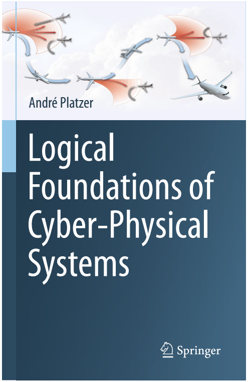
17: Game Proofs & Separations

Logical Foundations of Cyber-Physical Systems



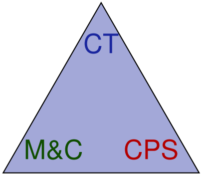
Stefan Mitsch

Carnegie Mellon University
Computer Science Department

Outline

Outline

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

Differential Game Logic: Syntax

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)

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

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)

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

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)

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

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

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

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

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

Outline

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 $\dfrac{P \to Q}{\langle\alpha\rangle P \to \langle\alpha\rangle Q}$

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

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

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

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

Soundness

Theorem (Soundness)

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

Soundness

Theorem (Soundness)

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

Do we have to prove anything at all?

More Axioms ???

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

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

$$\not{\mathrm{G}}\ \frac{P}{[\alpha]P}$$

More Axioms ???

$$\not{K}\ \ [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$$

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

$$\not{G}\ \frac{P}{[\alpha]P}$$

Separating Axioms

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

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

Separating Axioms

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

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

$\cancel{\text{G}}\ \dfrac{P}{[\alpha]P}$

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

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

Separating Axioms

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

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

$\cancel{\text{G}}$ $\dfrac{P}{[\alpha]P}$

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

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

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

ind $\dfrac{P \to [\alpha]P}{P \to [\alpha^*]P}$

$[*]$ $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$

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

Separating Axioms

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

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

$\cancel{\text{G}}\ \dfrac{P}{[\alpha]P}$

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

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

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

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

$[*]\quad [\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

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

Separating Axioms

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

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

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

~~$\overleftarrow{M}$~~ $\langle\alpha\rangle(P \vee Q) \rightarrow \langle\alpha\rangle P \vee \langle\alpha\rangle Q$

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 $\dfrac{P \rightarrow [\alpha]P}{P \rightarrow [\alpha^*]P}$

$[*]$ $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$

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

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

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

Separating Axioms

- $\cancel{\text{K}}$ $[\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q)$
- $\cancel{\overleftarrow{\text{M}}}$ $\langle\alpha\rangle(P \lor Q) \to \langle\alpha\rangle P \lor \langle\alpha\rangle Q$
- $\cancel{\text{I}}$ $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$
- $[*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$
- $\cancel{\text{B}}$ $\langle\alpha\rangle\exists x\, P \to \exists x\, \langle\alpha\rangle P \qquad (x \notin \alpha)$

- $\text{M}_{[\cdot]}$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$ $\qquad \cancel{\text{G}}$ $\dfrac{P}{[\alpha]P}$
- M $\langle\alpha\rangle P \lor \langle\alpha\rangle Q \to \langle\alpha\rangle(P \lor Q)$
- ind $\dfrac{P \to [\alpha]P}{P \to [\alpha^*]P}$
- $\cancel{\overleftarrow{[*]}}$ $[\alpha^*]P \leftrightarrow P \land [\alpha^*][\alpha]P$
- $\overleftarrow{\text{B}}$ $\exists x\, \langle\alpha\rangle P \to \langle\alpha\rangle\exists x\, P$

Separating Axioms

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

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

$\cancel{\text{G}}\ \dfrac{P}{[\alpha]P}$

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

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

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

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

$[*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

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

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

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

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

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

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

Separating Axioms

Separation: hybrid systems vs. hybrid games

Hybrid games add duality: $[\alpha^{\mathrm{d}}]P \leftrightarrow \langle\alpha\rangle P$

One game's boxes are another game's diamonds

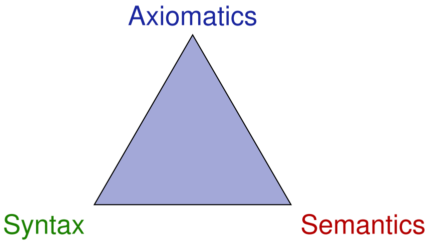
All hybrid game axioms must also be valid when diamonds and boxes are swapped!

All hybrid game axioms are also hybrid system axioms, but not the other way around

Soundness

Theorem (Soundness)

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



Soundness

Theorem (Soundness)

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

Proof.

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

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

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

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

□

Soundness

Theorem (Soundness)

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

Proof.

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

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

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

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

$[\cdot]$ is sound by determinacy

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

M Assume the premise $P \rightarrow Q$ 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.

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

□

The Miracle of Soundness

Soundness links semantics and axiomatics!

Compositional Soundness

- Soundness: If P provable then P valid $\vdash P$ implies $\vDash P$
- *Every* formula that it proves with *any* proof has to be valid

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.

Proving Repetitive Diamonds by Convergence

Duality turns angel winning questions into induction proofs

$$\langle^d\rangle \dfrac{\text{ind}\dfrac{x=0 \vdash [x:=0 \cap x:=1]x=0}{x=0 \vdash [(x:=0 \cap x:=1)^*]x=0}}{x=0 \vdash \langle (x:=0 \cup x:=1)^\times \rangle x=0}$$

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

Proving Repetitive Diamonds by Convergence

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

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

Proving Repetitive Diamonds by Convergence

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

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

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

Proving Repetitive Diamonds by Convergence

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

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

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

Proving Repetitive Diamonds by Convergence

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

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

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

Proving Repetitive Diamonds by Convergence

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

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

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

Proving Repetitive Diamonds by Convergence

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

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

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

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

$$\langle{}^*\rangle \quad \langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P \qquad \text{US} \ \frac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$$

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

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

$\langle * \rangle$ $\langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

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

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

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

$\langle{}^*\rangle \quad \langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P \qquad$ US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

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

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

$\langle^*\rangle$ $\langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

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

Example Proof: 2-Nim-type Game

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

Fixpoint style proof technique

$\langle{}^*\rangle$ $\quad \langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ $\qquad$ US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

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

$$x \geq 0 \to \langle\alpha^*\rangle 0\leq x<2$$

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

$\langle{}^*\rangle$ $\langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

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

Outline

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)

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

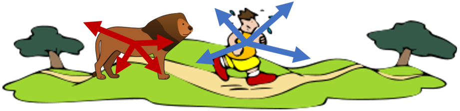
Definition (dGL Formula P)

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

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

All Reals | Some Reals | Angel Wins | Demon Wins

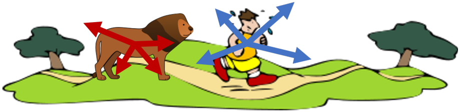
Lion and Man Game



$$m' = My, l' = Lz \&^d \underbrace{y \in B}_{y^2 \le 1} \& \underbrace{z \in B}_{z^2 \le 1}$$

- Both players can change speed at any time
- Man m choses $y \in B$ first
- Lion l can observe and react, choses $z \in B$ and duration

Lion and Man Game



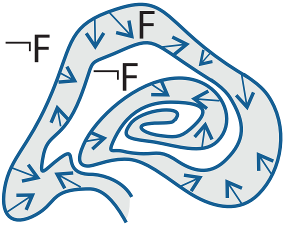
$$(l-m)^2 > 0 \to \left[m' = My, l' = Lz \,\&^d\, \underbrace{y \in B}_{y^2 \le 1} \,\&\, \underbrace{z \in B}_{z^2 \le 1}\right] (l-m)^2 > 0$$

- Both players can change speed at any time
- Man m choses $y \in B$ first
- Lion l can observe and react, choses $z \in B$ and duration

Differential Game Invariants

Theorem (Differential Game Invariants)

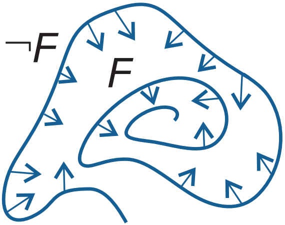
$$\text{DGI} \quad \frac{}{F \rightarrow [x' = f(x,y,z) \&^d y \in Y \& z \in Z]F}$$



Differential Game Invariants

Theorem (Differential Game Invariants)

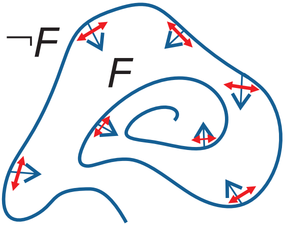
$$\text{DGI}\ \frac{}{F \rightarrow [x' = f(x,y,z) \&^d y \in Y \& z \in Z]F}$$



Differential Game Invariants

Theorem (Differential Game Invariants)

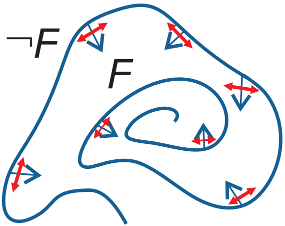
$$\text{DGI}\ \frac{}{F \rightarrow [x' = f(x,y,z) \&^d y \in Y \& z \in Z]F}$$



Differential Game Invariants

Theorem (Differential Game Invariants)

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

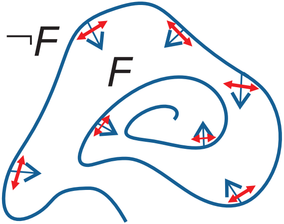


$$\text{DGI}\ \overline{\|l - m\|^2 > 0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\, \|l - m\|^2 > 0}$$

if $L \leq M$

Theorem (Differential Game Invariants)

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



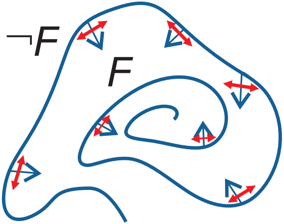
$$\dfrac{\overset{[:=]}{\overline{\qquad\qquad \vdash \exists y \in B \forall z \in B\, [m':=My][l':=Lz](2(l-m)\cdot(l'-m') \geq 0)}}}{\|l-m\|^2>0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\, \|l-m\|^2>0}\ \text{DGI}$$

if $L \leq M$

Differential Game Invariants

Theorem (Differential Game Invariants)

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

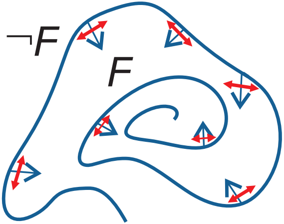


$$\cfrac{\cfrac{\cfrac{\overline{\quad\vdash \exists y \in B \forall z \in B\, (2(l-m)\cdot(Lz - My) \geq 0)}\ \mathbb{R}}{\vdash \exists y \in B \forall z \in B\, [m' := My][l' := Lz](2(l-m)\cdot(l'-m') \geq 0)}\ [:=]}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\, \|l-m\|^2 > 0}\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

if $L \leq M$

Theorem (Differential Game Invariants)

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



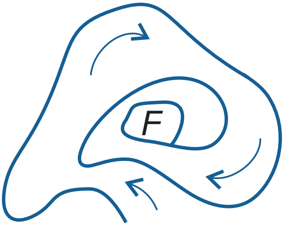
$$\dfrac{\dfrac{\dfrac{*}{\vdash \exists y \in B \forall z \in B\,(2(l-m)\cdot(Lz-My) \geq 0)}\,\mathbb{R}}{\vdash \exists y \in B \forall z \in B\,[m' := My][l' := Lz](2(l-m)\cdot(l'-m') \geq 0)}\,[:=]}{\|l-m\|^2 > 0 \vdash [m' = My, l' = Lz \&^d y \in B \& z \in B]\,\|l-m\|^2 > 0}\,\text{DGI}$$

if $L \leq M$

Differential Game Variants

Theorem (Differential Game Variants)

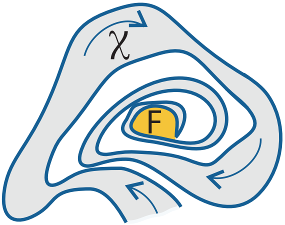
$$\text{DGV} \quad \frac{}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z \rangle g \geq 0}$$



Differential Game Variants

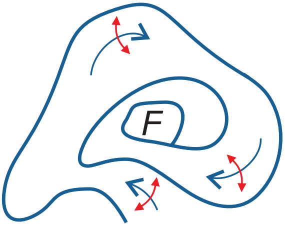
Theorem (Differential Game Variants)

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



Theorem (Differential Game Variants)

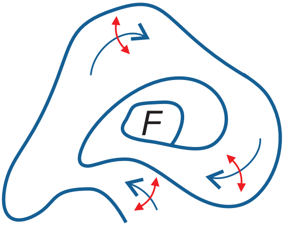
$$\text{DGV}\quad \frac{}{\langle x' = f(x,y,z) \&^d y \in Y \& z \in Z\rangle g \geq 0}$$



Differential Game Variants

Theorem (Differential Game Variants)

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



Differential Game Variants

Theorem (Differential Game Variants)

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

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

Differential Game Variants

Theorem (Differential Game Variants)

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

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

Differential Game Variants

Theorem (Differential Game Variants)

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

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

Differential Game Variants

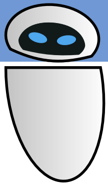
Theorem (Differential Game Variants)

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

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

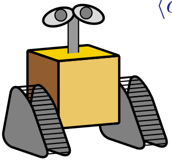
Outline

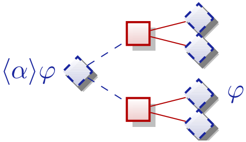
Summary



differential game logic

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





- Logic for hybrid games
- Compositional PL + logic
- Discrete + continuous + adversarial
- Winning regions iterate $\geq \omega^{\omega}$
- Sound & rel. complete axiomatization
- Hybrid games are more expressive than hybrid systems
- ${}^{\mathrm{d}}$ 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.