Constructive Hybrid Games

Brandon Bohrer and André Platzer

Logical Systems Lab
Computer Science Department
Carnegie Mellon University

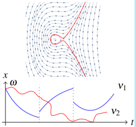
IJCAR'20

Safe Cyber-Physical Systems (CPS)

Hybrid Systems Theorem Proving

$$\Gamma \vdash [a]P$$

$$\Gamma \vdash \langle a \rangle P$$



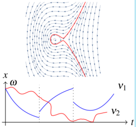
Cyber Physical System

Hybrid Games Model CPS

Hybrid Systems Theorem Proving

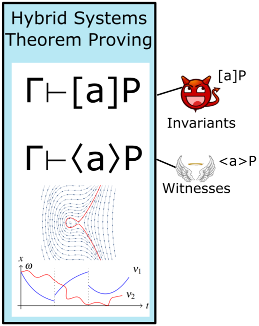
$\Gamma \vdash [a]P$

$\Gamma \vdash \langle a \rangle P$

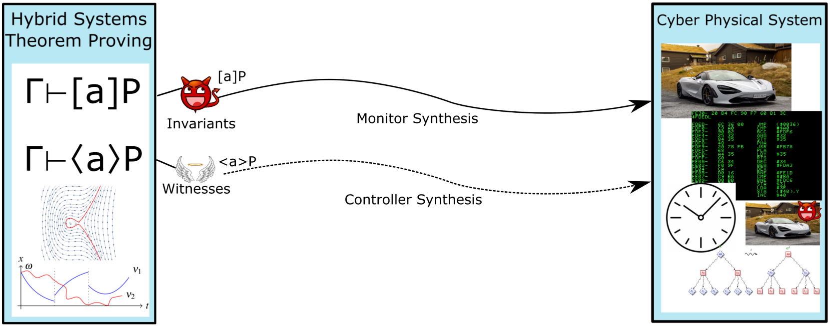


Cyber Physical System

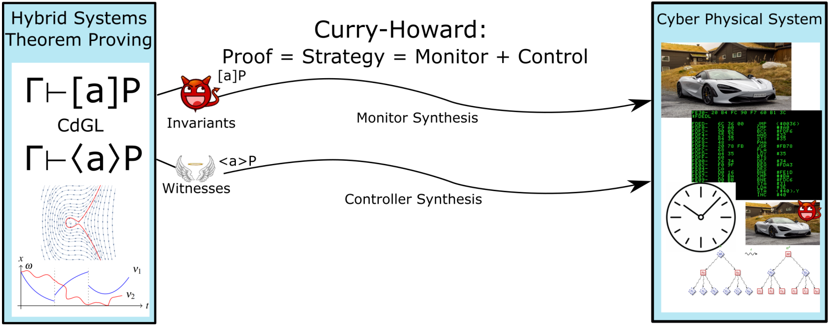
Hybrid Games Model CPS



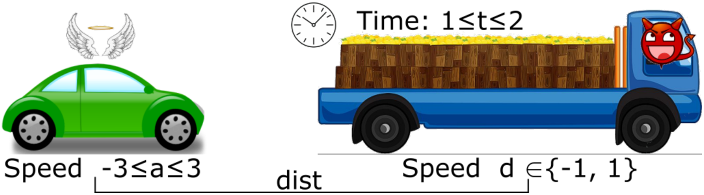
Hybrid Games Model CPS



Constructive Proofs for Synthesis (CdGL)



Game Syntax Example: Tailgating



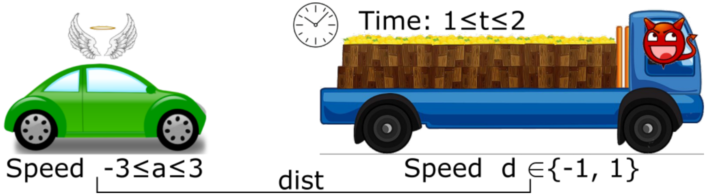
$$\text{actrl} \equiv a := *;\ \ ?(-3 \le a \le 3)$$

$$\text{dctrl} \equiv \{d := 1 \cup d := -1\}^d$$

$$\text{phys} \equiv \{t := 0; \{t' = 1, dist' = d - a \,\&\, t \le 2\}; ?(t \ge 1)\}^d$$

$$\text{game} \equiv \{\text{actrl}; \text{dctrl}; \text{phys}\}^* \text{ or } \{\text{actrl}; \text{dctrl}; \text{phys}\}^\times$$

Game Syntax Example: Tailgating



Pick speed

Within limits

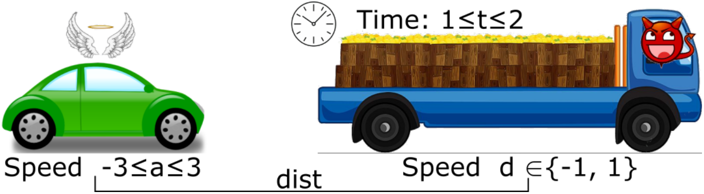
$$\text{actrl} \equiv a := *;\ ?(-3 \le a \le 3)$$

$$\text{dctrl} \equiv \{d := 1 \cup d := -1\}^d$$

$$\text{phys} \equiv \{t := 0; \{t' = 1, dist' = d - a \,\&\, t \le 2\}; ?(t \ge 1)\}^d$$

$$\text{game} \equiv \{\text{actrl}; \text{dctrl}; \text{phys}\}^* \text{ or } \{\text{actrl}; \text{dctrl}; \text{phys}\}^\times$$

Game Syntax Example: Tailgating



Pick speed

Within limits

Demon player

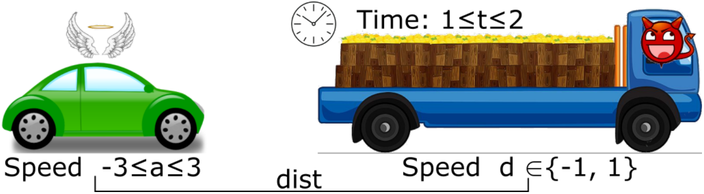
$$\text{actrl} \equiv a := *;\ ?(-3 \le a \le 3)$$

$$\text{dctrl} \equiv \{d := 1 \cup d := -1\}^d$$

$$\text{phys} \equiv \{t := 0; \{t' = 1, dist' = d - a \,\&\, t \le 2\}; ?(t \ge 1)\}^d$$

$$\text{game} \equiv \{\text{actrl}; \text{dctrl}; \text{phys}\}^* \text{ or } \{\text{actrl}; \text{dctrl}; \text{phys}\}^\times$$

Game Syntax Example: Tailgating



Pick speed | Within limits | Demon player

$$\text{actrl} \equiv a := *;\ ?(-3 \leq a \leq 3)$$

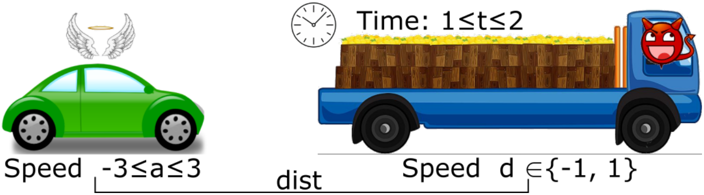
$$\text{dctrl} \equiv \{d := 1 \cup d := -1\}^d$$

$$\text{phys} \equiv \{t := 0; \{t' = 1, dist' = d - a \,\&\, t \leq 2\}; ?(t \geq 1)\}^d$$

Physics | Time constraint | Lower bound

$$\text{game} \equiv \{\text{actrl}; \text{dctrl}; \text{phys}\}^* \text{ or } \{\text{actrl}; \text{dctrl}; \text{phys}\}^\times$$

Game Syntax Example: Tailgating



Pick speed

Within limits

Demon player

$$\text{actrl} \equiv a := *;\ ?(-3 \le a \le 3)$$

$$\text{dctrl} \equiv \{d := 1 \cup d := -1\}^d$$

$$\text{phys} \equiv \{t := 0; \{t' = 1, dist' = d - a \,\&\, t \le 2\}; ?(t \ge 1)\}^d$$

Physics

Time constraint

Lower bound

$$\text{game} \equiv \{\text{actrl}; \text{dctrl}; \text{phys}\}^* \text{ or } \{\text{actrl}; \text{dctrl}; \text{phys}\}^\times$$

Angel or Demon Loop

“Correct” Tailgating

- Formula $P, Q ::= \cdots \mid \langle\alpha\rangle P \mid [\alpha]P$
- Angel or Demon achieves P after game α

$$\text{safety} \equiv \mathit{dist} > 0 \rightarrow \langle \text{game}^{\times} \rangle\, \mathit{dist} > 0$$

Don’t exceed goal

"Correct" Tailgating

- Formula $P, Q ::= \cdots \mid \langle\alpha\rangle P \mid [\alpha]P$
- Angel or Demon achieves P after game α

$$\text{safety} \equiv \mathit{dist} > 0 \rightarrow \langle \text{game}^{\times} \rangle\, \mathit{dist} > 0$$

Don't exceed goal

Figure: Animation of Safe Car

“Correct” Tailgating

- Formula $P, Q ::= \cdots \mid \langle\alpha\rangle P \mid [\alpha]P$
- Angel or Demon achieves P after game α

$$\text{safety} \equiv \mathit{dist} > 0 \rightarrow \langle \text{game}^{\times} \rangle\ \mathit{dist} > 0$$

$$\text{liveness} \equiv \mathit{dist} > 0 \rightarrow \langle \text{game}^{*} \rangle\ \mathit{dist} \leq \epsilon$$

Don’t exceed goal

Reach goal

"Correct" Tailgating

- Formula $P, Q ::= \cdots \mid \langle\alpha\rangle P \mid [\alpha]P$
- Angel or Demon achieves P after game α

$$\text{safety} \equiv dist > 0 \rightarrow \langle \text{game}^{\times} \rangle\, dist > 0$$

Don't exceed goal

$$\text{liveness} \equiv dist > 0 \rightarrow \langle \text{game}^{*} \rangle\, dist \leq \epsilon$$

Reach goal

$$\text{reachAvoid} \equiv dist > 0 \rightarrow \langle \{\text{game}; ?dist > 0\}^{*} \rangle dist \leq \epsilon$$

Reach safely

Constructive Foundations: What's New?

- What do constructive modalities $\langle\alpha\rangle P$ and $[\alpha]P$ mean?
- **Challenge:** Strategies must be *constructive* $\rightsquigarrow$ Types
- **Challenge:** Games both stronger and weaker (quantifier alternation, subnormal)

Constructive Foundations: What's New?

- What do constructive modalities $\langle\alpha\rangle P$ and $[\alpha]P$ mean?
- **Challenge:** Strategies must be *constructive* $\rightsquigarrow$ Types
- **Challenge:** Games both stronger and weaker (quantifier alternation, subnormal)

$$\text{K} \quad [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q) \quad \text{vs.} \quad \text{M} \quad \frac{P \vdash Q}{[\alpha]P \vdash [\alpha]Q}$$

Constructive Foundations: What's New?

- What do constructive modalities $\langle\alpha\rangle P$ and $[\alpha]P$ mean?
- **Challenge:** Strategies must be *constructive* $\rightsquigarrow$ Types
- **Challenge:** Games both stronger and weaker (quantifier alternation, subnormal)

$$\text{K} \quad [\alpha](P \to Q) \to ([\alpha]P \to [\alpha]Q) \quad \text{vs.} \quad \text{M} \quad \frac{P \vdash Q}{[\alpha]P \vdash [\alpha]Q}$$

- How do other proof rules change? $\rightsquigarrow$ Most don't!
- Real arithmetic $\rightsquigarrow$ *Constructive* real arithmetic
- Excluded middle $\rightsquigarrow$ Compare-with-epsilon

$$\text{cmp} \quad \epsilon > 0 \to (f > g \lor f < g + \epsilon)$$

Angel and Demon are Dual (Examples)

$$\ulcorner P \urcorner \quad : (\text{state} \Rightarrow \text{type})$$

$$\ulcorner \langle ?Q \rangle P \urcorner\ s \quad = \ulcorner Q \urcorner\ s * \ulcorner P \urcorner\ s$$

Prove test

$$\ulcorner [?Q] P \urcorner\ s \quad = \ulcorner Q \urcorner\ s \Rightarrow \ulcorner P \urcorner\ s$$

Assume test

Angel and Demon are Dual (Examples)

$$\ulcorner P \urcorner \quad : (\text{state} \Rightarrow \text{type})$$

$$\ulcorner \langle ?Q \rangle P \urcorner\ s \quad = \ulcorner Q \urcorner\ s * \ulcorner P \urcorner\ s$$

$$\ulcorner \langle x := * \rangle P \urcorner\ s \quad = \Sigma v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set } s\ x\ v)$$

Prove test

Choose x

$$\ulcorner [?Q] P \urcorner\ s \quad = \ulcorner Q \urcorner\ s \Rightarrow \ulcorner P \urcorner\ s$$

$$\ulcorner [x := *] P \urcorner\ s \quad = \Pi v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set } s\ x\ v)$$

Assume test

Receive x

Angel and Demon are Dual (Examples)

$$\ulcorner P \urcorner \quad : (\text{state} \Rightarrow \text{type})$$

$$\ulcorner \langle ?Q \rangle P \urcorner\ s = \ulcorner Q \urcorner\ s * \ulcorner P \urcorner\ s$$ — Prove test

$$\ulcorner \langle x := * \rangle P \urcorner\ s = \Sigma v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set}\ s\ x\ v)$$ — Choose x

$$\ulcorner \langle \alpha \cup \beta \rangle P \urcorner\ s = \ulcorner \langle \alpha \rangle P \urcorner\ s + \ulcorner \langle \beta \rangle P \urcorner\ s$$ — Choose branch

$$\ulcorner [?Q] P \urcorner\ s = \ulcorner Q \urcorner\ s \Rightarrow \ulcorner P \urcorner\ s$$ — Assume test

$$\ulcorner [x := *] P \urcorner\ s = \Pi v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set}\ s\ x\ v)$$ — Receive x

$$\ulcorner [\alpha \cup \beta] P \urcorner\ s = \ulcorner [\alpha] P \urcorner\ s * \ulcorner [\beta] P \urcorner\ s$$ — Can't choose

Angel and Demon are Dual (Examples)

$$\ulcorner P \urcorner \quad : (\text{state} \Rightarrow \text{type})$$

$$\ulcorner \langle ?Q \rangle P \urcorner\ s = \ulcorner Q \urcorner\ s * \ulcorner P \urcorner\ s$$ — Prove test

$$\ulcorner \langle x := * \rangle P \urcorner\ s = \Sigma v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set } s\ x\ v)$$ — Choose x

$$\ulcorner \langle \alpha \cup \beta \rangle P \urcorner\ s = \ulcorner \langle \alpha \rangle P \urcorner\ s + \ulcorner \langle \beta \rangle P \urcorner\ s$$ — Choose branch

$$\ulcorner \langle \alpha^d \rangle P \urcorner\ s = \ulcorner [\alpha] P\ s \urcorner$$ — Switch

$$\ulcorner [?Q] P \urcorner\ s = \ulcorner Q \urcorner\ s \Rightarrow \ulcorner P \urcorner\ s$$ — Assume test

$$\ulcorner [x := *] P \urcorner\ s = \Pi v : \mathbb{R}.\ \ulcorner P \urcorner\ (\text{set } s\ x\ v)$$ — Receive x

$$\ulcorner [\alpha \cup \beta] P \urcorner\ s = \ulcorner [\alpha] P \urcorner\ s * \ulcorner [\beta] P \urcorner\ s$$ — Can't choose

$$\ulcorner [\alpha^d] P \urcorner\ s = \ulcorner \langle \alpha \rangle P \urcorner\ s$$ — Switch

Angel and Demon are Dual (Examples)

$$\ulcorner P \urcorner \quad : (\text{state} \Rightarrow \text{type})$$

$$\ulcorner \langle ?Q \rangle P \urcorner \; s \quad = \ulcorner Q \urcorner \; s * \ulcorner P \urcorner \; s$$
Prove test

$$\ulcorner \langle x := * \rangle P \urcorner \; s \quad = \Sigma v : \mathbb{R}. \; \ulcorner P \urcorner \; (\text{set } s \; x \; v)$$
Choose x

$$\ulcorner \langle \alpha \cup \beta \rangle P \urcorner \; s \quad = \ulcorner \langle \alpha \rangle P \urcorner \; s + \ulcorner \langle \beta \rangle P \urcorner \; s$$
Choose branch

$$\ulcorner \langle \alpha^d \rangle P \urcorner \; s \quad = \ulcorner [\alpha] P \; s \urcorner$$
Switch

$$\ulcorner [?Q] P \urcorner \; s \quad = \ulcorner Q \urcorner \; s \Rightarrow \ulcorner P \urcorner \; s$$
Assume test

$$\ulcorner [x := *] P \urcorner \; s \quad = \Pi v : \mathbb{R}. \ulcorner P \urcorner \; (\text{set } s \; x \; v)$$
Receive x

$$\ulcorner [\alpha \cup \beta] P \urcorner \; s \quad = \ulcorner [\alpha] P \urcorner \; s * \ulcorner [\beta] P \urcorner \; s$$
Can't choose

$$\ulcorner [\alpha^d] P \urcorner \; s \quad = \ulcorner \langle \alpha \rangle P \urcorner \; s$$
Switch

Lemma (Existential Property)

If $(\Gamma \vdash \exists x \, p(x))$ is valid, there exist term f such that $(\Gamma \vdash p(f))$ is valid.

Natural Deduction Proofs (Selected)

- Want Curry-Howard $\rightsquigarrow$ Natural Deduction
- Implemented as Scala prototype

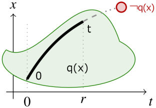
$$[;]\mathrm{I} \quad \frac{\Gamma \vdash [\alpha][\beta]P}{\Gamma \vdash [\alpha;\beta]P}$$

$$[:=]\mathrm{I} \quad \frac{\Gamma \vdash p(f)}{\Gamma \vdash [x := f]p(x)}$$

$$[*]\mathrm{I} \quad \frac{\Gamma \vdash J \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P}$$

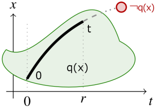
Differential Equation Proofs (Selected)

$$[']\quad \frac{\Gamma \vdash \forall t{:}\mathbb{R}_{\geq 0}\ \forall r{:}[0,t]\ q(sol(r)) \to p(sol(t))}{\Gamma \vdash [x'=f \ \&\ q(x)]p(x)}$$

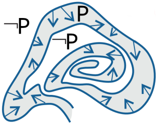


Differential Equation Proofs (Selected)

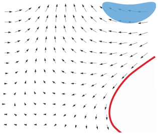
$$[']\quad \frac{\Gamma \vdash \forall t : \mathbb{R}_{\geq 0}\ \forall r : [0, t]\ \ q(sol(r)) \rightarrow p(sol(t))}{\Gamma \vdash [x' = f \,\&\, q(x)]p(x)}$$



$$\mathrm{DI}\quad \frac{\Gamma \vdash P \qquad \Gamma \vdash \forall x\, (Q \rightarrow [x' := f](P)')}{\Gamma \vdash [x' = f \,\&\, Q]P}$$



$$\mathrm{DC}\quad \frac{\Gamma \vdash [x' = f \,\&\, Q]R \qquad \Gamma \vdash [x' = f \,\&\, Q \land R]P}{\Gamma \vdash [x' = f \,\&\, Q]P}$$



Theorem (Soundness)

If $\Gamma \vdash P$ is provable, then sequent $(\Gamma \vdash P)$ is valid.

Operational Semantics

- **Ultimate Goal:** Compile proofs to control + monitor
- **First Step:** Interpret Angel proof against Demon environment

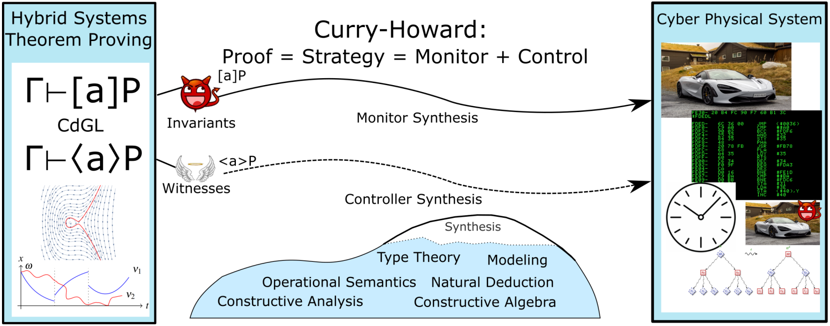
$$\mathsf{play}_\alpha \quad : \ulcorner\langle\alpha\rangle P\urcorner\ s \Rightarrow \ulcorner[\alpha]Q\urcorner\ s \Rightarrow \Sigma t : \mathsf{state}.\ P\ t * Q\ t$$

$\mathsf{play}_{?R}$	(A, B)	$(\lambda p : (\ulcorner R\urcorner\ s).\ C)$	$s = (s, (B, C^A_p))$
$\mathsf{play}_{x:=*}$	(f, A)	$(\lambda v : \mathbb{R}.\ B)$	$s = (\mathsf{set}\ s\ x\ f, (A, B^f_v))$
$\mathsf{play}_{\alpha\cup\beta}$	$(\ell \cdot A)$	(B, C)	$s = \mathsf{play}_\alpha\ s\ A\ B$
$\mathsf{play}_{\alpha\cup\beta}$	$(r \cdot A)$	(B, C)	$s = \mathsf{play}_\beta\ s\ A\ C$
play_{α^d}	A	B	$s = \mathsf{play}_\alpha\ s\ B\ A$

Theorem (Consistency)

Formulas $\ulcorner\langle\alpha\rangle P\urcorner\ s$ *and* $\ulcorner[\alpha]\neg P\urcorner\ s$ *are not both inhabited.*

Conclusion


Hybrid Systems Theorem Proving
Γ⊢[a]P
CdGL
Γ⊢⟨a⟩P
Curry-Howard:
Proof = Strategy = Monitor + Control
[a]P
Invariants
Monitor Synthesis
<a>P
Witnesses
Controller Synthesis
Synthesis
Type Theory
Modeling
Operational Semantics
Natural Deduction
Constructive Analysis
Constructive Algebra
Cyber Physical System