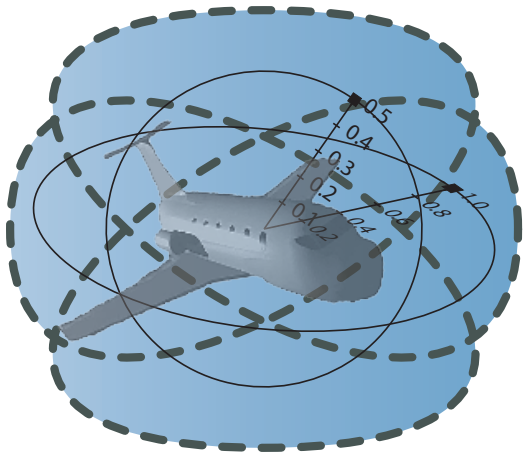
19: Game Proofs & Separations

15-424: Foundations of Cyber-Physical Systems

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

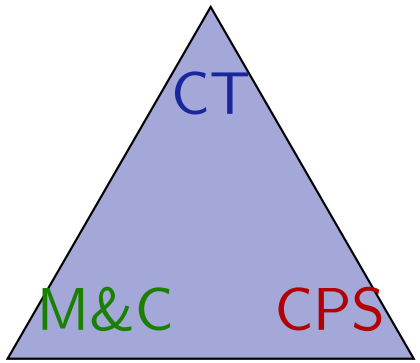


Outline

Outline

Learning Objectives
Game Proofs & Separations

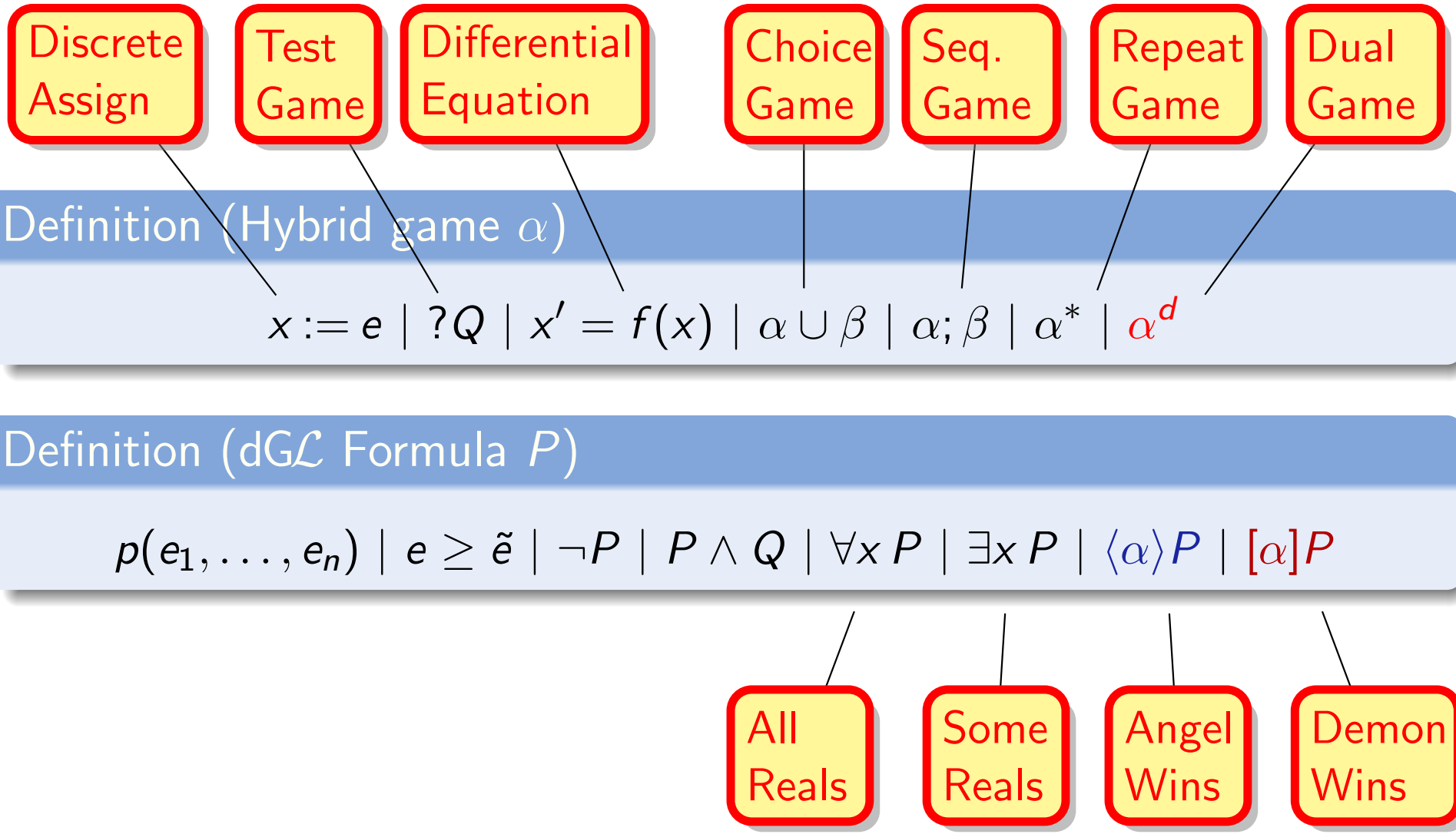
rigorous reasoning for adversarial dynamics
miracle of soundness
power of completeness
expressiveness
separations
axiomatization of dG$\mathcal{L}$
multi-dynamical systems
game invariants



discrete+adversarial
continuous+adversarial

multi-scale feedback

Differential Game Logic: Syntax



TOCL'15

Differential Game Logic: Denotational Semantics

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

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

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

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

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

$$\mathrm{US}\ \frac{\varphi}{\varphi^{\psi(\cdot)}_{p(\cdot)}}$$

TOCL'15

Outline

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

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

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

TOCL'15

Soundness

Theorem (Soundness)

dG$\mathcal{L}$ *proof calculus is sound*

Soundness

Theorem (Soundness)

dG$\mathcal{L}$ *proof calculus is sound*

Do we have to prove anything at all?

More Axioms

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

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

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

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

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

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

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

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

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

$\forall$I $\text{CI}_\forall\,(P \to [\alpha]P) \to (P \to [\alpha^*]P)$

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

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

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

More Axioms ???

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

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

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

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

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

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

~~FA~~ $\langle\alpha^*\rangle P \to P \vee \langle\alpha^*\rangle(\neg P \wedge \langle\alpha\rangle P)$

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

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

$\forall\text{I}$ $\text{CI}_\forall\,(P \to [\alpha]P) \to (P \to [\alpha^*]P)$

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

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

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

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

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

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

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

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

$\forall\mathsf{I}\quad \mathsf{CI}_\forall\,(P \to [\alpha]P) \to (P \to [\alpha^*]P)$

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

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

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

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

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

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

~~FA~~ $\langle\alpha^*\rangle P \to P \vee \langle\alpha^*\rangle(\neg P \wedge \langle\alpha\rangle P)$

Soundness

Theorem (Soundness)

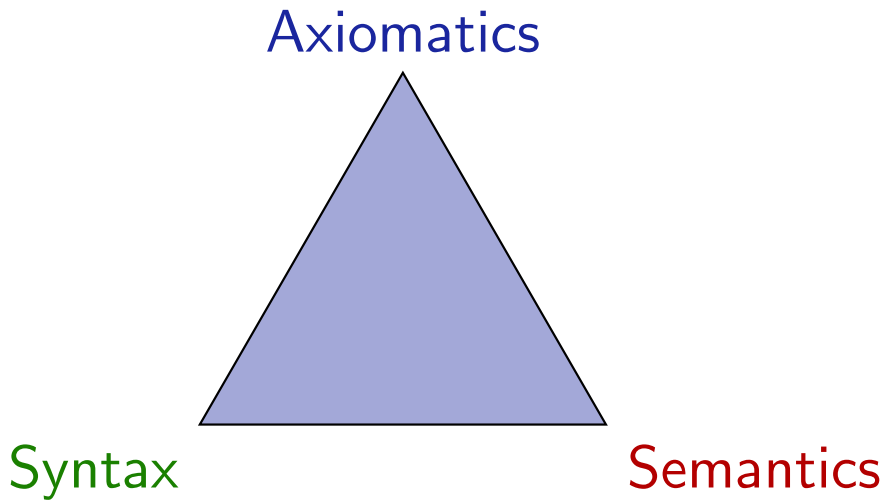
dG$\mathcal{L}$ *proof calculus is sound*

Do we have to prove anything at all?

Soundness

Theorem (Soundness)

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



Soundness

Theorem (Soundness)

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

Proof.

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

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

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

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

Soundness

Theorem (Soundness)

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

Proof.

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

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

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

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

$[\cdot]$ is sound by determinacy

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

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

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

The Miracle of Soundness

Soundness links semantics and axiomatics in perfect unison!

Compositional Soundness

- Soundness: If P provable then P valid — $\vdash P$ implies $\models P$
- *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. CADE'15
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. CADE'15
2. All proof rules are sound: take valid premises to valid conclusions.

Then

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

Soundness & Completeness

Theorem (Completeness)

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

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

TOCL'15

Soundness & Completeness: Consequences

Corollary (Constructive)

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

Remark (Coquand & Huet) (Inf.Comput'88)

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

Corollary (Meyer & Halpern) (J.ACM'82)

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

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

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

Corollary

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

Soundness & Completeness: Consequences

Corollary

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

Corollary (Characterization of hybrid game challenges)

- $[\alpha^*]G$: *Succinct invariants* *discrete* Π^0_2
- $[x' = f(x)]G$ *and* $\langle x' = f(x)\rangle G$: *Succinct differential (in)variants* Δ^1_1
- $\exists x\, G$: *Complexity depends on Herbrand disjunctions:* *discrete* Π^1_1
  ✓ *uninterpreted* ✓ *reals* × $\exists x\,[\alpha^*]G$ Π^1_1*-complete for discrete* α

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

**-free* dG$\mathcal{L}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*
^{d}*-free* dG$\mathcal{L}$ *complete relative to* d$\mathcal{L}$*, relative to continuous, or to discrete*

Expressiveness

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

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

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

"$\leq$" For every d$\mathcal{L}$ formula φ there is a dG$\mathcal{L}$ formula $\tilde{\varphi}$ that is equivalent.

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

TOCL'15

Expressiveness

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

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

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

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

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

TOCL'15

Expressiveness

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

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

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

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

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

Corollary

Hybrid games are strictly more than hybrid systems.

TOCL'15

Example Proof: 2-Nim-type Game

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

- Fixpoint style proof technique

$\mathbb{R}$

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

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

$$\frac{\dfrac{}{\mathit{true} \rightarrow \langle \alpha^* \rangle 0 \leq x < 2}\ \langle^*\rangle,\forall,\mathrm{MP}}{x \geq 0 \rightarrow \langle \alpha^* \rangle 0 \leq x < 2}\ \mathbb{R}$$

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

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

$$\langle^*\rangle,\forall,\text{MP}\ \frac{}{\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

$$\mathbb{R}\ \frac{}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

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

$$\langle\cup\rangle,\langle^d\rangle \quad \frac{}{\forall x\,(0{\leq}x{<}2 \vee \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}$$

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

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

$$\mathbb{R} \quad \frac{}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

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

$$\langle := \rangle \quad \frac{}{\forall x\,(0{\leq}x{<}2 \lor \langle\beta\rangle p(x) \land \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}$$

$$\langle \cup \rangle, \langle^d \rangle \quad \frac{}{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}$$

$$\mathrm{US} \quad \frac{}{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0{\leq}x{<}2 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2) \rightarrow (\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2)}$$

$$\langle^* \rangle, \forall, \mathrm{MP} \quad \frac{}{\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

$$\mathbb{R} \quad \frac{}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

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

$$\mathbb{R}\ \frac{\forall x\,(0{\leq}x{<}2 \lor p(x-1) \land p(x-2) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}{\forall x\,(0{\leq}x{<}2 \lor \langle\beta\rangle p(x) \land \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}$$

$$\langle:=\rangle\ \frac{\forall x\,(0{\leq}x{<}2 \lor \langle\beta\rangle p(x) \land \langle\gamma\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}$$

$$\langle\cup\rangle,\langle^d\rangle\ \frac{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle p(x) \rightarrow p(x)) \rightarrow (\mathit{true} \rightarrow p(x))}{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0{\leq}x{<}2 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2) \rightarrow (\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2)}$$

$$\mathrm{US}\ \frac{\forall x\,(0{\leq}x{<}2 \lor \langle\alpha\rangle\langle\alpha^*\rangle 0{\leq}x{<}2 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2) \rightarrow (\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2)}{\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

$$\langle^*\rangle,\forall,\mathrm{MP}\ \frac{\mathit{true} \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}{x \geq 0 \rightarrow \langle\alpha^*\rangle 0{\leq}x{<}2}$$

$$\mathbb{R}$$

Example Proof: 2-Nim-type Game

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

- Fixpoint style proof technique

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

*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

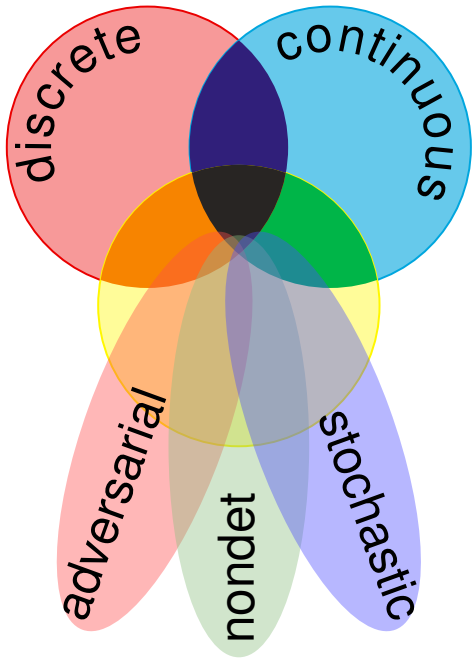
$$\langle^*\rangle\ \frac{}{\mathit{true} \to \langle\alpha^*\rangle 0{\leq}x{<}1}$$

Outline

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combine multiple simple dynamical effects.

Tame Parts

Exploiting compositionality tames CPS complexity.

Differential Game Logic: Syntax

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

Definition (Differential hybrid game α)

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

Definition (dG$\mathcal{L}$ 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

arXiv

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 (dG$\mathcal{L}$ 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

arXiv

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

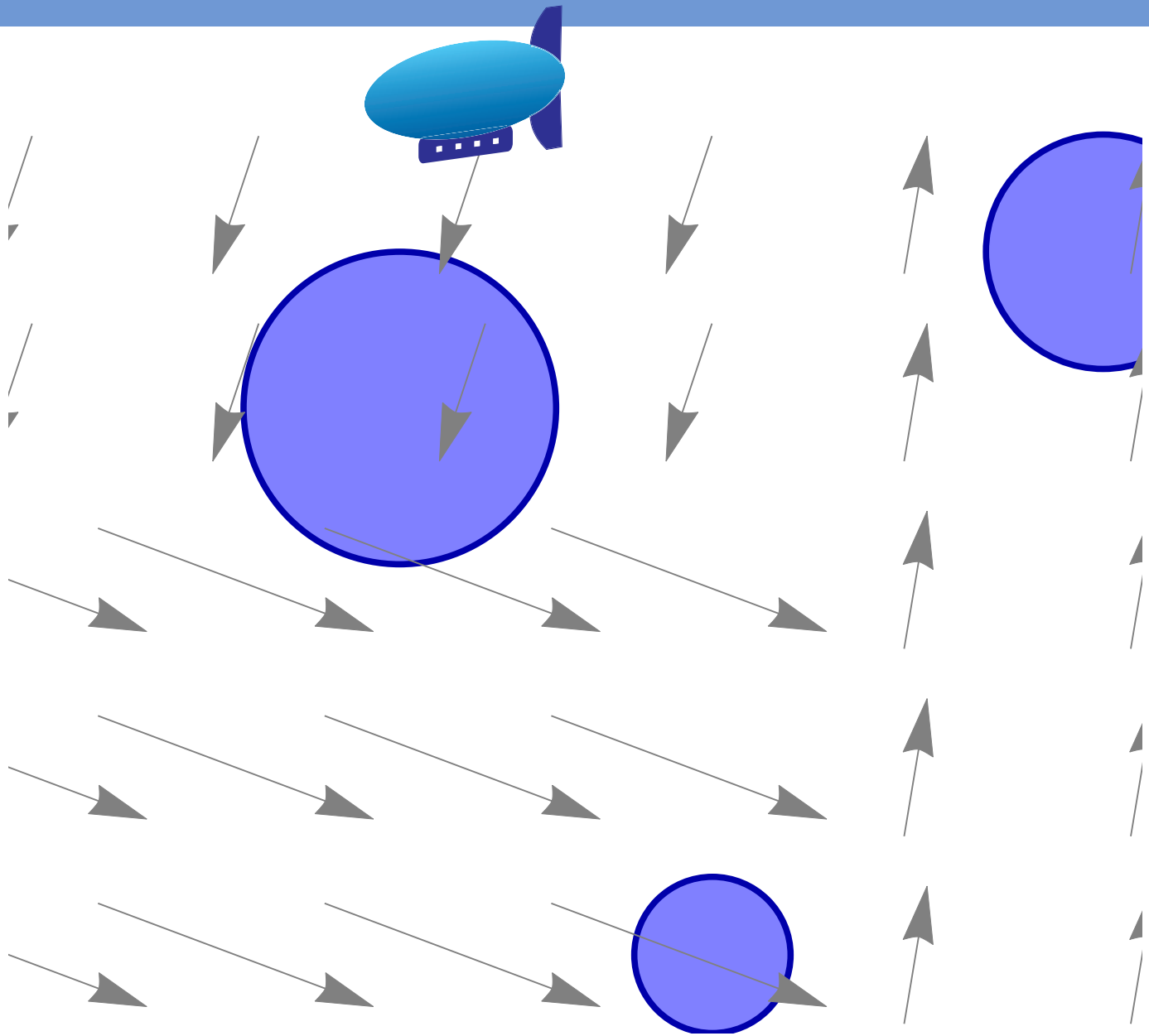
$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid \langle \alpha \rangle P \mid [\alpha] P$$

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

arXiv

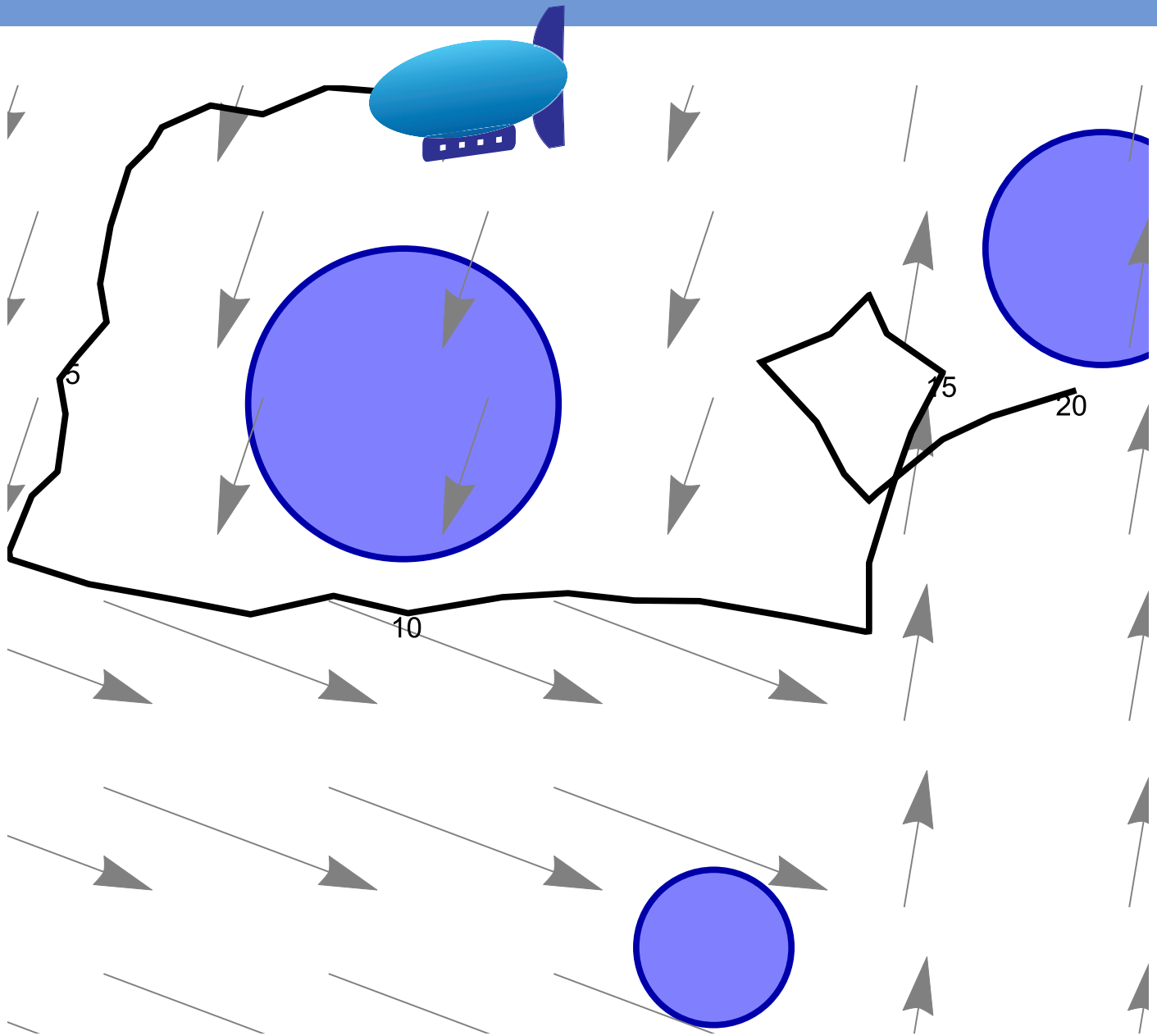
Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

arXiv

Zeppelin Obstacle Parcours

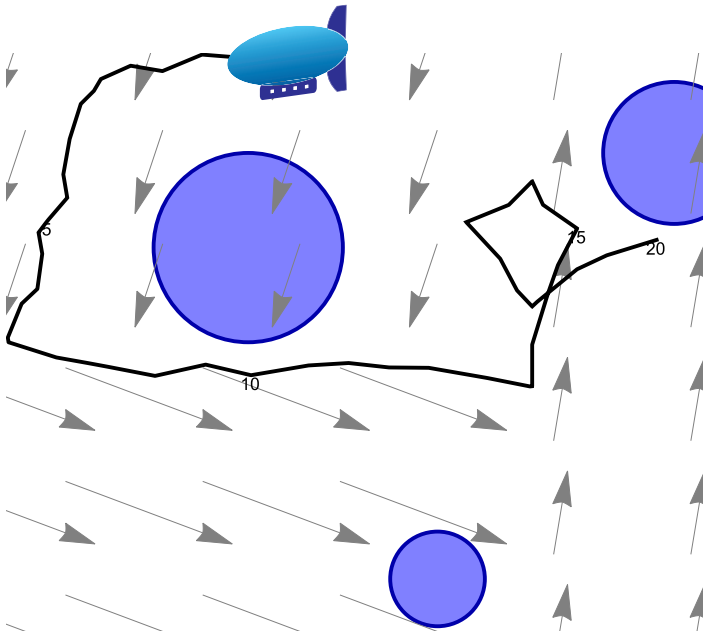


avoid obstacles
changing wind
local turbulence

arXiv

Zeppelin Obstacle Parcours

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

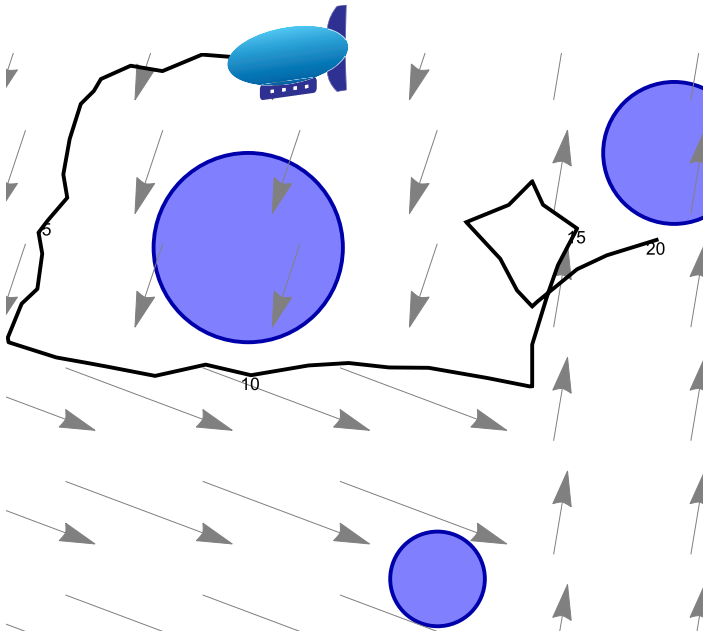


- ✓ airship at $x \in \mathbb{R}^2$
- ✓ propeller p controlled in any direction $y \in B$, i.e. $y_1^2 + y_2^2 \leq 1$
- × sporadically changing homogeneous wind field $v \in \mathbb{R}^2$
- × sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C
- × continuously local turbulence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

Zeppelin Obstacle Parcours

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

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



✓ airship at $x \in \mathbb{R}^2$

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

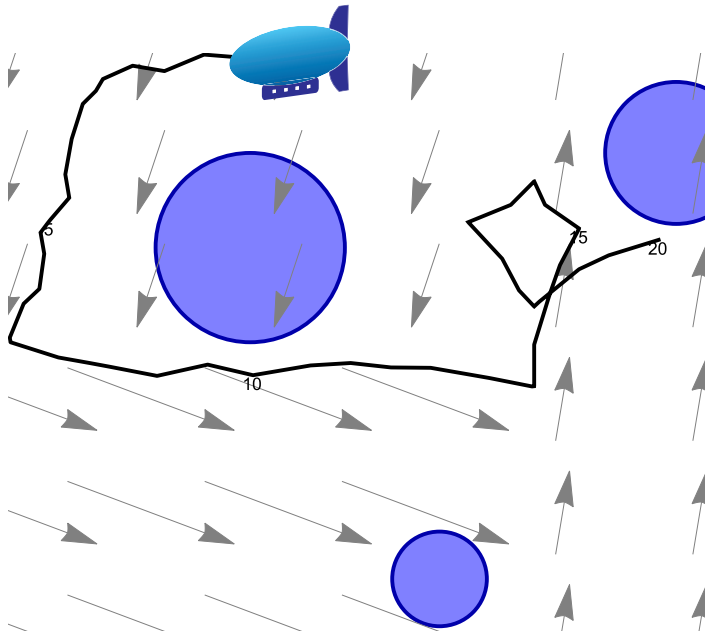
× sporadically changing homogeneous wind field $v \in \mathbb{R}^2$

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

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

Zeppelin Obstacle Parcours

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



× $r > p$ hopeless

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

✓ airship at $x \in \mathbb{R}^2$

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

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

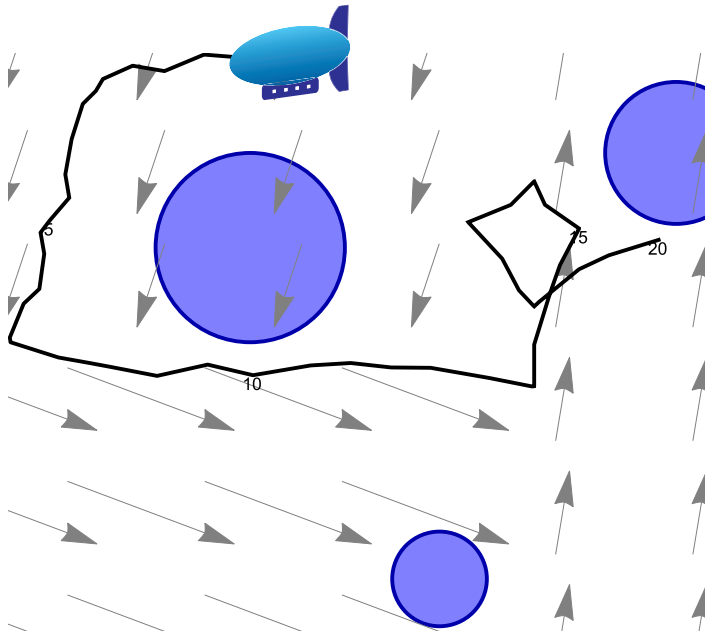
× sporadically changing obstacle $o \in \mathbb{R}^2$ of size c subject to C

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

Zeppelin Obstacle Parcours

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

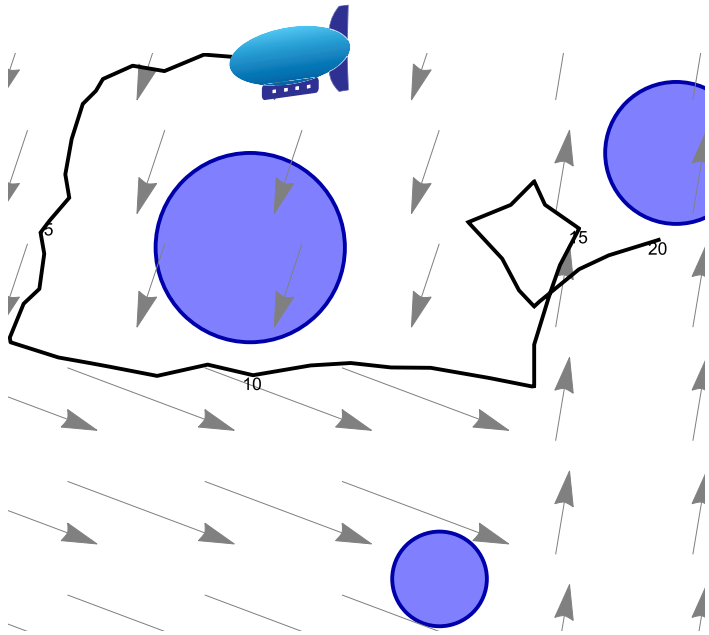
- $\times$ $r > p$ hopeless
- ✓ $p > \|v\| + r$ super-powered
  - $\|v\| + r > p > r$



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

Zeppelin Obstacle Parcours

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



- × $r > p$ hopeless
- ✓ $p > \|v\| + r$ super-powered
- ? $\|v\| + r > p > r$ 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 $z \in B$

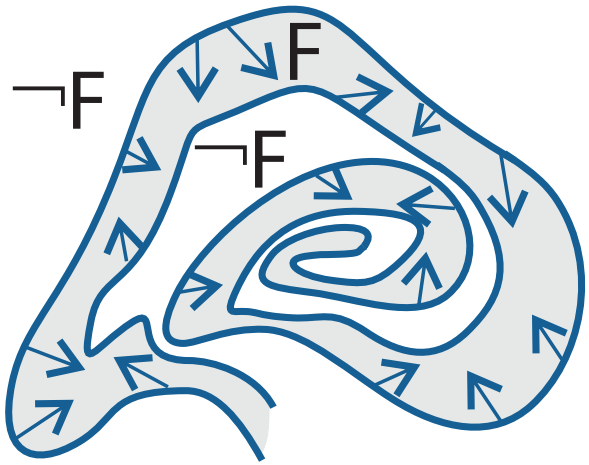
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



arXiv

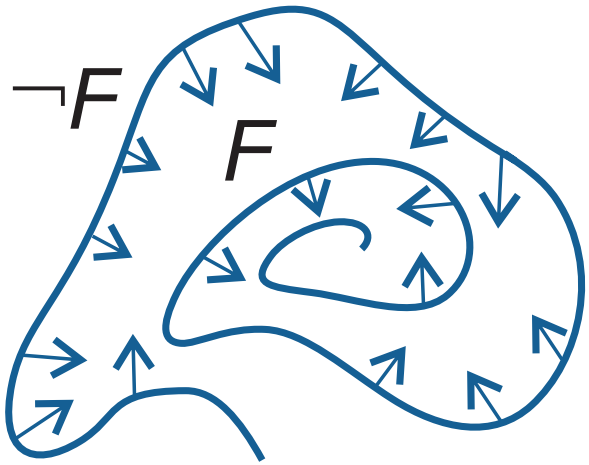
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



arXiv

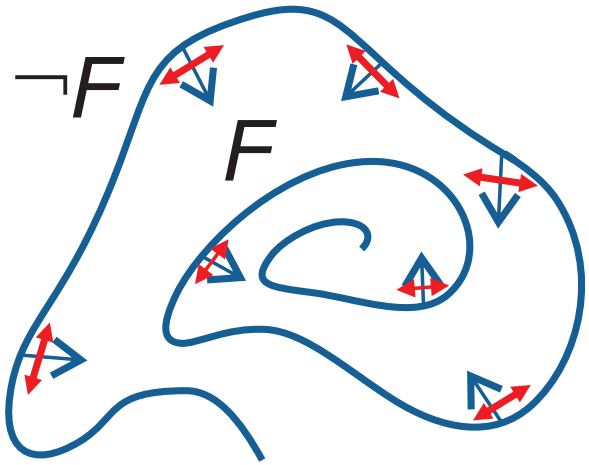
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



arXiv

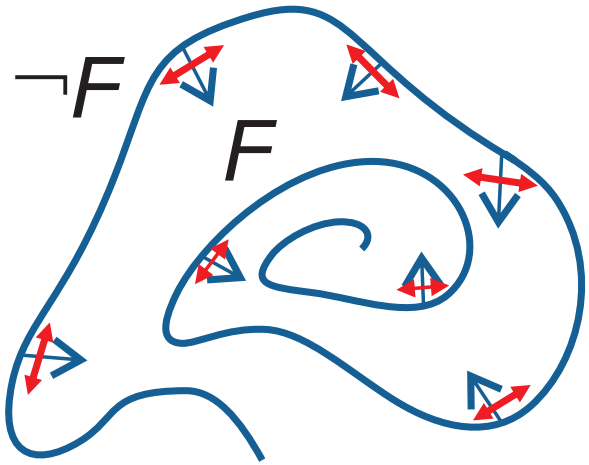
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



arXiv

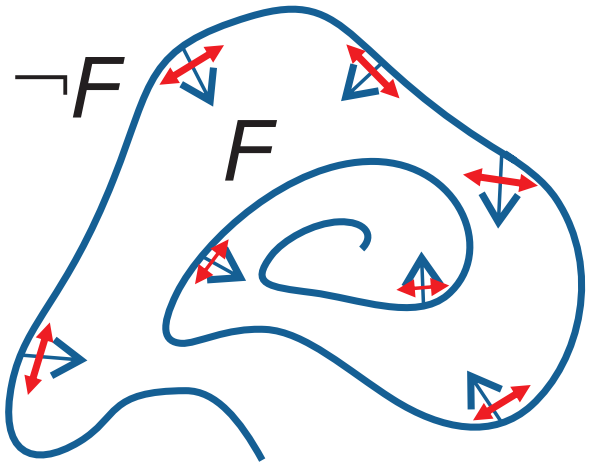
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



arXiv

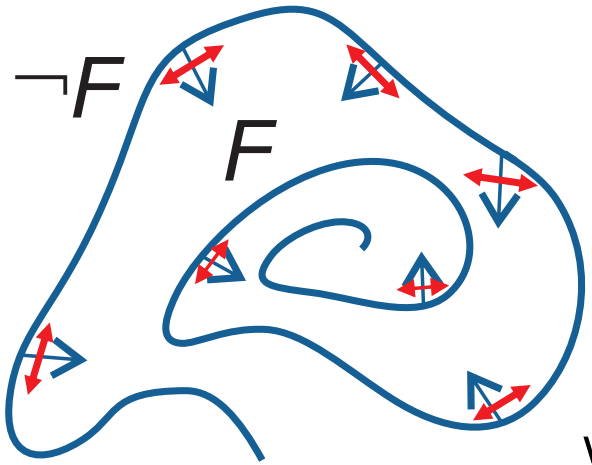
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



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

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

arXiv

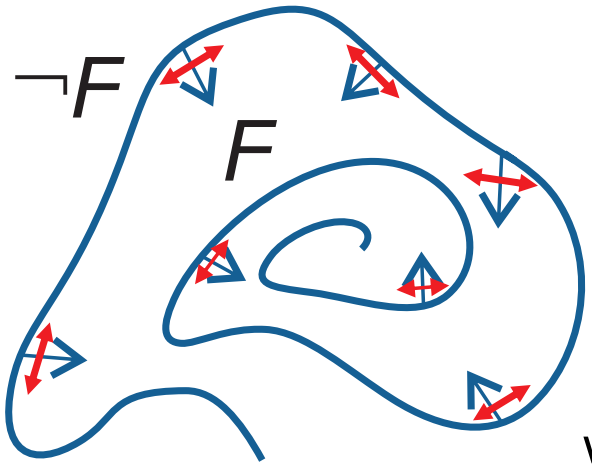
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



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

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

arXiv

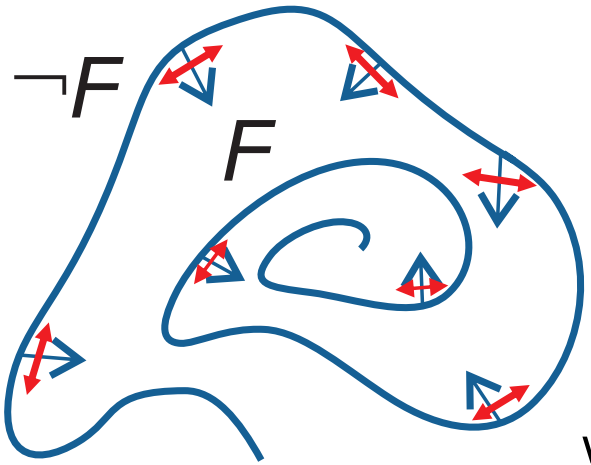
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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



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

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

arXiv

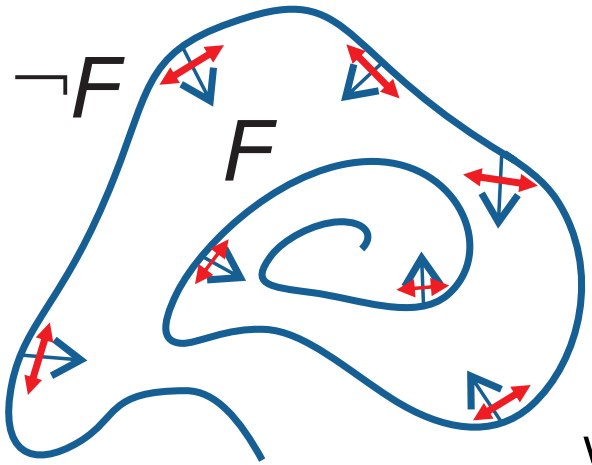
Differential Game Invariants

Theorem (Differential Game Invariants)

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

Theorem (Differential Game Refinement)

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

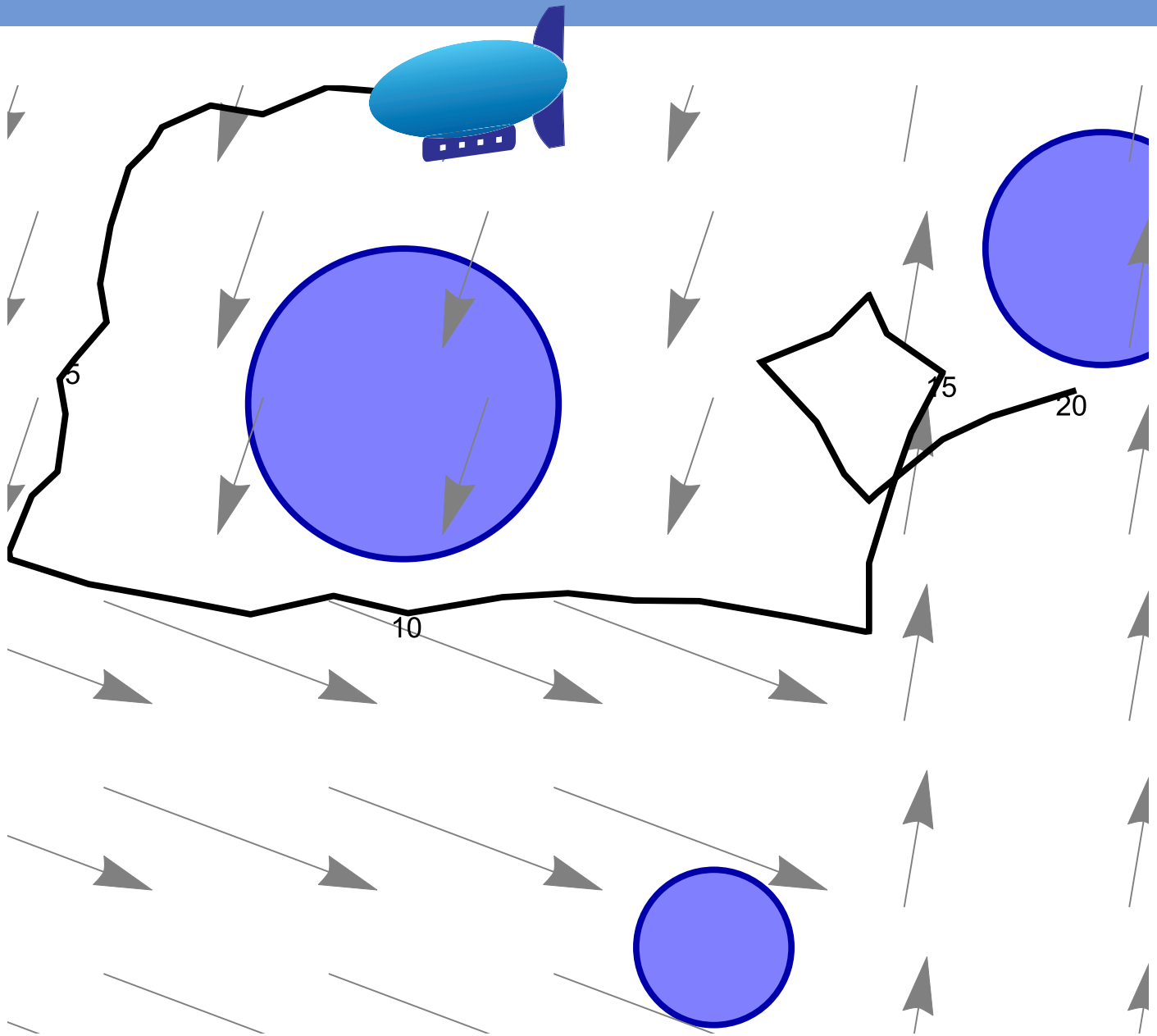


$$\dfrac{\dfrac{\dfrac{*}{\vdash \exists y{\in}I\, \forall z{\in}I\, 0 \le 3x^2(-1{+}2y{+}z)}\,\mathbb{R}}{\vdash \exists y{\in}I\, \forall z{\in}I\, [x':=-1{+}2y{+}z]0{\le}3x^2x'}\,[':=]}{1{\le}x^3 \vdash [x'=-1{+}2y{+}z\&^d y \in I \& z \in I]1{\le}x^3}\,\text{DGI}$$

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

arXiv

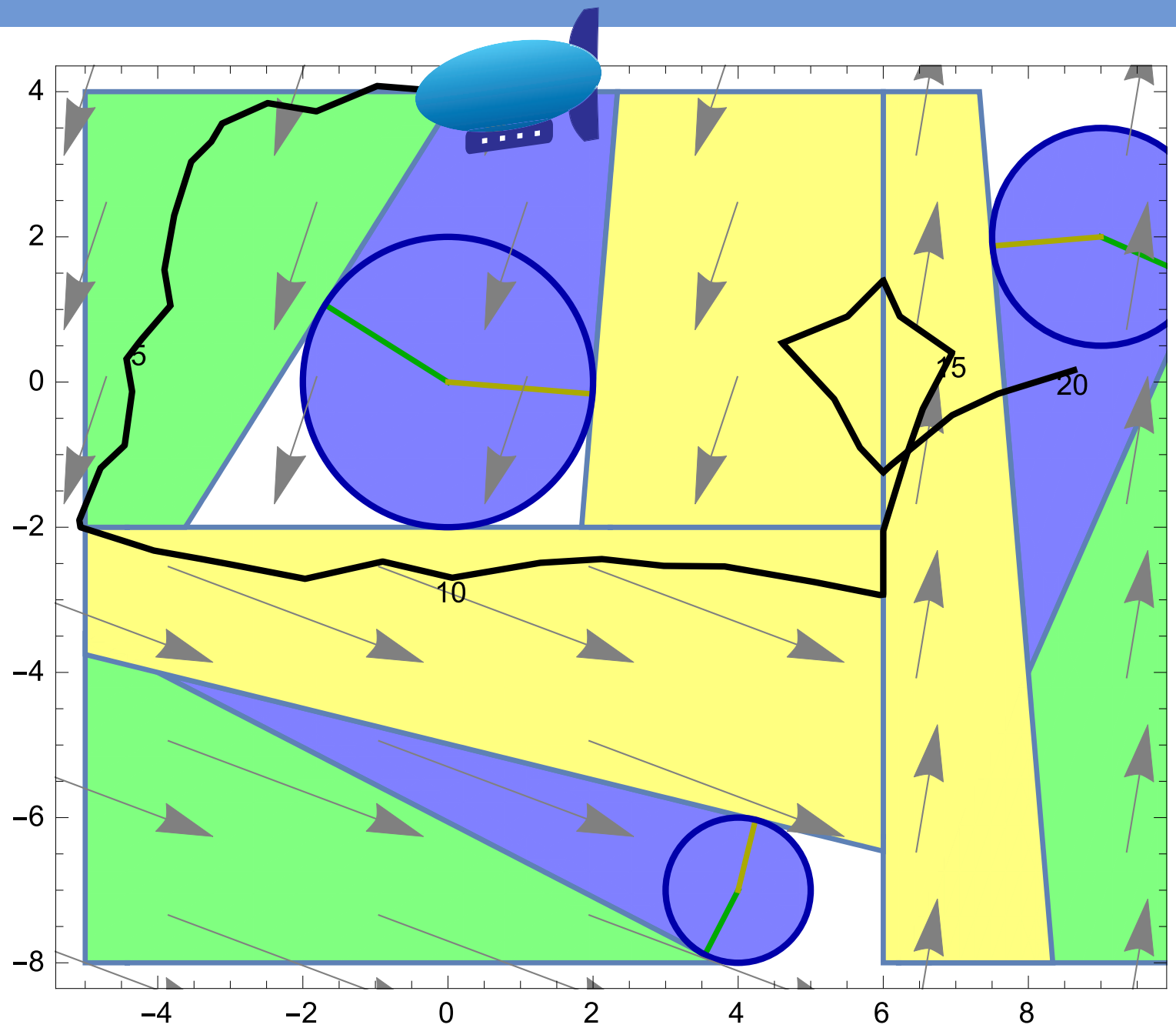
Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

arXiv

Zeppelin Obstacle Parcours



avoid obstacles
changing wind
local turbulence

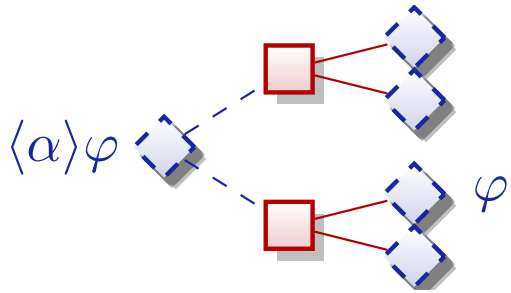
arXiv

Outline

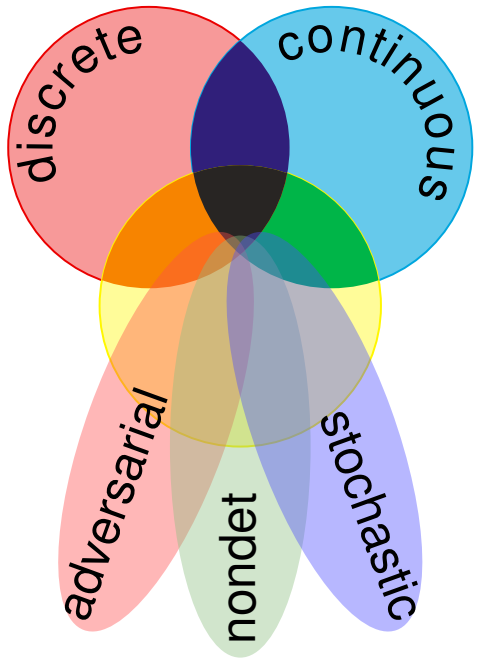
Summary

differential game logic

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



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



Outline

Proving Repetitive Diamonds by Convergence

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

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

Proving Repetitive Diamonds by Convergence

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

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\text{con}\ \frac{\dfrac{\overline{x{\geq}0 \vdash \exists n\, x{<}n{+}1} \quad \overline{x{<}n{+}2 \land n{+}1{>}0 \vdash \langle x := x{-}1\rangle x{<}n{+}1} \quad \overline{\exists n{\leq}0\, x{<}n{+}1 \vdash x{<}1}}{x \geq 0 \vdash \langle (x := x-1)^*\rangle x < 1}}{x \geq 0 \to \langle (x := x-1)^*\rangle x < 1}\ \to\text{R}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\mathbb{R}\frac{\overset{*}{\dfrac{x{\geq}0 \vdash \exists n\, x{<}n{+}1}{\langle:=\rangle}\ \dfrac{\dfrac{}{x{<}n{+}2 \wedge n{+}1{>}0 \vdash x{-}1{<}n{+}1}}{x{<}n{+}2 \wedge n{+}1{>}0 \vdash \langle x := x{-}1\rangle x{<}n{+}1} \quad \dfrac{}{\exists n{\leq}0\, x{<}n{+}1 \vdash x{<}1}}{\text{con}\ \dfrac{x \geq 0 \vdash \langle(x := x-1)^*\rangle x < 1}{\to\text{R}\ \dfrac{}{x \geq 0 \to \langle(x := x-1)^*\rangle x < 1}}}$$

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

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

Proving Repetitive Diamonds by Convergence

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

$v \notin \alpha$

$$\to\mathrm{R}\,\frac{\text{con}\,\dfrac{\mathbb{R}\,\dfrac{*}{x\geq 0 \vdash \exists n\, x<n+1}\langle:=\rangle \dfrac{\mathbb{R}\,\dfrac{*}{x<n+2 \land n+1>0 \vdash x-1<n+1}}{x<n+2 \land n+1>0 \vdash \langle x:=x-1\rangle x<n+1}\ \mathbb{R}\,\dfrac{*}{\exists n{\leq}0\, x<n+1 \vdash x<1}}{x \geq 0 \vdash \langle (x:=x-1)^*\rangle x<1}}{x \geq 0 \to \langle (x:=x-1)^*\rangle x<1}$$

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2016.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps16.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.

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

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.
doi:10.1007/978-3-319-21401-6_32.