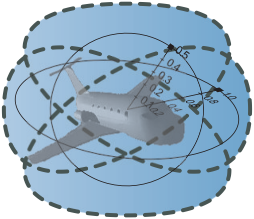
Differential Game Logic

André Platzer

Carnegie Mellon University

Summer School Marktoberdorf 2017



Outline

Outline

1. CPS Game Motivation
2. Differential Game Logic
   - Syntax
   - Example: Push-around Cart
   - Example: Robot Dance
   - Differential Hybrid Games
   - Denotational Semantics
   - Determinacy
   - Strategic Closure Ordinals
3. Axiomatization
   - Axiomatics
   - Example: Robot Soccer
   - Soundness and Completeness
   - Separating Axioms
4. Expressiveness
5. Differential Hybrid Games
6. Summary

Which control decisions are safe for aircraft collision avoidance?

Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.

Can you trust a computer to control physics?

Can you trust a computer to control physics?

1. Depends on how it has been programmed
2. And on what will happen if it malfunctions

Rationale

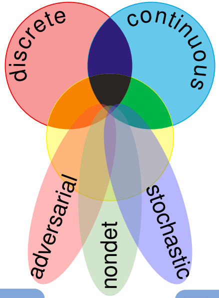
1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

CPSs deserve proofs as safety evidence!

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

Tame Parts

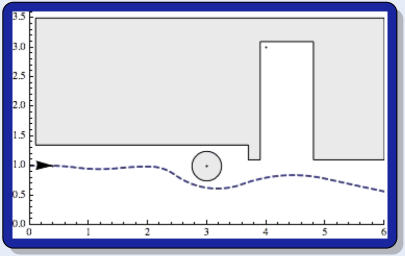
Exploiting compositionality tames CPS complexity.

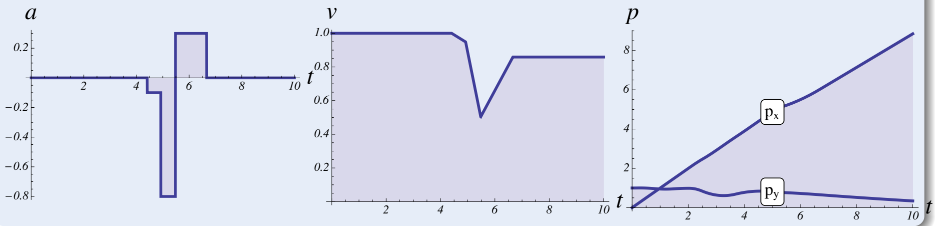
Analytic simplification

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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

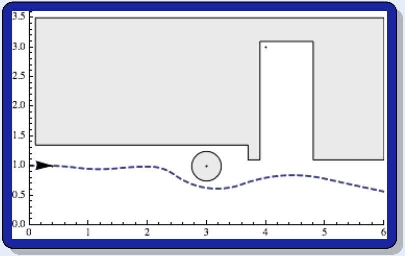


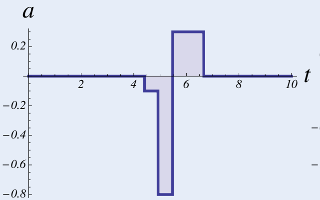


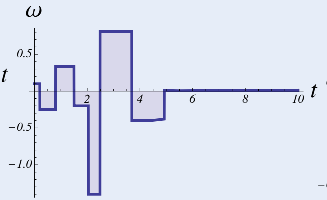
Challenge (Hybrid Systems)

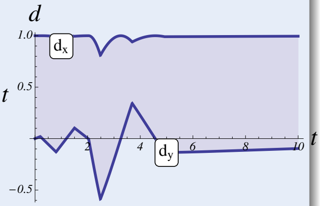
Fixed rule describing state evolution with both

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





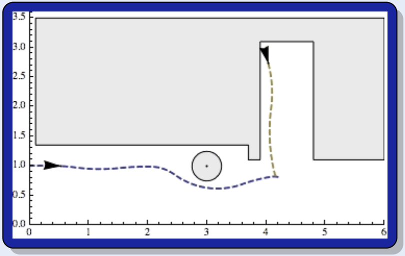


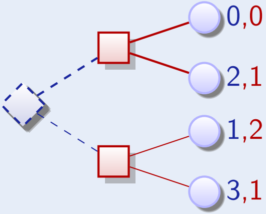


Challenge (Games)

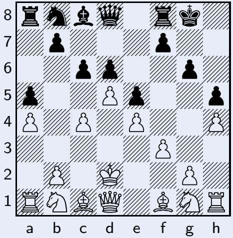
Game rules describing play evolution with both

- Angelic choices (player $\Diamond$ Angel)
- Demonic choices (player $\Box$ Demon)





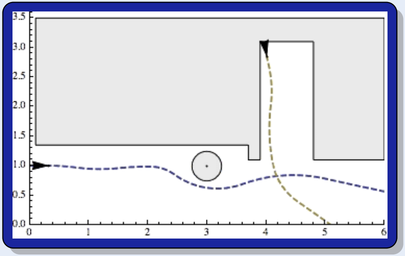
$\Diamond\backslash\Box$	Tr	Pl
Trash	1,2	0,0
Plant	0,0	2,1

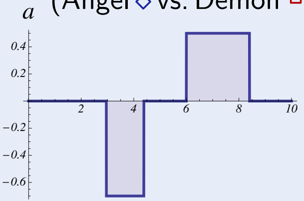


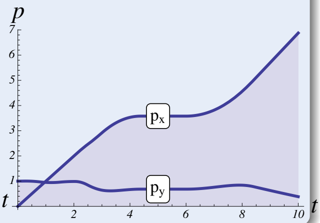
Challenge (Hybrid Games)

Game rules describing play evolution with

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





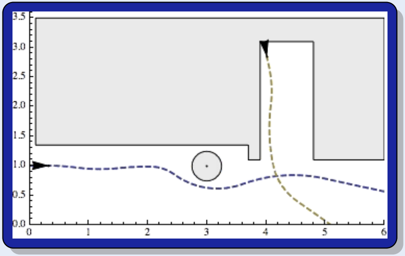


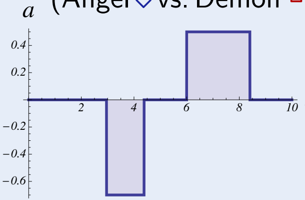
CPS Analysis: Robot Control

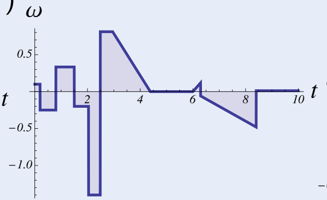
Challenge (Hybrid Games)

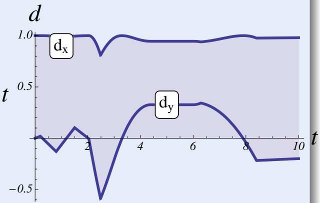
Game rules describing play evolution with

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





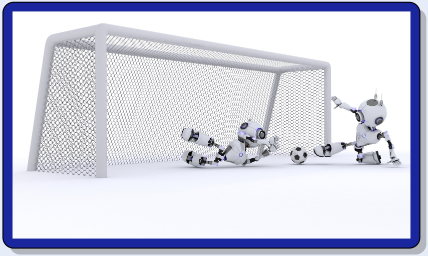


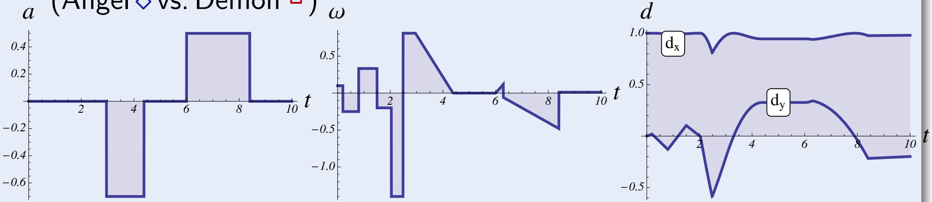


Challenge (Hybrid Games)

Game rules describing play evolution with

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

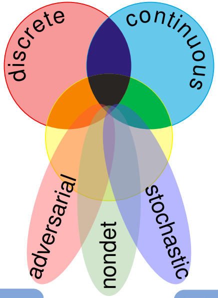




CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

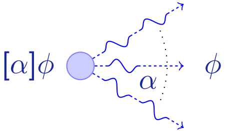
Tame Parts

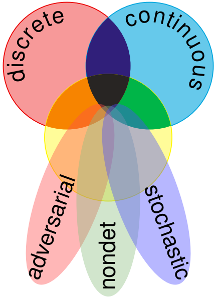
Exploiting compositionality tames CPS complexity.

Analytic simplification

differential dynamic logic

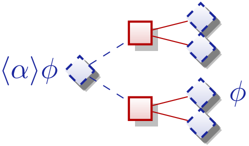
$d\mathcal{L} = \text{DL} + \text{HP}$





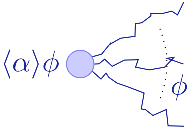
differential game logic

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



stochastic differential DL

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



quantified differential DL

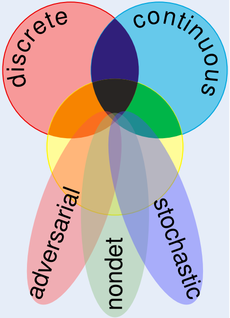
$Qd\mathcal{L} = \text{FOL} + \text{DL} + \text{QHP}$

JAR'08,CADE'11,LMCS'12,LICS'12,LICS'12

TOCL'15,JAR'17,TOCL'17,JACM'20

Dynamic Logics

- DL has been introduced for programs
  Pratt'76,Harel,Kozen
- Its real calling are dynamical systems
- DL excels at providing simple+elegant logical foundations for dynamical systems
- CPSs are multi-dynamical systems
- DL for CPS are multi-dynamical



JAR'08,CADE'11,LMCS'12,LICS'12,LICS'12 TOCL'15,JAR'17,TOCL'17,JACM'20

Contributions

Logical foundations for hybrid games

1. Compositional programming language for hybrid games
2. Compositional logic and proof calculus for winning strategy existence
3. Hybrid games determined
4. Winning region computations terminate after $\geq\omega_1^{CK}$ iterations
5. Separate truth ($\exists$ winning strategy) vs. proof (winning certificate) vs. proof search (automatic construction)
6. Sound & relatively complete
7. Expressiveness
8. Fragments successful in applications
9. Generalizations in logic enable more applications

TOCL'15

Outline

Differential Game Logic: Syntax

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula P)

$$p(e_1, \ldots, e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

TOCL'15

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

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

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

$$p(e_1,\dots,e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

All Reals | Some Reals

TOCL'15

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

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

$$p(e_1,\ldots,e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

All Reals | Some Reals

TOCL'15

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

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

$$p(e_1, \ldots, e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

All Reals | Some Reals | Angel Wins

TOCL'15

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

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

$$p(e_1,\ldots,e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

All Reals | Some Reals | Angel Wins | Demon Wins

TOCL'15

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

$$x := f(x) \mid ?Q \mid x' = f(x) \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

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

$$p(e_1, \ldots, e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

"Angel has Wings $\langle \alpha \rangle$"

All Reals | Some Reals | Angel Wins | Demon Wins

TOCL'15

◇ Angel Ops

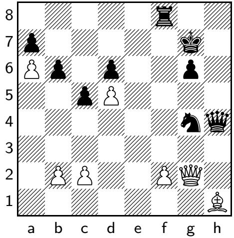
$\cup$	choice
$*$	repeat
$x' = f(x)$	evolve
$?Q$	challenge

$\xrightarrow{d}$ / $\xleftarrow{d}$

□ Demon Ops

$\cap$	choice
$\times$	repeat
$x' = f(x)^d$	evolve
$?Q^d$	challenge

Duality operator ^{d} passes control between players



Game Operators

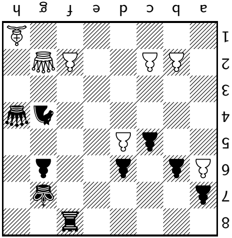
◇ Angel Ops	
$\cup$	choice
$*$	repeat
$x' = f(x)$	evolve
$?Q$	challenge

d

d

◻ Demon Ops	
$\cap$	choice
$\times$	repeat
$x' = f(x)^d$	evolve
$?Q^d$	challenge

Duality operator ^{d} passes control between players



Definable Game Operators

◇ Angel Ops

$\cup$	choice
$*$	repeat
$x' = f(x)$	evolve
$?Q$	challenge

$\xrightarrow{d}$ / $\xleftarrow{d}$

□ Demon Ops

$\cap$	choice
$\times$	repeat
$x' = f(x)^d$	evolve
$?Q^d$	challenge

$$
\begin{aligned}
\texttt{if}(Q)\,\alpha\,\texttt{else}\,\beta &\equiv \\
\texttt{while}(Q)\,\alpha &\equiv \\
\alpha \cap \beta &\equiv \\
\alpha^{\times} &\equiv \\
(x' = f(x)\,\&\,Q)^d &\quad x' = f(x)\,\&\,Q \\
(x := f(x))^d &\quad x := f(x) \\
?Q^d &\quad ?Q
\end{aligned}
$$

Definable Game Operators

◇ Angel Ops

$\cup$	choice
$*$	repeat
$x' = f(x)$	evolve
$?Q$	challenge

$\xrightarrow{d}$ / $\xleftarrow{d}$

□ Demon Ops

$\cap$	choice
$\times$	repeat
$x' = f(x)^d$	evolve
$?Q^d$	challenge

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

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

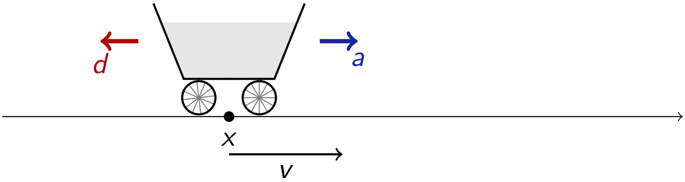
$$\alpha \cap \beta \equiv (\alpha^d \cup \beta^d)^d$$

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

$$(x' = f(x)\,\&\,Q)^d \not\equiv x' = f(x)\,\&\,Q$$

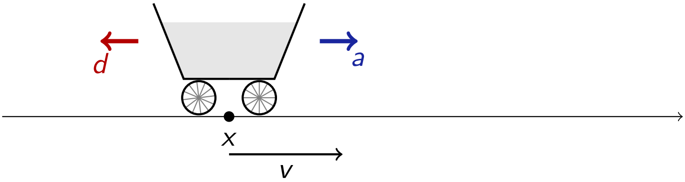
$$(x := f(x))^d \equiv x := f(x)$$

$$?Q^d \not\equiv ?Q$$

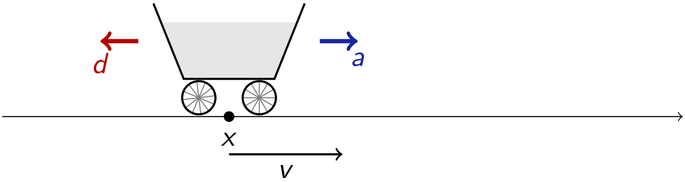


$$v \geq 1 \rightarrow$$
$$\left[\left((d := 1 \cup d := -1)^d; (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

Example: Push-around Cart

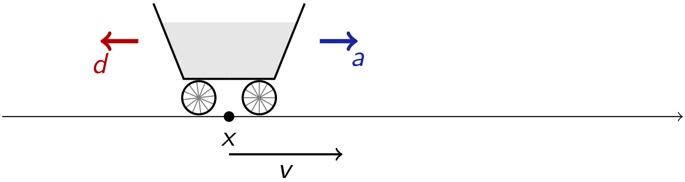


$$v \geq 1 \rightarrow$$
$$\left[\left((d := 1 \cup d := -1)^d ; (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$



$\vDash v \geq 1 \rightarrow$

$$\Big[\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*\Big] v \geq 0$$



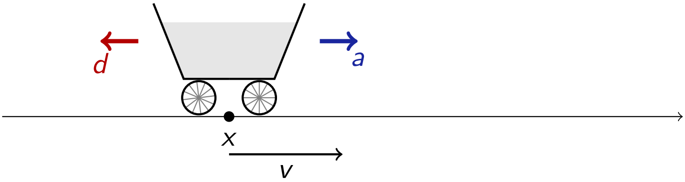
$\vDash v \geq 1 \rightarrow$ $\qquad$ d before a can compensate

$$[((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\})^*]\, v \geq 0$$

$x \geq 0 \land v \geq 0 \rightarrow$

$$[((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\})^*]\, x \geq 0$$

Example: Push-around Cart

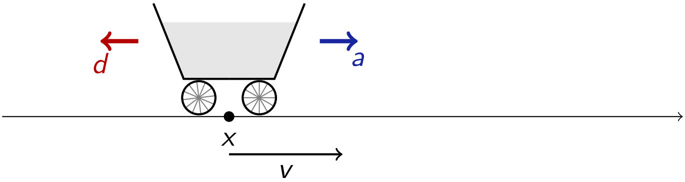


$\vDash v \geq 1 \rightarrow$ $\quad$ d before a can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$\vDash x \geq 0 \land v \geq 0 \rightarrow$

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] x \geq 0$$

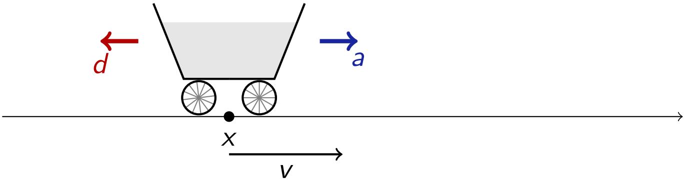


$\vDash v \geq 1 \rightarrow$ $\quad$ d before a can compensate

$$\Big[\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*\Big] v \geq 0$$

$x \geq 0 \quad \rightarrow$

$$\Big\langle\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*\Big\rangle x \geq 0$$

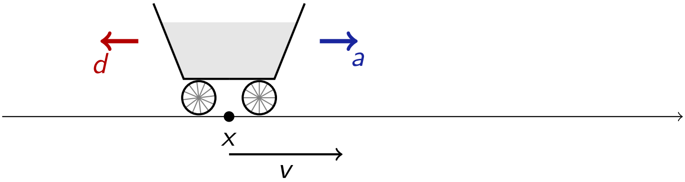


$\vDash v \geq 1 \rightarrow$ $\quad$ d before a can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$\vDash x \geq 0 \quad \rightarrow$ $\quad$ boring by skip

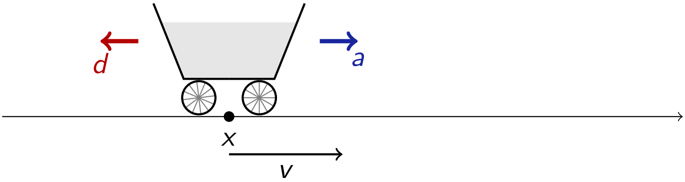
$$\left\langle\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$$



$\vDash v \geq 1 \rightarrow$ $\qquad$ d before a can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$$\left\langle\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$$

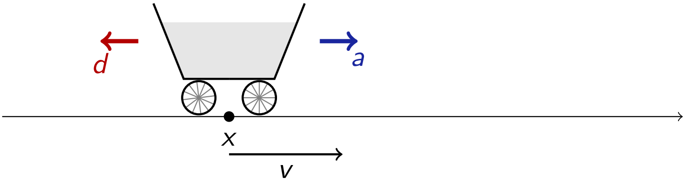


$\vDash\ v \geq 1 \rightarrow$ *d* before *a* can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$\nvDash$ counterstrategy $d := -1$

$$\left\langle\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$$



$\models v \geq 1 \rightarrow$ $\qquad$ d before a can compensate

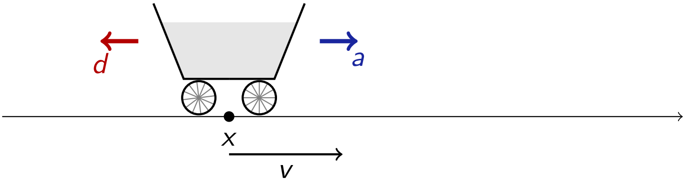
$$[((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\})^*] v \geq 0$$

$\not\models$ $\qquad$ counterstrategy $d := -1$

$$\langle((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\})^*\rangle x \geq 0$$

$$\langle((d := 1 \cap d := -1); (a := 2 \cup a := -2); \{x' = v, v' = a + d\})^*\rangle x \geq 0$$

Example: Push-around Cart



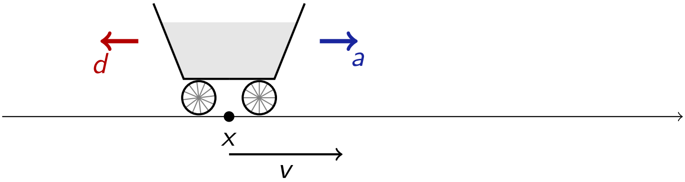
$\vDash$ $v \geq 1 \rightarrow$ — d before a can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$\nvDash$ — counterstrategy $d := -1$

$$\left\langle\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$$

$\vDash$ $\left\langle\left((d := 1 \cap d := -1); (a := 2 \cup a := -2); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$



$\models v \geq 1 \rightarrow$ *d* before *a* can compensate

$$\Big[\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*\Big] v \geq 0$$

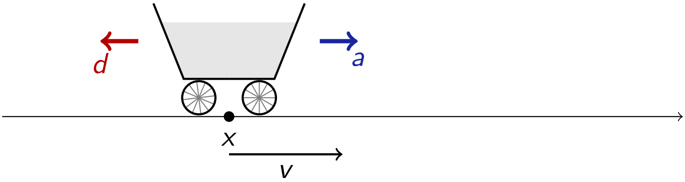
$\not\models$ counterstrategy $d := -1$

$$\Big\langle\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*\Big\rangle x \geq 0$$

$$\models \Big\langle\big((d := 1 \cap d := -1);\ (a := 2 \cup a := -2);\ \{x' = v, v' = a + d\}\big)^*\Big\rangle x \geq 0$$

$$\Big\langle\big((d := 2 \cap d := -2);\ (a := 2 \cup a := -2);\ t := 0;\ \{x' = v, v' = a + d, t' = 1 \,\&\, t \leq 1\}\big)^*\Big\rangle x^2 \geq 100$$

Example: Push-around Cart



$\vDash\ v \geq 1 \rightarrow$ *d* before *a* can compensate

$$\left[\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right] v \geq 0$$

$\nvDash$ counterstrategy $d := -1$

$$\left\langle\left((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$$

$\vDash\ \left\langle\left((d := 1 \cap d := -1);\ (a := 2 \cup a := -2);\ \{x' = v, v' = a + d\}\right)^*\right\rangle x \geq 0$

$\vDash\ \langle((d := 2 \cap d := -2);\ (a := 2 \cup a := -2);$ $a := d$ then $a := 2 \operatorname{sign} v$

$$t := 0;\ \{x' = v, v' = a + d, t' = 1 \,\&\, t \leq 1\})^*\rangle\, x^2 \geq 100$$

Example: EVE and WALL·E

$$
\begin{aligned}
&(w-e)^2 \le 1 \land v = f \rightarrow \\
&\Big\langle \Big((u := 1 \cap u := -1); \\
&\quad (g := 1 \cup g := -1); \\
&\quad t := 0; \\
&\quad (w' = v, v' = u, e' = f, f' = g, t' = 1 \,\&\, t \le 1)^d \\
&\Big)^{\times} \Big\rangle \, (w-e)^2 \le 1
\end{aligned}
$$

EVE at e plays Angel's part controlling g

WALL·E at w plays Demon's part controlling u

Example: EVE and WALL·E and the World

$$
\begin{aligned}
&(w-e)^2 \le 1 \land v = f \rightarrow \\
&\langle ((u := 1 \cap u := -1); \\
&\quad (g := 1 \cup g := -1); \\
&\quad t := 0; \\
&\quad (w' = v, v' = u, e' = f, f' = g, t' = 1 \,\&\, t \le 1)^d \\
&)^\times \rangle\ (w-e)^2 \le 1
\end{aligned}
$$

EVE at e plays Angel's part controlling g

WALL·E at w plays Demon's part controlling u

EVE assigned environment's time to WALL·E

Example: WALL·E and EVE

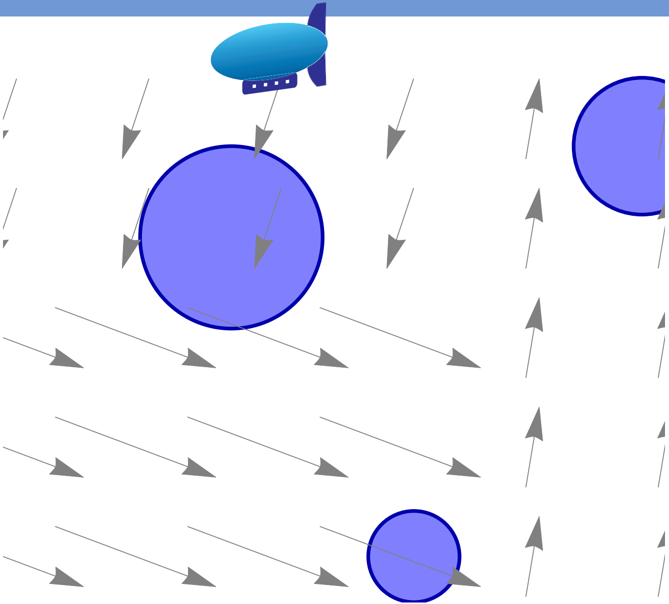
$$
\begin{aligned}
&(w-e)^2 \le 1 \land v = f \to \\
&[((u := 1 \cap u := -1); \\
&\quad (g := 1 \cup g := -1); \\
&\quad t := 0; \\
&\quad (w' = v, v' = u, e' = f, f' = g, t' = 1 \,\&\, t \le 1) \\
&)^{\times}]\ (w-e)^2 > 1
\end{aligned}
$$

WALL·E at w plays Demon's part controlling u

EVE at e plays Angel's part controlling g

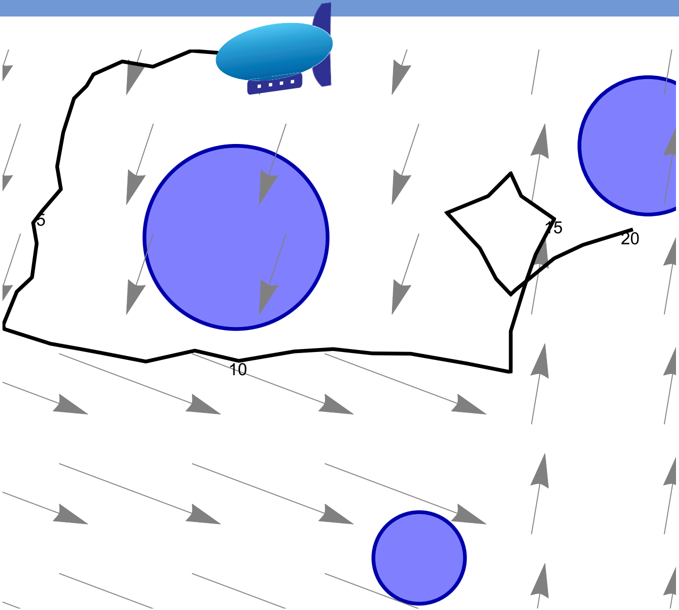
WALL·E assigned environment's time to EVE

Zeppelin Obstacle Parcours



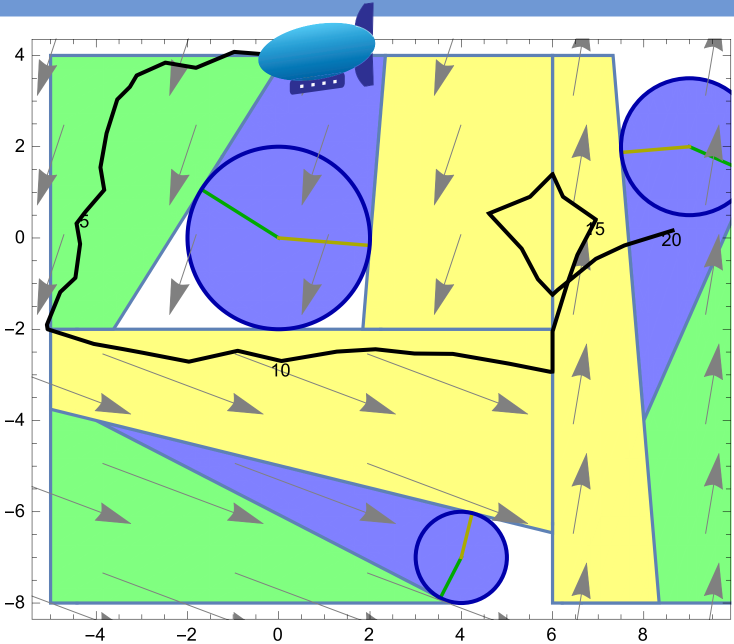
avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

TOCL'17



avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

TOCL'17



avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

TOCL'17

Differential Game Logic: Denotational Semantics

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

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

Definition (d$\mathcal{GL}$ Formula P) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S})$

$$\begin{aligned}
[\![e \geq \tilde{e}]\!] &= \{s \in \mathcal{S} \;:\; [\![e]\!]_s \geq [\![\tilde{e}]\!]_s\} \\
[\![\neg P]\!] &= ([\![P]\!])^\complement \\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle\alpha\rangle P]\!] &= \varsigma_\alpha([\![P]\!]) \\
[\![[\alpha]P]\!] &= \delta_\alpha([\![P]\!])
\end{aligned}$$

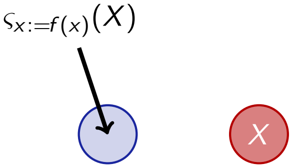
Definition (Hybrid game α: denotational semantics)

$\varsigma_{x:=f(x)}(X) =$

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

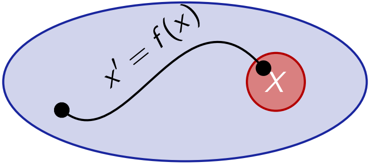
$$\varsigma_{x:=f(x)}(X) = \{s \in \mathcal{S} : s_x^{[\![f(x)]\!]_s} \in X\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

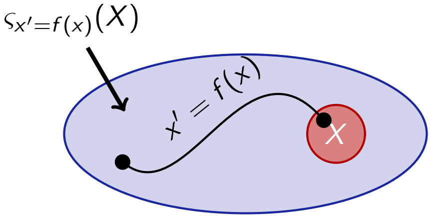
$\varsigma_{x'=f(x)}(X) =$



Differential Game Logic: Denotational Semantics

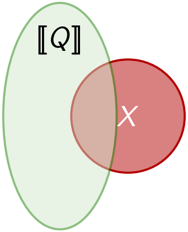
Definition (Hybrid game α: denotational semantics)

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



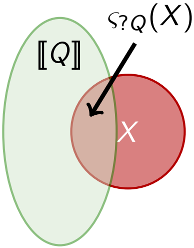
Definition (Hybrid game α: denotational semantics)

$\varsigma_{?Q}(X) =$



Definition (Hybrid game α: denotational semantics)

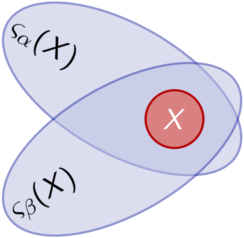
$$\varsigma_{?Q}(X) = [\![Q]\!] \cap X$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

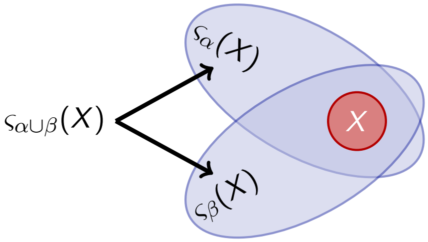
$\varsigma_{\alpha\cup\beta}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

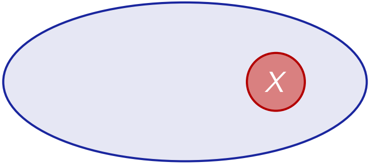
$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$



Differential Game Logic: Denotational Semantics

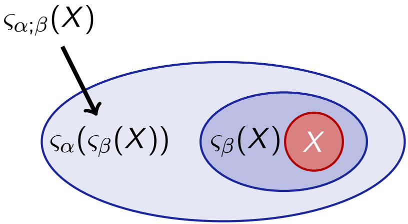
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

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



Differential Game Logic: Denotational Semantics

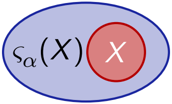
Definition (Hybrid game α: denotational semantics)

$\varsigma_{\alpha^*}(X) =$

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

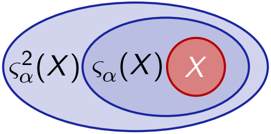
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

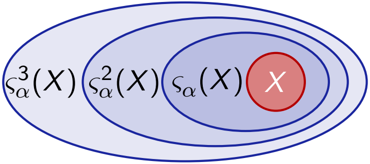
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

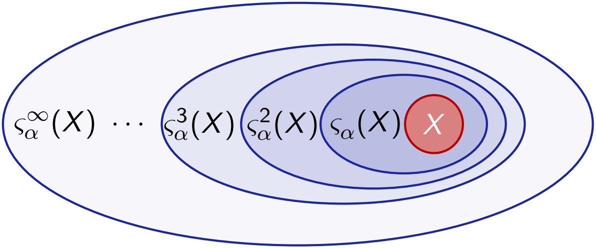
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

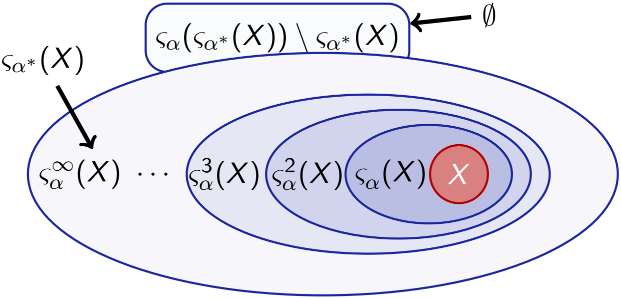
Definition (Hybrid game α: denotational semantics)

$\varsigma_{\alpha^*}(X) =$



Definition (Hybrid game α: denotational semantics)

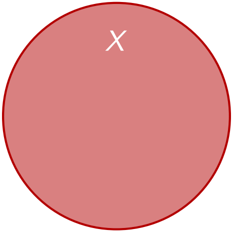
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

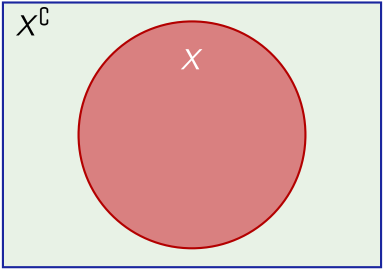
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

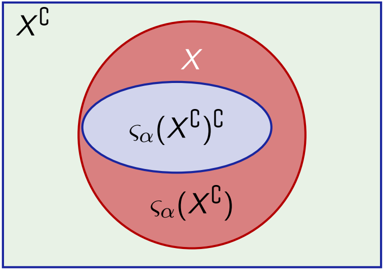
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

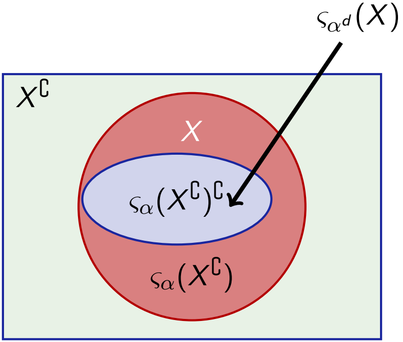
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

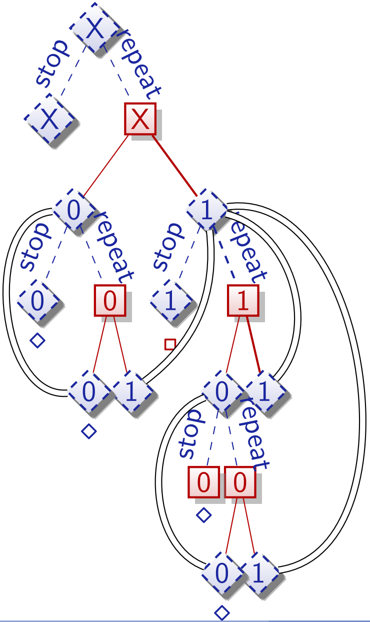
Definition (Hybrid game α: denotational semantics)

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



Filibusters

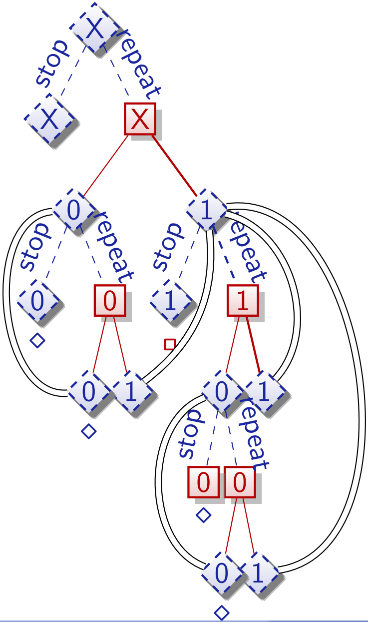
$\langle (x := 0 \cap x := 1)^* \rangle x = 0$



Filibusters & The Significance of Finitude

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

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



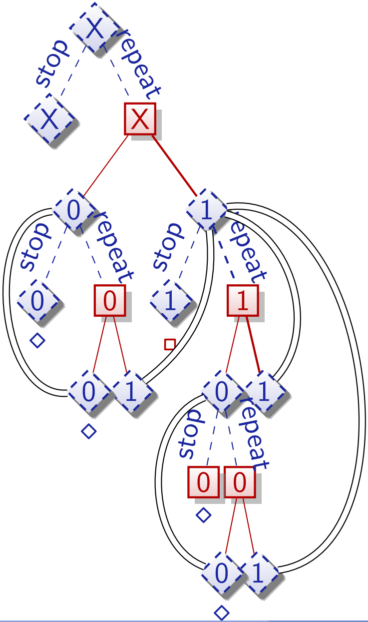
Filibusters & The Significance of Finitude

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

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

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

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



Filibusters & The Significance of Finitude

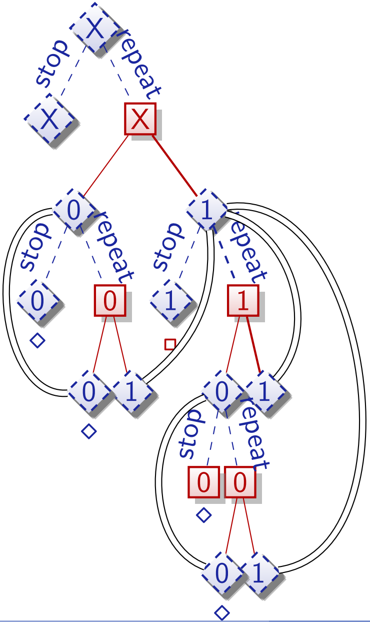
$\overset{<\infty}{\rightsquigarrow}$ true

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

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

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

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



Filibusters & The Significance of Finitude

$\overset{<\infty}{\rightsquigarrow}$ true

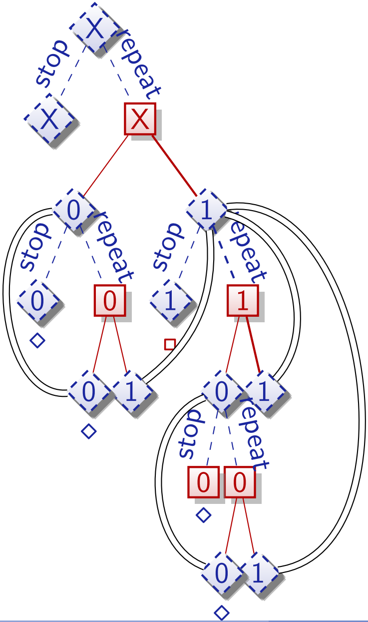
$\langle (x' = 1^d; x := 0)^* \rangle x = 0$

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

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

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

Well-defined games
can't be postponed forever



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

Winning Region Fixpoint Iterations

Definition (Hybrid game α)

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

Winning Region Fixpoint Iterations

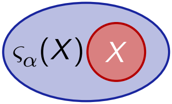
Definition (Hybrid game α)

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

Winning Region Fixpoint Iterations

Definition (Hybrid game α)

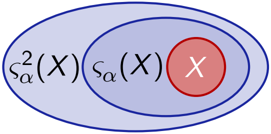
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Winning Region Fixpoint Iterations

Definition (Hybrid game α)

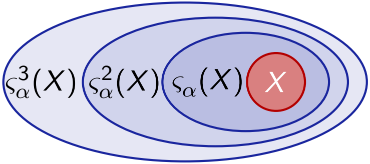
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Winning Region Fixpoint Iterations

Definition (Hybrid game α)

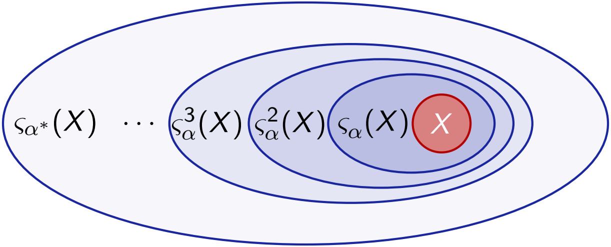
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \;:\; X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Winning Region Fixpoint Iterations

Definition (Hybrid game α)

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



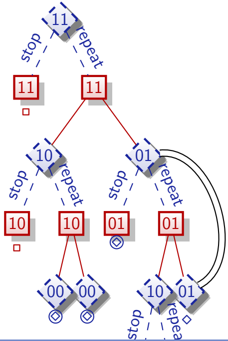
Winning Region Fixpoint Iterations

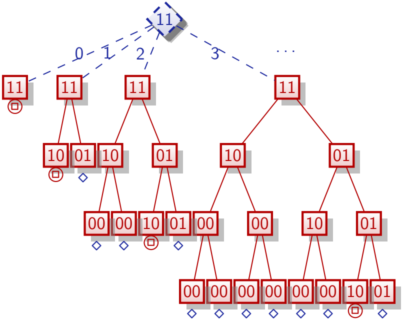
Definition (Hybrid game α)

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

Alternative (Advance notice semantics)

$$\varsigma_{\alpha^*}(X) \stackrel{?}{=} \bigcup_{n<\omega} \varsigma_{\alpha^n}(X) \qquad \text{where } \alpha^{n+1} \equiv \alpha^n;\alpha \quad \alpha^0 \equiv ?true$$





Winning Region Fixpoint Iterations

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

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

Winning Region Fixpoint Iterations

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

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

Winning Region Fixpoint Iterations

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)

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

$$\varsigma_\alpha^0(X) \overset{\text{def}}{=} X$$

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

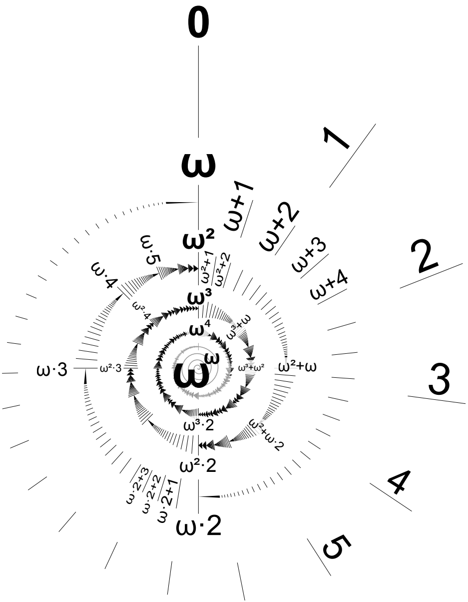
$$\varsigma_\alpha^\lambda(X) \overset{\text{def}}{=} \bigcup_{\kappa<\lambda} \varsigma_\alpha^\kappa(X) \qquad \lambda \neq 0 \text{ a limit ordinal}$$

Example

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

Theorem

Hybrid game closure ordinal $\geq \omega_1^{CK}$



Outline

Differential Game Logic: Axiomatization

$[\cdot]$ $[\alpha]P \leftrightarrow$

$\langle:=\rangle$ $\langle x := f(x)\rangle p(x) \leftrightarrow$

$\langle'\rangle$ $\langle x' = f(x)\rangle P \leftrightarrow$

$\langle?\rangle$ $\langle ?Q\rangle P \leftrightarrow$

$\langle\cup\rangle$ $\langle \alpha \cup \beta\rangle P \leftrightarrow$

$\langle;\rangle$ $\langle \alpha; \beta\rangle P \leftrightarrow$

$\langle^*\rangle$ $\langle \alpha^*\rangle P \leftrightarrow$

$\langle^d\rangle$ $\langle \alpha^d\rangle P \leftrightarrow$

TOCL'15

Differential Game Logic: Axiomatization

$[\cdot]$ $[\alpha]P \leftrightarrow \neg\langle\alpha\rangle\neg P$

$\langle:=\rangle$ $\langle x := f(x)\rangle p(x) \leftrightarrow p(f(x))$

$\langle'\rangle$ $\langle x' = f(x)\rangle P \leftrightarrow \exists t{\geq}0\, \langle x := y(t)\rangle P$

$\langle?\rangle$ $\langle ?Q\rangle P \leftrightarrow (Q \wedge P)$

$\langle\cup\rangle$ $\langle\alpha \cup \beta\rangle P \leftrightarrow \langle\alpha\rangle P \vee \langle\beta\rangle P$

$\langle;\rangle$ $\langle\alpha;\beta\rangle P \leftrightarrow \langle\alpha\rangle\langle\beta\rangle P$

$\langle^*\rangle$ $\langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$

$\langle^d\rangle$ $\langle\alpha^d\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$

M $\dfrac{P \rightarrow Q}{\langle\alpha\rangle P \rightarrow \langle\alpha\rangle Q}$

FP $\dfrac{P \vee \langle\alpha\rangle Q \rightarrow Q}{\langle\alpha^*\rangle P \rightarrow Q}$

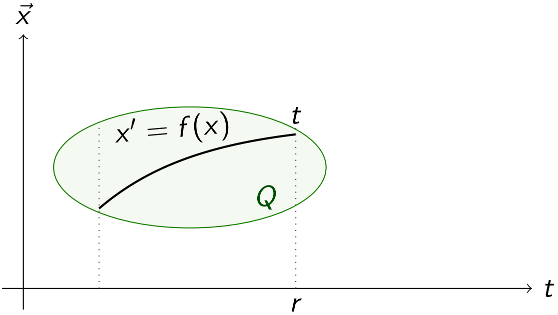
MP $\dfrac{P \quad P \rightarrow Q}{Q}$

$\forall$ $\dfrac{p \rightarrow Q}{p \rightarrow \forall x\, Q}$ $(x \notin \mathrm{FV}(p))$

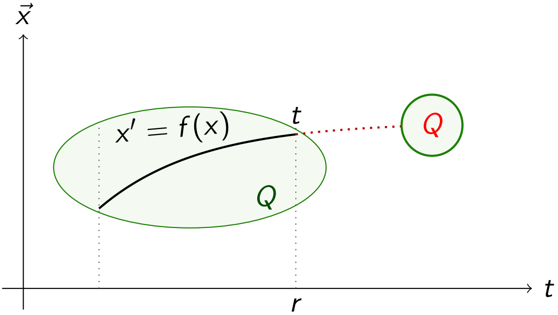
US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

TOCL'15

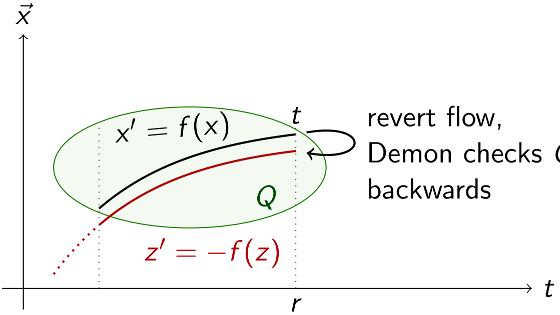
$x' = f(x) \,\&\, Q$ $\qquad\qquad$ $x' = f(x); ?(Q)$



$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); ?(Q)$

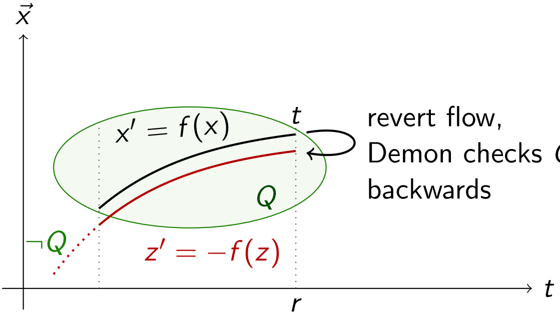


$x' = f(x) \,\&\, Q \qquad x' = f(x); (z := x; z' = -f(z))^d; ?(Q(z))$



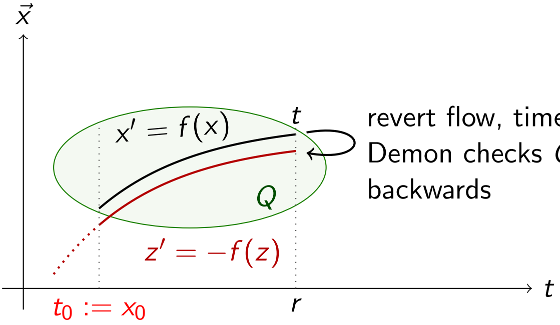
revert flow,
Demon checks Q
backwards

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



revert flow,
Demon checks Q
backwards

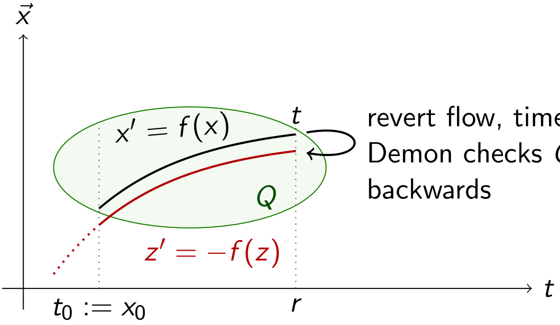
$$x' = f(x) \,\&\, Q \equiv t_0 := x_0; x' = f(x); (z := x; z' = -f(z))^d; ?(z_0 \geq t_0 \rightarrow Q(z))$$



revert flow, time x_0;
Demon checks Q
backwards

“There and Back Again” Game

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

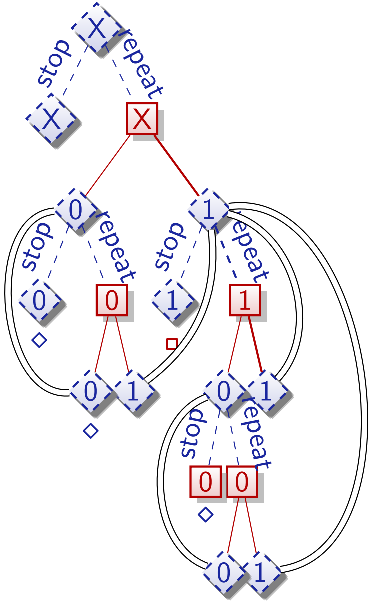


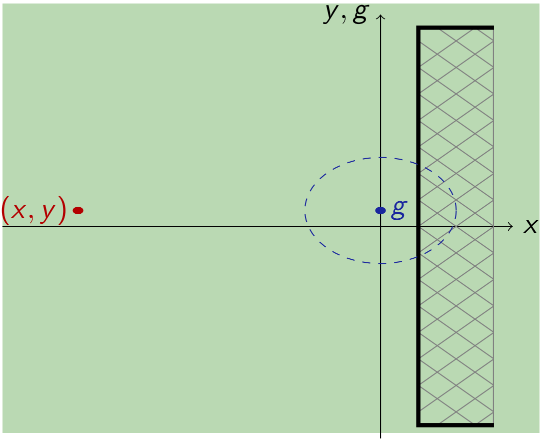
revert flow, time x_0;
Demon checks Q
backwards

Lemma

Evolution domains definable by games

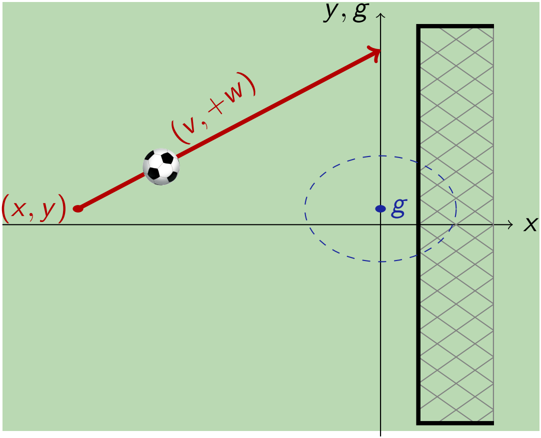
$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{x = 0 \rightarrow 0 = 0 \lor 1 = 0}\mathbb{R}}{x = 0 \rightarrow \langle x := 0\rangle x = 0 \lor \langle x := 1\rangle x = 0}\langle:=\rangle}{x = 0 \rightarrow \langle x := 0 \cup x := 1\rangle x = 0}\langle\cup\rangle}{x = 0 \rightarrow \neg\langle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





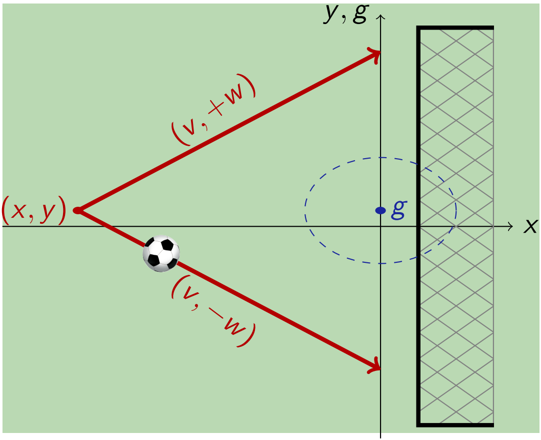
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\Big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^{*}\Big\rangle\, x^2 + (y-g)^2 \le 1$$

Example: Goalie in Robot Soccer



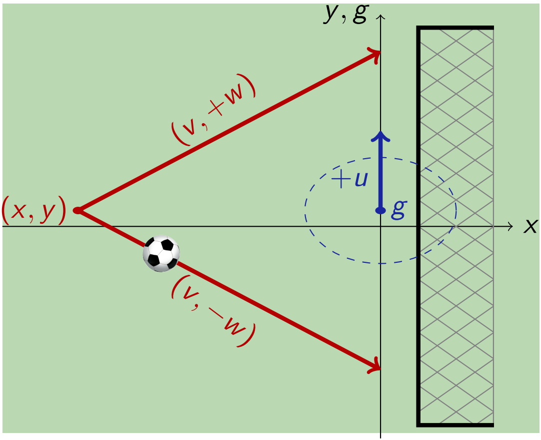
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\Big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\} \big)^* \Big\rangle\, x^2 + (y-g)^2 \le 1$$

Example: Goalie in Robot Soccer



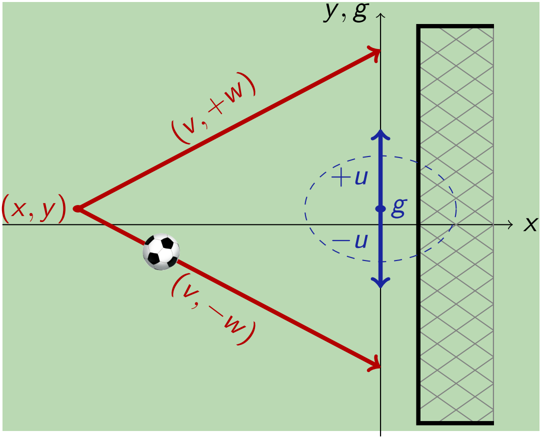
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\Big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \Big\rangle\, x^2 + (y-g)^2 \le 1$$

Example: Goalie in Robot Soccer

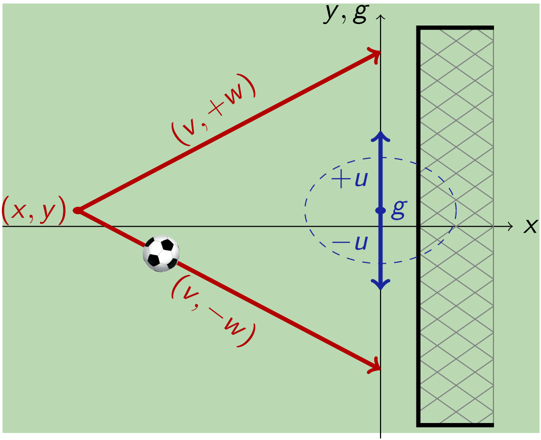


$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^* \rangle\, x^2 + (y - g)^2 \le 1$$

Example: Goalie in Robot Soccer



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

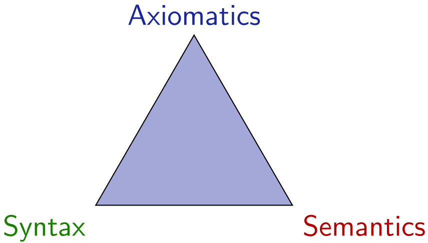


$$\left(\frac{x}{v}\right)^2 (u-w)^2 \le 1 \land$$
$$x < 0 \land v > 0 \land y = g \rightarrow$$
$$\big\langle (w := +w \cap w := -w);$$
$$\big((u := +u \cup u := -u); \{x' = v, y' = w, g' = u\}\big)^*\big\rangle\, x^2 + (y-g)^2 \le 1$$

Soundness

Theorem (Soundness)

dG$\mathcal{L}$ *proof calculus is sound i.e. all provable formulas are valid*



Soundness

Theorem (Soundness)

dGL *proof calculus is sound i.e. all provable formulas are valid*

Proof.

$$\langle\cup\rangle \quad \langle\alpha \cup \beta\rangle P \leftrightarrow \langle\alpha\rangle P \lor \langle\beta\rangle P$$

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

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

$$\text{M} \quad \frac{P \to Q}{\langle\alpha\rangle P \to \langle\alpha\rangle Q}$$

□

Soundness

Theorem (Soundness)

dGL *proof calculus is sound i.e. all provable formulas are valid*

Proof.

$\langle\cup\rangle$ $[\![\langle\alpha\cup\beta\rangle P]\!] = \varsigma_{\alpha\cup\beta}([\![P]\!]) = \varsigma_\alpha([\![P]\!]) \cup \varsigma_\beta([\![P]\!]) = [\![\langle\alpha\rangle P]\!] \cup [\![\langle\beta\rangle P]\!] = [\![\langle\alpha\rangle P \vee \langle\beta\rangle P]\!]$

$\langle\cup\rangle$ $\langle\alpha\cup\beta\rangle P \leftrightarrow \langle\alpha\rangle P \vee \langle\beta\rangle P$

$\langle;\rangle$ $[\![\langle\alpha;\beta\rangle P]\!] = \varsigma_{\alpha;\beta}([\![P]\!]) = \varsigma_\alpha(\varsigma_\beta([\![P]\!])) = \varsigma_\alpha([\![\langle\beta\rangle P]\!]) = [\![\langle\alpha\rangle\langle\beta\rangle P]\!]$

$\langle;\rangle$ $\langle\alpha;\beta\rangle P \leftrightarrow \langle\alpha\rangle\langle\beta\rangle P$

$[\cdot]$ is sound by determinacy

$[\cdot]$ $[\alpha]P \leftrightarrow \neg\langle\alpha\rangle\neg P$

M Assume the premise $P \to Q$ is valid, i.e. $[\![P]\!] \subseteq [\![Q]\!]$.
Then the conclusion $\langle\alpha\rangle P \to \langle\alpha\rangle Q$ is valid, i.e.
$[\![\langle\alpha\rangle P]\!] = \varsigma_\alpha([\![P]\!]) \subseteq \varsigma_\alpha([\![Q]\!]) = [\![\langle\alpha\rangle Q]\!]$ by monotonicity.

$$\text{M}\ \frac{P \to Q}{\langle\alpha\rangle P \to \langle\alpha\rangle Q}$$

□

Soundness & Completeness

Theorem (Completeness)

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

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

TOCL'15

Soundness & Completeness: Consequences

Corollary (Constructive)

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

Remark (Coquand & 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.

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
- $[x' = f(x)]G$ *and* $\langle x' = f(x)\rangle G$: *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*

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
- $[x' = f(x)]G$ and $\langle x' = f(x)\rangle G$: *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

set is Π^0_n iff it's $\{x : \forall y_1\, \exists y_2\, \forall y_3 \ldots y_n\, \varphi(x, y_1, \ldots, y_n)\}$ for a decidable φ
set is Σ^0_n iff it's $\{x : \exists y_1\, \forall y_2\, \exists y_3 \ldots y_n\, \varphi(x, y_1, \ldots, y_n)\}$ for a decidable φ
set is Π^1_1 iff it's $\{x : \forall f\, \exists y\, \varphi(x, y, f)\}$ for a decidable φ and functions f
set is Σ^1_1 iff it's $\{x : \exists f\, \forall y\, \varphi(x, y, f)\}$ for a decidable φ and functions f
$\Delta^i_n = \Sigma^i_n \cap \Pi^i_n$

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* $L_{\mu D}$*, continuous modal* μ*, 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

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

▸ Fixpoint style proof technique

$\mathbb{R}$ $\quad \forall x\,(0{\leq}x{<}1 \lor \forall t{\geq}0\, p(1+t) \lor p(x-1) \to p(x)) \to (true \to p(x))$

$\langle:=\rangle$ $\quad \forall x\,(0{\leq}x{<}1 \lor \langle x:=1\rangle\neg\exists t{\geq}0\,\langle x:=x+t\rangle\neg p(x) \lor p(x-1) \to p(x)) \to (true \to p(x))$

$\langle'\rangle$ $\quad \forall x\,(0{\leq}x{<}1 \lor \langle x:=1\rangle\neg\langle x'=1\rangle\neg p(x) \lor p(x-1) \to p(x)) \to (true \to p(x))$

$\langle;\rangle,\langle^d\rangle$ $\quad \forall x\,(0{\leq}x{<}1 \lor \langle\beta\rangle p(x) \lor \langle\gamma\rangle p(x) \to p(x)) \to (true \to p(x))$

$\langle\cup\rangle$ $\quad \forall x\,(0{\leq}x{<}1 \lor \langle\beta\cup\gamma\rangle p(x) \to p(x)) \to (true \to p(x))$

US $\quad \forall x\,(0{\leq}x{<}1 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0{\leq}x{<}1 \to \langle\alpha^*\rangle 0{\leq}x{<}1) \to (true \to \langle\alpha^*\rangle 0{\leq}x{<}1)$

$\langle^*\rangle$ $\quad true \to \langle\alpha^*\rangle 0{\leq}x{<}1$

More Axioms

$$\text{K} \quad [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q) \qquad \text{M}_{[\cdot]} \ \frac{P \to Q}{[\alpha]P \to [\alpha]Q}$$

$$\overleftarrow{\text{M}} \quad \langle\alpha\rangle(P \lor Q) \to \langle\alpha\rangle P \lor \langle\alpha\rangle Q \qquad \text{M} \quad \langle\alpha\rangle P \lor \langle\alpha\rangle Q \to \langle\alpha\rangle(P \lor Q)$$

$$\text{I} \quad [\alpha^*](P \to [\alpha]P) \to (P \to [\alpha^*]P) \qquad \forall\text{I} \quad (P\to[\alpha]P) \to (P\to[\alpha^*]P)$$

$$\text{B} \quad \langle\alpha\rangle\exists x\, P \to \exists x\, \langle\alpha\rangle P \quad (x \notin \alpha) \qquad \overleftarrow{\text{B}} \quad \exists x\, \langle\alpha\rangle P \to \langle\alpha\rangle\exists x\, P$$

$$\text{G} \quad \frac{P}{[\alpha]P} \qquad \text{M}_{[\cdot]} \ \frac{P \to Q}{[\alpha]P \to [\alpha]Q}$$

$$\text{R} \quad \frac{P_1 \land P_2 \to Q}{[\alpha]P_1 \land [\alpha]P_2 \to [\alpha]Q} \qquad \text{M}_{[\cdot]} \ \frac{P_1 \land P_2 \to Q}{[\alpha](P_1 \land P_2) \to [\alpha]Q}$$

$$\text{FA} \ \langle\alpha^*\rangle P \to P \lor \langle\alpha^*\rangle(\neg P \land \langle\alpha\rangle P) \qquad \overleftarrow{[*]} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*][\alpha]P$$

More Axioms ???

~~K~~	$[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$	$\text{M}_{[\cdot]}$	$\dfrac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$
~~$\overleftarrow{\text{M}}$~~	$\langle\alpha\rangle(P \lor Q) \rightarrow \langle\alpha\rangle P \lor \langle\alpha\rangle Q$	M	$\langle\alpha\rangle P \lor \langle\alpha\rangle Q \rightarrow \langle\alpha\rangle(P \lor Q)$
~~I~~	$[\alpha^*](P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$	$\forall$I	$(P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$
~~B~~	$\langle\alpha\rangle\exists x\, P \rightarrow \exists x\, \langle\alpha\rangle P \quad (x \notin \alpha)$	$\overleftarrow{\text{B}}$	$\exists x\, \langle\alpha\rangle P \rightarrow \langle\alpha\rangle\exists x\, P$
~~G~~	$\dfrac{P}{[\alpha]P}$	$\text{M}_{[\cdot]}$	$\dfrac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$
~~R~~	$\dfrac{P_1 \land P_2 \rightarrow Q}{[\alpha]P_1 \land [\alpha]P_2 \rightarrow [\alpha]Q}$	$\text{M}_{[\cdot]}$	$\dfrac{P_1 \land P_2 \rightarrow Q}{[\alpha](P_1 \land P_2) \rightarrow [\alpha]Q}$
~~FA~~	$\langle\alpha^*\rangle P \rightarrow P \lor \langle\alpha^*\rangle(\neg P \land \langle\alpha\rangle P)$	~~$\overleftarrow{[*]}$~~	$[\alpha^*]P \leftrightarrow P \land [\alpha^*][\alpha]P$

Separating Axioms

Theorem (Axiomatic separation: hybrid systems vs. hybrid games)

Axiomatic separation is exactly K, I, C, B, V, G. dG$\mathcal{L}$ is a subregular, sub-Barcan, monotonic modal logic without loop induction axioms.

~~K~~ $[\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$

$\mathrm{M}_{[\cdot]}$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$

~~$\overleftarrow{\mathrm{M}}$~~ $\langle\alpha\rangle(P \lor Q) \to \langle\alpha\rangle P \lor \langle\alpha\rangle Q$

M $\langle\alpha\rangle P \lor \langle\alpha\rangle Q \to \langle\alpha\rangle(P \lor Q)$

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

∀I $(P \to [\alpha]P) \to (P \to [\alpha^*]P)$

~~B~~ $\langle\alpha\rangle\exists x\, P \to \exists x\, \langle\alpha\rangle P$ $\quad (x \notin \alpha)$

$\overleftarrow{\mathrm{B}}$ $\exists x\, \langle\alpha\rangle P \to \langle\alpha\rangle\exists x\, P$

~~G~~ $\dfrac{P}{[\alpha]P}$

$\mathrm{M}_{[\cdot]}$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$

~~R~~ $\dfrac{P_1 \land P_2 \to Q}{[\alpha]P_1 \land [\alpha]P_2 \to [\alpha]Q}$

$\mathrm{M}_{[\cdot]}$ $\dfrac{P_1 \land P_2 \to Q}{[\alpha](P_1 \land P_2) \to [\alpha]Q}$

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

~~$\overleftarrow{[*]}$~~ $[\alpha^*]P \leftrightarrow P \land [\alpha^*][\alpha]P$

Outline

Expressiveness

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

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

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

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:*

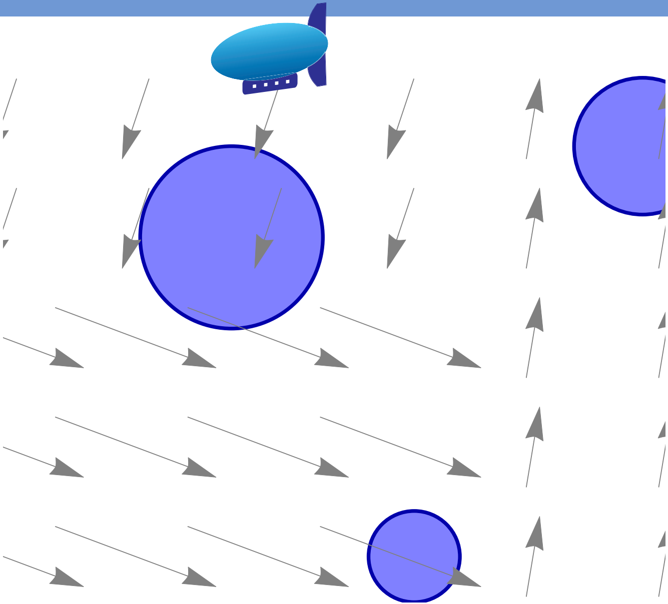
$$\mathsf{d}\mathcal{L} < \mathsf{dG}\mathcal{L}$$

First-order adm. $\mathbb{R}$

Inductive adm. $\mathbb{R}$

Outline

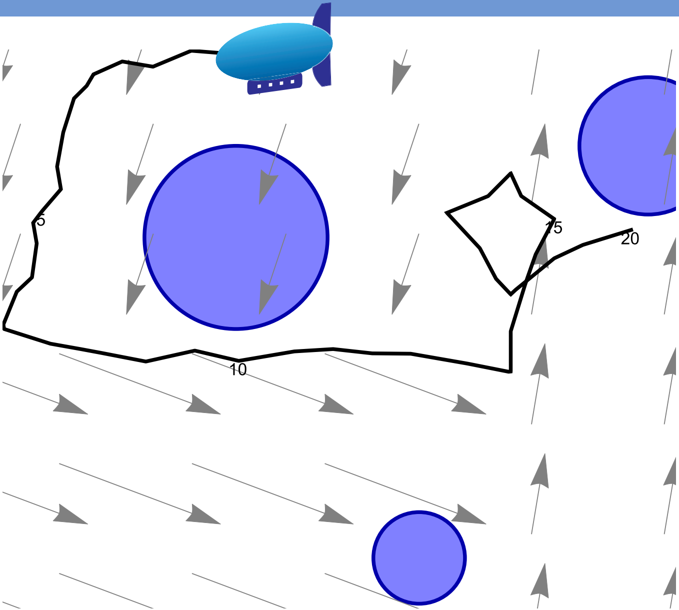
Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

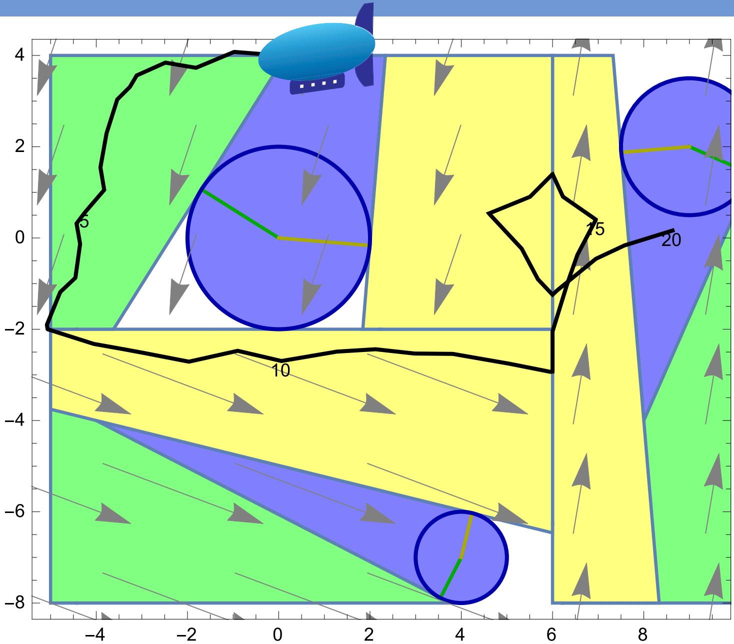
TOCL'17

Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

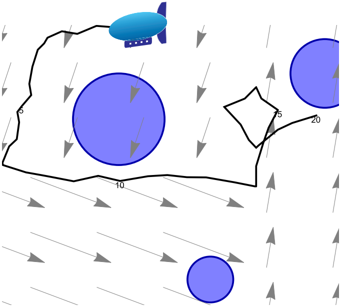
TOCL'17



avoid obstacles
changing wind
local turbulence
$x' = f(x, y, z)$

TOCL'17

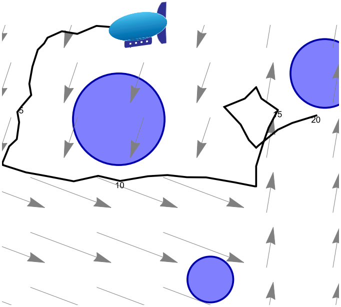
$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\Big[\Big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \&^d y \in B \& z \in B\}$$
$$\Big)^*\Big] \|x - o\|^2 \geq c^2$$



- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence of magnitude r in any direction $z \in B$

$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\big[\big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \&^d y \in B \& z \in B\}$$
$$\big)^*\big] \|x - o\|^2 \geq c^2$$

- $r > p$
- $p > \|v\| + r$
- $\|v\| + r > p > r$



✓ airship at $x \in \mathbb{R}^2$

✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$

× sporadically changing homogeneous wind field $v \in \mathbb{R}^2$

× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

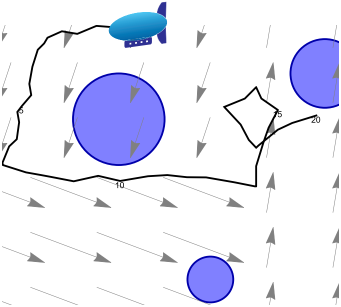
× continuously local turbulence of magnitude r in any direction $z \in B$

Zeppelin Obstacle Parcours

$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\Big[\Big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \&^d y \in B \& z \in B\}$$
$$\Big)^*\Big] \|x - o\|^2 \geq c^2$$

× $r > p$ hopeless

- $p > \|v\| + r$
- $\|v\| + r > p > r$



✓ airship at $x \in \mathbb{R}^2$

✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$

× sporadically changing homogeneous wind field $v \in \mathbb{R}^2$

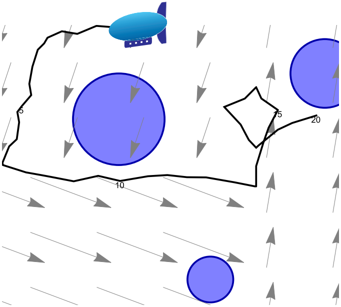
× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

× continuously local turbulence of magnitude r in any direction $z \in B$

Zeppelin Obstacle Parcours

$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\big[\big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \&^d y \in B \& z \in B\}$$
$$\big)^*\big] \|x - o\|^2 \geq c^2$$

- × $r > p$ hopeless
- ✓ $p > \|v\| + r$ super-powered
- $\|v\| + r > p > r$



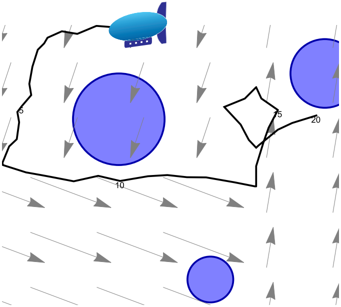
- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence of magnitude r in any direction $z \in B$

$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\Big[\big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \,\&^d\, y \in B \,\&\, z \in B\}$$
$$\big)^*\Big]\, \|x - o\|^2 \geq c^2$$

× $r > p$ hopeless

✓ $p > \|v\| + r$ super-powered

? $\|v\| + r > p > r$ our challenge



✓ airship at $x \in \mathbb{R}^2$

✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$

× sporadically changing homogeneous wind field $v \in \mathbb{R}^2$

× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

× continuously local turbulence of magnitude r in any direction $z \in B$

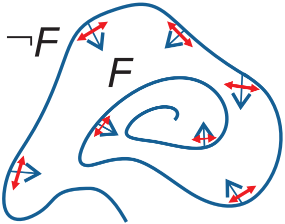
Differential Game Invariants

Theorem (Differential Game Invariants)

$$\text{DGI} \quad \frac{\exists y \in Y\, \forall z \in Z\, [x' := f(x, y, z)](F)'}{F \to [x' = f(x, y, z) \&^d y \in Y \& z \in Z]F}$$

Theorem (Differential Game Refinement)

$$\frac{\forall u \in U\, \exists y \in Y\, \forall z \in Z\, \exists v \in V\, \forall x\, (f(x, y, z) = g(x, u, v))}{[x' = g(x, u, v) \&^d u \in U \& v \in V]F \to [x' = f(x, y, z) \&^d y \in Y \& z \in Z]F}$$



TOCL'17

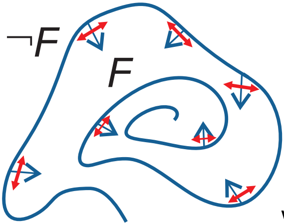
Differential Game Invariants

Theorem (Differential Game Invariants)

$$\text{DGI}\quad \frac{\exists y \in Y\, \forall z \in Z\, [x' := f(x,y,z)](F)'}{F \rightarrow [x' = f(x,y,z) \&^d y \in Y \& z \in Z] F}$$

Theorem (Differential Game Refinement)

$$\frac{\forall u \in U\, \exists y \in Y\, \forall z \in Z\, \exists v \in V\, \forall x\, (f(x,y,z) = g(x,u,v))}{[x' = g(x,u,v) \&^d u \in U \& v \in V] F \rightarrow [x' = f(x,y,z) \&^d y \in Y \& z \in Z] F}$$



$$\cfrac{\cfrac{\cfrac{*}{\exists y{\in}I\, \forall z{\in}I\; 0 \leq 3x^2(-1+2y+z)}\;??}{\exists y{\in}I\, \forall z{\in}I\; [x' := -1+2y+z] 0 \leq 3x^2 x'}}{1 \leq x^3 \rightarrow [x' = -1+2y+z \&^d y \in I \& z \in I] 1 \leq x^3}\;\text{DGI}$$

where $y \in I \overset{\text{def}}{\equiv} -1 \leq y \leq 1$

TOCL'17

Outline

Future Work

Several extensions . . .

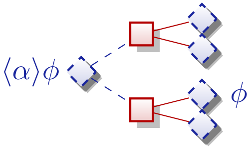
1. Draws
2. Cooperative games with coalitions
3. Rewards
4. Payoffs other than ± 1

. . . are all expressible already. Direct syntactic support?

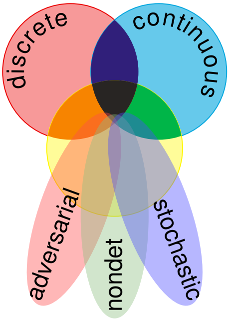
1. Compositional concurrent hybrid games
2. Imperfect information hybrid games
3. Constructive d$\mathcal{GL}$ to retain winning strategies as proof terms

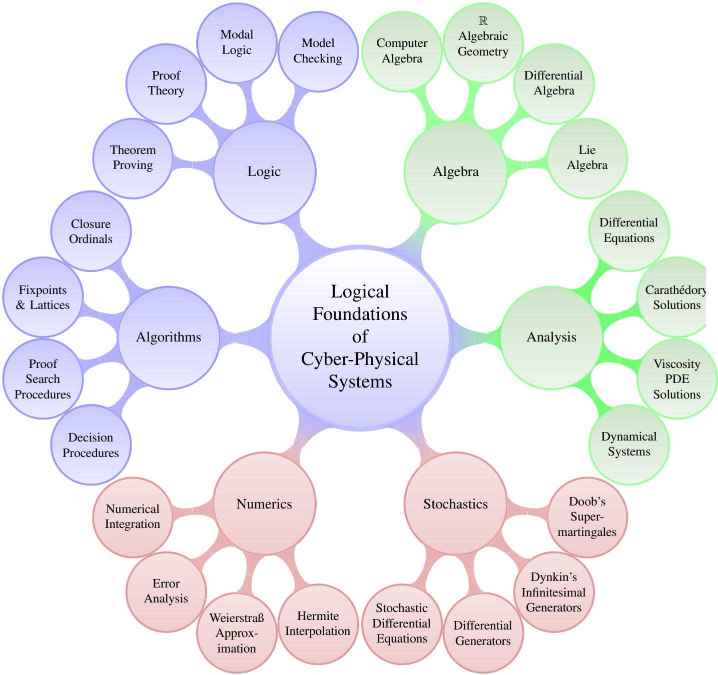
differential game logic

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



- Logic for hybrid games
- Compositional PL + logic
- Discrete + continuous + adversarial
- Winning region iteration $\geq\omega_1^{\mathrm{CK}}$
- Sound & rel. complete axiomatization
- Hybrid games > hybrid systems
- ^{d} radical challenge yet smooth extension
- Stochastic $\approx$ adversarial





Logical Foundations of Cyber-Physical Systems Springer

André Platzer [Carnegie Mellon University]

Ca. 12/2017, ca. 630 pp., 44.99 Euros, 49.99 US$, ISBN 978-3-319-63587-3

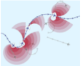
Overview

Cyber-physical systems (CPSs) combine cyber capabilities, such as computation or communication, with physical capabilities, such as motion or other physical processes. Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms. Designing these algorithms is challenging due to their tight coupling with physical behavior, while it is vital that these algorithms be correct because we rely on them for safety-critical tasks.

This textbook teaches undergraduate students the core principles behind CPSs. It shows them how to develop models and controls; identify safety specifications and critical properties; understand abstraction and system architectures; design by invariant; reason rigorously about CPS models; verify CPS models of appropriate scale; and develop an intuition for operational effects.

The book is supported with detailed lecture notes, lecture videos, homework assignments, and lab assignments.

Table of Contents



Comments

"This excellent textbook marries design and analysis of cyber-physical systems with a logical and computational way of thinking. The presentation is exemplary for finding the right balance between rigorous mathematical formalization and illustrative case studies rooted in practical problems in system design."

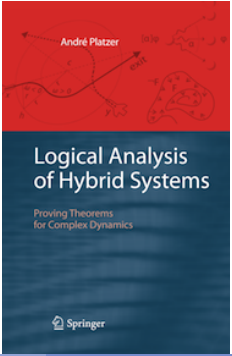
[Rajeev Alur, University of Pennsylvania]

"[The author] has developed major important tools for the design and control of those cyber-physical systems that increasingly shape our lives. This book is a 'must' for computer scientists, engineers, and mathematicians designing cyber-physical systems."

[Anil Nerode, Cornell University]

"This book provides a wonderful introduction to cyber-physical systems, covering fundamental concepts from computer science and control theory from the perspective of formal logic. The theory is brought to life through many didactic examples, illustrations, and exercises. A wealth of background material is provided in the text and in an appendix for each chapter, which makes the book self-contained and accessible to university students of all levels."

[Goran Frehse, Université Grenoble Alpes]



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

André Platzer.
Logic & proofs for cyber-physical systems.
In Nicola Olivetti and Ashish Tiwari, editors, *IJCAR*, volume 9706 of *LNCS*, pages 15–21, Cham, 2016. Springer.
doi:10.1007/978-3-319-40229-1_3.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.

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

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

André Platzer.
The complete proof theory of hybrid systems.
In LICS [13], pages 541–550.
doi:10.1109/LICS.2012.64.

André Platzer.
A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.
Log. Meth. Comput. Sci., 8(4:17):1–44, 2012.
Special issue for selected papers from CSL'10.
doi:10.2168/LMCS-8(4:17)2012.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.
In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *CADE*, volume 6803 of *LNCS*, pages 446–460, Berlin, 2011. Springer.
doi:10.1007/978-3-642-22438-6_34.

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.

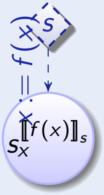
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.

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

Outline

Definition (Hybrid game α: operational semantics)

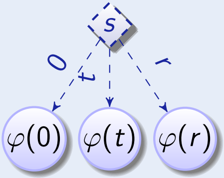
$x := f(x)$



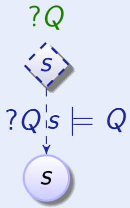
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)

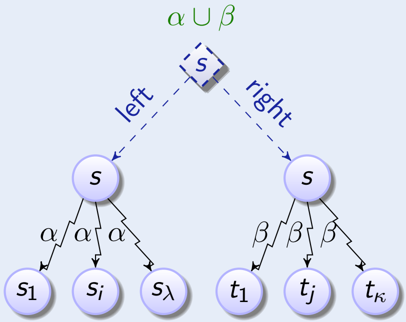
$x' = f(x) \,\&\, Q$



Definition (Hybrid game α: operational semantics)

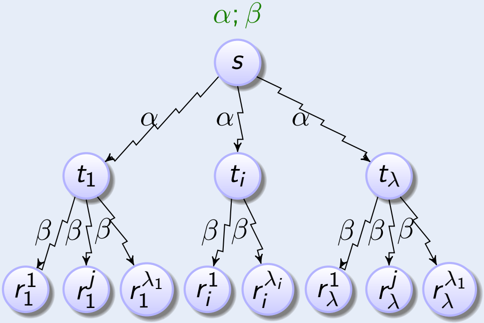


Definition (Hybrid game α: operational semantics)

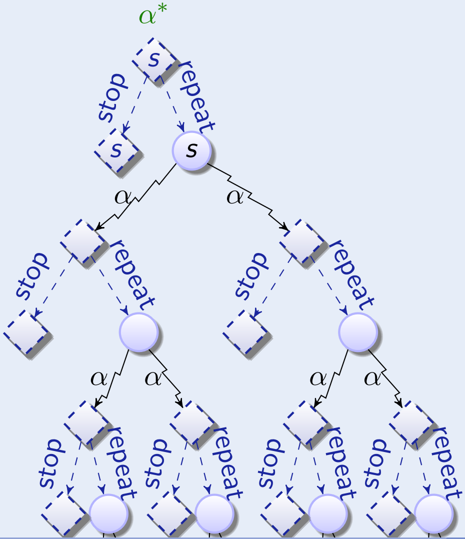


Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



Definition (Hybrid game α: operational semantics)



Definition (Hybrid game α: operational semantics)