \vee \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)}$$

$$\langle \cup \rangle \frac{}{j(x) \vdash \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x{>}0}$$

$$\langle ^d \rangle \frac{}{j(x) \vdash \langle (v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x{>}0}$$

$$\langle ; \rangle \frac{}{j(x) \vdash \langle (v := 2 \cup v := x)^d; x' = v\rangle x{>}0}$$

Example Proof

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

v can't have ODE

$$\text{US}\;\frac{\langle x' = f\rangle p(x) \leftrightarrow \exists t{\geq}0\, \langle x := x{+}ft\rangle p(x)}{\langle x' = v\rangle x{>}0 \leftrightarrow \exists t{\geq}0\, \langle x := x{+}vt\rangle x{>}0}$$

$$\begin{array}{ll}
\langle{:=}\rangle & \overline{j(x) \vdash \neg(\neg\exists t{\geq}0\, \langle x := x{+}2t\rangle x{>}0 \lor \langle v := x\rangle\neg\exists t{\geq}0\, \langle x := x{+}vt\rangle x{>}0)} \\
\langle{'}\rangle & \overline{j(x) \vdash \neg(\neg\langle x' = 2\rangle x{>}0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)} \\
\langle{:=}\rangle & \overline{j(x) \vdash \neg(\langle v := 2\rangle\neg\langle x' = v\rangle x{>}0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)} \\
\langle\cup\rangle & \overline{j(x) \vdash \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x{>}0} \\
\langle{}^d\rangle & \overline{j(x) \vdash \langle (v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x{>}0} \\
\langle ;\rangle & \overline{j(x) \vdash \langle (v := 2 \cup v := x)^d; x' = v\rangle x{>}0}
\end{array}$$

Example Proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{j(x) \vdash \neg(\neg\exists t{\geq}0\, x{+}2t{>}0 \lor \neg\exists t{\geq}0\, x{+}(x)t{>}0)}{j(x) \vdash \neg(\neg\exists t{\geq}0\, \langle x := x{+}2t\rangle x{>}0 \lor \langle v := x\rangle\neg\exists t{\geq}0\, \langle x := x{+}vt\rangle x{>}0)}\langle:=\rangle}{j(x) \vdash \neg(\neg\langle x' = 2\rangle x{>}0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)}\langle'\rangle}{j(x) \vdash \neg(\langle v := 2\rangle\neg\langle x' = v\rangle x{>}0 \lor \langle v := x\rangle\neg\langle x' = v\rangle x{>}0)}\langle:=\rangle}{j(x) \vdash \neg\langle v := 2 \cup v := x\rangle\neg\langle x' = v\rangle x{>}0}\langle\cup\rangle}{j(x) \vdash \langle(v := 2 \cup v := x)^d\rangle\langle x' = v\rangle x{>}0}\langle^d\rangle}{j(x) \vdash \langle(v := 2 \cup v := x)^d; x' = v\rangle x{>}0}\langle;\rangle
$$

Example Proof

Summarize:

$$\frac{j(x) \vdash \neg(\neg\exists t{\geq}0\, x{+}2t{>}0 \vee \neg\exists t{\geq}0\, x{+}(x)t{>}0)}{j(x) \vdash \langle (v := 2 \cup v := x)^d; x' = v \rangle x > 0}$$

Example Proof

Summarize:

$$\frac{j(x) \vdash \neg(\neg\exists t{\geq}0\, x{+}2t{>}0 \vee \neg\exists t{\geq}0\, x{+}(x)t{>}0)}{j(x) \vdash \langle(v := 2 \cup v := x)^d; x' = v\rangle x > 0}$$

Using $\sigma = \{j(\cdot) \mapsto \cdot{>}{-1}\}$ on above derived rule proves:

$$\text{USR}\dfrac{\mathbb{R}\dfrac{}{x > -1 \vdash \neg(\neg\exists t{\geq}0\, x + 2t > 0 \vee \neg\exists t{\geq}0\, x + (x)t > 0)}}{x > -1 \vdash \langle(v := 2 \cup v := x)^d; x' = v\rangle x > 0}$$

Static Semantics

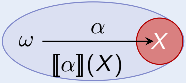
Lemma (Coincidence for formulas) (Only $FV(\phi)$ determine truth)

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

Static Semantics

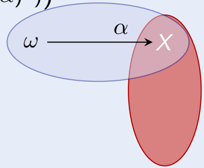
Lemma (Coincidence for games) (Only $\mathrm{FV}(\alpha)$ determine victory)

If $\omega = \tilde{\omega}$ *on* $V \supseteq \mathrm{FV}(\alpha)$, $I = J$ *on* $\Sigma(\alpha)$: $\omega \in [\![\alpha]\!](X{\uparrow}V)$ *iff* $\tilde{\omega} \in [\![\alpha]\!](X{\uparrow}V)$



Lemma (Bound effect) (Only $\mathrm{BV}(\alpha)$ change value)

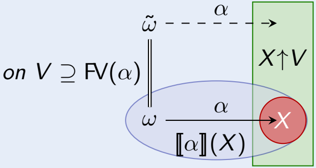
$\omega \in [\![\alpha]\!](X)$ *iff* $\omega \in [\![\alpha]\!](X{\downarrow}\omega(\mathrm{BV}(\alpha)^{\complement}))$



Static Semantics

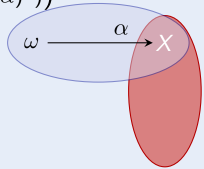
Lemma (Coincidence for games) (Only $\mathrm{FV}(\alpha)$ determine victory)

If $\omega = \tilde{\omega}$ *on* $V \supseteq \mathrm{FV}(\alpha)$, $I = J$ *on* $\Sigma(\alpha)$: $\omega \in [\![\alpha]\!](X{\uparrow}V)$ *iff* $\tilde{\omega} \in [\![\alpha]\!](X{\uparrow}V)$



Lemma (Bound effect) (Only $\mathrm{BV}(\alpha)$ change value)

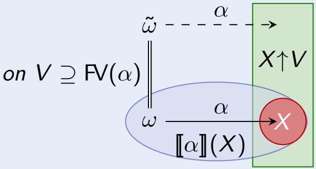
$\omega \in [\![\alpha]\!](X)$ *iff* $\omega \in [\![\alpha]\!](X{\downarrow}\omega(\mathrm{BV}(\alpha)^\complement))$



Static Semantics

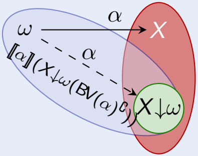
Lemma (Coincidence for games) (Only $FV(\alpha)$ determine victory)

If $\omega = \tilde{\omega}$ *on* $V \supseteq FV(\alpha)$, $I = J$ *on* $\Sigma(\alpha)$: $\omega \in [\![\alpha]\!](X\uparrow V)$ *iff* $\tilde{\omega} \in [\![\alpha]\!](X\uparrow V)$



Lemma (Bound effect) (Only $BV(\alpha)$ change value)

$\omega \in [\![\alpha]\!](X)$ *iff* $\omega \in [\![\alpha]\!](X\downarrow\omega(BV(\alpha)^\complement))$



Uniform Substitution

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

Modular interface: Prover vs. Logic

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

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 operator $\otimes$
are not 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 symb. $f(\theta)$ for any θ by $\eta(\theta)$
game symbol a by α

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

Soundness & Completeness

Theorem (Completeness)

dGL *calculus is a sound & complete axiomatization of hybrid games relative to any (differentially) expressive*[1] *logic L.*

$$\vDash \varphi \quad \text{iff} \quad Taut_L \vdash \varphi$$

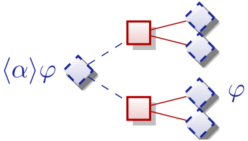
[1] $\forall \varphi \in \text{dGL} \; \exists \varphi^\flat \in L \quad \vDash \varphi \leftrightarrow \varphi^\flat$
$\langle x' = \theta \rangle G \leftrightarrow (\langle x' = \theta \rangle G)^\flat$ provable for $G \in L$

TOCL'15

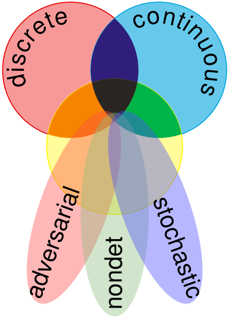
Uniform Substitution for Differential Game Logic

differential game logic

dGL = GL + HG = dL + ^{d}



- Uniform substitution for hybrid games
- Compositional PL + logic
- Sound & rel. complete axiomatization
- Modular: Logic $\|$ Prover
- Straightforward to implement (+10 LOC)
- Transfinite induction
- No transition relation
- Not conservative: $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha^*;\alpha]\phi$



A. Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer 2018

I Part: Elementary Cyber-Physical Systems

2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

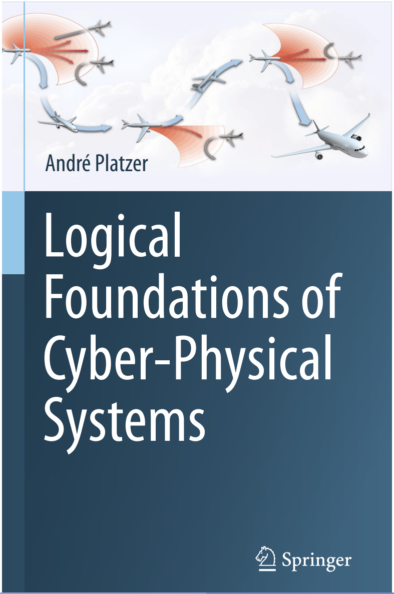
II Part: Differential Equations Analysis

10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems

14-17. Hybrid Systems & Hybrid Games

IV Part: Comprehensive CPS Correctness



André Platzer.
Uniform substitution for differential game logic.
In Didier Galmiche, Stephan Schulz, and Roberto Sebastiani, editors, *IJCAR*, volume 10900 of *LNCS*, pages 211–227. Springer, 2018.
doi:10.1007/978-3-319-94205-6_15.

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

André Platzer.
Differential hybrid games.
ACM Trans. Comput. Log., 18(3):19:1–19:44, 2017.
doi:10.1145/3091123.

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.
Logical Foundations of Cyber-Physical Systems.
Springer, Cham, 2018.
doi:10.1007/978-3-319-63588-0.

Differential Game Logic: Axiomatization

Axiom = one formula		Infinite axiom schema
$[a]p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$	$[\cdot]$	$[\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$
$\langle x:=f\rangle p(x) \leftrightarrow p(f)$	$\langle:=\rangle$	$\langle x:=\theta\rangle\phi \leftrightarrow \phi(\theta)$
$\langle x'=f\rangle p(x) \leftrightarrow \exists t{\geq}0\,\langle x:=x+ft\rangle p(x)$	$\langle'\rangle$	$\langle x'=\theta\rangle\phi \leftrightarrow \exists t{\geq}0\,\langle x:=y(t)\rangle\phi$
$\langle ?q\rangle p \leftrightarrow (q \land p)$	$\langle ?\rangle$	$\langle ?\psi\rangle\phi \leftrightarrow (\psi \land \phi)$
$\langle a\cup b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle p(\bar{x}) \lor \langle b\rangle p(\bar{x})$	$\langle\cup\rangle$	$\langle\alpha\cup\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi \lor \langle\beta\rangle\phi$
$\langle a;b\rangle p(\bar{x}) \leftrightarrow \langle a\rangle\langle b\rangle p(\bar{x})$	$\langle;\rangle$	$\langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$
$\langle a^*\rangle p(\bar{x}) \leftrightarrow p(\bar{x}) \lor \langle a\rangle\langle a^*\rangle p(\bar{x})$	$\langle{}^*\rangle$	$\langle\alpha^*\rangle\phi \leftrightarrow \phi \lor \langle\alpha\rangle\langle\alpha^*\rangle\phi$
$\langle a^d\rangle p(\bar{x}) \leftrightarrow \neg\langle a\rangle\neg p(\bar{x})$	$\langle{}^d\rangle$	$\langle\alpha^d\rangle\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$

IJCAR'18 TOCL'15

Differential Game Logic: Axiomatization

$\langle c\rangle\top$ uniformly substitutes to $\langle ?\phi\rangle\top$ alias ϕ

$[a]\langle c\rangle\top \leftrightarrow \neg\langle a\rangle\neg\langle c\rangle\top$	$[\cdot]$	$[\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$
$\langle x:=f\rangle p(x) \leftrightarrow p(f)$	$\langle:=\rangle$	$\langle x:=\theta\rangle\phi \leftrightarrow \phi(\theta)$
$\langle x'=f\rangle p(x) \leftrightarrow \exists t{\geq}0\,\langle x:=x+ft\rangle p(x)$	$\langle'\rangle$	$\langle x'=\theta\rangle\phi \leftrightarrow \exists t{\geq}0\,\langle x:=y(t)\rangle\phi$
$\langle ?q\rangle p \leftrightarrow (q\wedge p)$	$\langle ?\rangle$	$\langle ?\psi\rangle\phi \leftrightarrow (\psi\wedge\phi)$
$\langle a\cup b\rangle\langle c\rangle\top \leftrightarrow \langle a\rangle\langle c\rangle\top \vee \langle b\rangle\langle c\rangle\top$	$\langle\cup\rangle$	$\langle\alpha\cup\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi\vee\langle\beta\rangle\phi$
$\langle a;b\rangle\langle c\rangle\top \leftrightarrow \langle a\rangle\langle b\rangle\langle c\rangle\top$	$\langle;\rangle$	$\langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$
$\langle a^*\rangle\langle c\rangle\top \leftrightarrow \langle c\rangle\top \vee \langle a\rangle\langle a^*\rangle\langle c\rangle\top$	$\langle^*\rangle$	$\langle\alpha^*\rangle\phi \leftrightarrow \phi\vee\langle\alpha\rangle\langle\alpha^*\rangle\phi$
$\langle a^d\rangle\langle c\rangle\top \leftrightarrow \neg\langle a\rangle\neg\langle c\rangle\top$	$\langle^d\rangle$	$\langle\alpha^d\rangle\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$

IJCAR'18 TOCL'15

Axiom Schemata Need Side Conditions: Solving ODEs

$\langle ' \rangle \quad \langle x' = \theta \rangle \phi \leftrightarrow \exists t \geq 0 \, \langle x := y(t) \rangle \phi$

Axiom schema with side conditions:

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

Quite nontrivial soundness-critical algorithms ...

Static Semantics

$$\mathsf{FV}(\theta) = \{x \in \mathcal{V} : \exists I, \omega, \tilde{\omega} \text{ such that } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement} \text{ and } \omega[\![\theta]\!] \neq \tilde{\omega}[\![\theta]\!]\}$$
$$\mathsf{FV}(\phi) = \{x \in \mathcal{V} : \exists I, \omega, \tilde{\omega} \text{ such that } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement} \text{ and } \omega \in [\![\phi]\!] \not\ni \tilde{\omega}\}$$
$$\mathsf{FV}(\alpha) = \{x \in \mathcal{V} : \exists I, \omega, \tilde{\omega}, X \text{ with } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement},\ \omega \in [\![\alpha]\!](X{\uparrow}\{x\}^{\complement}) \not\ni \tilde{\omega}\}$$
$$\mathsf{BV}(\alpha) = \{x \in \mathcal{V} : \exists I, \omega, X \text{ such that } [\![\alpha]\!](X) \ni \omega \notin [\![\alpha]\!](X{\downarrow}\omega(\{x\}))\}$$

Soundness of Uniform Substitutions

"Syntactic uniform substitution = semantic replacement"

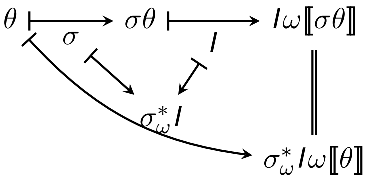
Lemma (Uniform substitution lemma)

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

$$I\omega[\![\sigma\theta]\!] = \sigma^*_\omega I\omega[\![\theta]\!]$$

$$\omega \in [\![\sigma\phi]\!] \text{ iff } \omega \in [\![\phi]\!]$$

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



Uniform Substitution of Rules

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

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi} \text{ locally sound} \quad \text{implies} \quad \frac{\sigma\phi_1 \quad \dots \quad \sigma\phi_n}{\sigma\psi} \text{ locally sound}$$

Uniform Substitution of Rules

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

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi} \text{ locally sound} \quad \text{implies} \quad \frac{\sigma\phi_1 \quad \dots \quad \sigma\phi_n}{\sigma\psi} \text{ locally sound}$$

Uniform Substitution of Rules

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

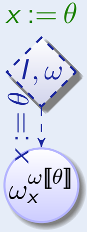
$$\frac{\phi_1 \quad \dots \quad \phi_n}{\psi} \textit{ locally sound} \quad \textit{implies} \quad \frac{\sigma\phi_1 \quad \dots \quad \sigma\phi_n}{\sigma\psi} \textit{ locally sound}$$

Locally sound

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

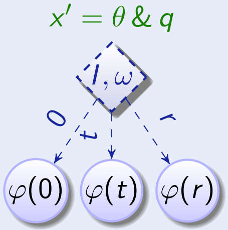
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



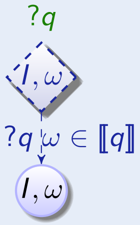
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



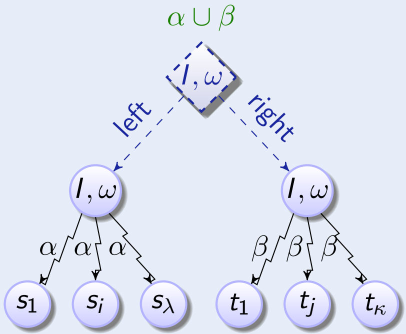
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



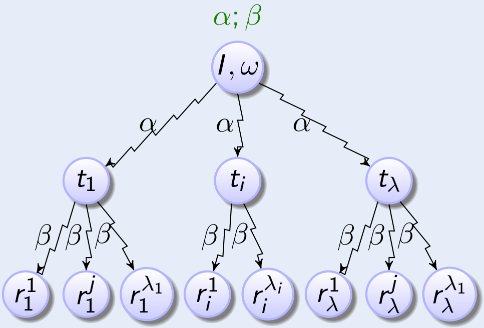
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



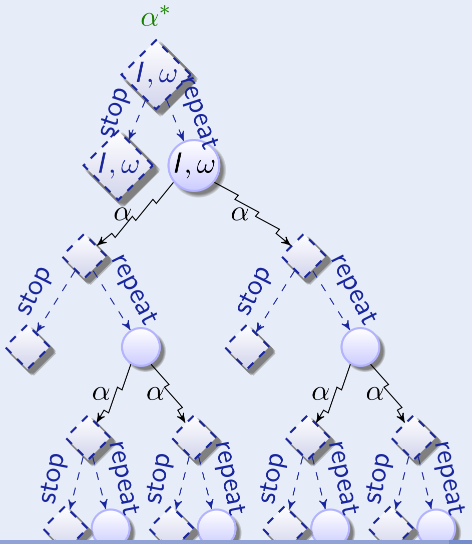
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)