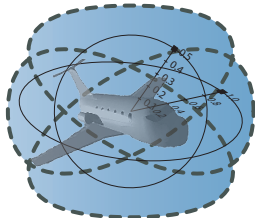


Logic of Hybrid Games

André Platzer

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

<http://symbolaris.com/>





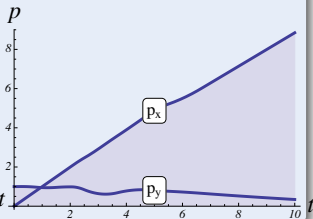
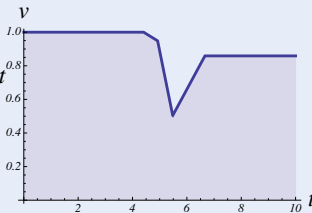
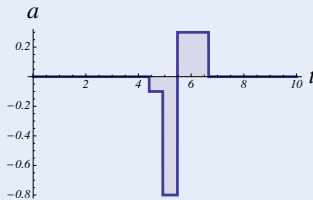
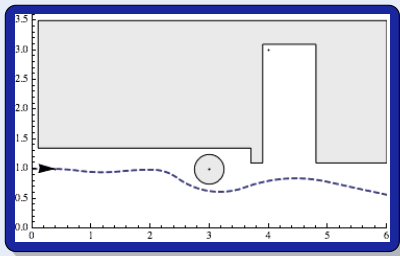
- 1 Hybrid Systems Applications
- 2 Differential Game Logic
 - Operational Semantics
 - Denotational Semantics
 - Determinacy
 - Strategic Closure Ordinals
- 3 Proofs for Hybrid Systems
 - Axiomatization
 - Soundness and Completeness
 - Corollaries
- 4 Summary

Can you trust a computer to control physics?

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

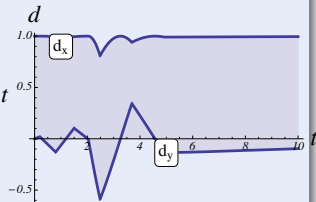
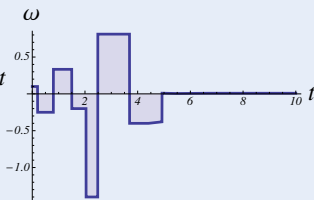
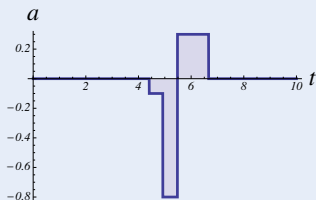
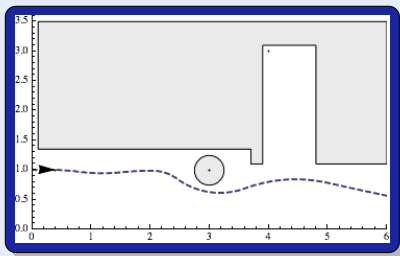
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

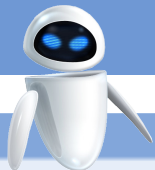


Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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

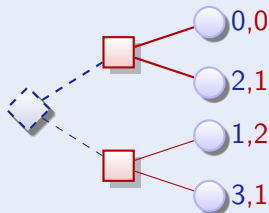
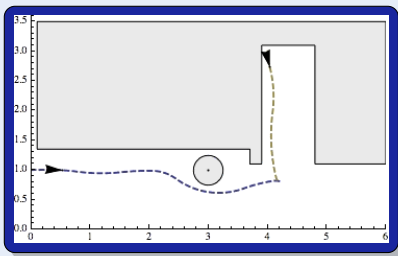




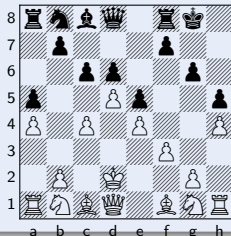
Challenge (Games)

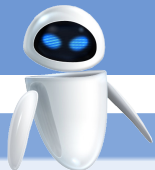
Game rules describing play evolution with both

- 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

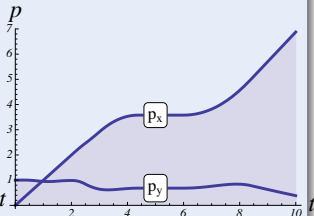
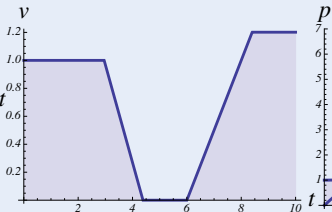
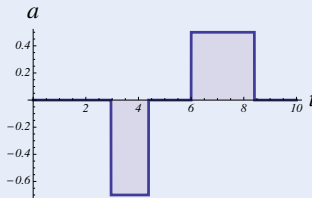
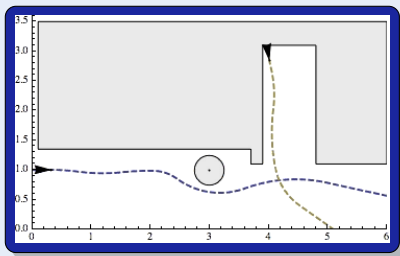


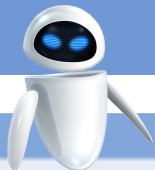


Challenge (Hybrid Games)

Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Angel/demon choices

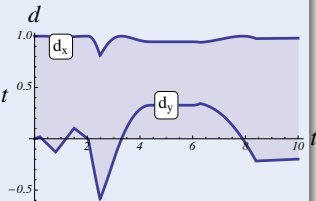
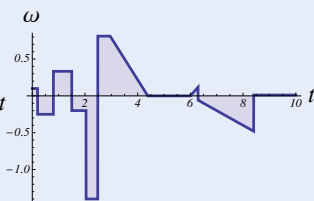
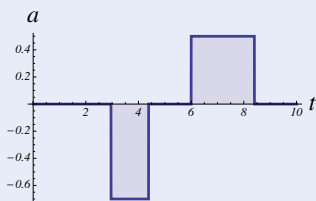
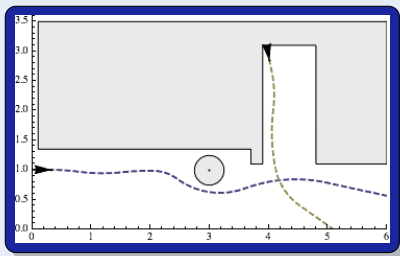


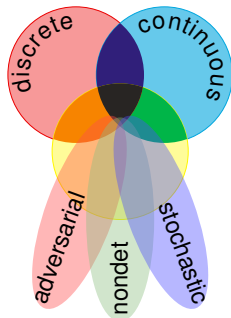


Challenge (Hybrid Games)

Game rules describing play evolution with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Angel/demon choices

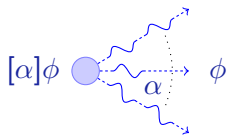




Family of Differential Dynamic Logics

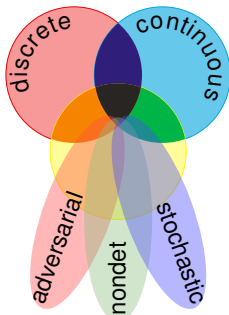
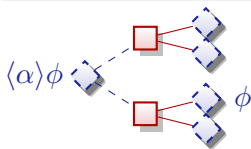
differential dynamic logic

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



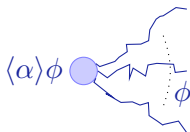
differential game logic

$$d\mathcal{GL} = \text{GL} + \text{HG}$$



stochastic differential DL

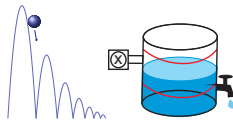
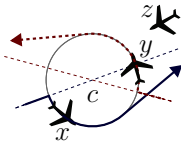
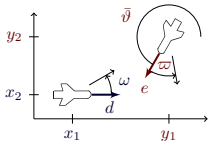
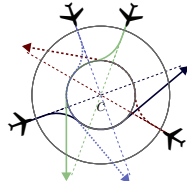
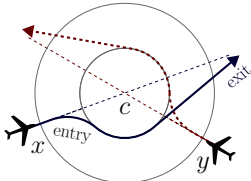
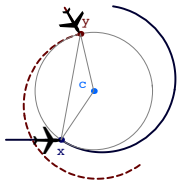
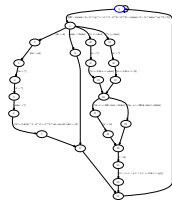
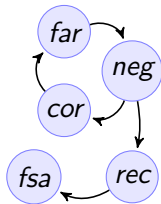
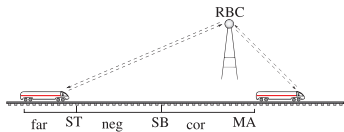
$$\text{Sd}\mathcal{L} = \text{DL} + \text{SHP}$$



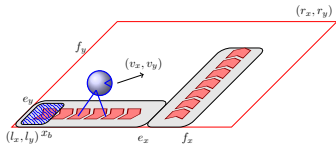
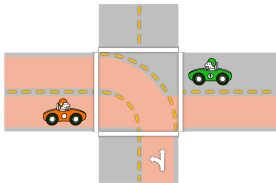
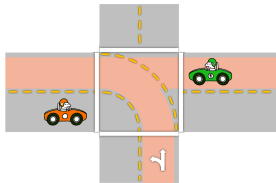
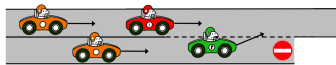
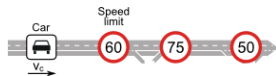
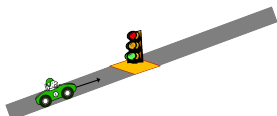
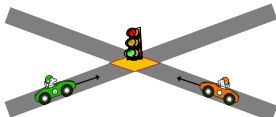
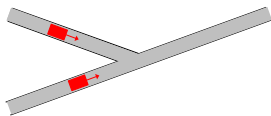
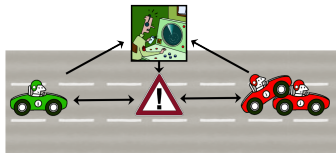
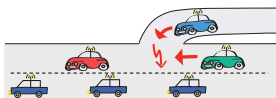
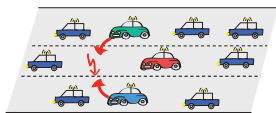
quantified differential DL

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

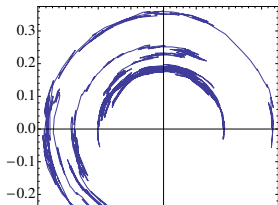
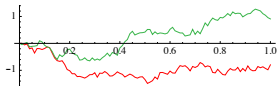
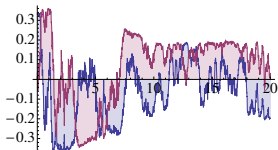
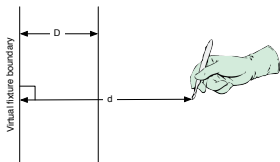
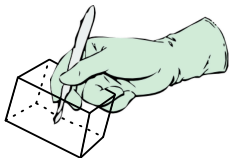
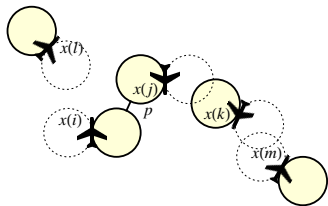
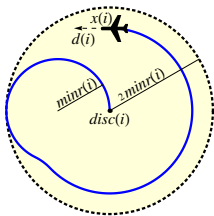
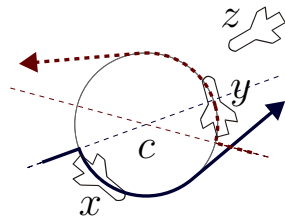
Successful Hybrid Systems Proofs



Successful Hybrid Systems Proofs



Successful Hybrid Systems Proofs



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)

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

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)

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

All
Reals

Some
Reals



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)

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

All
Reals

Some
Reals



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)

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

All
Reals

Some
Reals

Angel
Wins

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 (dGL Formula ϕ)

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

All
Reals

Some
Reals

Angel
Wins

Demon
Wins

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

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

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

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

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

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



Repeat α as long as both Angel and Demon want to repeat:

$$\begin{aligned}\alpha^{*\wedge\times} &\equiv (c := 0 \wedge c := 1); (?c \neq 0; \alpha; (c := 0 \wedge c := 1))^* \\ &\equiv ((c := 0 \wedge c := 1); ?c \neq 0; \alpha)^*\end{aligned}$$



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

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

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



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

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

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



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

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

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



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

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

$$\not\models \left\langle \left((\omega := 1 \cup \omega := -1 \cup \omega := 0); \right. \right. \\ \left. (\varrho := 1 \cap \varrho := -1 \cap \varrho := 0); \right. \\ \left. (x'' = \omega x'^{\perp}, y'' = \varrho y'^{\perp})^d \right)^* \rangle \|x - y\| \leq 1$$



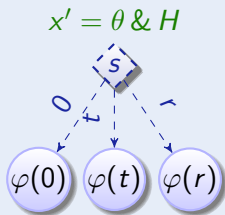
Definition (Hybrid game α : operational semantics)



$x := \theta$



Definition (Hybrid game α : operational semantics)



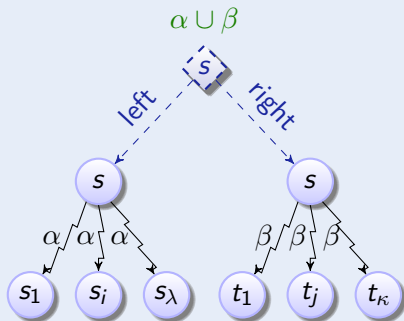


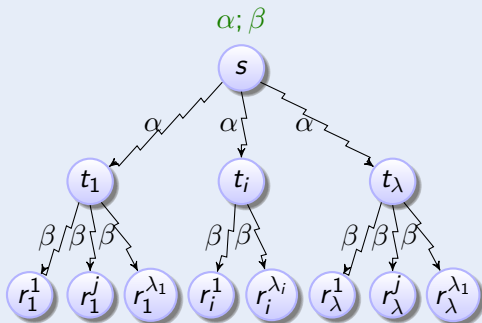
Definition (Hybrid game α : operational semantics)





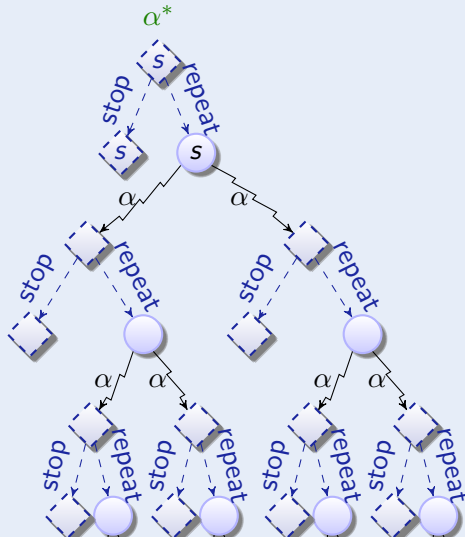
Definition (Hybrid game $\alpha \cup \beta$: operational semantics)



Definition (Hybrid game α : operational semantics)

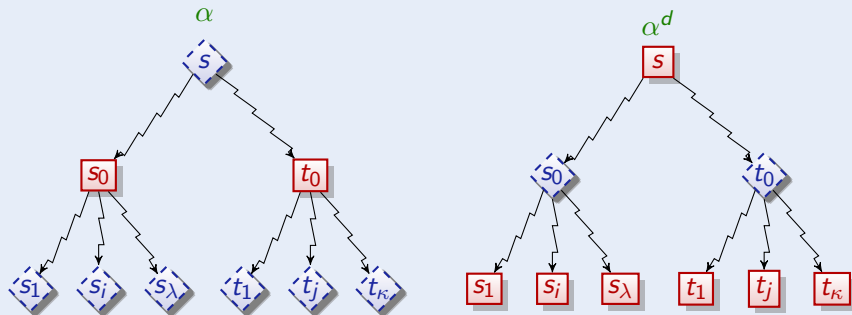


Definition (Hybrid game α : operational semantics)





Definition (Hybrid game α : operational semantics)



Definition (Hybrid game α : denotational semantics)

$$\varsigma_{x:=\theta}(X) = \{s \in \mathcal{S} : s_x^{\llbracket \theta \rrbracket_s} \in X\}$$

$$\varsigma_{x'=\theta}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X, \frac{d\varphi(t)(x)}{dt}(\zeta) = \llbracket \theta \rrbracket_{\varphi(\zeta)} \text{ for all } \zeta\}$$

$$\varsigma_{?\phi}(X) = \llbracket \phi \rrbracket \cap X$$

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

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

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

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

Definition (dGL Formula ϕ)

$$\llbracket \theta_1 \geq \theta_2 \rrbracket = \{s \in \mathcal{S} : \llbracket \theta_1 \rrbracket_s \geq \llbracket \theta_2 \rrbracket_s\}$$

$$\llbracket \neg \phi \rrbracket = (\llbracket \phi \rrbracket)^c$$

$$\llbracket \phi \wedge \psi \rrbracket = \llbracket \phi \rrbracket \cap \llbracket \psi \rrbracket$$

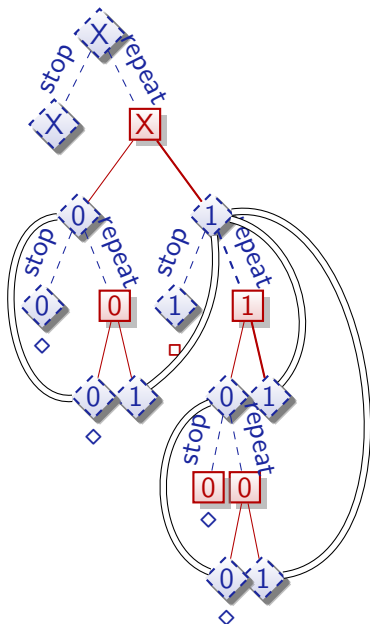
$$\llbracket \langle \alpha \rangle \phi \rrbracket = \varsigma_{\alpha}(\llbracket \phi \rrbracket)$$

$$\llbracket [\alpha] \phi \rrbracket = \delta_{\alpha}(\llbracket \phi \rrbracket)$$



Filibusters & The Importance of Determinacy

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

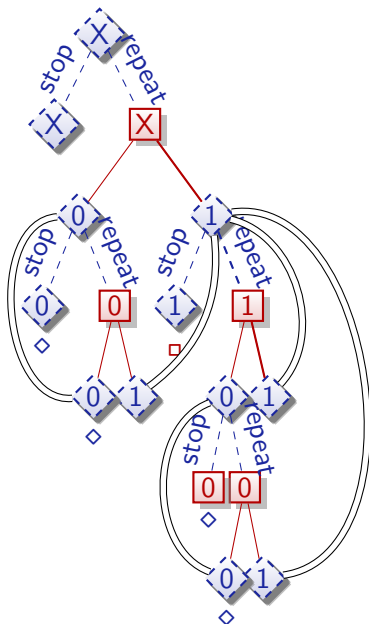




Filibusters & The Importance of Determinacy

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

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



Theorem (Consistency & determinacy)

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

Corollary (Determinacy: At least one player wins)

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

Corollary (Consistency: At most one player wins)

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

Definition (Hybrid game α)

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

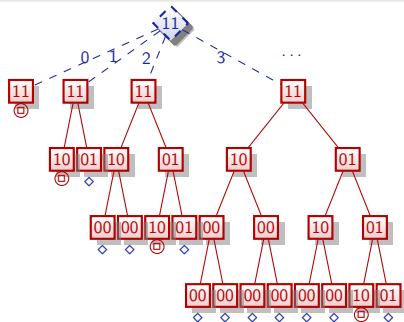
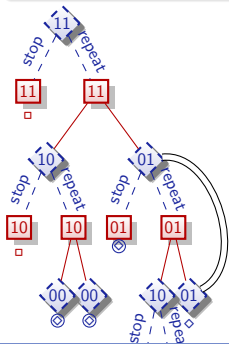
“When Strategizing Stops”

Definition (Hybrid game α)

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

Alternative (Advance notice semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n \in \mathbb{N}} \varsigma_{\alpha^n}(X)$$



“When Strategizing Stops”

Definition (Hybrid game α)

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

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n \in \mathbb{N}} \varsigma_{\alpha}^n(X)$$

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

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

Example

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

“When Strategizing Stops”

Definition (Hybrid game α)

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

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n \in \mathbb{N}} \varsigma_{\alpha}^n(X)$$

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

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

Example

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

“When Strategizing Stops”

Definition (Hybrid game α)

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

Alternative (ω semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n \in \mathbb{N}} \varsigma_{\alpha}^n(X)$$

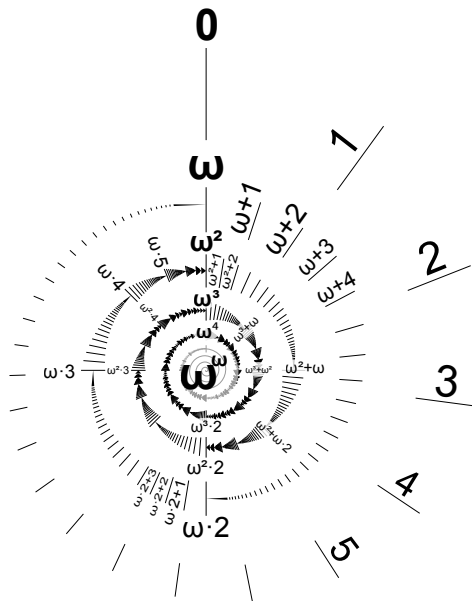
$$\varsigma_{\alpha}^0(x) \stackrel{\text{def}}{=} x$$

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

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

Example

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





$$[\cdot] \quad [\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$$

$$\langle := \rangle \quad \langle x := \theta \rangle \phi(x) \leftrightarrow \phi(\theta)$$

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

$$\langle ? \rangle \quad \langle ?\psi \rangle \phi \leftrightarrow (\psi \wedge \phi)$$

$$\langle \cup \rangle \quad \langle \alpha \cup \beta \rangle \phi \leftrightarrow \langle \alpha \rangle \phi \vee \langle \beta \rangle \phi$$

$$\langle ; \rangle \quad \langle \alpha ; \beta \rangle \phi \leftrightarrow \langle \alpha \rangle \langle \beta \rangle \phi$$

$$\langle * \rangle \quad \phi \vee \langle \alpha \rangle \langle \alpha^* \rangle \phi \rightarrow \langle \alpha^* \rangle \phi$$

$$\langle d \rangle \quad \langle \alpha^d \rangle \phi \leftrightarrow \neg\langle \alpha \rangle \neg\phi$$



$$\text{M} \quad \frac{\phi \rightarrow \psi}{\langle \alpha \rangle \phi \rightarrow \langle \alpha \rangle \psi}$$

$$\text{FP} \quad \frac{\phi \vee \langle \alpha \rangle \psi \rightarrow \psi}{\langle \alpha^* \rangle \phi \rightarrow \psi}$$



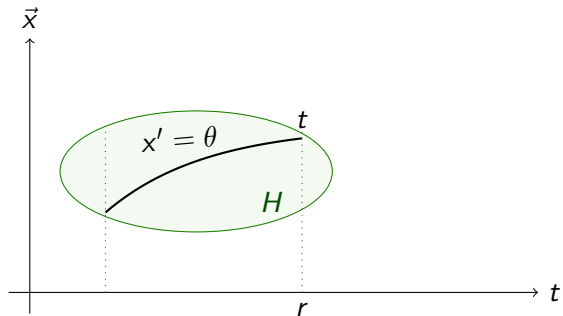
$$\text{MP} \quad \frac{\phi \quad \phi \rightarrow \psi}{\psi}$$

$$\forall \quad \frac{\phi \rightarrow \psi}{\phi \rightarrow \forall x \psi} \quad (x \notin \text{FV}(\phi))$$

$$\text{US} \quad \frac{\phi}{\phi \overset{\psi(\cdot)}{\underset{\rho(\cdot)}{\rho(\cdot)}}}$$

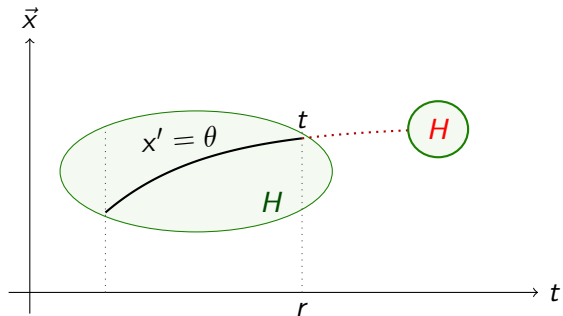
$$x' = \theta \ \& \ H$$

$$x' = \theta; ?(H)$$



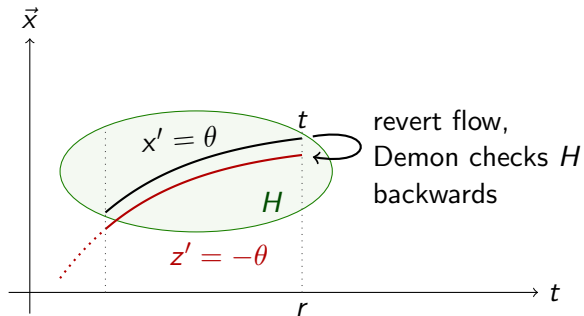
$$x' = \theta \ \& \ H$$

$$x' = \theta; ?(H)$$



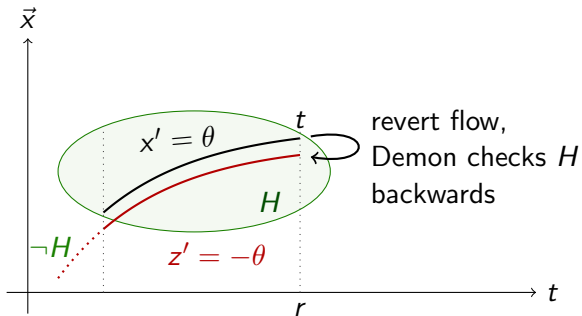
$$x' = \theta \ \& \ H$$

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

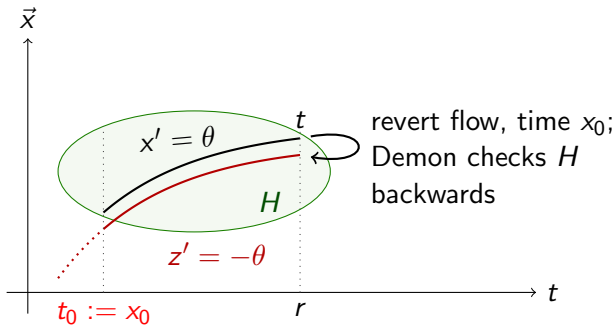


$$x' = \theta \ \& \ H$$

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

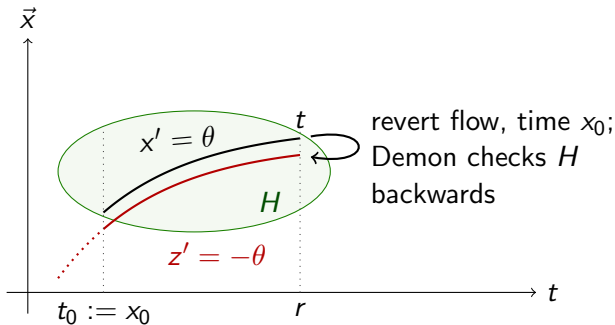


$$x' = \theta \ \& \ H \equiv t_0 := x_0; x' = \theta; (z := x; z' = -\theta)^d; ?(z_0 \geq t_0 \rightarrow H(z))$$



“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

Theorem (Completeness)

dGL calculus is a sound & complete axiomatization of hybrid games relative to fixpoints of differential equations.

$$\models \phi \quad \text{iff} \quad \text{Taut}_{L_{\mu D}} \vdash \phi$$

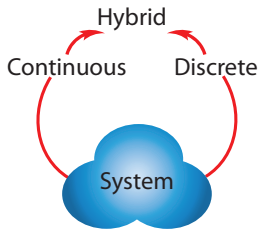
Remark ($L_{\mu D}$ = modal μ -calculus of differential equations)

$$\phi ::= X(\theta) \mid p(\theta) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \langle x' = \theta \rangle \phi \mid \mu X. \phi$$

Theorem (Completeness)

dGL calculus is a sound & complete axiomatization of hybrid games relative to fixpoints of differential equations.

$$\models \phi \quad \text{iff} \quad \text{Taut}_{L_{\mu D}} \vdash \phi$$



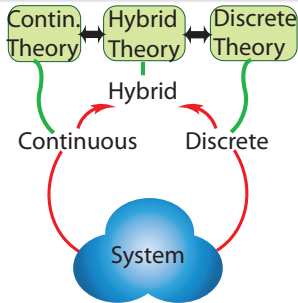
Remark ($L_{\mu D}$ = modal μ -calculus of differential equations)

$$\phi ::= X(\theta) \mid p(\theta) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \langle x' = \theta \rangle \phi \mid \mu X. \phi$$

Theorem (Completeness)

dGL calculus is a sound & complete axiomatization of hybrid games relative to fixpoints of differential equations.

$$\models \phi \quad \text{iff} \quad \text{Taut}_{L_{\mu D}} \vdash \phi$$



Remark ($L_{\mu D}$ = modal μ -calculus of differential equations)

$$\phi ::= X(\theta) \mid p(\theta) \mid \theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \langle x' = \theta \rangle \phi \mid \mu X. \phi$$



Corollary

Constructive and (except $x' = \theta$, \exists and $[\beta^]$) coding-free.*

Corollary (Conquand & Huet)

(Inf.Comput'88)

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

Corollary (Meyer & Halpern)

(J.ACM'82)

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

Corollary (Schmitt)

(Inf.Control.'84)

$[\alpha]$ -free semidecidable for uninterpreted programs (if \exists -free).

Corollary

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



Corollary

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

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: Find succinct weaker invariants
- $[x' = \theta]G$ and $\langle x' = \theta \rangle G$: Find succinct differential (in)variants
- $\exists x G$: Complexity depends on Herbrand disjunctions:
 - ✓ uninterpreted
 - ✓ reals
 - ✗ $\exists x [\alpha^*]G$ Π_1^1 -complete for discrete α

Corollary (Hybrid version of Parikh's result)

(FOCS'83)

**-free dGL complete relative to dL, relative to continuous, or to discrete*

d-free dGL complete relative to dL, relative to continuous, or to discrete



Corollary ()

(+LICS'12)

dGL complete relative to ODE for hybrid games with finite-rank Borel winning regions.

Corollary ()

(+LICS'12)

dGL + Euler axiom complete relative to discrete L_μ over \mathbb{R}

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

► Fixpoint style proof technique

$$\forall x (0 \leq x < 1 \vee \forall t \geq 0 p(0 + t) \vee p(x - 1) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$$

$$\forall x (0 \leq x < 1 \vee \langle x := 1 \rangle \neg \exists t \geq 0 \langle x := x + t \rangle \neg p(x) \vee p(x - 1) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$$

$$\forall x (0 \leq x < 1 \vee \langle x := 1 \rangle \neg \langle x' = 1 \rangle \neg p(x) \vee p(x - 1) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$$

$$\forall x (0 \leq x < 1 \vee \langle \beta \rangle p(x) \vee \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$$

$$\forall x (0 \leq x < 1 \vee \langle \beta \cup \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$$

$$\forall x (0 \leq x < 1 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 1 \rightarrow \langle \alpha^* \rangle 0 \leq x < 1) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1)$$

$$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1$$

Theorem (Hybrid system vs. hybrid game)

dGL is a subregular, sub-Barcan, monotonic modal logic without the induction axiom of dynamic logic.

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

$$M \quad \langle \alpha \rangle \phi \vee \langle \alpha \rangle \psi \rightarrow \langle \alpha \rangle (\phi \vee \psi)$$

$$\cancel{G} \quad \frac{\phi}{[\alpha]\phi}$$

$$M_{[\cdot]} \quad \frac{\phi \rightarrow \psi}{[\beta]\phi \rightarrow [\beta]\psi}$$

$$\cancel{R} \quad \frac{\phi_1 \wedge \phi_2 \rightarrow \psi}{[\alpha]\phi_1 \wedge [\alpha]\phi_2 \rightarrow [\alpha]\psi}$$

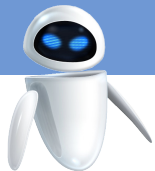
$$\cancel{B} \quad \langle \alpha \rangle \exists x \phi \rightarrow \exists x \langle \alpha \rangle \phi \quad (x \notin \alpha)$$

$$\overleftarrow{B} \quad \exists x \langle \alpha \rangle \phi \rightarrow \langle \alpha \rangle \exists x \phi \quad (x \notin \alpha)$$

$$\cancel{I} \quad [\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$$

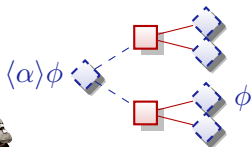
$$\forall I \quad \text{Cl}_\forall(\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$$

$$\cancel{FA} \quad \langle \alpha^* \rangle \phi \rightarrow \phi \vee \langle \alpha^* \rangle (\neg \phi \wedge \langle \alpha \rangle \phi)$$

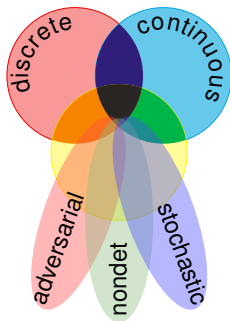


differential game logic

$$\text{dGL} = \text{GL} + \text{HG}$$



- Logic for hybrid games
- Game logic + logic for hybrid
- Sound & complete / $L_{\mu D}$
- Fixpoint-style proofs
- Complete fragments \rightsquigarrow expressibility
- Stochastic \approx adversarial





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-13-100, School of Computer Science,
Carnegie Mellon University, Pittsburgh, PA, January 2013.

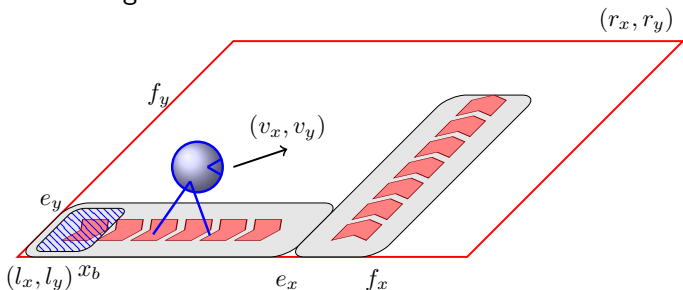


Jan-David Quesel and André Platzer.

Playing hybrid games with KeYmaera.

In Bernhard Gramlich, Dale Miller, and Ulrike Sattler, editors, *IJCAR*, volume 7364 of *LNCS*, pages 439–453. Springer, 2012.

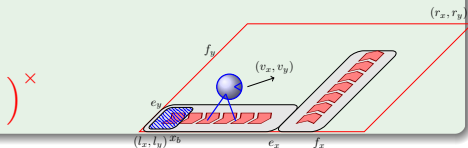
Verification Challenge:



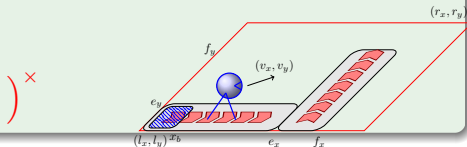
Hybrid games proving also for proving relaxed notions of system similarity

Example (Environment vs. Robot)

$$\left(\left(?true \wedge (? (x < e_x \wedge y < e_y \wedge \text{eff}_1 = 1)); v_x := v_x + c_x; \text{eff}_1 := 0 \right) \right. \\ \left. \wedge (? (e_x \leq x \wedge y \leq f_y \wedge \text{eff}_2 = 1); v_y := v_y + c_y; \text{eff}_2 := 0) \right);$$

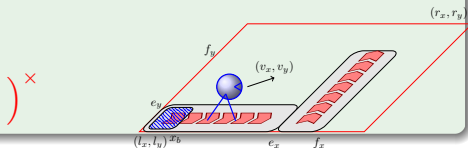


Example (Environment vs. Robot)

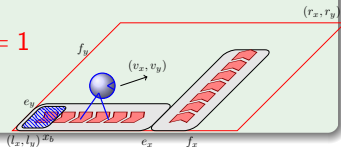
$$\begin{aligned} & \left((?true \wedge (? (x < e_x \wedge y < e_y \wedge \text{eff}_1 = 1); v_x := v_x + c_x; \text{eff}_1 := 0) \right. \\ & \quad \left. \wedge (? (e_x \leq x \wedge y \leq f_y \wedge \text{eff}_2 = 1); v_y := v_y + c_y; \text{eff}_2 := 0) \right); \\ & (a_x := *; ?(-A \leq a_x \leq A); \\ & a_y := *; ?(-A \leq a_y \leq A); \\ & t_s := 0); \end{aligned}$$


Example (Environment vs. Robot)

$$\begin{aligned}
 & \left((?true \wedge (? (x < e_x \wedge y < e_y \wedge \text{eff}_1 = 1); v_x := v_x + c_x; \text{eff}_1 := 0) \right. \\
 & \quad \left. \wedge (? (e_x \leq x \wedge y \leq f_y \wedge \text{eff}_2 = 1); v_y := v_y + c_y; \text{eff}_2 := 0) \right); \\
 & (a_x := *; ?(-A \leq a_x \leq A); \\
 & \quad a_y := *; ?(-A \leq a_y \leq A); \\
 & \quad t_s := 0); \\
 & (x' = v_x, y' = v_y, v'_x = a_x, v'_y = a_y, t' = 1, t'_s = 1 \& t_s \leq \varepsilon)^d;
 \end{aligned}$$



Example (Environment vs. Robot)

$$\begin{aligned}
 & \left((?true \wedge (?(x < e_x \wedge y < e_y \wedge \text{eff}_1 = 1); v_x := v_x + c_x; \text{eff}_1 := 0) \right. \\
 & \quad \left. \wedge (?(e_x \leq x \wedge y \leq f_y \wedge \text{eff}_2 = 1); v_y := v_y + c_y; \text{eff}_2 := 0)); \right. \\
 & \quad (a_x := *; ?(-A \leq a_x \leq A); \\
 & \quad \quad a_y := *; ?(-A \leq a_y \leq A); \\
 & \quad \quad t_s := 0); \\
 & \left((x' = v_x, y' = v_y, v'_x = a_x, v'_y = a_y, t' = 1, t'_s = 1 \wedge t_s \leq \varepsilon)^d ; \right. \\
 & \quad \cup ((?a_x v_x \leq 0 \wedge a_y v_y \leq 0; \\
 & \quad \quad \text{if } v_x = 0 \text{ then } a_x := 0 \text{ fi}; \\
 & \quad \quad \text{if } v_y = 0 \text{ then } a_y := 0 \text{ fi}); \\
 & \quad \left(x' = v_x, y' = v_y, v'_x = a_x, v'_y = a_y, t' = 1, t'_s = 1 \right. \\
 & \quad \left. \left. \wedge t_s \leq \varepsilon \wedge a_x v_x \leq 0 \wedge a_y v_y \leq 0 \right)^d \right))^\times
 \end{aligned}$$


Proposition (Robot stays in \square)

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

Proposition (Stays in \square + leaves shaded region in time)

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

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