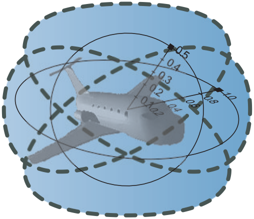
Differential Game Logic

André Platzer

Carnegie Mellon University

ACM TOCL 2015



Outline

Outline

1. CPS Game Motivation
2. Differential Game Logic
   - Syntax
   - Example: Robot Dance
   - Differential Hybrid Games
   - Denotational Semantics
   - Determinacy
3. Axiomatization
   - Axiomatics
   - Soundness and Completeness
   - Separating Axioms
4. Expressiveness
5. Summary

Cyber-Physical Systems Analysis: Aircraft Example

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.

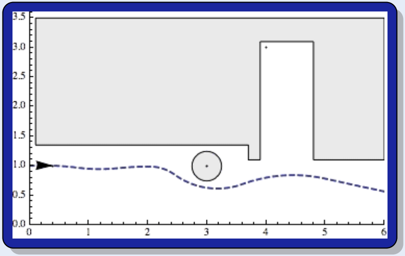
CPSs deserve proofs as safety evidence!

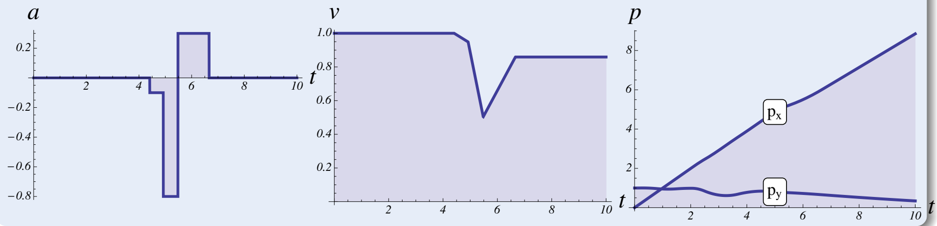
CPS Analysis: Robot Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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



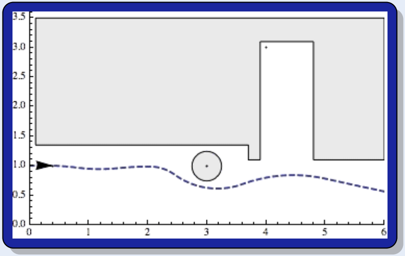


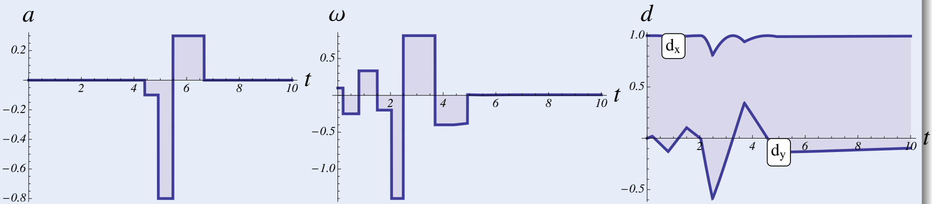
CPS Analysis: Robot Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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



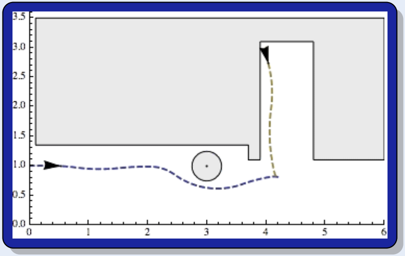


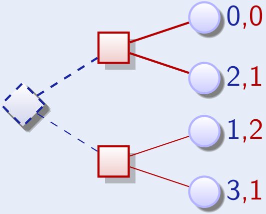
CPS Analysis: Robot Control

Challenge (Games)

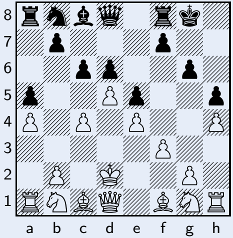
Game rules describing play evolution with both

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





◇\□	Tr	Pl
Trash	1,2	0,0
Plant	0,0	2,1

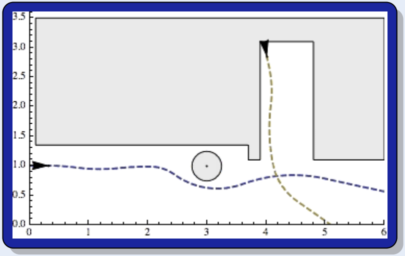


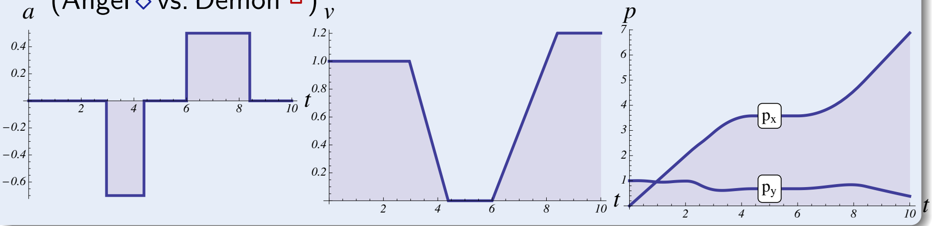
CPS Analysis: Robot Control

Challenge (Hybrid Games)

Game rules describing play evolution with

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



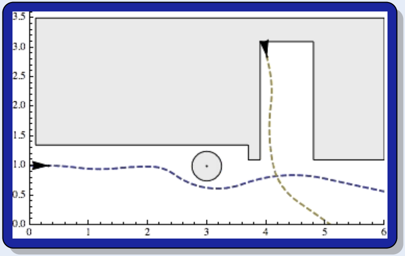


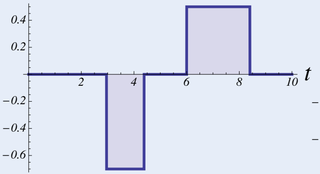
CPS Analysis: Robot Control

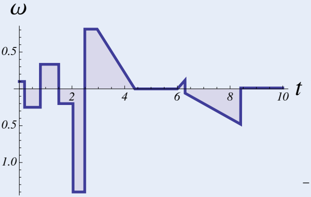
Challenge (Hybrid Games)

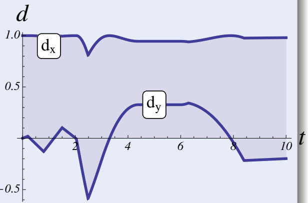
Game rules describing play evolution with

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







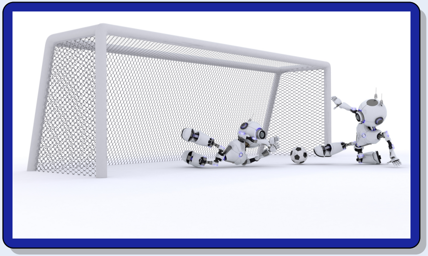


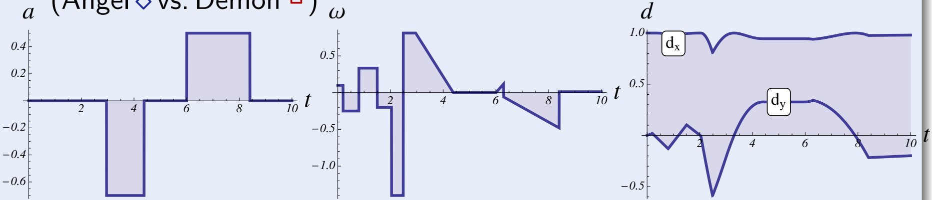
CPS Analysis: RoboCup Soccer

Challenge (Hybrid Games)

Game rules describing play evolution with

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





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

1. CPS Game Motivation
2. Differential Game Logic
    - Syntax
    - Example: Robot Dance
    - Differential Hybrid Games
    - Denotational Semantics
    - Determinacy
3. Axiomatization
    - Axiomatics
    - Soundness and Completeness
    - Separating Axioms
4. Expressiveness
5. Summary

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 (d$\mathcal{GL}$ 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

Differential Game Logic: Syntax

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)

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

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)

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

All Reals

Some Reals

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)

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

All Reals | Some Reals | Angel Wins

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)

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

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)

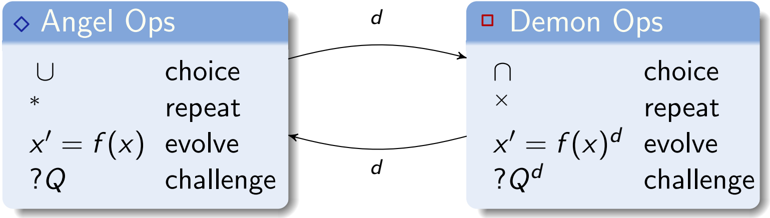
$$p(e_1, \dots, e_n) \mid e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

“Angel has Wings $\langle\alpha\rangle$”

All Reals **Some Reals** **Angel Wins** **Demon Wins**

TOCL’15

Game Operators



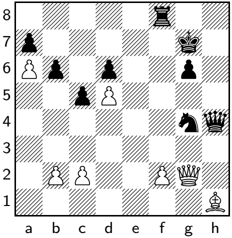
◇ Angel Ops

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

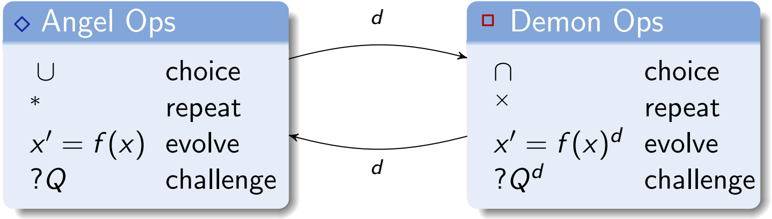
◻ Demon Ops

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

Duality operator ^{d} passes control between players



Game Operators



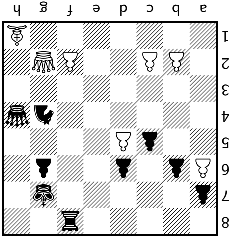
◇ **Angel Ops**

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

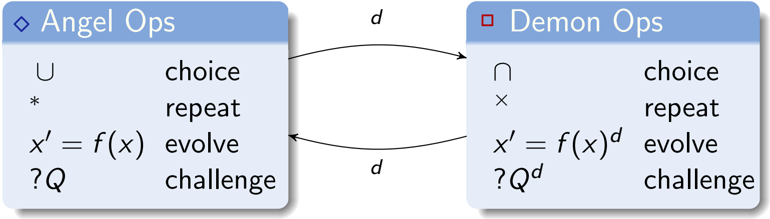
□ **Demon Ops**

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

Duality operator ^{d} passes control between players



Definable Game Operators



◇ Angel Ops

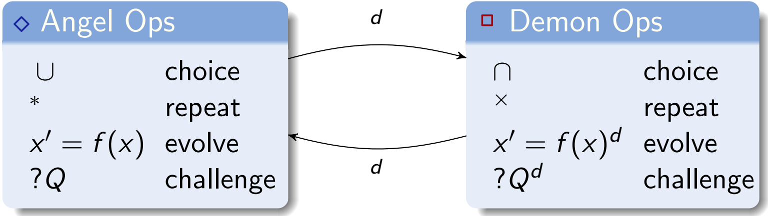
$\cup$	choice
$*$	repeat
$x' = f(x)$	evolve
$?Q$	challenge

◻ Demon Ops

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

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

Definable Game Operators



◇ Angel Ops

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

□ Demon Ops

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

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

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

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

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

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

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

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

Example: EVE and WALL•E

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

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

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

EVE at e plays Angel's part controlling g

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

EVE assigned environment's time to WALL·E

Differential Game Logic: Denotational Semantics

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

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

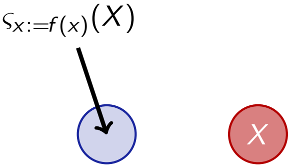
Definition (d$\mathcal{GL}$ Formula P) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S})$

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

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

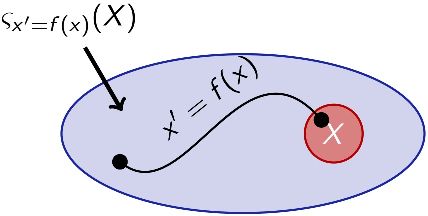
$$\varsigma_{x:=f(x)}(X) = \{s \in \mathcal{S} : s_x^{[\![f(x)]\!]_s} \in X\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

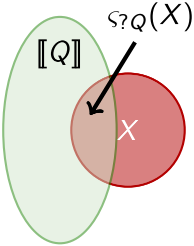
$$\varsigma_{x'=f(x)}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X, \frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![f(x)]\!]_{\varphi(\zeta)} \text{ for all } \zeta\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

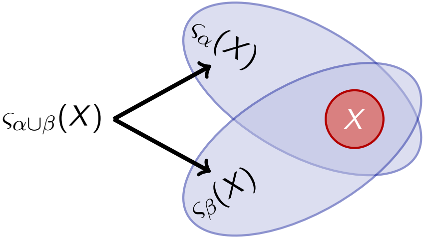
$$\varsigma_{?Q}(X) = [\![Q]\!] \cap X$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

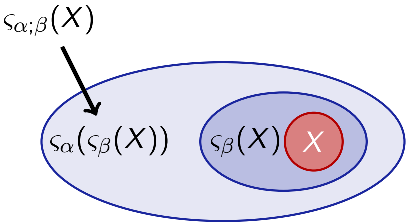
$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

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



Differential Game Logic: Denotational Semantics

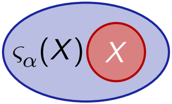
Definition (Hybrid game α: denotational semantics)

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

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

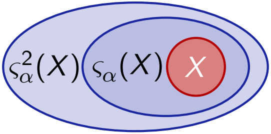
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

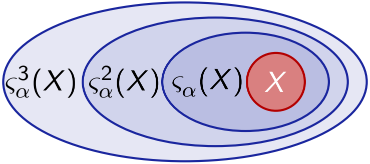
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

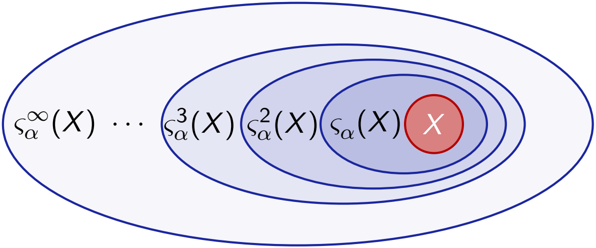
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

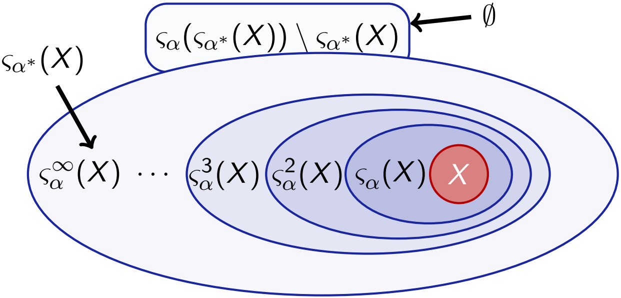
$\varsigma_{\alpha^*}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

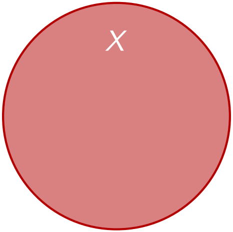
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

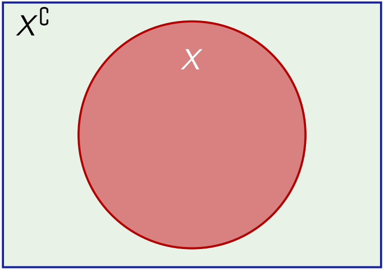
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

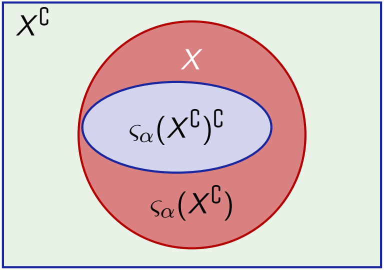
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

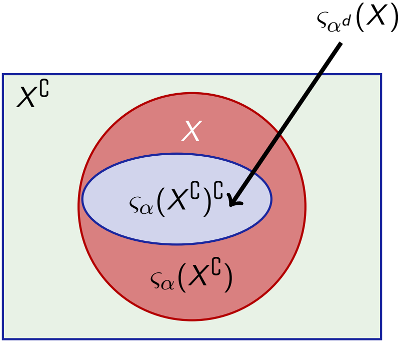
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

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



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

Outline

1. CPS Game Motivation
2. Differential Game Logic
    - Syntax
    - Example: Robot Dance
    - Differential Hybrid Games
    - Denotational Semantics
    - Determinacy
3. Axiomatization
    - Axiomatics
    - Soundness and Completeness
    - Separating Axioms
4. Expressiveness
5. Summary

Differential Game Logic: Axiomatization

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

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

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

$$\langle ? \rangle \quad \langle ?Q\rangle P \leftrightarrow (Q \land P)$$

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

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

$$\langle {}^* \rangle \quad \langle\alpha^*\rangle P \leftrightarrow P \lor \langle\alpha\rangle\langle\alpha^*\rangle P$$

$$\langle {}^d \rangle \quad \langle\alpha^d\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

TOCL'15

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

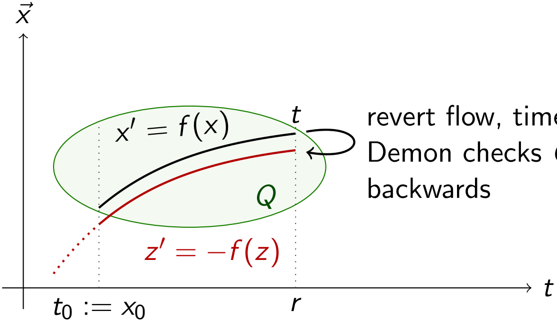
$\forall$ $\dfrac{p \rightarrow Q}{p \rightarrow \forall x\, Q}$ $(x \notin \mathrm{FV}(p))$

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

TOCL'15

“There and Back Again” Game

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



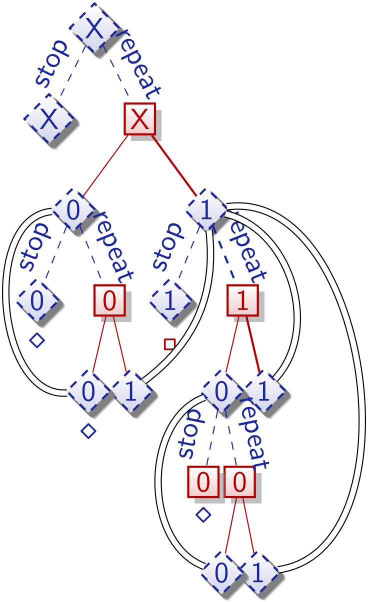
revert flow, time x_0;
Demon checks Q
backwards

Lemma

Evolution domains definable by games

Example Proof: Dual Filibuster

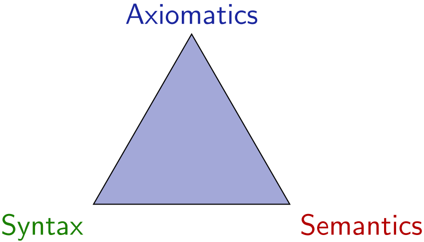
$$
\begin{array}{rl}
 & \qquad * \\ \hline
\mathbb{R} & x=0 \to 0=0 \lor 1=0 \\ \hline
\langle:=\rangle & x=0 \to \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0 \\ \hline
\langle\cup\rangle & x=0 \to \langle x:=0 \cup x:=1\rangle x=0 \\ \hline
\langle^d\rangle & x=0 \to \neg\langle x:=0 \cap x:=1\rangle \neg x=0 \\ \hline
[\cdot] & x=0 \to [x:=0 \cap x:=1]x=0 \\ \hline
\text{ind} & x=0 \to [(x:=0 \cap x:=1)^*]x=0 \\ \hline
\langle^d\rangle & x=0 \to \langle (x:=0 \cup x:=1)^\times \rangle x=0
\end{array}
$$



Soundness

Theorem (Soundness)

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



Soundness

Theorem (Soundness)

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

Proof.

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

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

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

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

□

Soundness

Theorem (Soundness)

dG$\mathcal{L}$ *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 $P \rightarrow Q$ is valid, i.e. $[\![P]\!] \subseteq [\![Q]\!]$.
Then the conclusion $\langle\alpha\rangle P \rightarrow \langle\alpha\rangle Q$ is valid, i.e.
$[\![\langle\alpha\rangle P]\!] = \varsigma_\alpha([\![P]\!]) \subseteq \varsigma_\alpha([\![Q]\!]) = [\![\langle\alpha\rangle Q]\!]$ by monotonicity.

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

□

Soundness & Completeness

Theorem (Completeness)

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

$$\vDash \varphi \quad \textit{iff} \quad \mathit{Taut}_L \vdash \varphi$$

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)

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

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

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

Corollary

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

Soundness & Completeness: Consequences

Corollary

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

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: *Succinct invariants* *discrete* Π^0_2
- $[x' = f(x)]G$ *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* d$\mathcal{GL}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*
^{d}*-free* d$\mathcal{GL}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*

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

set is Π^0_n iff it's $\{x : \forall y_1\,\exists y_2\,\forall y_3\,\dots y_n\,\varphi(x, y_1, \dots, y_n)\}$ for a decidable φ
set is Σ^0_n iff it's $\{x : \exists y_1\,\forall y_2\,\exists y_3\,\dots y_n\,\varphi(x, y_1, \dots, y_n)\}$ 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

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

▸ Fixpoint style proof technique

$$\begin{array}{lr}
\hline
\mathbb{R} & \forall x\,(0{\le}x{<}1 \lor \forall t{\ge}0\, p(1+t) \lor p(x-1) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle:=\rangle & \forall x\,(0{\le}x{<}1{\lor}\langle x:=1\rangle\neg\exists t{\ge}0\,\langle x:=x{+}t\rangle\neg p(x){\lor}p(x{-}1){\to}p(x)) \to (\mathit{true}{\to}p(x)) \\ \hline
\langle'\rangle & \forall x\,(0{\le}x{<}1 \lor \langle x:=1\rangle\neg\langle x'=1\rangle\neg p(x) \lor p(x-1) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle;\rangle,\langle^d\rangle & \forall x\,(0{\le}x{<}1 \lor \langle\beta\rangle p(x) \lor \langle\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle\cup\rangle & \forall x\,(0{\le}x{<}1 \lor \langle\beta\cup\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\text{US} & \forall x\,(0{\le}x{<}1{\lor}\langle\alpha\rangle\langle\alpha^*\rangle 0{\le}x{<}1 \to \langle\alpha^*\rangle 0{\le}x{<}1) \to (\mathit{true} \to \langle\alpha^*\rangle 0{\le}x{<}1) \\ \hline
\langle^*\rangle & \mathit{true} \to \langle\alpha^*\rangle 0{\le}x{<}1
\end{array}$$

More Axioms

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

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

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

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

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

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

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

More Axioms ???

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

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.*

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

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

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

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

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

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

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

Outline

1. CPS Game Motivation
2. Differential Game Logic
   - Syntax
   - Example: Robot Dance
   - Differential Hybrid Games
   - Denotational Semantics
   - Determinacy
3. Axiomatization
   - Axiomatics
   - Soundness and Completeness
   - Separating Axioms
4. Expressiveness
5. Summary

Expressiveness

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

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

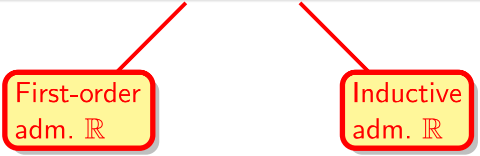
$$\mathrm{d}\mathcal{L} < \mathrm{dG}\mathcal{L}$$

Expressiveness

Theorem (Expressive Power: hybrid systems < hybrid games)

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

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



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

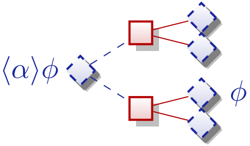
Inductive adm. $\mathbb{R}$

Outline

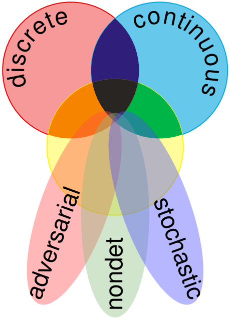
Differential Game Logic

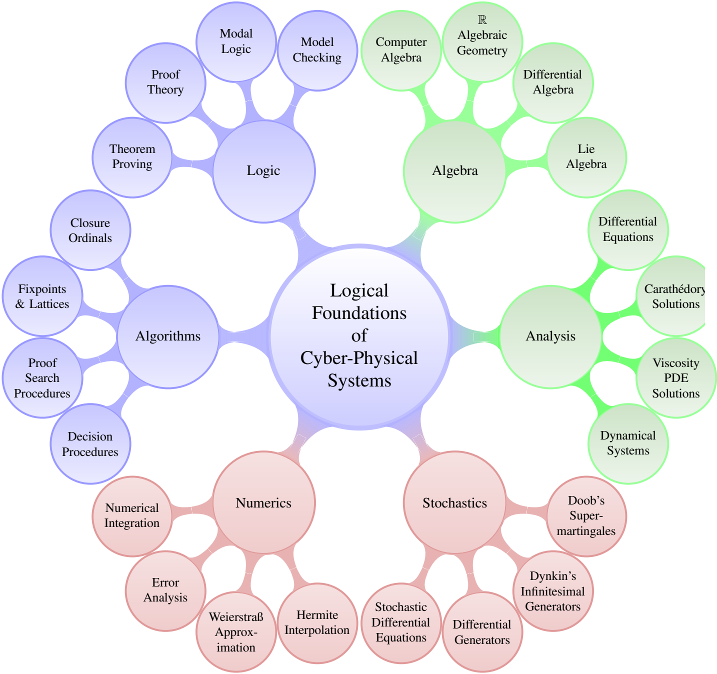
differential game logic

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

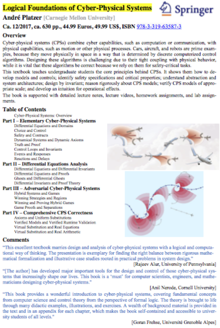


- Logic for hybrid games
- Compositional PL + logic
- Discrete + continuous + adversarial
- Winning region iteration $\geq\omega_1^{\text{CK}}$
- Sound & rel. complete axiomatization
- Hybrid games > hybrid systems
- ^{d} radical challenge yet smooth extension
- Stochastic ≈ adversarial





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



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."

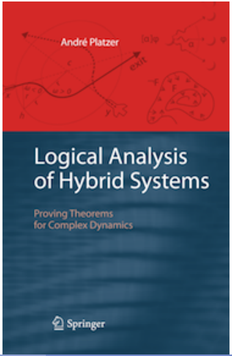
[Rajeev Alur, University of Pennsylvania]

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

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.

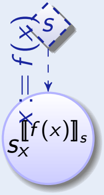
Outline

6 Operational Semantics

Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)

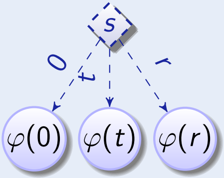
$x := f(x)$



Differential Game Logic: Operational Semantics

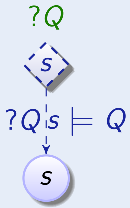
Definition (Hybrid game α: operational semantics)

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



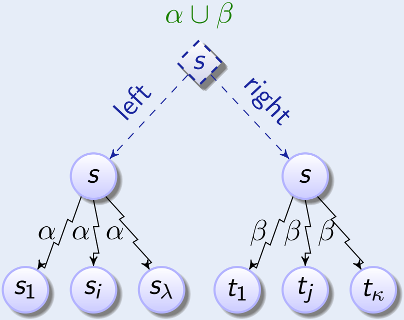
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



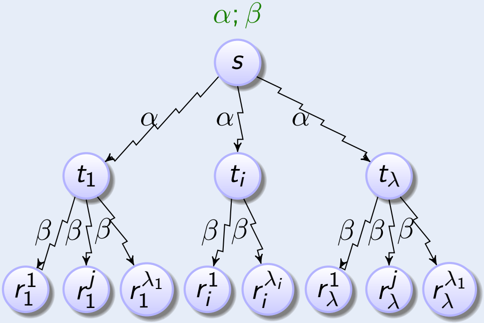
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



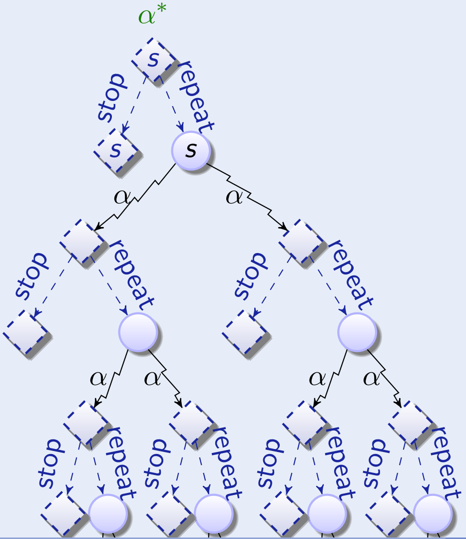
Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)



Differential Game Logic: Operational Semantics

Definition (Hybrid game α: operational semantics)