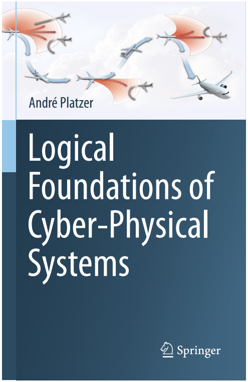
17: Game Proofs & Separations

Logical Foundations of Cyber-Physical Systems



André Platzer

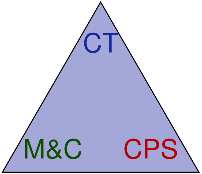
Carnegie Mellon University
Computer Science Department

Outline

Outline

Learning Objectives

rigorous reasoning for adversarial dynamics
miracle of soundness
separations
axiomatization of dGL
multi-dynamical systems
differential game invariants



differential games
systems vs. games

CPS semantics
multi-scale feedback

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P,Q \ ::= \ e \geq \tilde{e} \mid \neg P \mid P \land Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha] P$$

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P,Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P, Q \ ::= \ e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P, Q \ ::= \ e \geq \tilde{e} \mid \neg P \mid P \land Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals | Angel Wins

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals | Angel Wins | Demon Wins

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

$$P, Q \ ::= \ e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

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

All Reals | Some Reals | Angel Wins | Demon Wins

Differential Game Logic: Denotational Semantics

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

$$
\begin{aligned}
\varsigma_{x:=e}(X) &= \{\omega \in \mathscr{S} : \omega_x^{\omega[\![e]\!]} \in X\} \\
\varsigma_{x'=f(x)}(X) &= \{\varphi(0) \in \mathscr{S} : \varphi(r) \in X \text{ for some } \varphi{:}[0,r]\to\mathscr{S},\ \varphi \models x' = f(x)\} \\
\varsigma_{?Q}(X) &= [\![Q]\!] \cap X \\
\varsigma_{\alpha\cup\beta}(X) &= \varsigma_\alpha(X) \cup \varsigma_\beta(X) \\
\varsigma_{\alpha;\beta}(X) &= \varsigma_\alpha(\varsigma_\beta(X)) \\
\varsigma_{\alpha^*}(X) &= \bigcap\{Z \subseteq \mathscr{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} \\
\varsigma_{\alpha^d}(X) &= (\varsigma_\alpha(X^\complement))^\complement
\end{aligned}
$$

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

$$
\begin{aligned}
[\![e_1 \geq e_2]\!] &= \{\omega \in \mathscr{S} : \omega[\![e_1]\!] \geq \omega[\![e_2]\!]\} \\
[\![\neg P]\!] &= ([\![P]\!])^\complement \\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle\alpha\rangle P]\!] &= \varsigma_\alpha([\![P]\!]) \\
[\![[\alpha]P]\!] &= \delta_\alpha([\![P]\!])
\end{aligned}
$$

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

Outline

Differential Game Logic: Axiomatization

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

$$\langle:=\rangle \quad \langle x := e\rangle p(x) \leftrightarrow p(e)$$

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

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

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

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

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

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

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

$$\text{FP} \quad \frac{P \lor \langle\alpha\rangle Q \to Q}{\langle\alpha^*\rangle P \to Q}$$

$$\text{MP} \quad \frac{P \quad P \to Q}{Q}$$

$$\forall \quad \frac{p \to Q}{p \to \forall x\, Q} \qquad (x \notin \mathrm{FV}(p))$$

$$\text{US} \quad \frac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$$

Soundness

Theorem (Soundness)

dGL *proof calculus is sound*

Theorem (Soundness)

dGL *proof calculus is sound*

Do we have to prove anything at all?

$$\text{K} \quad [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$$

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

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

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

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

$$\text{ind} \quad \frac{P \to [\alpha]P}{P \to [\alpha^*]P}$$

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

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

$$\text{G} \quad \frac{P}{[\alpha]P}$$

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

$$\text{R} \quad \frac{P_1 \land P_2 \to Q}{[\alpha]P_1 \land [\alpha]P_2 \to [\alpha]Q}$$

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

$$\text{FA} \quad \langle\alpha^*\rangle P \to P \lor \langle\alpha^*\rangle(\neg P \land \langle\alpha\rangle P)$$

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

More Axioms ???

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

Separating Axioms

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

Axiomatic separation is K, I, C, B, V, G. So, dGL *is a subregular, sub-Barcan, monotonic modal logic without loop induction axioms.*

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

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

Axiomatic separation is K, I, C, B, V, G. So, dGL *is a subregular, sub-Barcan, monotonic modal logic without loop induction axioms.*

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

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

Axiomatic separation is K, I, C, B, V, G. So, dGL *is a subregular, sub-Barcan, monotonic modal logic without loop induction axioms.*

One game's boxes are another game's diamonds.
Don't use axioms that do not belong to you!

Soundness

Theorem (Soundness)

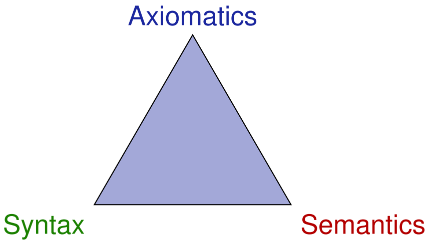
dGL *proof calculus is sound*

Do we have to prove anything at all?

Soundness

Theorem (Soundness)

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



Theorem (Soundness)

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

Proof.

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

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

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

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

□

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 $P \rightarrow Q$ 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.

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

□

The Miracle of Soundness

Soundness links semantics and axiomatics in perfect unison!

Compositional Soundness

- Soundness: If P provable then P valid $\vdash P$ implies $\vDash P$
- *Conditio sine qua non* for logic
- *Every* formula that it proves with *any* proof has to be valid.
- Fortunately, proofs are composed from axioms by proof rules.

Sufficient:

1. All axioms are sound: valid formulas.
2. All proof rules are sound: take valid premises to valid conclusions.

Then

- Proof is a long combination of many simple arguments.
- Each individual step is a sound axiom or sound proof rule, so sound.

The Miracle of Soundness

Soundness+Completeness links semantics and axiomatics in perfect unison!

Compositional Soundness

- Soundness: If P provable then P valid $\vdash P$ implies $\vDash P$
- *Conditio sine qua non* for logic
- *Every* formula that it proves with *any* proof has to be valid.
- Fortunately, proofs are composed from axioms by proof rules.

Sufficient:

1. All axioms are sound: valid formulas.
2. All proof rules are sound: take valid premises to valid conclusions.

Then

- Proof is a long combination of many simple arguments.
- Each individual step is a sound axiom or sound proof rule, so sound.

Soundness & Completeness

Theorem (Completeness)

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

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

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

Soundness & Completeness: Consequences

Corollary (Constructive)

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

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

Soundness & Completeness: Consequences

Corollary (Constructive)

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

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
$\Delta^i_n = \Sigma^i_n \cap \Pi^i_n$

Expressiveness

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

dGL *for hybrid games strictly more expressive than* dL *for hybrid systems:*

$$\mathrm{dL} < \mathrm{dGL}$$

"$\leq$" For every dL formula φ there is a dGL formula $\tilde{\varphi}$ that is equivalent.

"$\not\geq$" Not the other way around.

Expressiveness

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

dGL *for hybrid games strictly more expressive than* dL *for hybrid systems:*

$$\mathsf{dL} < \mathsf{dGL}$$

"$\leq$" For every dL formula φ there is a dGL formula $\tilde{\varphi}$ that is equivalent.
Easy: same formula where Angel plays for nondeterminism.

"$\not\geq$" Not the other way around.
Hard: see proof. TOCL'15

Expressiveness

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

dGL *for hybrid games strictly more expressive than* dL *for hybrid systems:*

$$\text{dL} < \text{dGL}$$

"$\leq$" For every dL formula φ there is a dGL formula $\tilde{\varphi}$ that is equivalent.
Easy: same formula where Angel plays for nondeterminism.

"$\not\geq$" Not the other way around.
Hard: see proof. TOCL'15

Corollary

Hybrid games are strictly more than hybrid systems.

$$\text{con}\ \frac{}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta}$$

$$\frac{}{\vdash x \geq 0 \rightarrow \langle (x := x - 1)^* \rangle x < 1}$$

Proving Repetitive Diamonds by Convergence

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\, (p(v) \rightarrow \langle\alpha\rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle\alpha^*\rangle Q, \Delta}$$

$$\frac{}{\vdash x \geq 0 \rightarrow \langle(x := x-1)^*\rangle x < 1}$$

$$\text{con}\quad \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\, (p(v) \rightarrow \langle\alpha\rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle\alpha^*\rangle Q, \Delta}(v \notin \alpha)$$

$$\frac{}{\vdash x \geq 0 \rightarrow \langle (x := x - 1)^* \rangle x < 1}$$

Proving Repetitive Diamonds by Convergence

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\,(p(v) \rightarrow \langle \alpha \rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta}(v \notin \alpha)$$

$$\rightarrow\text{R}\ \dfrac{\dfrac{}{x \ge 0 \vdash \langle (x := x-1)^* \rangle x < 1}}{\vdash x \ge 0 \rightarrow \langle (x := x-1)^* \rangle x < 1}$$

Proving Repetitive Diamonds by Convergence

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\, (p(v) \to \langle \alpha \rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta}(v \notin \alpha)$$

$$\begin{array}{l} \text{con} \\ \to\!\text{R} \end{array} \dfrac{\dfrac{\overline{x{\ge}0 \vdash \exists n\, x{<}n{+}1} \quad \overline{x{<}n{+}1 \wedge n{>}0 \vdash \langle x := x{-}1 \rangle x{<}n{-}1{+}1} \quad \overline{\exists n{\le}0\, x{<}n{+}1 \vdash x{<}1}}{x \ge 0 \vdash \langle (x := x-1)^* \rangle x < 1}}{\vdash x \ge 0 \to \langle (x := x-1)^* \rangle x < 1}$$

$p(n) \equiv x < n + 1$

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\, (p(v) \rightarrow \langle \alpha \rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta} (v \notin \alpha)$$

$$\rightarrow\text{R}\ \dfrac{\text{con}\ \dfrac{\mathbb{R}\ \dfrac{*}{x{\ge}0 \vdash \exists n\, x{<}n{+}1} \quad \dfrac{}{x{<}n{+}1 \land n{>}0 \vdash \langle x := x{-}1 \rangle x{<}n{-}1{+}1} \quad \dfrac{}{\exists n{\le}0\, x{<}n{+}1 \vdash x{<}1}}{x \ge 0 \vdash \langle (x := x-1)^* \rangle x < 1}}{\vdash x \ge 0 \rightarrow \langle (x := x-1)^* \rangle x < 1}$$

$p(n) \equiv x < n+1$

Proving Repetitive Diamonds by Convergence

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\, (p(v) \rightarrow \langle\alpha\rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle\alpha^*\rangle Q, \Delta}(v \notin \alpha)$$

$$\rightarrow\!\text{R}\ \dfrac{\text{con}\ \dfrac{\mathbb{R}\ \dfrac{*}{x{\ge}0 \vdash \exists n\, x{<}n{+}1} \quad \langle{:=}\rangle\ \dfrac{\overline{x{<}n{+}1 \land n{>}0 \vdash x{-}1{<}n{-}1{+}1}}{x{<}n{+}1 \land n{>}0 \vdash \langle x := x{-}1\rangle x{<}n{-}1{+}1} \quad \dfrac{}{\exists n{\le}0\, x{<}n{+}1 \vdash x{<}1}}{x \ge 0 \vdash \langle (x := x-1)^*\rangle x < 1}}{\vdash x \ge 0 \rightarrow \langle (x := x-1)^*\rangle x < 1}$$

$p(n) \equiv x < n+1$

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\,(p(v) \rightarrow \langle \alpha \rangle p(v-1)) \quad \exists v{\leq}0\, p(v) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta}\,(v \notin \alpha)$$

$$\rightarrow\!\text{R}\ \dfrac{\text{con}\ \dfrac{\mathbb{R}\ \dfrac{*}{x{\geq}0 \vdash \exists n\, x{<}n{+}1} \quad \langle{:=}\rangle\ \dfrac{\mathbb{R}\ \dfrac{*}{x{<}n{+}1 \land n{>}0 \vdash x{-}1{<}n{-}1{+}1}}{x{<}n{+}1 \land n{>}0 \vdash \langle x := x{-}1 \rangle x{<}n{-}1{+}1} \quad \dfrac{}{\exists n{\leq}0\, x{<}n{+}1 \vdash x{<}1}}{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1}}{\vdash x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1}$$

$$p(n) \equiv x < n+1$$

$$\text{con}\ \frac{\Gamma \vdash \exists v\, p(v), \Delta \quad \vdash \forall v{>}0\,(p(v) \to \langle\alpha\rangle p(v-1)) \quad \exists v{\le}0\, p(v) \vdash Q}{\Gamma \vdash \langle\alpha^*\rangle Q, \Delta}(v \notin \alpha)$$

$$\rightarrow\text{R}\ \dfrac{\text{con}\ \dfrac{\mathbb{R}\dfrac{*}{x{\ge}0 \vdash \exists n\, x{<}n{+}1} \quad \langle{:=}\rangle\dfrac{\mathbb{R}\dfrac{*}{x{<}n{+}1 \land n{>}0 \vdash x{-}1{<}n{-}1{+}1}}{x{<}n{+}1 \land n{>}0 \vdash \langle x := x{-}1\rangle x{<}n{-}1{+}1} \quad \mathbb{R}\dfrac{*}{\exists n{\le}0\, x{<}n{+}1 \vdash x{<}1}}{x \ge 0 \vdash \langle(x := x-1)^*\rangle x < 1}}{\vdash x \ge 0 \to \langle(x := x-1)^*\rangle x < 1}$$

$p(n) \equiv x < n+1$

Example Proof: 2-Nim-type Game

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x - 1}_{\beta} \cap \underbrace{x := x - 2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\dfrac{}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0 \leq x < 2} \; \langle^*\rangle,\forall,\text{MP}$$

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x-1}_{\beta} \cap \underbrace{x := x-2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\dfrac{\overline{\text{US} \quad \forall x\,(0\leq x<2 \vee \langle\alpha\rangle\langle\alpha^*\rangle 0\leq x<2 \rightarrow \langle\alpha^*\rangle 0\leq x<2) \rightarrow (x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2)}}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2}\ \langle^*\rangle,\forall,\text{MP}$$

Example Proof: 2-Nim-type Game

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x-1}_{\beta} \cap \underbrace{x := x-2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{}{\forall x\,(0\leq x<2 \lor \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\langle\cup\rangle,\langle^d\rangle}{\dfrac{\forall x\,(0\leq x<2 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0\leq x<2 \rightarrow \langle\alpha^*\rangle 0\leq x<2) \rightarrow (x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2)}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2}\langle^*\rangle,\forall,\text{MP}}\text{US}$$

Example Proof: 2-Nim-type Game

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x - 1}_{\beta} \cap \underbrace{x := x - 2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\overline{\forall x\,(0\leq x<2 \vee \langle\beta\rangle p(x) \wedge \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\ \langle:=\rangle}{\forall x\,(0\leq x<2 \vee \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\ \langle\cup\rangle,\langle^d\rangle}{\forall x\,(0\leq x<2 \vee \langle\alpha\rangle\langle\alpha^*\rangle 0\leq x<2 \rightarrow \langle\alpha^*\rangle 0\leq x<2) \rightarrow (x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2)}\ \text{US}}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0\leq x<2}\ \langle^*\rangle,\forall,\text{MP}$$

Example Proof: 2-Nim-type Game

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x - 1}_{\beta} \cap \underbrace{x := x - 2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\mathbb{R}\quad \forall x\,(0 \leq x < 2 \vee p(x-1) \wedge p(x-2) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))$$

$$\langle := \rangle\quad \forall x\,(0 \leq x < 2 \vee \langle\beta\rangle p(x) \wedge \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))$$

$$\langle\cup\rangle,\langle^d\rangle\quad \forall x\,(0 \leq x < 2 \vee \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))$$

$$\text{US}\quad \forall x\,(0 \leq x < 2 \vee \langle\alpha\rangle\langle\alpha^*\rangle 0 \leq x < 2 \rightarrow \langle\alpha^*\rangle 0 \leq x < 2) \rightarrow (x \geq 0 \rightarrow \langle\alpha^*\rangle 0 \leq x < 2)$$

$$\langle^*\rangle,\forall,\text{MP}\quad x \geq 0 \rightarrow \langle\alpha^*\rangle 0 \leq x < 2$$

Example Proof: 2-Nim-type Game

$$x \geq 0 \rightarrow \langle(\underbrace{\underbrace{x := x-1}_{\beta} \cap \underbrace{x := x-2}_{\gamma}}_{\alpha})^*\rangle 0 \leq x < 2$$

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\forall x\,(0\le x<2 \vee p(x-1)\wedge p(x-2) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\ \mathbb{R}}{\forall x\,(0\le x<2 \vee \langle\beta\rangle p(x) \wedge \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\ \langle:=\rangle}{\forall x\,(0\le x<2 \vee \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}\ \langle\cup\rangle,\langle^d\rangle}{\forall x\,(0\le x<2 \vee \langle\alpha\rangle\langle\alpha^*\rangle 0\le x<2 \rightarrow \langle\alpha^*\rangle 0\le x<2) \rightarrow (x \geq 0 \rightarrow \langle\alpha^*\rangle 0\le x<2)}\ \text{US}}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0\le x<2}\ \langle^*\rangle,\forall,\text{MP}$$

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

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

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

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

$$\langle{}^*\rangle\ \dfrac{}{true \to \langle\alpha^*\rangle 0\le x<1}$$

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

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

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

$$\langle{}^*\rangle\ \frac{}{true\to\langle\alpha^*\rangle 0\le x<1}$$

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x\,(0\le x<1\vee\langle\beta\rangle p(x)\vee\langle\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\;\langle;\rangle,\langle^d\rangle}{\forall x\,(0\le x<1\vee\langle\beta\cup\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\;\langle\cup\rangle}{\forall x\,(0\le x<1\vee\langle\alpha\rangle\langle\alpha^*\rangle 0\le x<1\to\langle\alpha^*\rangle 0\le x<1)\to(true\to\langle\alpha^*\rangle 0\le x<1)}\;\mathrm{US}}{true\to\langle\alpha^*\rangle 0\le x<1}\;\langle^*\rangle$$

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x\,(0\leq x<1\lor\langle x:=1\rangle\neg\langle x'=1\rangle\neg p(x)\lor p(x-1)\to p(x))\to(true\to p(x))}{\forall x\,(0\leq x<1\lor\langle\beta\rangle p(x)\lor\langle\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\langle;\rangle,\langle^{d}\rangle}{\forall x\,(0\leq x<1\lor\langle\beta\cup\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\langle\cup\rangle}{\forall x\,(0\leq x<1\lor\langle\alpha\rangle\langle\alpha^{*}\rangle 0\leq x<1\to\langle\alpha^{*}\rangle 0\leq x<1)\to(true\to\langle\alpha^{*}\rangle 0\leq x<1)}\text{US}}{true\to\langle\alpha^{*}\rangle 0\leq x<1}\langle^{*}\rangle$$

The top step is labelled $\langle'\rangle$.

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

▸ Fixpoint style proof technique

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x\,(0\leq x<1\vee\langle x:=1\rangle\neg\exists t\geq 0\,\langle x:=x+t\rangle\neg p(x)\vee p(x-1)\to p(x))\to(true\to p(x))}\langle:=\rangle}{\forall x\,(0\leq x<1\vee\langle x:=1\rangle\neg\langle x'=1\rangle\neg p(x)\vee p(x-1)\to p(x))\to(true\to p(x))}\langle'\rangle}{\forall x\,(0\leq x<1\vee\langle\beta\rangle p(x)\vee\langle\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\langle;\rangle,\langle^d\rangle}{\forall x\,(0\leq x<1\vee\langle\beta\cup\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\langle\cup\rangle}{\forall x\,(0\leq x<1\vee\langle\alpha\rangle\langle\alpha^*\rangle 0\leq x<1\to\langle\alpha^*\rangle 0\leq x<1)\to(true\to\langle\alpha^*\rangle 0\leq x<1)}\text{US}}{true\to\langle\alpha^*\rangle 0\leq x<1}\langle^*\rangle$$

Example Proof: Hybrid Game

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

Fixpoint style proof technique

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

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

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

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

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

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

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

Example Proof: Hybrid Game

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

▸ Fixpoint style proof technique

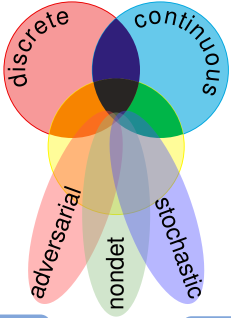
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\forall x\,(0\le x<1\lor\forall t\ge 0\,p(1+t)\lor p(x-1)\to p(x))\to(true\to p(x))}\mathbb{R}}{\forall x\,(0\le x<1\lor\langle x:=1\rangle\neg\exists t\ge 0\,\langle x:=x+t\rangle\neg p(x)\lor p(x-1)\to p(x))\to(true\to p(x))}\langle:=\rangle}{\forall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

Outline

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

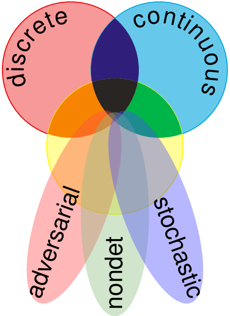
Exploiting compositionality tames CPS complexity.

Analytic simplification

CPSs are Multi-Dynamical Systems

hybrid systems

HS = discrete + ODE

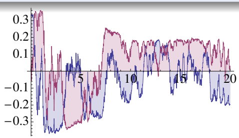


hybrid games

HG = HS + adversary

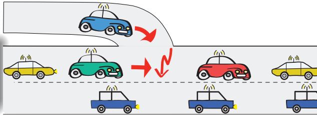
stochastic hybrid sys.

SHS = HS + stochastics



distributed hybrid sys.

DHS = HS + distributed



Differential Game Logic: Syntax

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

Definition (Differential hybrid game α) (TOCL'17)

$$x := e \mid ?Q \mid x' = f(x,y,z) \&^d y \in Y \& z \in Z \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula P)

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals | Angel Wins | Demon Wins

Differential Game Logic: Syntax

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

Definition (Differential hybrid game α) (TOCL'17)

$$x := e \mid ?Q \mid x' = f(x,y,z) \&^d y \in Y \& z \in Z \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^* \mid \alpha^d$$

Definition (dGL Formula P)

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

All Reals | Some Reals | Angel Wins | Demon Wins

Differential Game Logic: Syntax

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

Definition (Differential hybrid game α) (TOCL'17)

$$x := e \mid ?Q \mid x' = f(x,y,z) \&^d y \in Y \& z \in Z \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

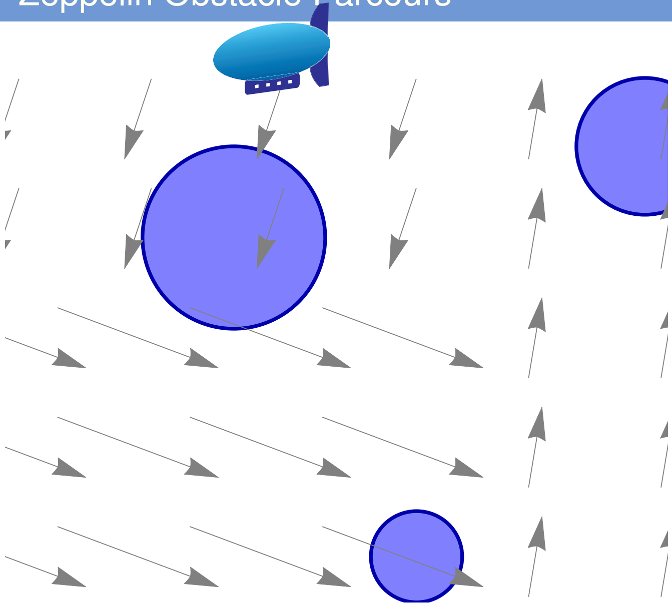
Definition (dGL Formula P)

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle\alpha\rangle P \mid [\alpha]P$$

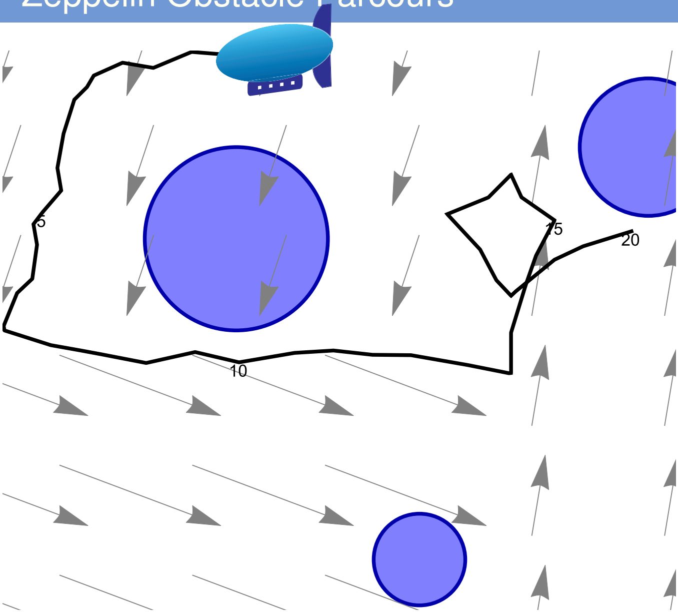
Demon controls $y \in Y$
Angel controls $z \in Z$
Demon chooses "first"
Angel controls duration

All Reals | Some Reals | Angel Wins | Demon Wins

Zeppelin Obstacle Parcours



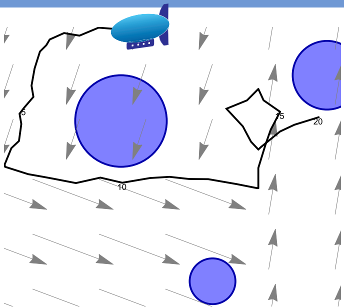
avoid obstacles
changing wind
local turbulence



avoid obstacles
changing wind
local turbulence

Zeppelin Obstacle Parcours

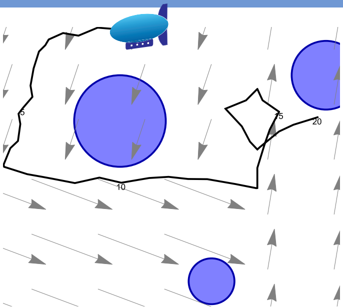
$$c > 0 \land \|x - o\|^2 \geq c^2 \rightarrow$$
$$\Big[\Big(v := *; o := *; c := *; ?C;$$
$$\{x' = v + py + rz \,\&^d\, y \in B \,\&\, z \in B\}$$
$$\Big)^*\Big] \|x - o\|^2 \geq c^2$$



- ✓ 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 $z \in B$

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

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



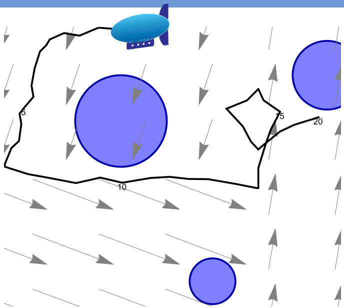
- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e., $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence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

Zeppelin Obstacle Parcours

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

× If $r > p$ hopeless turbulence

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



✓ 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 $v \in \mathbb{R}^2$

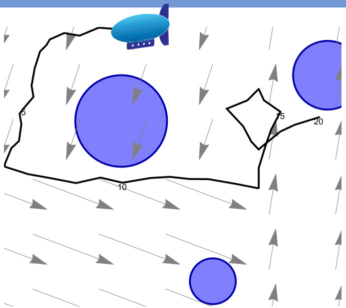
× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

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

Zeppelin Obstacle Parcours

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

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

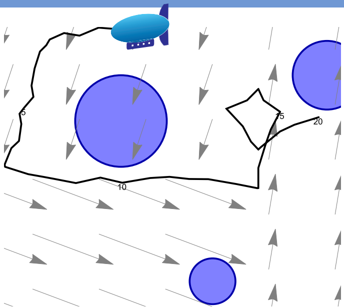


- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e., $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence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

Zeppelin Obstacle Parcours

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

- × If $r > p$ hopeless turbulence
- ✓ If $p > \|v\| + r$ super-powered prop
- ? If $\|v\| + r > p > r$ our challenge



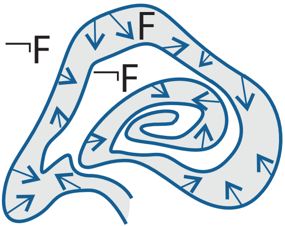
- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e., $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence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

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

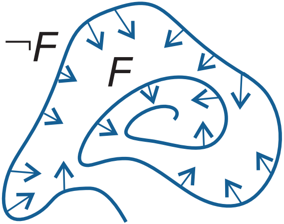


Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

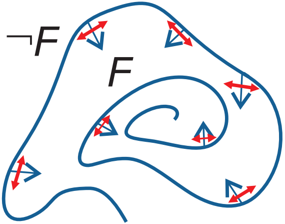


Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



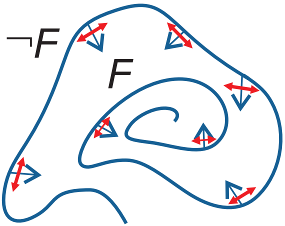
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



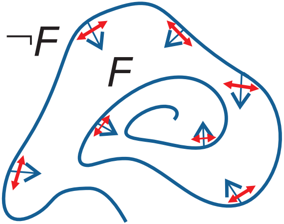
Differential Game Invariants

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)

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

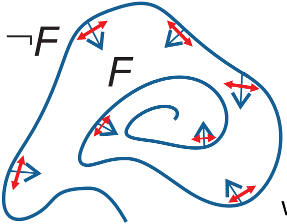


Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



$$\text{DGI}\ \frac{}{1 \le x^3 \vdash [x' = -1 + 2y + z \&^d y \in I \& z \in I] 1 \le x^3}$$

where $y \in I \equiv -1 \le y \le 1$

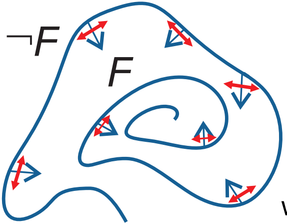
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



$$\text{DGI}\ \frac{[:=]\ \dfrac{}{\vdash \exists y{\in}I \forall z{\in}I\, [x' := -1+2y+z]0 \leq 3x^2 x'}}{1 \leq x^3 \vdash [x' = -1+2y+z \&^d y \in I \& z \in I]1 \leq x^3}$$

where $y \in I \equiv -1 \leq y \leq 1$

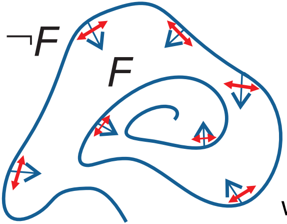
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



$$\text{DGI}\ \dfrac{[:=]\ \dfrac{\mathbb{R}\ \dfrac{}{\vdash \exists y{\in}I\, \forall z{\in}I\; 0 \le 3x^2(-1+2y+z)}}{\vdash \exists y{\in}I\, \forall z{\in}I\, [x' := -1+2y+z]\, 0 \le 3x^2 x'}}{1 \le x^3 \vdash [x' = -1+2y+z \,\&^d\, y \in I \,\&\, z \in I]\, 1 \le x^3}$$

where $y \in I \equiv -1 \le y \le 1$

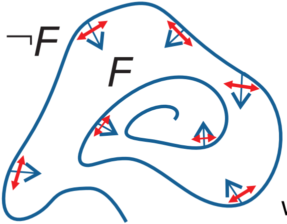
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



$$\dfrac{\dfrac{\dfrac{*}{\vdash \exists y{\in}I \forall z{\in}I\, 0 \le 3x^2(-1+2y+z)}\ \mathbb{R}}{\vdash \exists y{\in}I \forall z{\in}I\, [x' := -1+2y+z] 0 \le 3x^2 x'}\ [:=]}{1 \le x^3 \vdash [x' = -1+2y+z \&^d y \in I \& z \in I] 1 \le x^3}\ \text{DGI}$$

where $y \in I \equiv -1 \le y \le 1$

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

$$\text{DGI}\ \frac{}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \,\&^d\, y \in B \,\&\, z \in B]\, \|l-m\|^2 > 0}$$

if $L \leq M$

Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

$$\text{DGI}\ \frac{[:=]\ \overline{\vdash \exists y \in B \forall z \in B\, [m':=My][l':=Lz](2(l-m)\cdot(l'-m') \geq 0)}}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\, \|l-m\|^2 > 0}$$

if $L \leq M$

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

$$\text{DGI}\ \dfrac{[{:=}]\ \dfrac{\mathbb{R}\ \dfrac{}{\vdash \exists y \in B \forall z \in B\, (2(l-m) \cdot (Lz - My) \geq 0)}}{\vdash \exists y \in B \forall z \in B\, [m' := My][l' := Lz](2(l-m) \cdot (l' - m') \geq 0)}}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\, \|l-m\|^2 > 0}$$

if $L \leq M$

Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

$$\text{DGI}\ \cfrac{[:=]\ \cfrac{\mathbb{R}\ \cfrac{*}{\vdash \exists y \in B \forall z \in B\, (2(l-m)\cdot(Lz - My) \geq 0)}}{\vdash \exists y \in B \forall z \in B\, [m' := My][l' := Lz](2(l-m)\cdot(l' - m') \geq 0)}}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \,\&^d\, y \in B \,\&\, z \in B]\, \|l-m\|^2 > 0}$$

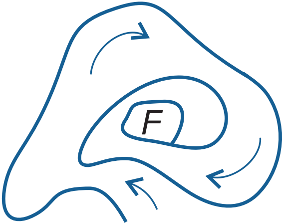
if $L \leq M$

Theorem (Differential Game Variants)

DGV $$\frac{}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z \rangle g \geq 0}$$

Theorem (Differential Game Refinement)

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



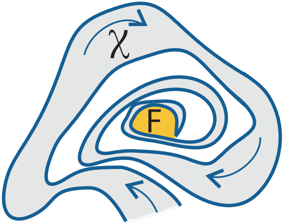
Differential Game Variants

Theorem (Differential Game Variants)

$$\text{DGV}\ \frac{}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z \rangle g \geq 0}$$

Theorem (Differential Game Refinement)

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

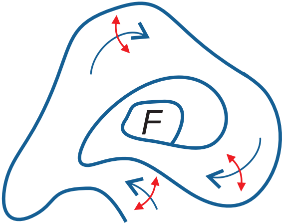


Theorem (Differential Game Variants)

$$\text{DGV}\ \frac{}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z \rangle g \geq 0}$$

Theorem (Differential Game Refinement)

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

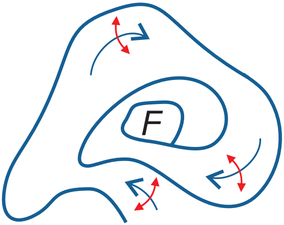


Theorem (Differential Game Variants)

$$\text{DGV}\quad \frac{\exists \varepsilon{>}0\,\forall x\,\exists z \in Z\,\forall y \in Y\,(g \le 0 \to [x' := f(x,y,z)](g)' \ge \varepsilon)}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z\rangle g \ge 0}$$

Theorem (Differential Game Refinement)

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



Differential Game Variants

Theorem (Differential Game Variants)

$$\text{DGV}\quad \frac{\exists \varepsilon{>}0\,\forall x\,\exists z \in Z\,\forall y \in Y\,(g \leq 0 \rightarrow [x'{:=}f(x,y,z)](g)' \geq \varepsilon)}{\langle x' = f(x,y,z)\,\&^d\, y \in Y \,\&\, z \in Z\rangle g \geq 0}$$

Theorem (Differential Game Refinement)

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

$$\overline{\vdash \langle x' = zx - yu, u' = zu + yx\,\&^d\, {-2}{\leq}y{\leq}2 \,\&\, {-1}{\leq}z{\leq}1\rangle\, 1 - x^2 - u^2 \geq 0}$$

Differential Game Variants

Theorem (Differential Game Variants)

$$\text{DGV} \quad \frac{\exists \varepsilon{>}0\, \forall x\, \exists z \in Z\, \forall y \in Y\, (g \leq 0 \rightarrow [x' := f(x,y,z)](g)' \geq \varepsilon)}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z \rangle g \geq 0}$$

Theorem (Differential Game Refinement)

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

$$\frac{\vdash \exists \varepsilon{>}0\, \forall x\, \forall u\, \exists{-1}{\leq}z{\leq}1\, \forall{-2}{\leq}y{\leq}2\, \left(1 - x^2 - u^2 \leq 0 \rightarrow [x' :=][u' :=] -2xx' - 2uu' \geq \varepsilon\right)}{\vdash \langle x' = zx - yu, u' = zu + yx \&^d -2{\leq}y{\leq}2 \& -1{\leq}z{\leq}1 \rangle\, 1 - x^2 - u^2 \geq 0}$$

Differential Game Variants

Theorem (Differential Game Variants)

$$\text{DGV}\quad \frac{\exists \varepsilon{>}0\,\forall x\,\exists z \in Z\,\forall y \in Y\,(g \le 0 \rightarrow [x' {:=} f(x,y,z)](g)' \ge \varepsilon)}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z\rangle g \ge 0}$$

Theorem (Differential Game Refinement)

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

$$\frac{\vdash \exists \varepsilon{>}0\,\forall x\,\forall u\,\exists{-1}{\le}z{\le}1\,\forall{-2}{\le}y{\le}2\,\left(x^2{+}u^2{\ge}1 \rightarrow -2x(zx{-}yu){-}2u(zu{+}yx){\ge}\varepsilon\right)}{\dfrac{\vdash \exists \varepsilon{>}0\,\forall x\,\forall u\,\exists{-1}{\le}z{\le}1\,\forall{-2}{\le}y{\le}2\,\left(1{-}x^2{-}u^2{\le}0 \rightarrow [x' {:=}][u' {:=}]{-}2xx'{-}2uu'{\ge}\varepsilon\right)}{\vdash \langle x' = zx - yu, u' = zu + yx \&^d {-2}{\le}y{\le}2 \& {-1}{\le}z{\le}1\rangle\, 1 - x^2 - u^2 \ge 0}}$$

Differential Game Variants

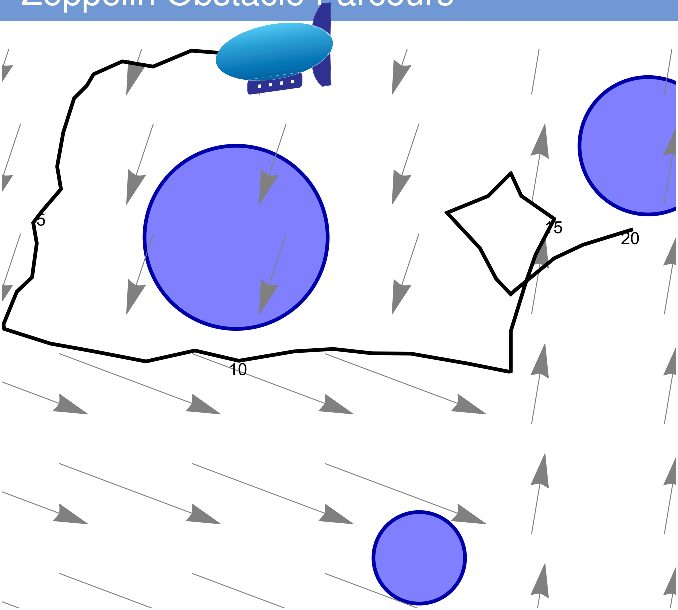
Theorem (Differential Game Variants)

$$\text{DGV}\quad \frac{\exists\varepsilon{>}0\,\forall x\,\exists z\in Z\,\forall y\in Y\,(g\leq 0\rightarrow [x':=f(x,y,z)](g)'\geq\varepsilon)}{\langle x'=f(x,y,z)\&^d y\in Y\&z\in Z\rangle g\geq 0}$$

Theorem (Differential Game Refinement)

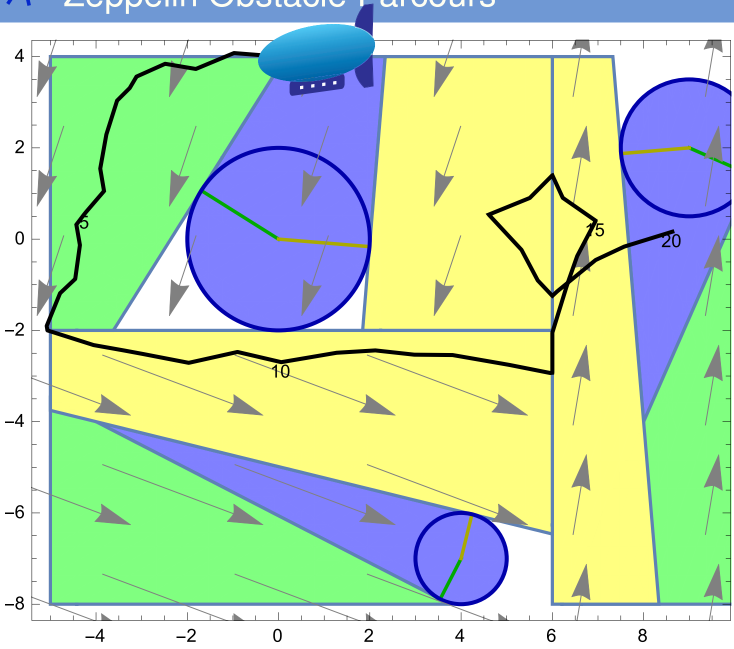
$$\frac{\forall u\in U\,\exists y\in Y\,\forall z\in Z\,\exists v\in V\,\forall x\,(f(x,y,z)=g(x,u,v))}{[x'=g(x,u,v)\&^d u\in U\&v\in V]P\rightarrow[x'=f(x,y,z)\&^d y\in Y\&z\in Z]P}$$

$$\cfrac{\cfrac{\cfrac{*}{\vdash\exists\varepsilon{>}0\,\forall x\,\forall u\,\exists{-1}{\leq}z{\leq}1\,\forall{-2}{\leq}y{\leq}2\,\big(x^2{+}u^2{\geq}1\rightarrow -2x(zx{-}yu){-}2u(zu{+}yx){\geq}\varepsilon\big)}}{\vdash\exists\varepsilon{>}0\,\forall x\,\forall u\,\exists{-1}{\leq}z{\leq}1\,\forall{-2}{\leq}y{\leq}2\,\big(1{-}x^2{-}u^2{\leq}0\rightarrow [x':=][u':=]{-}2xx'{-}2uu'{\geq}\varepsilon\big)}}{\vdash\langle x'=zx-yu,u'=zu+yx\&^d{-2}{\leq}y{\leq}2\&{-1}{\leq}z{\leq}1\rangle\,1-x^2-u^2\geq 0}$$



avoid obstacles
changing wind
local turbulence

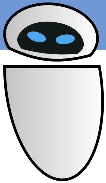
Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

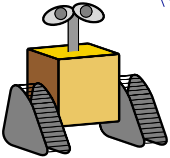
Outline

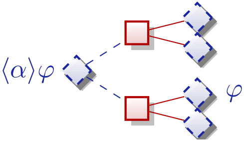
Summary



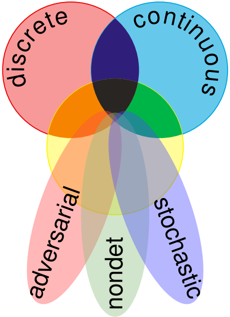
differential game logic

$\mathsf{dGL} = \mathsf{GL} + \mathsf{HG} = \mathsf{dL} + {}^{d}$





- Logic for hybrid games
- Compositional PL + logic
- Discrete + continuous + adversarial
- Winning regions iterate $\geq \omega^{\omega}$
- Sound & rel. complete axiomatization
- Hybrid games $>$ hybrid systems
- ^{d} radical challenge yet smooth extension
- Don't use systems thinking for games



André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3, doi:10.1007/978-3-319-63588-0.

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*, pages 13–24, Los Alamitos, 2012. IEEE.
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, Berlin, 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.