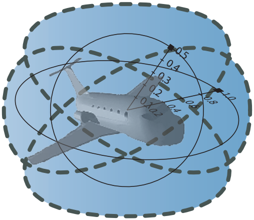
Logic of Hybrid Games

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

http://symbolaris.com/



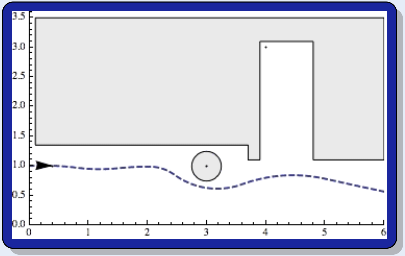
Outline

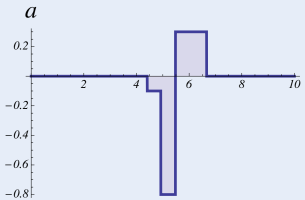
Can you trust a computer to control physics?

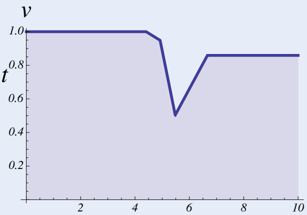
Challenge (Hybrid Systems)

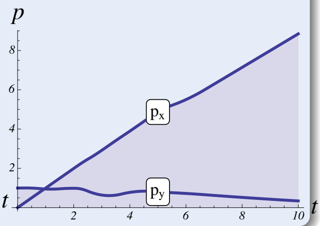
Fixed rule describing state evolution with both

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





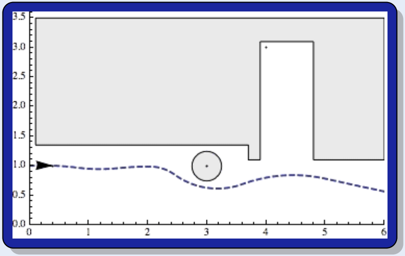


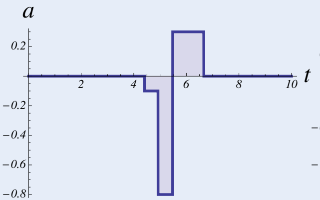


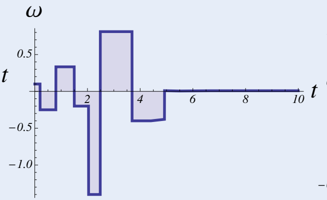
Challenge (Hybrid Systems)

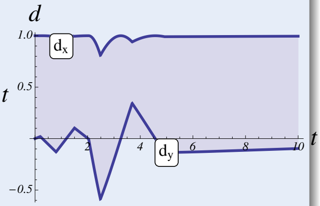
Fixed rule describing state evolution with both

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





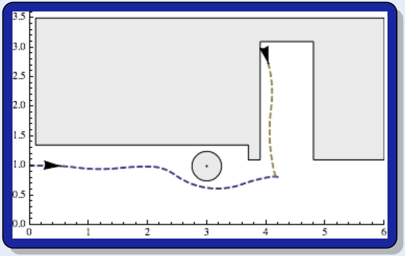


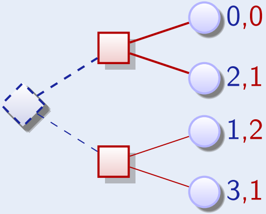


Challenge (Games)

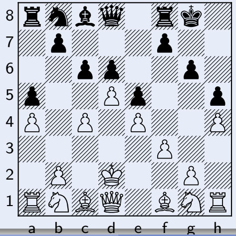
Game rules describing play evolution with both

- Angelic choices (player $\diamond$ Angel)
- Demonic choices (player $\square$ Demon)





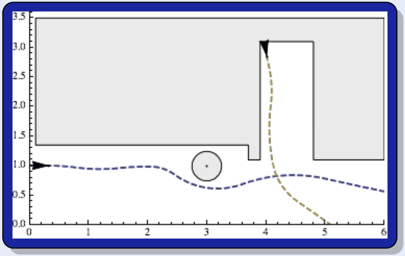
$\diamond \backslash \square$	Tr	Pl
Trash	1,2	0,0
Plant	0,0	2,1

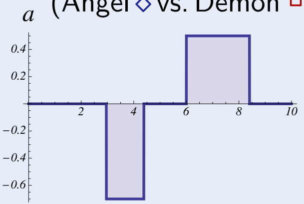


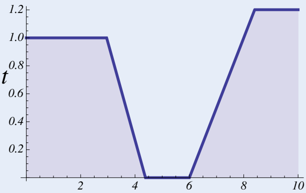
Challenge (Hybrid Games)

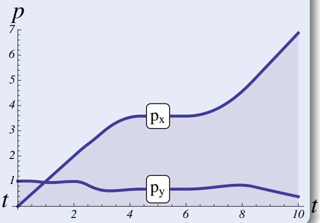
Game rules describing play evolution with

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





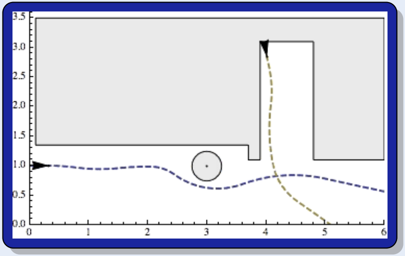


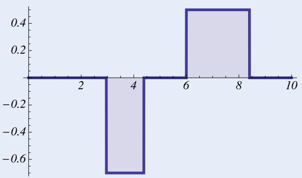


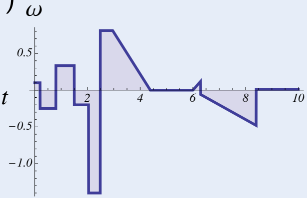
Challenge (Hybrid Games)

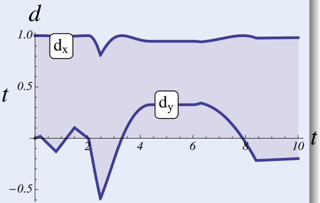
Game rules describing play evolution with

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





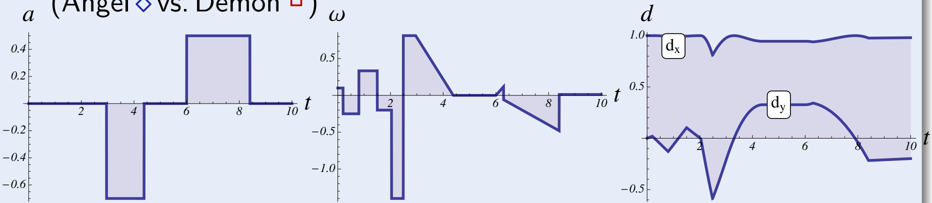




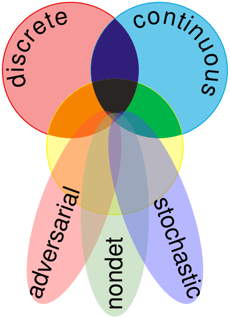
Challenge (Hybrid Games)

Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel $\Diamond$ vs. Demon $\Box$)



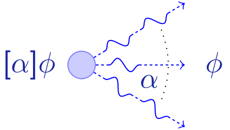
Family of Differential Dynamic Logics

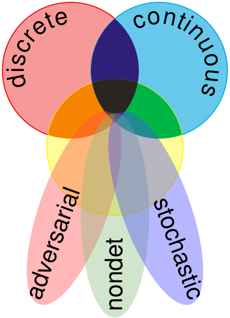


Family of Differential Dynamic Logics

differential dynamic logic

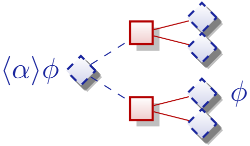
$d\mathcal{L} = DL + HP$





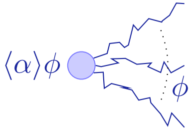
differential game logic

$dG\mathcal{L} = GL + HG$



stochastic differential DL

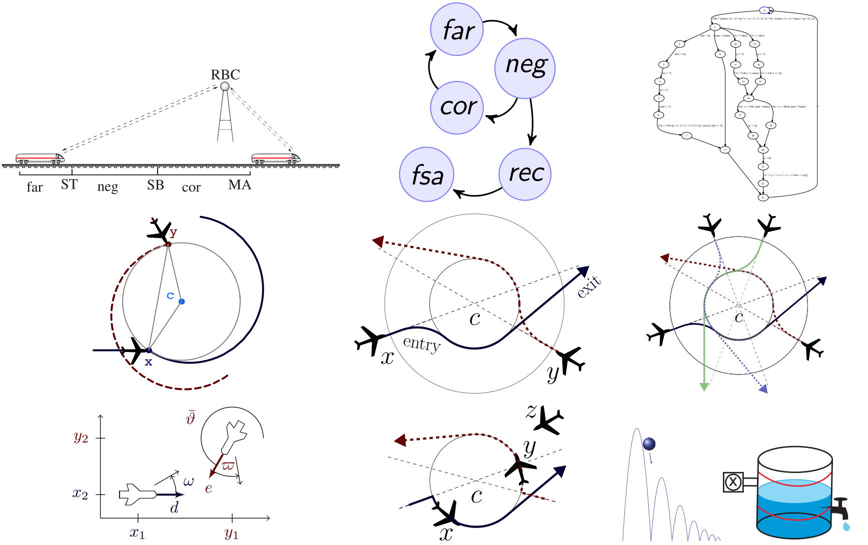
$Sd\mathcal{L} = DL + SHP$



quantified differential DL

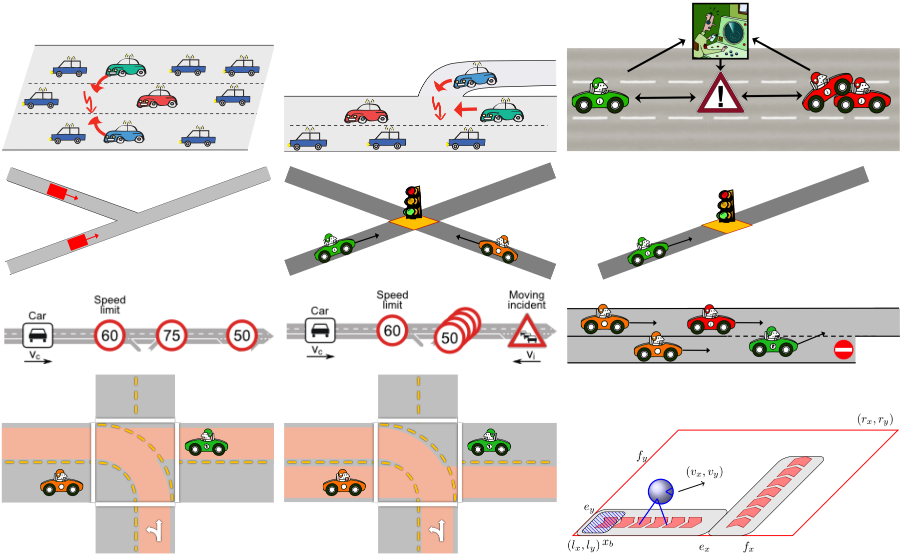
$Qd\mathcal{L} = FOL + DL + QHP$

Successful Cyber-Physical Systems Proofs

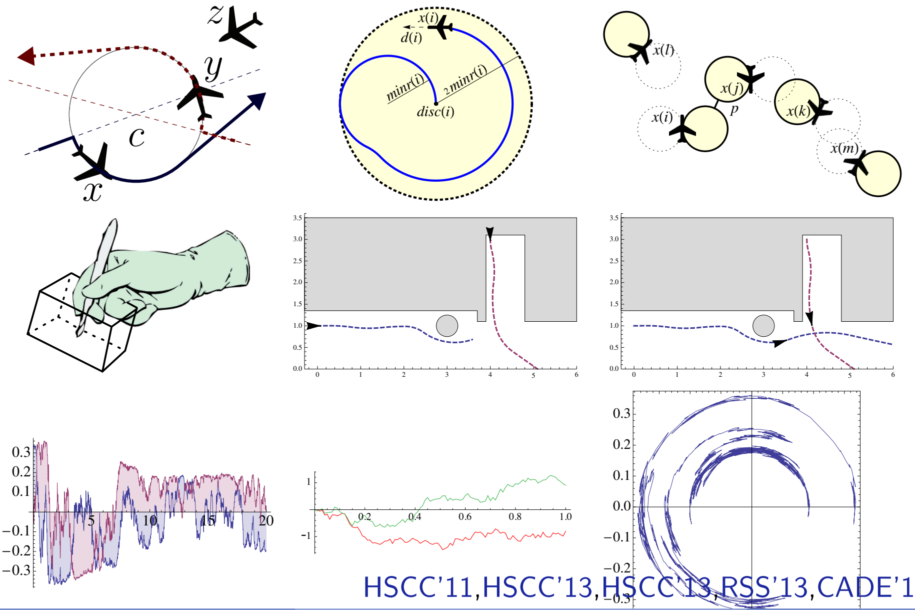


ICFEM'09,CAV'08,FM'09,HSCC'11

Successful Cyber-Physical Systems Proofs



FM'11,LMCS'12,ICCPS'12,ITSC'11,IJCAR'12



HSCC'11,HSCC'13,HSCC'13,RSS'13,CADE'12

Differential Game Logic dG$\mathcal{L}$: Syntax

Definition (Hybrid game α)

$$x := \theta \mid ?H \mid x' = \theta \,\&\, H \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dG$\mathcal{L}$ Formula ϕ)

$$p(\theta_1, \ldots, \theta_n) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi$$

Differential Game Logic dGℒ: Syntax

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

Definition (Hybrid game α)

$$x := \theta \mid ?H \mid x' = \theta \,\&\, H \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dGℒ Formula ϕ)

$$p(\theta_1, \ldots, \theta_n) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi$$

All Reals | Some Reals

Differential Game Logic dG$\mathcal{L}$: Syntax

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

Definition (Hybrid game α)

$$x := \theta \mid ?H \mid x' = \theta \,\&\, H \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dG$\mathcal{L}$ Formula ϕ)

$$p(\theta_1, \ldots, \theta_n) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi$$

All Reals | Some Reals

Differential Game Logic dG$\mathcal{L}$: Syntax

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

Definition (Hybrid game α)

$$x := \theta \mid ?H \mid x' = \theta \,\&\, H \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dG$\mathcal{L}$ Formula ϕ)

$$p(\theta_1, \ldots, \theta_n) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi$$

All Reals | Some Reals | Angel Wins

Differential Game Logic dG$\mathcal{L}$: Syntax

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

Definition (Hybrid game α)

$$x := \theta \mid ?H \mid x' = \theta \,\&\, H \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dG$\mathcal{L}$ Formula ϕ)

$$p(\theta_1, \ldots, \theta_n) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi$$

All Reals | Some Reals | Angel Wins | Demon Wins

Definable Game Operators

$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

$$\alpha \cap \beta \equiv (\alpha^d \cup \beta^d)^d$$

$$\alpha^\times \equiv ((\alpha^d)^*)^d$$

$$(x' = \theta \,\&\, H)^d \not\equiv x' = \theta \,\&\, H$$

$$(x := \theta)^d \equiv x := \theta$$

$$?H^d \not\equiv ?H$$

◇ Angel Ops

$\cup$	choice
$*$	repeat
$x' = \theta$	evolve
$?H$	challenge

d

d

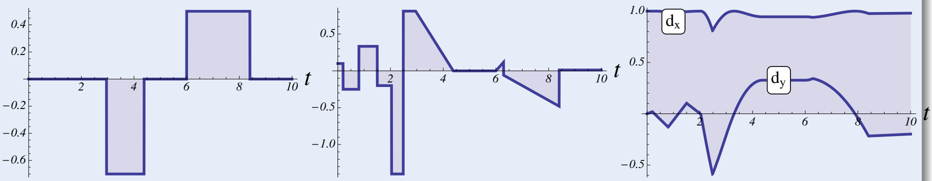
□ Demon Ops

$\cap$	choice
$\times$	repeat
$x' = \theta^d$	evolve
$?H^d$	challenge

Challenge (Hybrid Games)

Game rules describing play evolution with

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



Simple Examples

$$\langle (x := x+1; (x' = x^2)^d \cup x := x-1)^* \rangle\, (0 \leq x < 1)$$

$$\langle (x := x+1; (x' = x^2)^d \cup (x := x-1 \cap x := x-2))^* \rangle (0 \leq x < 1)$$

$$\Big\langle \Big(\, (v := a \cup v := -a \cup v := 0); \\ (w := b \cap w := -b \cap w := 0); \\ x' = v, y' = w \, \Big)^* \Big\rangle\, (x-y)^2 \leq 1$$

$$\bigg\langle \bigg(\, (\omega := 1 \cup \omega := -1 \cup \omega := 0); \\ (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0); \\ (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d \, \bigg)^* \bigg\rangle\, \|x-y\| \leq 1$$

Simple Examples

$$\vDash \langle (x := x+1; (x' = x^2)^d \cup x := x-1)^* \rangle\, (0 \leq x < 1)$$

$$\langle (x := x+1; (x' = x^2)^d \cup (x := x-1 \cap x := x-2))^* \rangle (0 \leq x < 1)$$

$$\Big\langle \Big((v := a \cup v := -a \cup v := 0);\\ (w := b \cap w := -b \cap w := 0);\\ x' = v, y' = w \Big)^* \Big\rangle\, (x-y)^2 \leq 1$$

$$\Big\langle \Big((\omega := 1 \cup \omega := -1 \cup \omega := 0);\\ (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0);\\ (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d \Big)^* \Big\rangle\, \|x - y\| \leq 1$$

Simple Examples

$$\vDash \langle (x := x+1; (x' = x^2)^d \cup x := x-1)^* \rangle \, (0 \le x < 1)$$

$$\nvDash \langle (x := x+1; (x' = x^2)^d \cup (x := x-1 \cap x := x-2))^* \rangle (0 \le x < 1)$$

$$\Big\langle \Big((v := a \cup v := -a \cup v := 0); \\ (w := b \cap w := -b \cap w := 0); \\ x' = v, y' = w \Big)^* \Big\rangle \, (x-y)^2 \le 1$$

$$\Bigg\langle \Bigg((\omega := 1 \cup \omega := -1 \cup \omega := 0); \\ (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0); \\ (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d \Bigg)^* \Bigg\rangle \, \|x-y\| \le 1$$

Simple Examples

$$\vDash \langle (x := x+1; (x' = x^2)^d \cup x := x-1)^* \rangle\, (0 \le x < 1)$$

$$\nvDash \langle (x := x+1; (x' = x^2)^d \cup (x := x-1 \cap x := x-2))^* \rangle (0 \le x < 1)$$

$$\begin{aligned}\vDash\ \Big\langle\Big(\, & (v := a \cup v := -a \cup v := 0);\\ & (w := b \cap w := -b \cap w := 0);\\ & x' = v, y' = w\ \Big)^* \Big\rangle\, (x-y)^2 \le 1\\ \leftrightarrow\ & a^2 > b^2 \lor (x-y)^2 \le 1\end{aligned}$$

$$\begin{aligned}\Bigg\langle\Bigg(\, & (\omega := 1 \cup \omega := -1 \cup \omega := 0);\\ & (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0);\\ & (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d\ \Bigg)^* \Bigg\rangle\, \|x - y\| \le 1\end{aligned}$$

Simple Examples

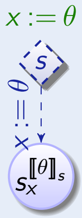
$$\vDash \langle (x := x+1; (x' = x^2)^d \cup x := x-1)^* \rangle\, (0 \le x < 1)$$

$$\not\vDash \langle (x := x+1; (x' = x^2)^d \cup (x := x-1 \cap x := x-2))^* \rangle (0 \le x < 1)$$

$$\begin{aligned} \vDash\ & \Big\langle \big((v := a \cup v := -a \cup v := 0); \\ & \quad (w := b \cap w := -b \cap w := 0); \\ & \quad x' = v, y' = w \ \big)^* \Big\rangle\, (x-y)^2 \le 1 \\ & \leftrightarrow a^2 > b^2 \lor (x-y)^2 \le 1 \end{aligned}$$

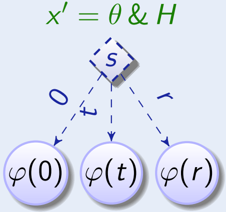
$$\begin{aligned} \not\vDash\ & \Bigg\langle \Bigg((\omega := 1 \cup \omega := -1 \cup \omega := 0); \\ & \quad (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0); \\ & \quad (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d \ \Bigg)^* \Bigg\rangle\, \|x - y\| \le 1 \end{aligned}$$

Definition (Hybrid game α: operational semantics)

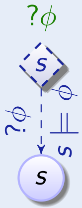


Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)

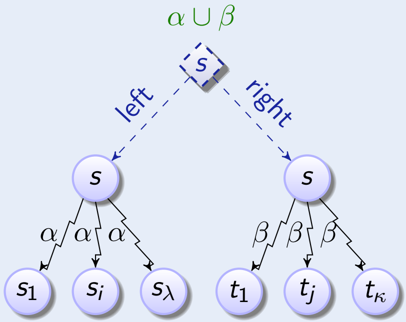


Definition (Hybrid game α: operational semantics)



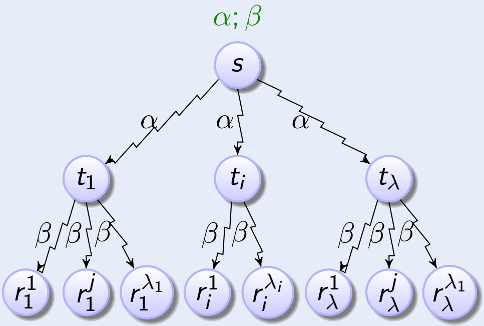
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)

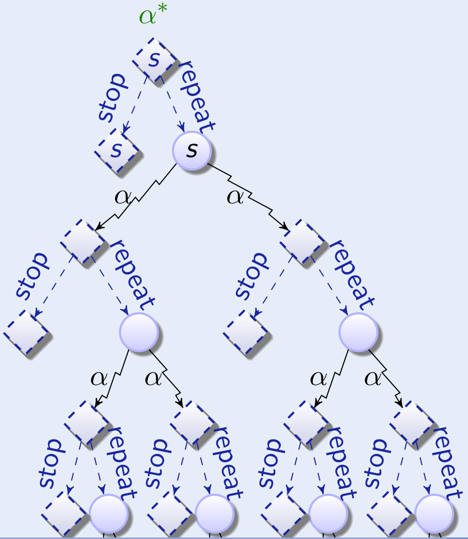


Differential Game Logic: Operational Semantics

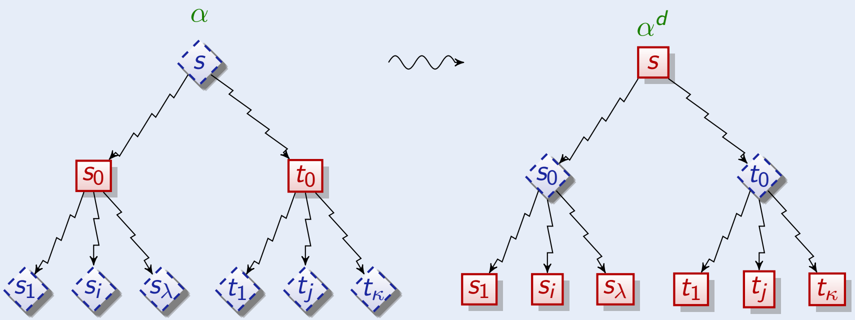
Definition (Hybrid game α: operational semantics)



Definition (Hybrid game α: operational semantics)



Definition (Hybrid game α: operational semantics)



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

$$\varsigma_{x:=\theta}(X) = \{s \in \mathcal{S} : s_x^{[\![\theta]\!]_s} \in X\}$$

$$\varsigma_{x'=\theta}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X, \frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![\theta]\!]_{\varphi(\zeta)} \text{ for all } \zeta\}$$

$$\varsigma_{?\phi}(X) = [\![\phi]\!] \cap X$$

$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$

$$\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X))$$

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

$$\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement$$

Definition (dG$\mathcal{L}$ Formula ϕ)

$$[\![\theta_1 \geq \theta_2]\!] = \{s \in \mathcal{S} : [\![\theta_1]\!]_s \geq [\![\theta_2]\!]_s\}$$

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

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

$$[\![\langle\alpha\rangle\phi]\!] = \varsigma_\alpha([\![\phi]\!])$$

$$[\![[\alpha]\phi]\!] = \delta_\alpha([\![\phi]\!])$$

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

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

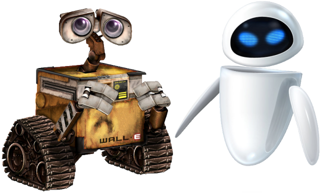
Winning Region

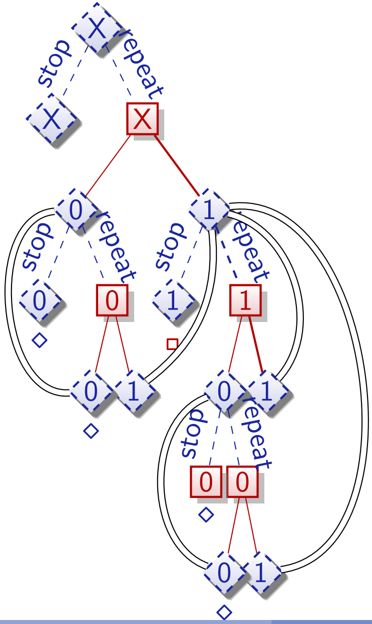
Definition (dG$\mathcal{L}$ Formula ϕ)

$$
\begin{aligned}
[\![\theta_1 \geq \theta_2]\!] &= \{s \in \mathcal{S} : [\![\theta_1]\!]_s \geq [\![\theta_2]\!]_s\}\\
[\![\neg\phi]\!] &= ([\![\phi]\!])^\complement\\
[\![\phi \wedge \psi]\!] &= [\![\phi]\!] \cap [\![\psi]\!]\\
[\![\langle\alpha\rangle\phi]\!] &= \varsigma_\alpha([\![\phi]\!])\\
[\![[\alpha]\phi]\!] &= \delta_\alpha([\![\phi]\!])
\end{aligned}
$$

Filibusters & The Importance of Determinacy

$$\langle (x := 0 \cap x := 1)^* \rangle x = 0$$

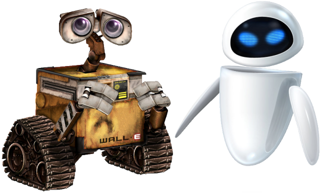


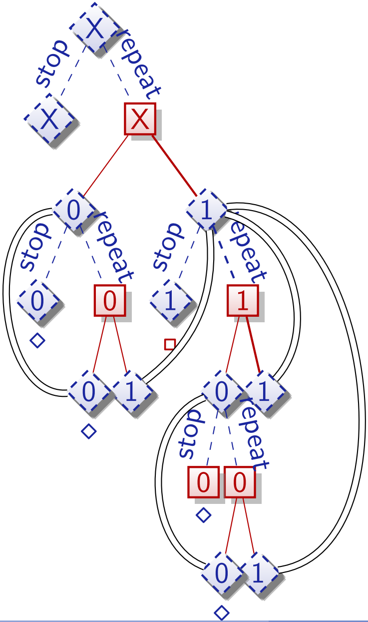


Filibusters & The Importance of Determinacy

$$\langle (x := 0 \cap x := 1)^{*} \rangle x = 0$$

$\overset{\text{wfd}}{\rightsquigarrow}$ false unless $x = 0$

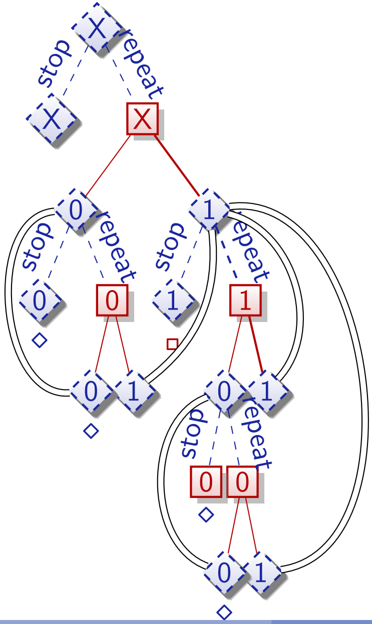


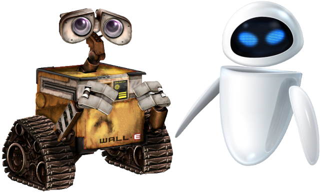


$$\langle (x := 0; x' = 1^d)^* \rangle x = 0$$

$$\langle (x := 0 \cap x := 1)^* \rangle x = 0$$

$\overset{\text{wfd}}{\rightsquigarrow}$ false unless $x = 0$





Consistency & Determinacy

Theorem (Consistency & determinacy)

Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg\phi \leftrightarrow [\alpha]\phi$.

Corollary (Determinacy: At least one player wins)

$\vDash \neg\langle\alpha\rangle\neg\phi \rightarrow [\alpha]\phi$, *thus* $\vDash \langle\alpha\rangle\neg\phi \vee [\alpha]\phi$.

Corollary (Consistency: At most one player wins)

$\vDash [\alpha]\phi \rightarrow \neg\langle\alpha\rangle\neg\phi$, *thus* $\vDash \neg([\alpha]\phi \wedge \langle\alpha\rangle\neg\phi)$

"When Strategizing Stops"

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \; : \; X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

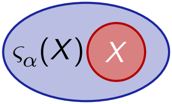
"When Strategizing Stops"

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ : \ X \cup \varsigma_{\alpha}(Z) \subseteq Z\}$$

Definition (Hybrid game α)

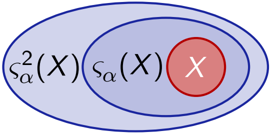
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



"When Strategizing Stops"

Definition (Hybrid game α)

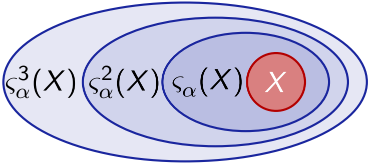
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \;:\; X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



“When Strategizing Stops”

Definition (Hybrid game α)

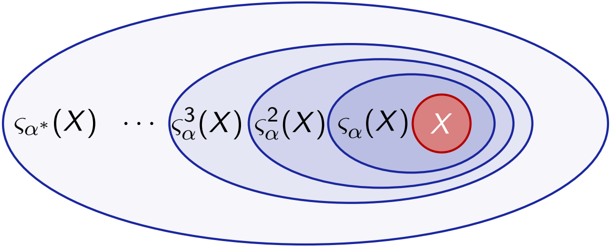
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



“When Strategizing Stops”

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_\alpha^\infty(X) \qquad \text{(Knaster-Tarski)}$$

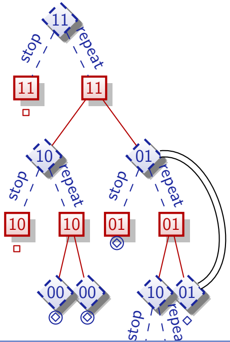


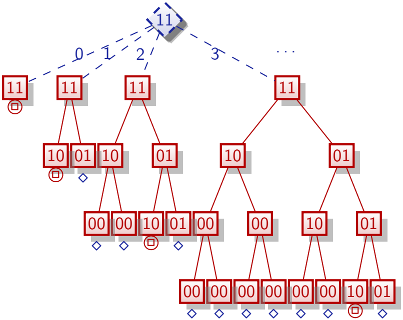
Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_\alpha^\infty(X) \qquad \text{(Knaster-Tarski)}$$

Alternative (Advance notice semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n<\omega} \varsigma_{\alpha^n}(X)$$





“When Strategizing Stops”

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_\alpha^\infty(X) \qquad \text{(Knaster-Tarski)}$$

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n<\omega} \varsigma_\alpha^n(X)$$

$$\varsigma_\alpha^0(x) \stackrel{\text{def}}{=} x$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

Example

$$\langle(x := 1; x' = 1^d \cup x := x - 1)^*\rangle\,(0 \leq x < 1)$$

“When Strategizing Stops”

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_\alpha^\infty(X) \qquad \text{(Knaster-Tarski)}$$

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n<\omega} \varsigma_\alpha^n(X)$$

$$\varsigma_\alpha^0(x) \stackrel{\text{def}}{=} x$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

Example

$$\langle(x := 1; x' = 1^d \cup x := x - 1)^*\rangle (0 \leq x < 1) \qquad \varsigma_\alpha^n([0,1)) = [0,n) \neq \mathbb{R}$$

“When Strategizing Stops”

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_\alpha^\infty(X) \qquad \text{(Knaster-Tarski)}$$

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n<\omega} \varsigma_\alpha^n(X)$$

$$\varsigma_\alpha^0(x) \stackrel{\text{def}}{=} x$$

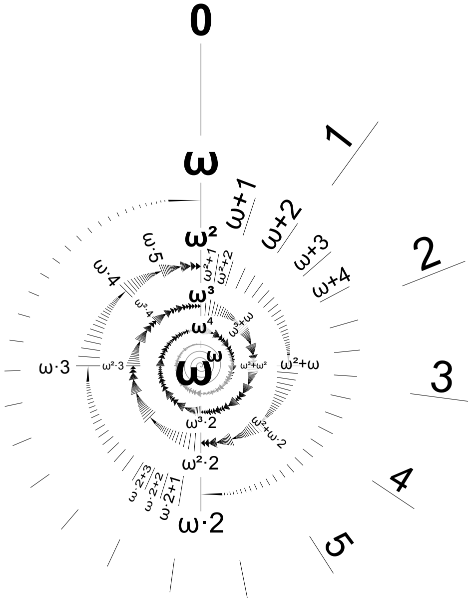
$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

$$\varsigma_\alpha^\lambda(X) \stackrel{\text{def}}{=} \bigcup_{\kappa<\lambda} \varsigma_\alpha^\kappa(X) \qquad \lambda \neq 0 \text{ a limit ordinal}$$

Example

$$\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle (0 \leq x < 1) \qquad \varsigma_\alpha^n([0,1)) = [0,n) \neq \mathbb{R}$$

Strategic Closure Ordinal



$[\cdot]$	$[\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$	
$\langle:=\rangle$	$\langle x := \theta\rangle\phi(x) \leftrightarrow \phi(\theta)$	
$\langle'\rangle$	$\langle x' = \theta\rangle\phi \leftrightarrow \exists t{\geq}0\, \langle x := y(t)\rangle\phi$	$(y'(t) = \theta)$
$\langle ?\rangle$	$\langle ?\psi\rangle\phi \leftrightarrow (\psi \wedge \phi)$	
$\langle\cup\rangle$	$\langle\alpha \cup \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi \vee \langle\beta\rangle\phi$	
$\langle;\rangle$	$\langle\alpha; \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$	
$\langle^*\rangle$	$\phi \vee \langle\alpha\rangle\langle\alpha^*\rangle\phi \rightarrow \langle\alpha^*\rangle\phi$	
$\langle^d\rangle$	$\langle\alpha^d\rangle\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$	

M $$\frac{\phi \to \psi}{\langle\alpha\rangle\phi \to \langle\alpha\rangle\psi}$$

FP $$\frac{\phi \lor \langle\alpha\rangle\psi \to \psi}{\langle\alpha^*\rangle\phi \to \psi}$$

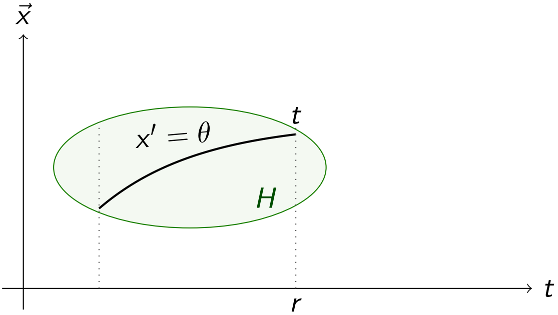
Differential Game Logic: Axiomatization

$$\text{MP} \quad \frac{\phi \quad \phi \rightarrow \psi}{\psi}$$

$$\forall \quad \frac{\phi \rightarrow \psi}{\phi \rightarrow \forall x\, \psi} \qquad (x \notin \mathrm{FV}(\phi))$$

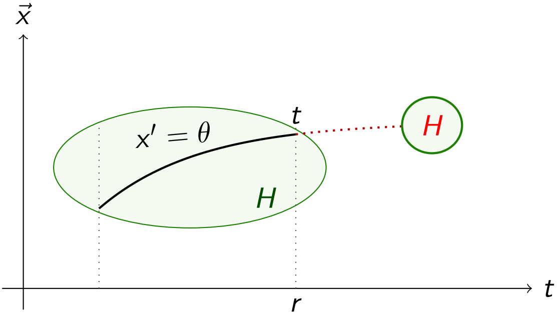
$$\text{US} \quad \frac{\phi}{\phi_{p(\cdot)}^{\psi(\cdot)}}$$

$x' = \theta \,\&\, H$ $\qquad$ $x' = \theta; ?(H)$

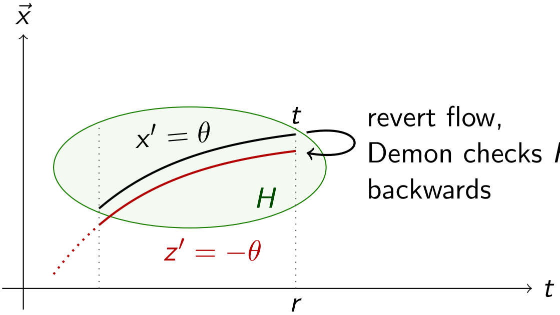


Defining Evolution Domain Constraints

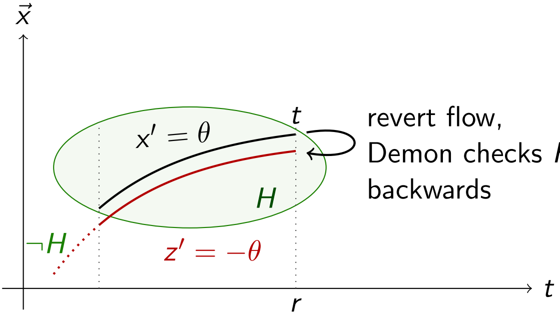
$x' = \theta \,\&\, H$ $\qquad\qquad$ $x' = \theta; ?(H)$



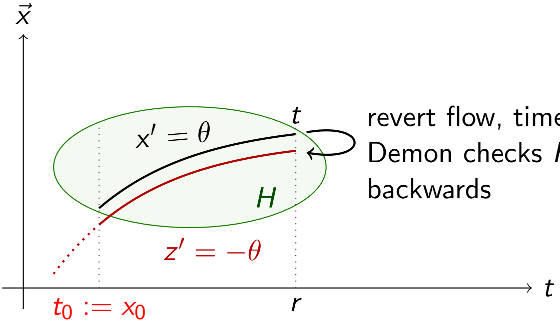
$x' = \theta \,\&\, H$ $\qquad$ $x' = \theta; (z := x; z' = -\theta)^d; ?(H(z))$



$x' = \theta \,\&\, H$ $\qquad$ $x' = \theta; (z := x; z' = -\theta)^d; ?(H(z))$



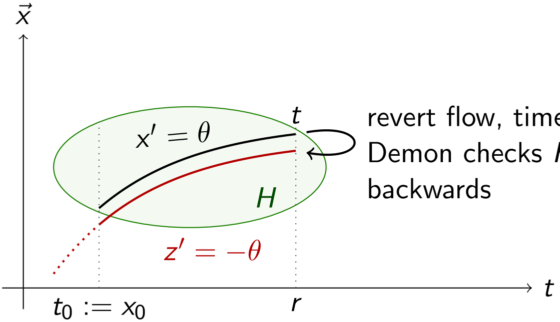
$$x' = \theta \,\&\, H \;\equiv\; t_0 := x_0;\, x' = \theta;\, (z := x;\, z' = -\theta)^d;\, ?(z_0 \geq t_0 \rightarrow H(z))$$



revert flow, time x_0;
Demon checks H
backwards

"There and Back Again" Game

$$x' = \theta \,\&\, H \;\equiv\; t_0 := x_0; x' = \theta; (z := x; z' = -\theta)^d; ?(z_0 \geq t_0 \rightarrow H(z))$$



Lemma

Evolution domain is definable by game

Example Proof: Dual Filibuster

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{x=0 \rightarrow 0=0 \lor 1=0}\ \mathbb{R}}{x=0 \rightarrow \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0}\ \langle:=\rangle}{x=0 \rightarrow \langle x:=0 \cup x:=1\rangle x=0}\ \langle\cup\rangle}{x=0 \rightarrow \neg\langle x:=0 \cap x:=1\rangle \neg x=0}\ \langle^d\rangle}{x=0 \rightarrow [x:=0 \cap x:=1]x=0}\ [\cdot]}{x=0 \rightarrow [(x:=0 \cap x:=1)^*]x=0}\ \text{ind}}{x=0 \rightarrow \langle (x:=0 \cup x:=1)^\times \rangle x=0}\ \langle^d\rangle
$$

Soundness & Completeness

Theorem (Completeness)

dG$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid games relative to any expressive logic L.*

$$\vDash \phi \quad \textit{iff} \quad Taut_L \vdash \phi$$

Soundness & Completeness: Consequences

Corollary

Constructive and Moschovakis-coding-free. (Minimal: $x' = \theta$, $\exists$ and $[\alpha^*]$)

Corollary (Conquand & Huet) (Inf.Comput'88)

Modal analogue for $\langle\alpha^*\rangle$ of characterizations in Calculus of Constructions

Corollary (Meyer & Halpern) (J.ACM'82)

$F \to \langle\alpha\rangle G$ semidecidable for uninterpreted programs.

Corollary (Schmitt) (Inf.Control.'84)

$[\alpha]$-free semidecidable for uninterpreted programs.

Corollary

Uninterpreted game logic with even ^{d} in $\langle\alpha\rangle$ is semidecidable.

Soundness & Completeness: Consequences

Corollary

Harel'77 convergence rule unnecessary for hybrid games, hybrid systems, discrete programs.

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: *Succinct invariants* — *discrete* Π^0_2
- $[x' = \theta]G$ *and* $\langle x' = \theta \rangle G$: *Succinct differential (in)variants* — Δ^1_1
- $\exists x\, G$: *Complexity depends on Herbrand disjunctions:* — *discrete* Π^1_1
  ✓ *uninterpreted* ✓ *reals* × $\exists x\, [\alpha^*]G$ Π^1_1*-complete for discrete* α

Corollary (Hybrid version of Parikh's result) (FOCS'83)

**-free* dG$\mathcal{L}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*
^{d}*-free* dG$\mathcal{L}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*

Soundness & Completeness: Consequences

Corollary (ODE Completeness) (+LICS'12)

d$\mathcal{GL}$ *complete relative to ODE for hybrid games with finite-rank Borel winning regions.*

Corollary (Continuous Completeness)

d$\mathcal{GL}$ *complete relative to continuous* $L_{\mu D}$ *over* $\mathbb{R}$

Corollary (Discrete Completeness) (+LICS'12)

d$\mathcal{GL}$ + *Euler axiom complete relative to discrete* L_{μ} *over* $\mathbb{R}$

Soundness & Completeness: Consequences

$$\langle(\underbrace{\underbrace{x := 1; x' = 1^d}_{\beta} \cup \underbrace{x := x - 1}_{\gamma}}_{\alpha})^*\rangle 0 \le x < 1$$

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x\, (0{\le}x{<}1 \lor \forall t{\ge}0\, p(0+t) \lor p(x-1) \to p(x)) \to (true \to p(x))}{\forall x\, (0{\le}x{<}1 \lor \langle x := 1\rangle \neg\exists t{\ge}0\, \langle x := x{+}t\rangle \neg p(x) \lor p(x{-}1) \to p(x)) \to (true \to p(x))}}{\forall x\, (0{\le}x{<}1 \lor \langle x := 1\rangle \neg\langle x' = 1\rangle \neg p(x) \lor p(x-1) \to p(x)) \to (true \to p(x))}}{\forall x\, (0{\le}x{<}1 \lor \langle\beta\rangle p(x) \lor \langle\gamma\rangle p(x) \to p(x)) \to (true \to p(x))}}{\forall x\, (0{\le}x{<}1 \lor \langle\beta \cup \gamma\rangle p(x) \to p(x)) \to (true \to p(x))}}{\forall x\, (0{\le}x{<}1 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0{\le}x{<}1 \to \langle\alpha^*\rangle 0{\le}x{<}1) \to (true \to \langle\alpha^*\rangle 0{\le}x{<}1)}}{true \to \langle\alpha^*\rangle 0{\le}x{<}1}$$

Separating Axioms

Theorem (Hybrid system vs. hybrid game)

dG$\mathcal{L}$ *is a subregular, sub-Barcan, monotonic modal logic without the induction axiom of dynamic logic.*

~~K~~ $[\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$

~~G~~ $$\frac{\phi}{[\alpha]\phi}$$

~~R~~ $$\frac{\phi_1 \land \phi_2 \to \psi}{[\alpha]\phi_1 \land [\alpha]\phi_2 \to [\alpha]\psi}$$

~~B~~ $\langle\alpha\rangle\exists x\,\phi \to \exists x\,\langle\alpha\rangle\phi \qquad (x \notin \alpha)$

~~I~~ $[\alpha^*](\phi \to [\alpha]\phi) \to (\phi \to [\alpha^*]\phi)$

~~FA~~ $\langle\alpha^*\rangle\phi \to \phi \lor \langle\alpha^*\rangle(\neg\phi \land \langle\alpha\rangle\phi)$

M $\langle\alpha\rangle\phi \lor \langle\alpha\rangle\psi \to \langle\alpha\rangle(\phi \lor \psi)$

$\mathrm{M}_{[\cdot]}$ $$\frac{\phi \to \psi}{[\beta]\phi \to [\beta]\psi}$$

$\overleftarrow{\mathrm{B}}$ $\exists x\,\langle\alpha\rangle\phi \to \langle\alpha\rangle\exists x\,\phi \qquad (x \notin \alpha)$

∀I $\mathrm{Cl}_\forall(\phi \to [\alpha]\phi) \to (\phi \to [\alpha^*]\phi)$

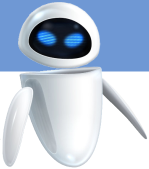
Expressiveness

Theorem (Expressive Power: hybrid systems $<$ hybrid games)

$\mathsf{dG}\mathcal{L}$ *for hybrid games strictly more expressive than* $\mathsf{d}\mathcal{L}$ *for hybrid games:*

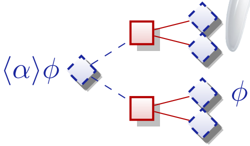
$$\mathsf{d}\mathcal{L} < \mathsf{dG}\mathcal{L}$$

Logic of Hybrid Games

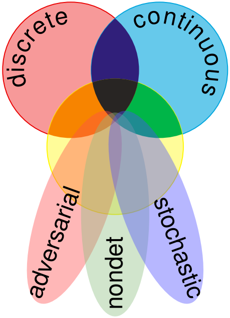


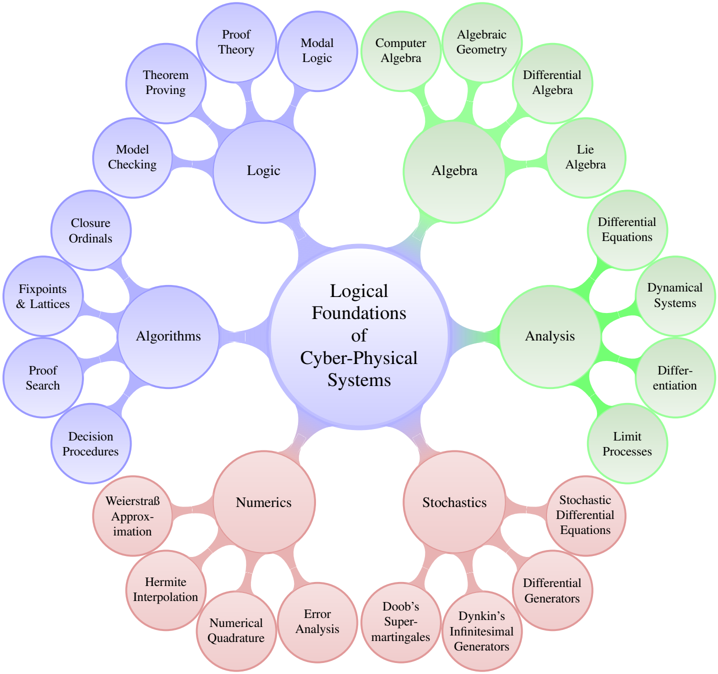
differential game logic

$$\mathrm{d}\mathcal{GL} = \mathrm{GL} + \mathrm{HG} = \mathrm{d}\mathcal{L} + {}^{d}$$



- Logic for hybrid games
- Discrete + continuous + adversarial
- Winning regions closure $\geq \omega_1^{\mathrm{CK}}$
- Sound & rel. complete axiomatization
- Fixpoint proofs, hybrid analogues
- Hybrid games > hybrid systems
- ^{d} super challenge + smooth extension
- Stochastic $\approx$ adversarial




Logical Foundations of Cyber-Physical Systems
Logic
Proof Theory
Modal Logic
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Lie Algebra
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search
Decision Procedures
Analysis
Differential Equations
Dynamical Systems
Differ-entiation
Limit Processes
Numerics
Weierstraß Approx-imation
Hermite Interpolation
Numerical Quadrature
Error Analysis
Stochastics
Stochastic Differential Equations
Differential Generators
Dynkin's Infinitesimal Generators
Doob's Super-martingales

Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012. IEEE, 2012.

André Platzer.
The complete proof theory of hybrid systems.
In *LICS* [1], pages 541–550.

André Platzer.
Differential game logic for hybrid games.
Technical Report CMU-CS-12-105, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, March 2012.

André Platzer.
Logics of dynamical systems.
In *LICS* [1], pages 13–24.

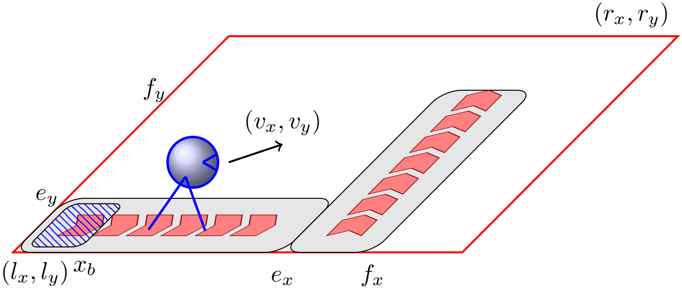
André Platzer.
A complete axiomatization of differential game logic for hybrid games.

Technical Report CMU-CS-13-100R, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, January, Revised and extended in July 2013.

Jan-David Quesel and André Platzer.
Playing hybrid games with KeYmaera.
In Bernhard Gramlich, Dale Miller, and Ulrike Sattler, editors, *IJCAR*, volume 7364 of *LNCS*, pages 439–453. Springer, 2012.

Successful Hybrid Games Proofs

Verification Challenge:



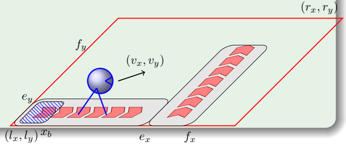
Hybrid games proving also for proving relaxed notions of system similarity

Example (Environment vs. Robot)

$$\Big((\,?true \cap (?(x < e_x \wedge y < e_y \wedge \mathrm{eff}_1 = 1);\ v_x := v_x + c_x;\ \mathrm{eff}_1 := 0)$$

$$\cap\,(?(e_x \leq x \wedge y \leq f_y \wedge \mathrm{eff}_2 = 1);\ v_y := v_y + c_y;\ \mathrm{eff}_2 := 0)\,)\,;$$

$$\Big)^{\times}$$



Example (Environment vs. Robot)

$$\Big((\,?true \cap (?(x < e_x \wedge y < e_y \wedge \mathrm{eff}_1 = 1);\ v_x := v_x + c_x;\ \mathrm{eff}_1 := 0)$$

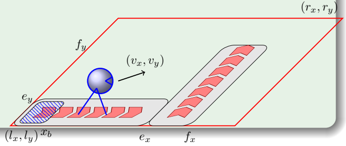
$$\cap\, (?(e_x \le x \wedge y \le f_y \wedge \mathrm{eff}_2 = 1);\ v_y := v_y + c_y;\ \mathrm{eff}_2 := 0)\,)\,;$$

$$(\,a_x := *;\ ?(-A \le a_x \le A);$$

$$a_y := *;\ ?(-A \le a_y \le A);$$

$$t_s := 0\,)\,;$$

$$\Big)^{\times}$$



Example (Environment vs. Robot)

$$\Big(\big(\,?true \cap (?(x < e_x \land y < e_y \land \mathrm{eff}_1 = 1);\; v_x := v_x + c_x;\; \mathrm{eff}_1 := 0)$$

$$\cap\, (?(e_x \le x \land y \le f_y \land \mathrm{eff}_2 = 1);\; v_y := v_y + c_y;\; \mathrm{eff}_2 := 0)\,\big)\,;$$

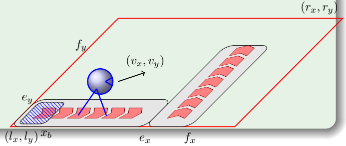
$$(\,a_x := *;\; ?(-A \le a_x \le A);$$

$$a_y := *;\; ?(-A \le a_y \le A);$$

$$t_s := 0\,)\,;$$

$$(\,x' = v_x, y' = v_y, v_x' = a_x, v_y' = a_y, t' = 1, t_s' = 1 \,\&\, t_s \le \varepsilon\,)^d\,;$$

$$\Big)^\times$$



Example (Environment vs. Robot)

$$\Big(\big(?true \cap (?(x < e_x \wedge y < e_y \wedge \mathrm{eff}_1 = 1);\; v_x := v_x + c_x;\; \mathrm{eff}_1 := 0)$$

$$\cap\, (?(e_x \le x \wedge y \le f_y \wedge \mathrm{eff}_2 = 1);\; v_y := v_y + c_y;\; \mathrm{eff}_2 := 0)\big);$$

$$(a_x := *;\; ?(-A \le a_x \le A);$$

$$a_y := *;\; ?(-A \le a_y \le A);$$

$$t_s := 0);$$

$$\big((x' = v_x, y' = v_y, v_x' = a_x, v_y' = a_y, t' = 1, t_s' = 1 \,\&\, t_s \le \varepsilon)^d;$$

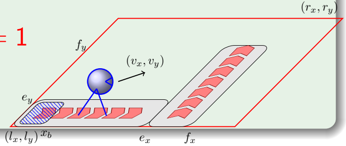
$$\cup\, \big((?a_x v_x \le 0 \wedge a_y v_y \le 0;$$

$$\text{if } v_x = 0 \text{ then } a_x := 0 \text{ fi};$$

$$\text{if } v_y = 0 \text{ then } a_y := 0 \text{ fi});$$

$$(x' = v_x, y' = v_y, v_x' = a_x, v_y' = a_y, t' = 1, t_s' = 1$$

$$\&\, t_s \le \varepsilon \wedge a_x v_x \le 0 \wedge a_y v_y \le 0)^d\big)\big)\Big)^\times$$



Robotic Factory Automation (*RF*)

Proposition (Robot stays in □)

$$\models (x = y = 0 \land v_x = v_y = 0 \land \text{Controllability Assumptions}) \\ \to (RF)(x \in [l_x, r_x] \land y \in [l_y, r_y])$$

Proposition (Stays in □ + leaves shaded region in time)

$RF|_x$: RF projected to the x-axis

$$\models (x = 0 \land v_x = 0 \land \text{Controllability Assumptions}) \\ \to (RF|_x)(x \in [l_x, r_x] \land (t \geq \varepsilon \to (x \geq x_b)))$$