

19: Game Proofs & Separations

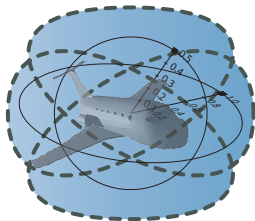
15-424: Foundations of Cyber-Physical Systems

André Platzer

aplatzer@cs.cmu.edu

Computer Science Department

Carnegie Mellon University, Pittsburgh, PA



- 1 Learning Objectives
- 2 Hybrid Game Proofs
 - Soundness
 - Separations
 - Soundness & Completeness
 - Expressiveness
 - Example Proofs
- 3 Differential Hybrid Games
 - Syntax
 - Example: Zeppelin
 - Differential Game Invariants
 - Example: Zeppelin Proof
- 4 Summary

1 Learning Objectives

2 Hybrid Game Proofs

- Soundness
- Separations
- Soundness & Completeness
- Expressiveness
- Example Proofs

3 Differential Hybrid Games

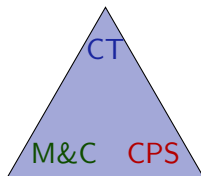
- Syntax
- Example: Zeppelin
- Differential Game Invariants
- Example: Zeppelin Proof

4 Summary

Learning Objectives

Game Proofs & Separations

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



discrete+adversarial
continuous+adversarial

multi-scale feedback

Differential Game Logic: Syntax

Discrete
Assign

Test
Game

Differential
Equation

Choice
Game

Seq.
Game

Repeat
Game

Dual
Game

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

All
Reals

Some
Reals

Angel
Wins

Demon
Wins

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α)

$\llbracket \cdot \rrbracket : \text{HG} \rightarrow (\wp(\mathcal{S}) \rightarrow \wp(\mathcal{S}))$

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

Definition (dGL Formula P)

$\llbracket \cdot \rrbracket : \text{Fml} \rightarrow \wp(\mathcal{S})$

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

$$\text{FP} \quad \frac{P \vee \langle \alpha \rangle Q \rightarrow Q}{\langle \alpha^* \rangle P \rightarrow Q}$$

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

$$\forall \quad \frac{p \rightarrow Q}{p \rightarrow \forall x Q} \quad (x \notin \text{FV}(p))$$

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

- 1 Learning Objectives
- 2 Hybrid Game Proofs
 - Soundness
 - Separations
 - Soundness & Completeness
 - Expressiveness
 - Example Proofs
- 3 Differential Hybrid Games
 - Syntax
 - Example: Zeppelin
 - Differential Game Invariants
 - Example: Zeppelin Proof
- 4 Summary

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

$$\text{FP} \quad \frac{P \vee \langle \alpha \rangle Q \rightarrow Q}{\langle \alpha^* \rangle P \rightarrow Q}$$

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

$$\forall \quad \frac{p \rightarrow Q}{p \rightarrow \forall x Q} \quad (x \notin \text{FV}(p))$$

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

Theorem (Soundness)

dGL proof calculus is sound

Theorem (Soundness)

dGL proof calculus is sound

Do we have to prove anything at all?

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

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

$$I \quad [\alpha^*](P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$$

$$B \quad \langle \alpha \rangle \exists x P \rightarrow \exists x \langle \alpha \rangle P$$

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

$$R \quad \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha]P_1 \wedge [\alpha]P_2 \rightarrow [\alpha]Q}$$

$$FA \quad \langle \alpha^* \rangle P \rightarrow P \vee \langle \alpha^* \rangle (\neg P \wedge \langle \alpha \rangle P)$$

$$M_{[\cdot]} \quad \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

$$M \quad \langle \alpha \rangle P \vee \langle \alpha \rangle Q \rightarrow \langle \alpha \rangle (P \vee Q)$$

$$\forall I \quad C_{\forall} (P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$$

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

$$M_{[\cdot]} \quad \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

$$M_{[\cdot]} \quad \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha](P_1 \wedge P_2) \rightarrow [\alpha]Q}$$

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

More Axioms ???

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

$$\cancel{M} \quad \langle \alpha \rangle (P \vee Q) \rightarrow \langle \alpha \rangle P \vee \langle \alpha \rangle Q$$

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

$$\cancel{B} \quad \langle \alpha \rangle \exists x P \rightarrow \exists x \langle \alpha \rangle P$$

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

$$\cancel{R} \quad \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha]P_1 \wedge [\alpha]P_2 \rightarrow [\alpha]Q}$$

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

$$M_{[\cdot]} \quad \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

$$M \quad \langle \alpha \rangle P \vee \langle \alpha \rangle Q \rightarrow \langle \alpha \rangle (P \vee Q)$$

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

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

$$M_{[\cdot]} \quad \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

$$M_{[\cdot]} \quad \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha](P_1 \wedge P_2) \rightarrow [\alpha]Q}$$

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

Separating Axioms

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

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

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

$$M_{[\cdot]} \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

~~$[M] \ \langle \alpha \rangle (P \vee Q) \rightarrow \langle \alpha \rangle P \vee \langle \alpha \rangle Q$~~

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

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

$$\forall I \ Cl_{\forall} (P \rightarrow [\alpha]P) \rightarrow (P \rightarrow [\alpha^*]P)$$

~~$[B] \ \langle \alpha \rangle \exists x P \rightarrow \exists x \langle \alpha \rangle P$~~

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

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

$$M_{[\cdot]} \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

~~$[R] \ \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha]P_1 \wedge [\alpha]P_2 \rightarrow [\alpha]Q}$~~

$$M_{[\cdot]} \frac{P_1 \wedge P_2 \rightarrow Q}{[\alpha](P_1 \wedge P_2) \rightarrow [\alpha]Q}$$

~~$[FA] \ \langle \alpha^* \rangle P \rightarrow P \vee \langle \alpha^* \rangle (\neg P \wedge \langle \alpha \rangle P)$~~

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

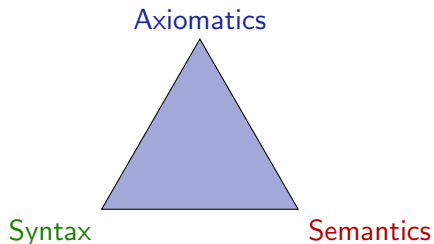
Theorem (Soundness)

dGL proof calculus is sound

Do we have to prove anything at all?

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.

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

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

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

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



Theorem (Soundness)

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

Proof.

$$\langle \cup \rangle \quad \llbracket \langle \alpha \cup \beta \rangle P \rrbracket = s_{\alpha \cup \beta}(\llbracket P \rrbracket) = s_{\alpha}(\llbracket P \rrbracket) \cup s_{\beta}(\llbracket P \rrbracket) = \llbracket \langle \alpha \rangle P \rrbracket \cup \llbracket \langle \beta \rangle P \rrbracket = \llbracket \langle \alpha \rangle P \vee \langle \beta \rangle P \rrbracket$$

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

$$\langle ; \rangle \quad \llbracket \langle \alpha ; \beta \rangle P \rrbracket = s_{\alpha ; \beta}(\llbracket P \rrbracket) = s_{\alpha}(s_{\beta}(\llbracket P \rrbracket)) = s_{\alpha}(\llbracket \langle \beta \rangle P \rrbracket) = \llbracket \langle \alpha \rangle \langle \beta \rangle P \rrbracket$$

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

$$[\cdot] \text{ is sound by determinacy} \quad [\cdot] \quad [\alpha]P \leftrightarrow \neg \langle \alpha \rangle \neg P$$

M Assume the premise $P \rightarrow Q$ is valid, i.e. $\llbracket P \rrbracket \subseteq \llbracket Q \rrbracket$.

Then the conclusion $\langle \alpha \rangle P \rightarrow \langle \alpha \rangle Q$ is valid, i.e.

$\llbracket \langle \alpha \rangle P \rrbracket = s_{\alpha}(\llbracket P \rrbracket) \subseteq s_{\alpha}(\llbracket Q \rrbracket) = \llbracket \langle \alpha \rangle Q \rrbracket$ by monotonicity.

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



Soundness links semantics and axiomatics in perfect unison!

Compositional Soundness

- Soundness: If P provable then P valid $\vdash P$ implies $\models P$
- *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. JAR'16
- 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 $\models P$
- *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. JAR'16
- 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.

Theorem (Completeness)

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

$$\models \varphi \quad \text{iff} \quad \text{Taut}_L \vdash \varphi$$

Soundness & Completeness: Consequences

Corollary (Constructive)

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

Remark (Coquand & Huet)

(Inf.Comput'88)

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

Corollary (Meyer & Halpern)

(J.ACM'82)

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

Corollary (Schmitt)

(Inf.Control.'84)

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

Corollary

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

Soundness & Completeness: Consequences

Corollary

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

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: Succinct invariants discrete Π_2^0
- $[x' = f(x)]G$ and $\langle x' = f(x) \rangle G$: Succinct differential (in)variants Δ_1^1
- $\exists x G$: Complexity depends on Herbrand disjunctions: discrete Π_1^1
✓ uninterpreted ✓ reals ✗ $\exists x [\alpha^*]G$ Π_1^1 -complete for discrete α

Corollary (Hybrid version of Parikh's result) (FOCS'83)

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

Soundness & Completeness: Consequences

Corollary

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

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: Succinct invariants discrete Π_2^0
- $[x' = f(x)]G$ 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_n^0 iff it's $\{x : \forall y_1 \exists y_2 \forall y_3 \dots y_n \varphi(x, y_1, \dots, y_n)\}$ for a decidable φ

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

set is Π_1^1 iff it's $\{x : \forall f \exists y \varphi(x, y, f)\}$ for a decidable φ and functions f

set is Σ_1^1 iff it's $\{x : \exists f \forall y \varphi(x, y, f)\}$ for a decidable φ and functions f

$$\Delta_n^i = \Sigma_n^i \cap \Pi_n^i$$

Theorem (Expressive Power: hybrid systems < hybrid games)

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

$$dL < dGL$$

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

“ $\not\leq$ ” Not the other way around.

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

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

$$dL < dGL$$

- “ \leq ” For every dL formula φ there is a dGL formula $\tilde{\varphi}$ that is equivalent.
Easy: same formula where Angel plays for nondeterminism.
- “ $\not\leq$ ” Not the other way around.
Hard: see proof.

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

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

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

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

“ $\not\leq$ ” Not the other way around.
Hard: see proof.

Corollary

Hybrid games are strictly more than hybrid systems.

Example Proof: 2-Nim-type Game

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

$\underbrace{\hspace{15em}}_{\alpha}$

► Fixpoint style proof technique

\mathbb{R}

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

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

$\langle * \rangle, \forall, \text{MP}$

$\text{true} \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$

\mathbb{R}

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

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

US	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 2 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2)$
$\langle * \rangle, \forall, MP$	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$
IR	$x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

$\langle \cup \rangle, \langle d \rangle$	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
US	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 2 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2)$
$\langle * \rangle, \forall, MP$	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$
\mathbb{R}	$x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

⟨:=⟩	$\forall x (0 \leq x < 2 \vee \langle \beta \rangle p(x) \wedge \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
⟨∪⟩, ⟨ ^d ⟩	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
US	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 2 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2)$
⟨*⟩, ∇, MP	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$
ℝ	$x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

IR	$\forall x (0 \leq x < 2 \vee p(x-1) \wedge p(x-2) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle := \rangle$	$\forall x (0 \leq x < 2 \vee \langle \beta \rangle p(x) \wedge \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle \cup \rangle, \langle ^d \rangle$	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
US	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 2 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2)$
$\langle * \rangle, \forall, MP$	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$
IR	$x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$

Example Proof: 2-Nim-type Game

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

► Fixpoint style proof technique

		*
IR	$\forall x (0 \leq x < 2 \vee p(x-1) \wedge p(x-2) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$	
⟨:=⟩	$\forall x (0 \leq x < 2 \vee \langle \beta \rangle p(x) \wedge \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$	
⟨∪⟩, ⟨ ^d ⟩	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$	
US	$\forall x (0 \leq x < 2 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 2 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2)$	
⟨*⟩, ∇, MP	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$	
IR	$x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2$	

Example Proof: Hybrid Game

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

$\underbrace{\hspace{15em}}_{\alpha}$

► Fixpoint style proof technique

$\langle^* \rangle$

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

Example Proof: Hybrid Game

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

$\underbrace{\hspace{15em}}_{\alpha}$

► Fixpoint style proof technique

US

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

$\langle * \rangle$

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

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

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

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

$\langle ; \rangle, \langle ^d \rangle$	$\forall x (0 \leq x < 1 \vee \langle \beta \rangle p(x) \vee \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle \cup \rangle$	$\forall x (0 \leq x < 1 \vee \langle \beta \cup \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
US	$\forall x (0 \leq x < 1 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 1 \rightarrow \langle \alpha^* \rangle 0 \leq x < 1) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1)$
$\langle * \rangle$	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1$

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

$\langle \rangle$	$\forall x (0 \leq x < 1 \vee \langle x := 1 \rangle \neg \langle x' = 1 \rangle \neg p(x) \vee p(x-1) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle ; \rangle, \langle ^d \rangle$	$\forall x (0 \leq x < 1 \vee \langle \beta \rangle p(x) \vee \langle \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle \cup \rangle$	$\forall x (0 \leq x < 1 \vee \langle \beta \cup \gamma \rangle p(x) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
US	$\forall x (0 \leq x < 1 \vee \langle \alpha \rangle \langle \alpha^* \rangle 0 \leq x < 1 \rightarrow \langle \alpha^* \rangle 0 \leq x < 1) \rightarrow (true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1)$
$\langle * \rangle$	$true \rightarrow \langle \alpha^* \rangle 0 \leq x < 1$

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

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

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

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

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

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

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

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

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

Example Proof: Hybrid Game

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

► Fixpoint style proof technique

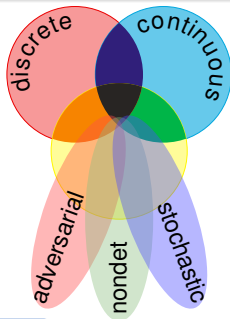
\mathbb{R}	$\forall x (0 \leq x < 1 \vee \forall t \geq 0 p(1+t) \vee p(x-1) \rightarrow p(x)) \rightarrow (true \rightarrow p(x))$
$\langle := \rangle$	$\forall x (0 \leq x < 1 \vee \langle x := 1 \rangle \neg \exists t \geq 0 \langle x := x+t \rangle \neg p(x) \vee p(x-1) \rightarrow p(x)) \rightarrow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

- 1 Learning Objectives
- 2 Hybrid Game Proofs
 - Soundness
 - Separations
 - Soundness & Completeness
 - Expressiveness
 - Example Proofs
- 3 Differential Hybrid Games
 - Syntax
 - Example: Zeppelin
 - Differential Game Invariants
 - Example: Zeppelin Proof
- 4 Summary

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

Tame Parts

Exploiting compositionality tames CPS complexity.

Analytic simplification

Differential Game Logic: Syntax

Discrete
Assign

Test
Game

Choice
Game

Seq.
Game

Repeat
Game

Dual
Game

Definition (Differential hybrid game α)

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

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)

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

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)

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

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 $z \in Z$
Angel knows Demon's y
Angel controls duration

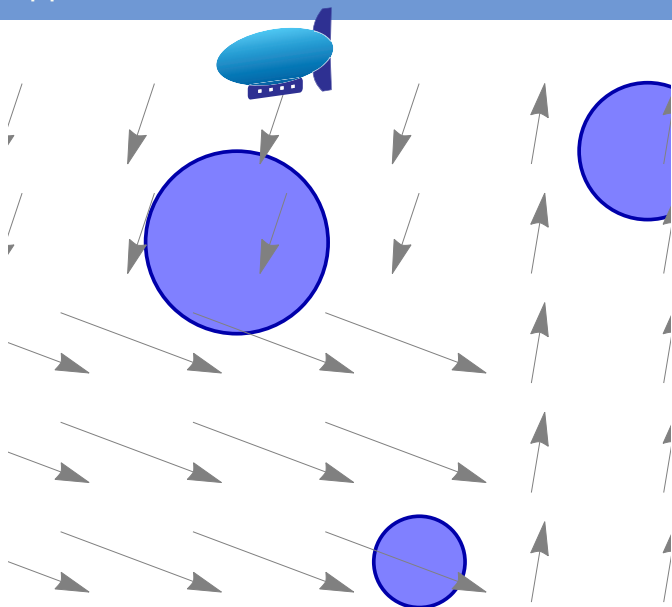
All
Reals

Some
Reals

Angel
Wins

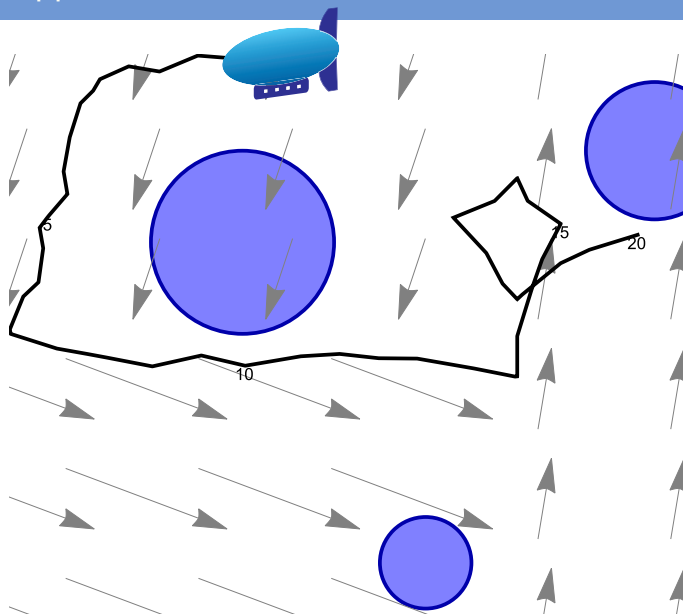
Demon
Wins

Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

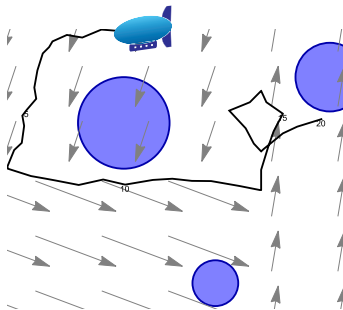
Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

Zeppelin Obstacle Parcours

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

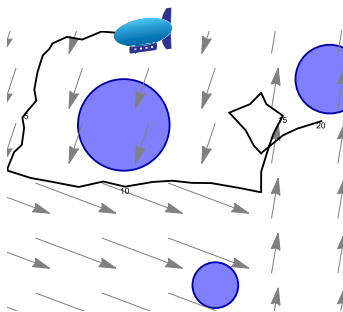


- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence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

Zeppelin Obstacle Parcours

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

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



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

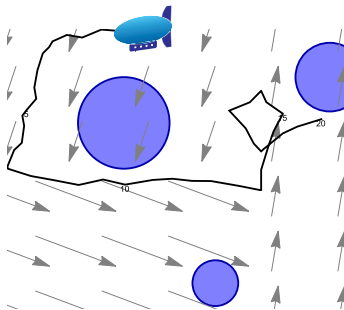
Zeppelin Obstacle Parcours

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

× $r > p$ hopeless turbulence

• $p > \|v\| + r$

• $\|v\| + r > p > r$



✓ airship at $x \in \mathbb{R}^2$

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

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

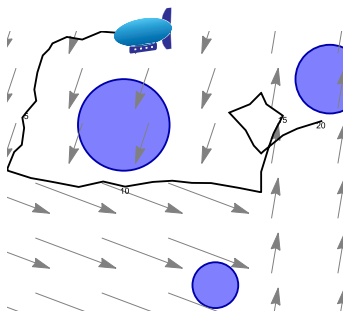
× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

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

Zeppelin Obstacle Parcours

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

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



- ✓ 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 $z \in B$

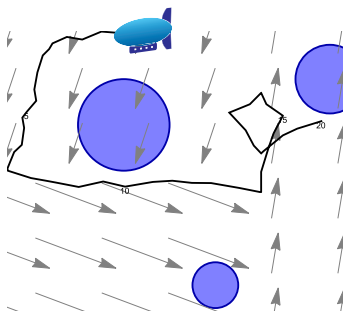
Zeppelin Obstacle Parcours

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

× $r > p$ hopeless turbulence

✓ $p > \|v\| + r$ super-powered prop

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



✓ airship at $x \in \mathbb{R}^2$

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

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

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

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

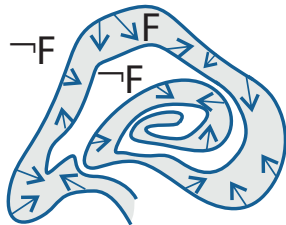
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



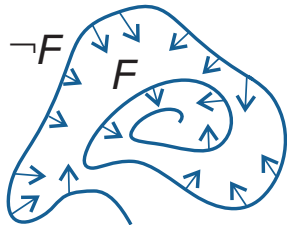
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



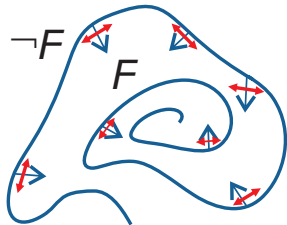
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



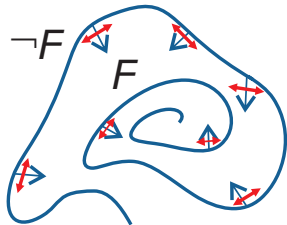
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



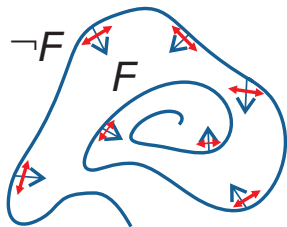
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



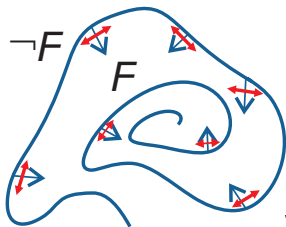
Differential Game Invariants

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)

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



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

where $y \in I \stackrel{\text{def}}{=} -1 \leq y \leq 1$

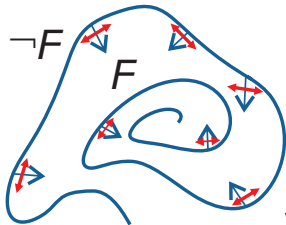
Differential Game Invariants

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)

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



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

where $y \in I \stackrel{\text{def}}{=} -1 \leq y \leq 1$

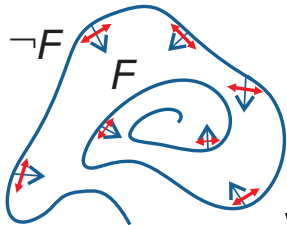
Differential Game Invariants

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)

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



$$\begin{array}{l} \mathbb{R} \frac{}{\vdash \exists y \in I \forall z \in I 0 \leq 3x^2(-1+2y+z)} \\ [':=] \frac{}{\vdash \exists y \in I \forall z \in I [x' := -1+2y+z] 0 \leq 3x^2 x'} \\ \text{DGI} \frac{}{1 \leq x^3 \vdash [x' = -1+2y+z \&^d y \in I \& z \in I] 1 \leq x^3} \end{array}$$

where $y \in I \stackrel{\text{def}}{=} -1 \leq y \leq 1$

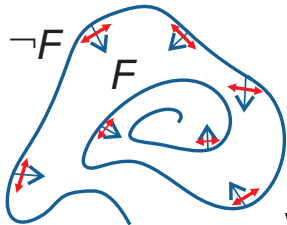
Differential Game Invariants

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)

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



$$\begin{array}{l} \mathbb{R} \frac{*}{\vdash \exists y \in I \forall z \in I 0 \leq 3x^2(-1+2y+z)} \\ [\prime :=] \frac{}{\vdash \exists y \in I \forall z \in I [x' := -1+2y+z] 0 \leq 3x^2 x'} \\ \text{DGI} \frac{}{1 \leq x^3 \vdash [x' = -1+2y+z \&^d y \in I \& z \in I] 1 \leq x^3} \end{array}$$

where $y \in I \stackrel{\text{def}}{=} -1 \leq y \leq 1$

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)

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

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

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)

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

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

if $L \leq M$

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)

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

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

if $L \leq M$

Theorem (Differential Game 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)

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

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

if $L \leq M$

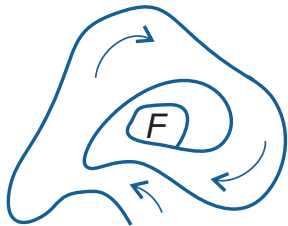
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



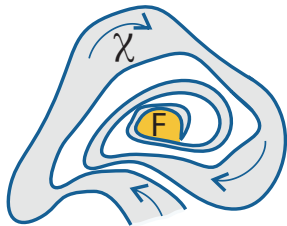
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



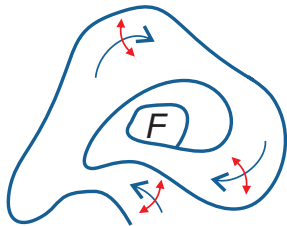
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



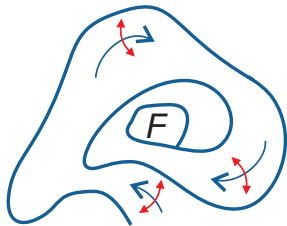
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



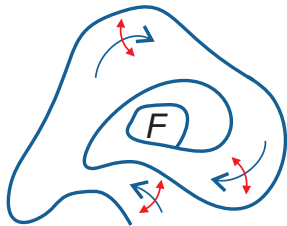
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



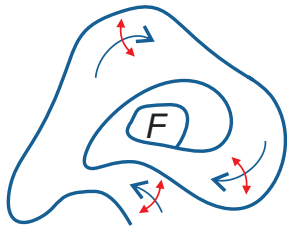
Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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



Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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

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

Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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

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

Differential Game Variants

Theorem (Differential Game Variants)

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

Theorem (Differential Game Refinement)

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

$$\vdash \exists \varepsilon > 0 \forall x \forall u \exists -1 \leq z \leq 1 \forall -2 \leq y \leq 2 (x^2 + u^2 \geq 1 \rightarrow -2x(zx - yu) - 2u(zu + yx) \geq \varepsilon)$$

$$\vdash \exists \varepsilon > 0 \forall x \forall u \exists -1 \leq z \leq 1 \forall -2 \leq y \leq 2 (1 - x^2 - u^2 \leq 0 \rightarrow (-2xx' - 2uu') \frac{zx - yu}{x'} \frac{zu + yx}{u'} \geq \varepsilon)$$

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

Differential Game Variants

Theorem (Differential Game Variants)

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

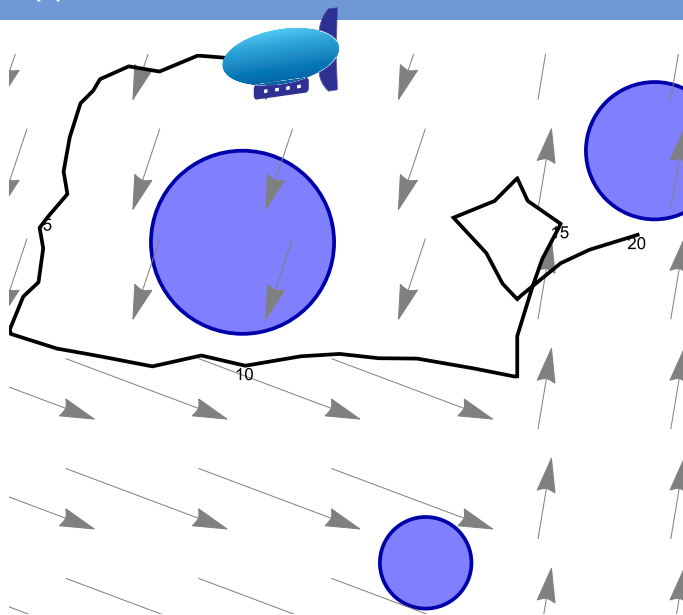
Theorem (Differential Game Refinement)

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

*

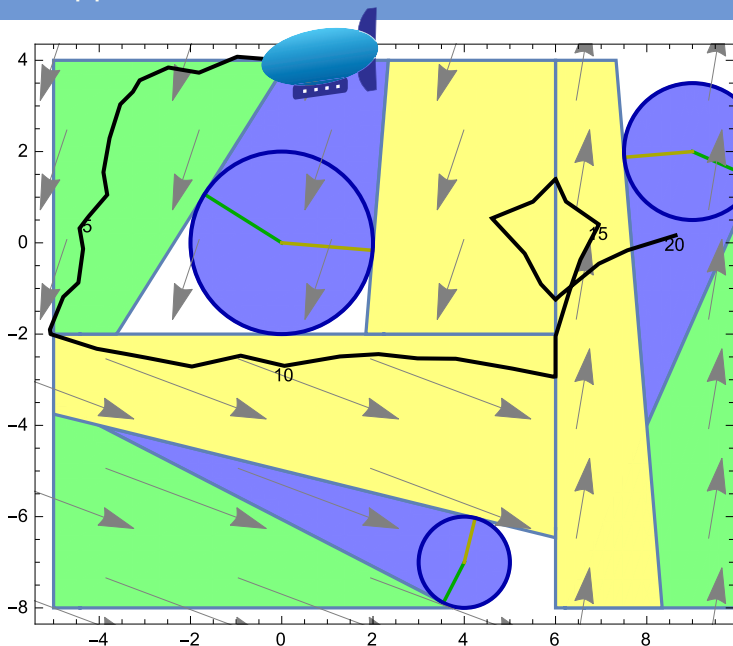
$$\begin{array}{l} \vdash \exists \varepsilon > 0 \forall x \forall u \exists -1 \leq z \leq 1 \forall -2 \leq y \leq 2 (x^2 + u^2 \geq 1 \rightarrow -2x(zx - yu) - 2u(zu + yx) \geq \varepsilon) \\ \vdash \exists \varepsilon > 0 \forall x \forall u \exists -1 \leq z \leq 1 \forall -2 \leq y \leq 2 (1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

Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

Zeppelin Obstacle Parcours



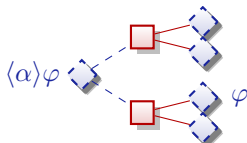
avoid obstacles
changing wind
local turbulence

- 1 Learning Objectives
- 2 Hybrid Game Proofs
 - Soundness
 - Separations
 - Soundness & Completeness
 - Expressiveness
 - Example Proofs
- 3 Differential Hybrid Games
 - Syntax
 - Example: Zeppelin
 - Differential Game Invariants
 - Example: Zeppelin Proof
- 4 Summary

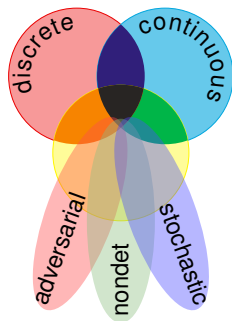
Summary

differential game logic

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



- 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



5 Convergence for Repetitive Diamonds

Proving Repetitive Diamonds by Convergence

con

$$\Gamma \vdash \langle \alpha^* \rangle Q, \Delta$$

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

Proving Repetitive Diamonds by Convergence

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

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\begin{array}{c} \text{con} \\ \hline \frac{\overline{x \geq 0 \vdash \exists n x < n+1} \quad \overline{x < n+2 \wedge n+1 > 0 \vdash \langle x := x-1 \rangle x < n+1} \quad \overline{\exists n \leq 0 x < n+1 \vdash x < 1}}{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1} \\ \rightarrow R \\ \hline \vdash x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1 \end{array}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\begin{array}{c} \mathbb{R} \frac{*}{x \geq 0 \vdash \exists n x < n+1} \quad \frac{}{x < n+2 \wedge n+1 > 0 \vdash \langle x := x-1 \rangle x < n+1} \quad \frac{}{\exists n \leq 0 x < n+1 \vdash x < 1} \\ \text{con} \frac{}{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1} \\ \rightarrow \mathbb{R} \frac{}{\vdash x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1} \end{array}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\begin{array}{c} \mathbb{R} \frac{*}{x \geq 0 \vdash \exists n x < n+1} \stackrel{(\Leftarrow)}{\frac{x < n+2 \wedge n+1 > 0 \vdash x-1 < n+1}{x < n+2 \wedge n+1 > 0 \vdash \langle x := x-1 \rangle x < n+1}}{\frac{\exists n \leq 0 x < n+1 \vdash x < 1}{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1}} \\ \text{con} \frac{\rightarrow \mathbb{R}}{\vdash x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1} \end{array}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\begin{array}{c} \text{con} \\ \rightarrow R \end{array} \frac{\begin{array}{c} \text{con} \\ \rightarrow R \end{array} \frac{\begin{array}{c} \mathbb{R} \\ \text{con} \end{array} \frac{\begin{array}{c} * \\ x \geq 0 \vdash \exists n x < n+1 \end{array} \quad \begin{array}{c} * \\ x < n+2 \wedge n+1 > 0 \vdash x-1 < n+1 \end{array} \quad \begin{array}{c} * \\ \exists n \leq 0 x < n+1 \vdash x < 1 \end{array}}{\begin{array}{c} \mathbb{R} \\ \text{con} \end{array} \frac{x < n+2 \wedge n+1 > 0 \vdash \langle x := x-1 \rangle x < n+1}{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1}}{x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\begin{array}{c} \mathbb{R} \frac{*}{x \geq 0 \vdash \exists n x < n+1} \quad \mathbb{R} \frac{*}{x < n+2 \wedge n+1 > 0 \vdash x-1 < n+1} \quad \mathbb{R} \frac{*}{\exists n \leq 0 x < n+1 \vdash x < 1} \\ \text{con} \frac{\langle \Rightarrow \rangle}{x < n+2 \wedge n+1 > 0 \vdash \langle x := x-1 \rangle x < n+1} \\ \rightarrow \mathbb{R} \frac{x \geq 0 \vdash \langle (x := x-1)^* \rangle x < 1}{\vdash x \geq 0 \rightarrow \langle (x := x-1)^* \rangle x < 1} \end{array}$$



André Platzer.

Foundations of cyber-physical systems.

Lecture Notes 15-424/624/824, Carnegie Mellon University, 2017.

URL: <http://1fcps.org/course/fcps17.html>.



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.

CoRR, abs/1507.04943, 2015.

arXiv:1507.04943.



André Platzer.

Logics of dynamical systems.

In *LICS*, pages 13–24. IEEE, 2012.

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. Springer, 2016.

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., 2016.

doi:10.1007/s10817-016-9385-1.