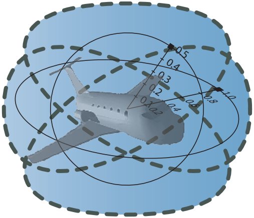
18: Winning & Proving Hybrid Games

15-424: Foundations of Cyber-Physical Systems

André Platzer

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

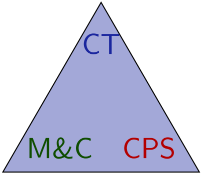


Outline

Outline

1. Learning Objectives
2. Semantical Considerations
   - Determinacy & Monotonicity
3. Dynamic Axioms for Hybrid Games
   - Hybrid Game Axioms
   - Example Proof: Demon's Choice
4. Repetitions
   - Proofs for Loops
   - Example Proof: Dual Filibuster
   - Example Proof: Push-around Cart
5. Summary

rigorous reasoning for adversarial dynamics
compositional reasoning from compositional semantics
modular addition of adversarial dynamics
axiomatization of dGL



analytical&semantical interaction
discrete+continuous+adversarial

CPS semantics
align semantics&reasoning
operational CPS effects

Outline

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)

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

All Reals | Some Reals | Angel Wins | Demon Wins

TOCL'15

Differential Game Logic: Denotational Semantics

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

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

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

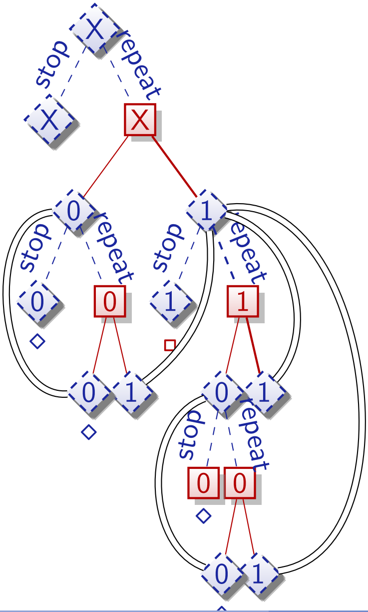
$$
\begin{aligned}
[\![e_1 \geq e_2]\!] &= \{\omega \in \mathcal{S} \;:\; \omega[\![e_1]\!] \geq \omega[\![e_2]\!]\} \\
[\![\neg P]\!] &= ([\![P]\!])^\complement \\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle\alpha\rangle P]\!] &= \varsigma_\alpha([\![P]\!]) \\
[\![[\alpha]P]\!] &=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

Differential Game Logic: Axiomatization

TOCL'15

$\langle(x := 0 \cap x := 1)^*\rangle x = 0$

$\overset{\text{wfd}}{\rightsquigarrow}$ false unless $x = 0$



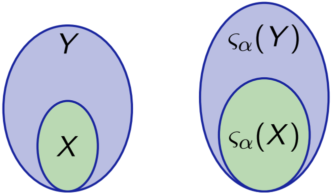
Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

Lemma (Monotonicity)

$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y)$ *and* $\delta_\alpha(X) \subseteq \delta_\alpha(Y)$ *for all* $X \subseteq Y$



Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

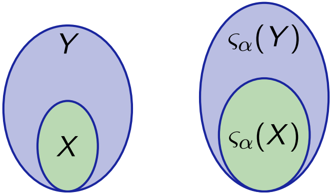
Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

Corollary

Determined: At least one player wins: $\neg\langle\alpha\rangle\neg P \rightarrow [\alpha]P$ *so* $\langle\alpha\rangle\neg P \vee [\alpha]P$
Consistent: At most one player wins: $[\alpha]P \rightarrow \neg\langle\alpha\rangle P$ *so* $\neg([\alpha]P \wedge \langle\alpha\rangle\neg P)$

Lemma (Monotonicity)

$$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y) \text{ and } \delta_\alpha(X) \subseteq \delta_\alpha(Y) \text{ for all } X \subseteq Y$$



Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

Proof Sketch.

$\varsigma_{\alpha\cup\beta}(X^\complement)^\complement = (\varsigma_\alpha(X^\complement) \cup \varsigma_\beta(X^\complement))^\complement = \varsigma_\alpha(X^\complement)^\complement \cap \varsigma_\beta(X^\complement)^\complement = \delta_\alpha(X) \cap \delta_\beta(X) = \delta_{\alpha\cup\beta}(X)$ □

Lemma (Monotonicity)

$$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y) \textit{ and } \delta_\alpha(X) \subseteq \delta_\alpha(Y) \textit{ for all } X \subseteq Y$$

Proof Sketch.

$X \subseteq Y$ so $X^\complement \supseteq Y^\complement$ so $\varsigma_\alpha(X^\complement) \supseteq \varsigma_\alpha(Y^\complement)$ so
$\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement \subseteq (\varsigma_\alpha(Y^\complement))^\complement = \varsigma_{\alpha^d}(Y)$. □

Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

Lemma (Monotonicity)

$$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y) \textit{ and } \delta_\alpha(X) \subseteq \delta_\alpha(Y) \textit{ for all } X \subseteq Y$$

Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

Hybrid games are consistent and determined, i.e. $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

Corollary (Axiom: Determinacy)

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

Lemma (Monotonicity)

$$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y) \text{ and } \delta_\alpha(X) \subseteq \delta_\alpha(Y) \text{ for all } X \subseteq Y$$

Corollary (Rule: Monotonicity)

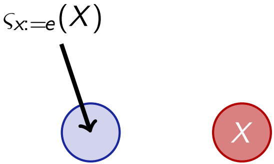
$$M \quad \frac{P \rightarrow Q}{\langle\alpha\rangle P \rightarrow \langle\alpha\rangle Q}$$

Outline

Hybrid Game Axioms

Axiom (Assignment) TOCL'15

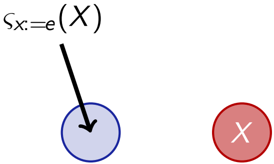
$\langle :=\rangle \quad \langle x := e\rangle p(x) \leftrightarrow$



Hybrid Game Axioms

Axiom (Assignment) TOCL'15

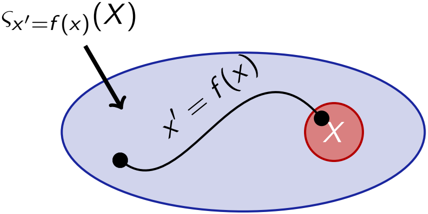
$\langle := \rangle \quad \langle x := e \rangle p(x) \leftrightarrow p(e)$



Hybrid Game Axioms

Axiom (Differential Equation) TOCL'15

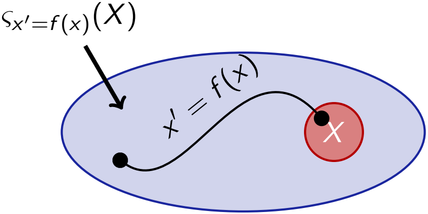
$\langle ' \rangle \quad \langle x' = f(x) \rangle P \leftrightarrow \qquad (y'(t) = f(y))$



Hybrid Game Axioms

Axiom (Differential Equation) TOCL'15

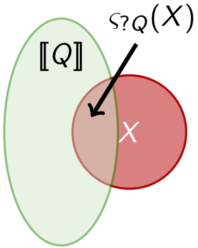
$\langle ' \rangle \quad \langle x' = f(x) \rangle P \leftrightarrow \exists t{\geq}0\, \langle x := y(t) \rangle P \qquad (y'(t) = f(y))$



Hybrid Game Axioms

Axiom (Test / Challenge) TOCL'15

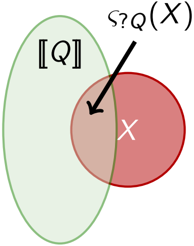
$\langle ? \rangle \quad \langle ?Q \rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Test / Challenge) TOCL'15

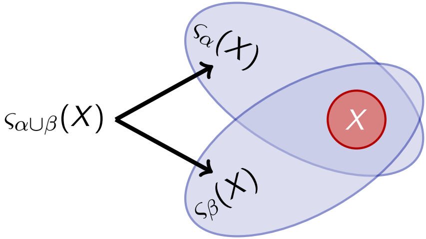
$\langle ? \rangle \quad \langle ?Q \rangle P \leftrightarrow (Q \land P)$



Hybrid Game Axioms

Axiom (Choice Game) TOCL'15

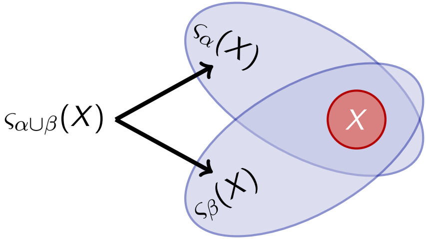
$\langle\cup\rangle \quad \langle\alpha \cup \beta\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Choice Game) TOCL'15

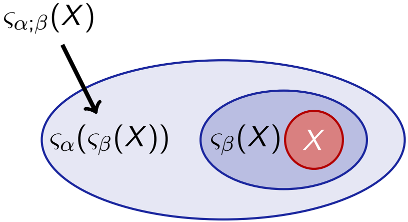
$\langle\cup\rangle \quad \langle \alpha \cup \beta \rangle P \leftrightarrow \langle \alpha \rangle P \lor \langle \beta \rangle P$



Hybrid Game Axioms

Axiom (Sequential Game) TOCL'15

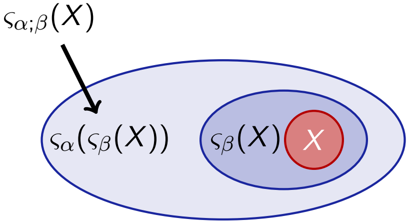
$\langle;\rangle \quad \langle\alpha;\beta\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Sequential Game) TOCL'15

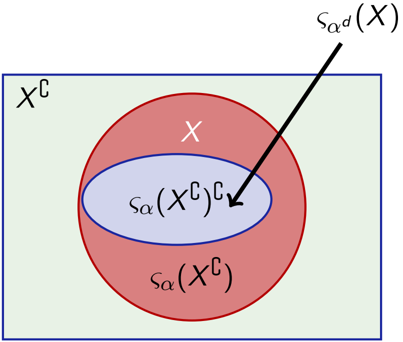
$\langle ; \rangle \quad \langle \alpha; \beta \rangle P \leftrightarrow \langle \alpha \rangle \langle \beta \rangle P$



Hybrid Game Axioms

Axiom (Dual Game) TOCL'15

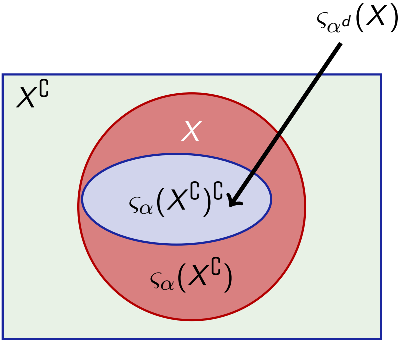
$\langle^d\rangle \quad \langle\alpha^d\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Dual Game) TOCL'15

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



Example: Demon's Choice Derives by Duality

$$\frac{}{\vdash \langle \alpha \cap \beta \rangle P \leftrightarrow \langle \alpha \rangle P \land \langle \beta \rangle P}$$

Example: Demon's Choice Derives by Duality

$$\langle^d\rangle \dfrac{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}$$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\langle\cup\rangle\;\overline{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\langle^d\rangle\;\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}$$

Example: Demon's Choice Derives by Duality

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \neg(\langle\alpha^d\rangle\neg P \lor \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}
$$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \neg(\neg\langle\alpha\rangle\neg\neg P \lor \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\langle\alpha^d\rangle\neg P \lor \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle$$

$$\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\vdash \langle\alpha\rangle P \land \langle\beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\neg\langle\alpha\rangle\neg\neg P \lor \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\langle\alpha^d\rangle\neg P \lor \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}$$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \langle\alpha\rangle P \land \langle\beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\neg\langle\alpha\rangle\neg\neg P \lor \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\langle\alpha^d\rangle\neg P \lor \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}$$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \langle\alpha\rangle P \land \langle\beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\neg\langle\alpha\rangle\neg\neg P \lor \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}}{\vdash \neg(\langle\alpha^d\rangle\neg P \lor \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}\langle^d\rangle}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P}$$

Note: Can now use this derived axiom

$$\langle\cap\rangle \quad \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$$

Example: Demon's Choice Derives by Duality

$$[\cdot]\ \frac{}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Example: Demon's Choice Derives by Duality

$$\langle\cap\rangle \frac{}{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}$$
$$[\cdot] \frac{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Example: Demon's Choice Derives by Duality

$$
\langle\cap\rangle\,[\cdot]\;
\dfrac{\dfrac{\overline{\vdash \neg(\langle\alpha\rangle\neg P \land \langle\beta\rangle\neg P) \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}
$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Example: Demon's Choice Derives by Duality

$$
\dfrac{\dfrac{\dfrac{\overline{\vdash \neg\langle\alpha\rangle\neg P \lor \neg\langle\beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\;[\cdot]}{\vdash \neg(\langle\alpha\rangle\neg P \land \langle\beta\rangle\neg P) \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\;\langle\cap\rangle}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}\;[\cdot]
$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Example: Demon's Choice Derives by Duality

$$
\dfrac{\dfrac{\dfrac{\dfrac{\vdash [\alpha]P \lor [\beta]P \leftrightarrow [\alpha]P \lor [\beta]P}{\vdash \neg\langle\alpha\rangle\neg P \lor \neg\langle\beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\,[\cdot]}{\vdash \neg(\langle\alpha\rangle\neg P \land \langle\beta\rangle\neg P) \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\,\langle\cap\rangle}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}\,[\cdot]
$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Example: Demon's Choice Derives by Duality

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash [\alpha]P \lor [\beta]P \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash \neg\langle\alpha\rangle\neg P \lor \neg\langle\beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\,[\cdot]}{\vdash \neg(\langle\alpha\rangle\neg P \land \langle\beta\rangle\neg P) \leftrightarrow [\alpha]P \lor [\beta]P}}{\vdash \neg\langle\alpha \cap \beta\rangle\neg P \leftrightarrow [\alpha]P \lor [\beta]P}\,\langle\cap\rangle}{\vdash [\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P}\,[\cdot]$$

This proof derives $[\cap]$ from $\langle\cap\rangle$

$[\cap]$ $[\alpha \cap \beta]P \leftrightarrow [\alpha]P \lor [\beta]P$

$\langle\cap\rangle$ $\langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P$

Differential Game Logic: Axiomatization

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

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

$\langle'\rangle$ $\langle x' = f(x)\rangle P \leftrightarrow$

$\langle?\rangle$ $\langle ?Q\rangle P \leftrightarrow$

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

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

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

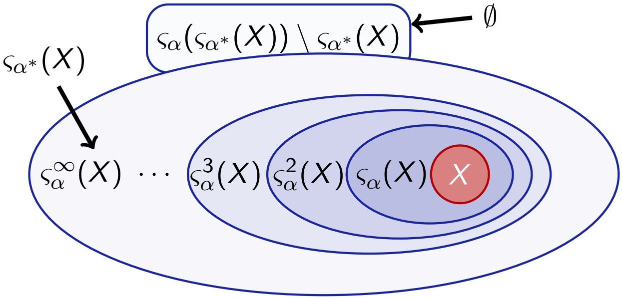
$\langle^d\rangle$ $\langle\alpha^d\rangle P \leftrightarrow$

TOCL'15

Outline

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ :\ X \cup \varsigma_\alpha(Z) = Z\}$$



Proofs for Loops

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \;:\; X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Proofs for Loops

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ : \ X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Corollary (Axiom:)

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

Proofs for Loops

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ : \ X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Corollary (Axiom: Iteration)

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

Proofs for Loops

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ : \ X \cup \varsigma_\alpha(Z) \subseteq Z\}$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Corollary (Axiom: Iteration)

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

Corollary (Rule:)

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

Proofs for Loops

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ : \ X \cup \varsigma_\alpha(Z) \subseteq Z\}$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Corollary (Axiom: Iteration)

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

Corollary (Rule: Least Fixpoint)

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

Corollary (Derived Rule:)

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

Proofs for Loops

Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \;:\; X \cup \varsigma_\alpha(Z) \subseteq Z\}$$

$$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$$

Corollary (Axiom: Iteration)

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

Corollary (Rule: Least Fixpoint)

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

Corollary (Derived Rule: Loop)

$$loop \quad \frac{P \rightarrow [\alpha]P}{P \rightarrow [\alpha^*]P}$$

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

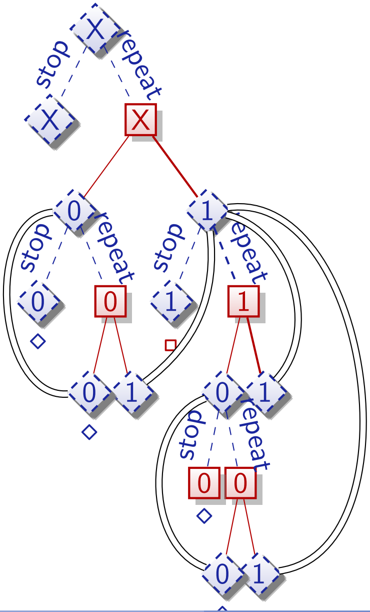
$$\text{FP}\quad \frac{P \lor \langle\alpha\rangle Q \rightarrow Q}{\langle\alpha^*\rangle P \rightarrow Q}$$

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

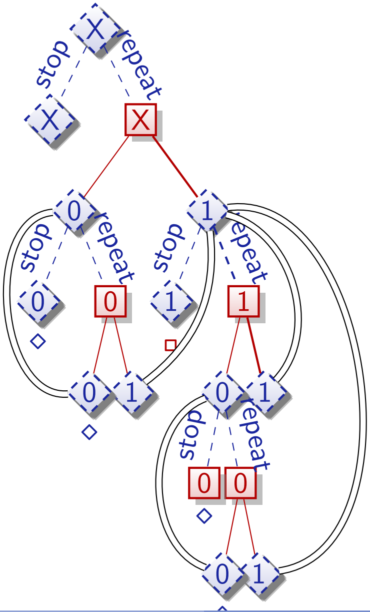
$$\forall\quad \frac{p \rightarrow Q}{p \rightarrow \forall x\, Q} \qquad (x \notin \text{FV}(p))$$

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

TOCL'15



$$\langle^d\rangle \frac{}{x = 0 \vdash \langle (x := 0 \cup x := 1)^\times \rangle x = 0}$$

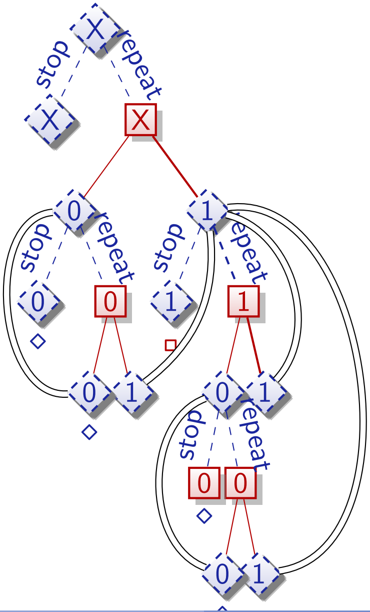


$$\text{ind}\ \frac{x = 0 \vdash [(x := 0 \cap x := 1)^*]x = 0}{x = 0 \vdash \langle (x := 0 \cup x := 1)^{\times} \rangle x = 0}\ \langle^d\rangle$$

Example Proof: Dual Filibuster

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

([·], ind, $\langle^d\rangle$)



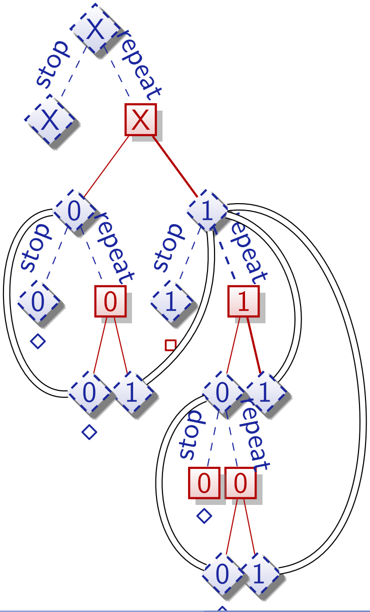
Example Proof: Dual Filibuster

$$\langle^d\rangle \quad \overline{x = 0 \vdash \neg\langle x := 0 \cap x := 1\rangle \neg x = 0}$$

$$[\cdot] \quad \overline{x = 0 \vdash [x := 0 \cap x := 1] x = 0}$$

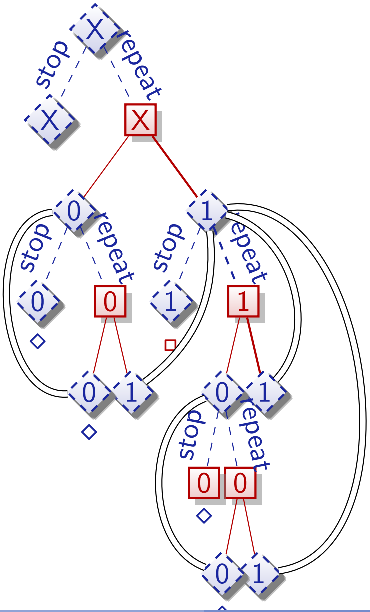
$$\text{ind} \quad \overline{x = 0 \vdash [(x := 0 \cap x := 1)^*] x = 0}$$

$$\langle^d\rangle \quad \overline{x = 0 \vdash \langle (x := 0 \cup x := 1)^\times \rangle x = 0}$$



Example Proof: Dual Filibuster

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



Example Proof: Dual Filibuster

$$\langle:=\rangle \quad x=0 \vdash \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0$$

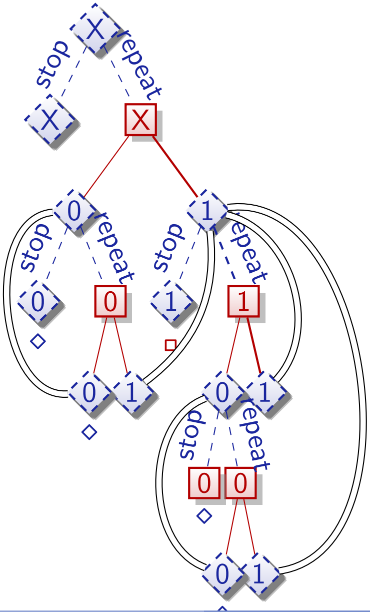
$$\langle\cup\rangle \quad x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0$$

$$\langle^d\rangle \quad x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle \neg x=0$$

$$[\cdot] \quad x=0 \vdash [x:=0 \cap x:=1] x=0$$

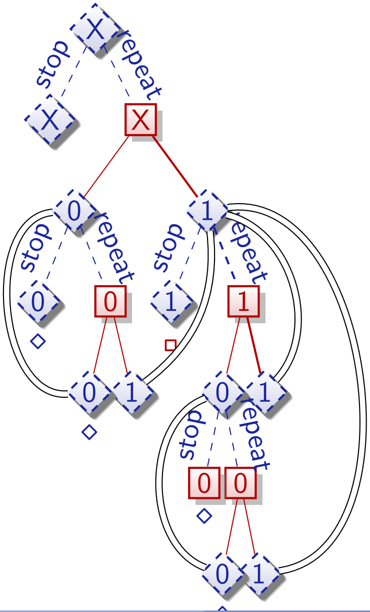
$$\text{ind} \quad x=0 \vdash [(x:=0 \cap x:=1)^*] x=0$$

$$\langle^d\rangle \quad x=0 \vdash \langle (x:=0 \cup x:=1)^\times \rangle x=0$$



Example Proof: Dual Filibuster

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



Example Proof: Dual Filibuster

$$*$$

$\mathbb{R}$ $\quad x = 0 \vdash 0 = 0 \lor 1 = 0$

$\langle := \rangle$ $\quad x = 0 \vdash \langle x := 0 \rangle x = 0 \lor \langle x := 1 \rangle x = 0$

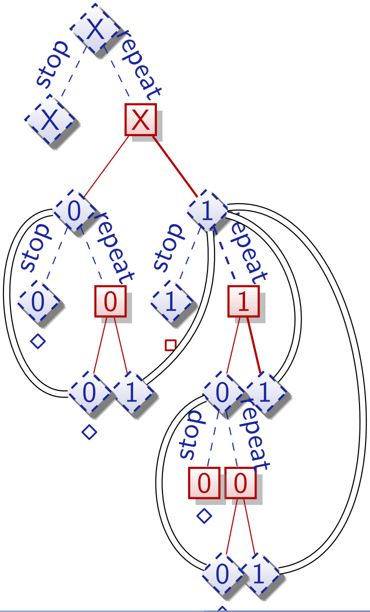
$\langle \cup \rangle$ $\quad x = 0 \vdash \langle x := 0 \cup x := 1 \rangle x = 0$

$\langle ^d \rangle$ $\quad x = 0 \vdash \neg \langle x := 0 \cap x := 1 \rangle \neg x = 0$

$[\cdot]$ $\quad x = 0 \vdash [x := 0 \cap x := 1] x = 0$

ind $\quad x = 0 \vdash [(x := 0 \cap x := 1)^*] x = 0$

$\langle ^d \rangle$ $\quad x = 0 \vdash \langle (x := 0 \cup x := 1)^\times \rangle x = 0$



Example Proof: Push-around Cart

$$\text{ind}\ \frac{}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}$$

Example Proof: Push-around Cart

$$\text{[;]}\ \frac{}{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}$$

$$\text{ind}\ \frac{}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}$$

Example Proof: Push-around Cart

$$\begin{array}{ll} [\cap] & \overline{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J} \\ [;] & \overline{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J} \\ \text{ind} & \overline{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq} \end{array}$$

Example Proof: Push-around Cart

$$\vee R,WR \dfrac{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \vee [d := -1] \ldots}{}$$

$$[\cap] \dfrac{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}{}$$

$$[;] \dfrac{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}{}$$

$$\text{ind} \dfrac{}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\ [:=]}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \vee [d := -1] \dots}\ \vee R, WR}{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\ [\cap]}{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\ [;]}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}\ \text{ind}
$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a + 1\}]J}\;[;]}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\;[:=]}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \vee [d := -1] \ldots}\;\vee\text{R,WR}}{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\;[\cap]}{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}\;[;]}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}\;\text{ind}
$$

Example Proof: Push-around Cart

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [a := 1 \cup a := -1][\{x' = v, v' = a+1\}]J}}{J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a+1\}]J}[\cup]}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a+d\}]J}[;]}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a+d\}]J \lor [d := -1]\dots}[:=]}{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a+d\}]J}\lor R, WR}{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a+d\}]J}[\cap]}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a+d\}\big)^*]x \geq}[;]$$

ind

Example Proof: Push-around Cart

$$\text{[:=]}\quad J \vdash [a := 1][\{x' = v, v' = a + 1\}]J \land [a := -1][\{x' = v, v' = a + 1\}]J$$

$$[\cup]\quad J \vdash [a := 1 \cup a := -1][\{x' = v, v' = a + 1\}]J$$

$$[;]\quad J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a + 1\}]J$$

$$\text{[:=]}\quad J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$$\lor\text{R,WR}\quad J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \lor [d := -1]\ldots$$

$$[\cap]\quad J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$$[;]\quad J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$$\text{ind}\quad J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq$$

Example Proof: Push-around Cart

$$J \vdash [\{x' = v, v' = 1 + 1\}]J \land [\{x' = v, v' = -1 + 1\}]J$$

$[:=]$ $$J \vdash [a := 1][\{x' = v, v' = a + 1\}]J \land [a := -1][\{x' = v, v' = a + 1\}]J$$

$[\cup]$ $$J \vdash [a := 1 \cup a := -1][\{x' = v, v' = a + 1\}]J$$

$[;]$ $$J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a + 1\}]J$$

$[:=]$ $$J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$\lor$R,WR $$J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \lor [d := -1] \ldots$$

$[\cap]$ $$J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$[;]$ $$J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

ind $$J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq$$

Example Proof: Push-around Cart

$$J \vdash [\{x' = v, v' = 1 + 1\}]J \wedge [\{x' = v, v' = -1 + 1\}]J$$

$[:=]$
$$J \vdash [a := 1][\{x' = v, v' = a + 1\}]J \wedge [a := -1][\{x' = v, v' = a + 1\}]J$$

$[\cup]$
$$J \vdash [a := 1 \cup a := -1][\{x' = v, v' = a + 1\}]J$$

$[;]$
$$J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a + 1\}]J$$

$[:=]$
$$J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$\vee$R,WR
$$J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \vee [d := -1] \dots$$

$[\cap]$
$$J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

$[;]$
$$J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J$$

ind
$$J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq$$

$$J \stackrel{\text{def}}{\equiv} x \geq 0 \wedge v \geq 0$$

Example Proof: Push-around Cart

$$
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
J \vdash [\{x' = v, v' = 1 + 1\}]J \land [\{x' = v, v' = -1 + 1\}]J
}{J \vdash [a := 1][\{x' = v, v' = a + 1\}]J \land [a := -1][\{x' = v, v' = a + 1\}]J}[:=]
}{J \vdash [a := 1 \cup a := -1][\{x' = v, v' = a + 1\}]J}[\cup]
}{J \vdash [(a := 1 \cup a := -1); \{x' = v, v' = a + 1\}]J}[;]
}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}[:=]
}{J \vdash [d := 1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J \lor [d := -1] \dots}\lor R, WR
}{J \vdash [d := 1 \cap d := -1][(a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}[\cap]
}{J \vdash [(d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}]J}[;]
}{J \vdash [\big((d := 1 \cap d := -1); (a := 1 \cup a := -1); \{x' = v, v' = a + d\}\big)^*]x \geq}\text{ind}
$$

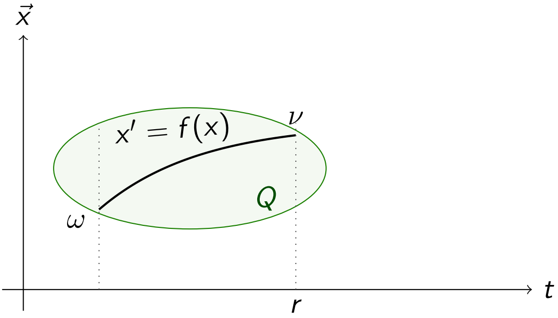
$$J \overset{\text{def}}{\equiv} x \geq 0 \land v \geq 0$$

$$
{[']},[:=]\ \frac{x \geq 0 \land v \geq 0 \vdash \forall t {\geq} 0 \, (x + vt + t^2 \geq 0 \land v + 2t \geq 0)}{J \vdash [\{x' = v, v' = 1 + 1\}]J}
$$

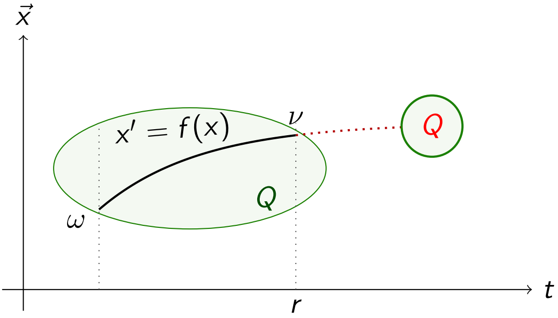
$$
{[']},[:=]\ \frac{x \geq 0 \land v \geq 0 \vdash \forall t {\geq} 0 \, (x + vt \geq 0 \land v \geq 0)}{J \vdash [\{x' = v, v' = 0\}]J}
$$

Defining Evolution Domain Constraints

$x' = f(x) \,\&\, Q$ $\qquad\qquad$ $x' = f(x); ?(Q)$

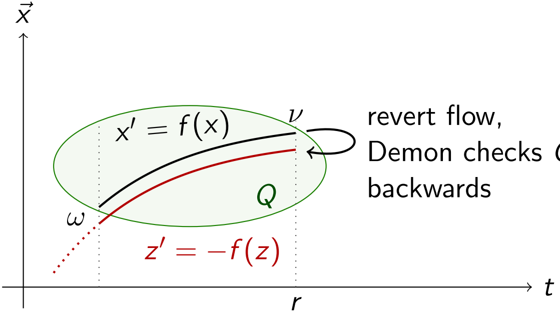


$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); ?(Q)$



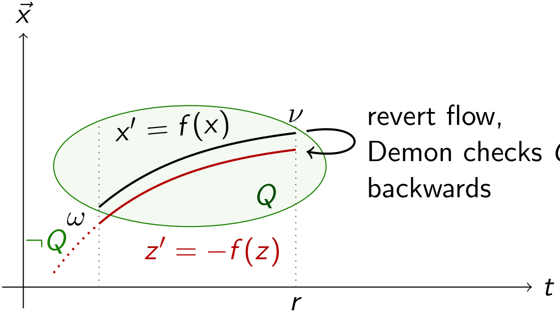
Defining Evolution Domain Constraints $x_0' = 1$

$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); (z := x; z' = -f(z))^d; ?(Q(z))$



revert flow,
Demon checks Q
backwards

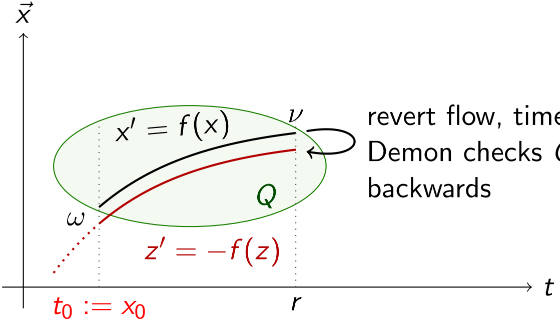
$x' = f(x) \,\&\, Q$ $\qquad\qquad$ $x' = f(x); (z := x; z' = -f(z))^d; ?(Q(z))$



revert flow,
Demon checks Q
backwards

Defining Evolution Domain Constraints

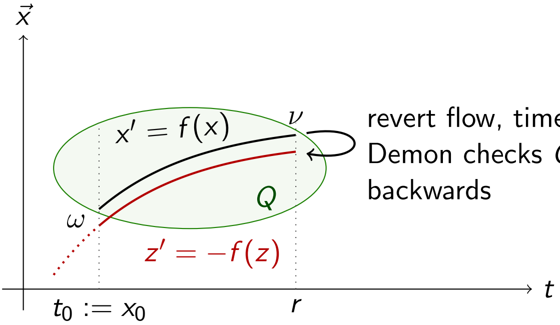
$$x' = f(x)\,\&\,Q \equiv t_0 := x_0; x' = f(x); (z := x; z' = -f(z))^d; ?(z_0 \ge t_0 \rightarrow Q(z))$$



revert flow, time x_0;
Demon checks Q
backwards

"There and Back Again" Game

$$x' = f(x) \,\&\, Q \equiv t_0 := x_0; x' = f(x); (z := x; z' = -f(z))^d; ?(z_0 \geq t_0 \to Q(z))$$



revert flow, time x_0;
Demon checks Q
backwards

Lemma

Evolution domains definable by games

Outline

Differential Game Logic: Denotational Semantics

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

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

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

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

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

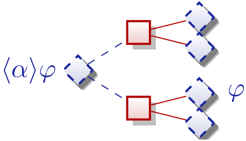
US $\dfrac{\varphi}{\varphi_{p(\cdot)}^{\psi(\cdot)}}$

TOCL'15

Summary

differential game logic

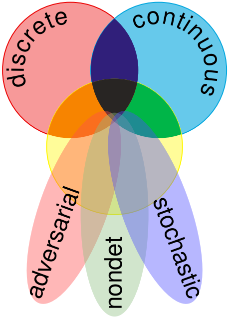
$\text{dGL} = \text{GL} + \text{HG} = \text{dL} + {}^d$



- Axiomatics for hybrid games
- Proving winning strategies

Next lecture

1. Soundness
2. Proofs
3. Separations



André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624/824, Carnegie Mellon University, 2017.
URL: `http://lfcps.org/course/fcps17.html`.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.
doi:10.1145/2817824.