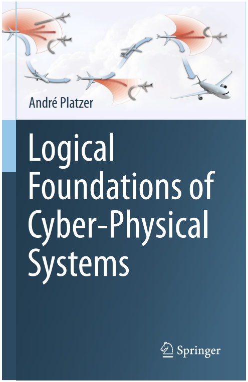
16: Winning & Proving Hybrid Games

Logical Foundations of Cyber-Physical Systems



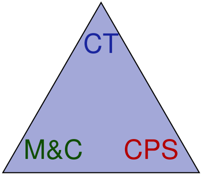
André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Outline

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



analytical&semantical interaction
discrete+continuous+adversarial
fixpoints

CPS semantics
align semantics&reasoning
operational CPS effects

Outline

Differential Game Logic: Syntax

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

Discrete Assign | Test Game | Differential Equation | Choice Game | Seq. Game | Repeat Game

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

All Reals | Some Reals

Differential Game Logic: Syntax

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

All Reals | Some Reals

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

All Reals | Some Reals | Angel Wins

Differential Game Logic: Syntax

Discrete Assign
Test Game
Differential Equation
Choice Game
Seq. Game
Repeat Game
Dual Game

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

All Reals
Some Reals
Angel Wins
Demon Wins

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

Definition (Hybrid game α)

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

Definition (dGL Formula P)

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

"Angel has Wings $\langle \alpha \rangle$"

All Reals | Some Reals | Angel Wins | Demon Wins

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

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

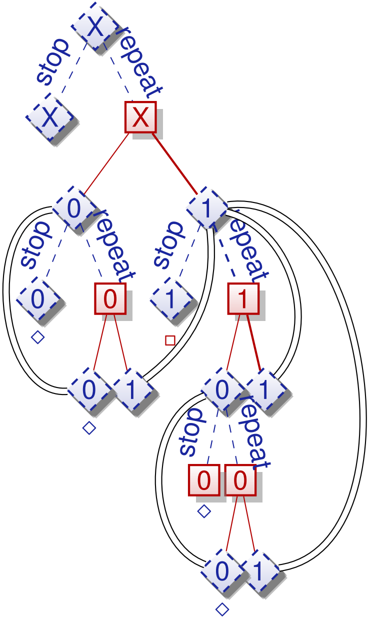
Definition (dGL Formula P) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S})$

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

Differential Game Logic: Axiomatization

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

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



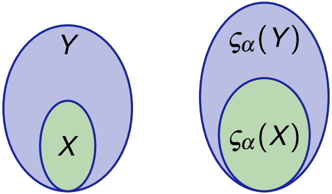
Consistency & Determinacy & Monotonicity

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., $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

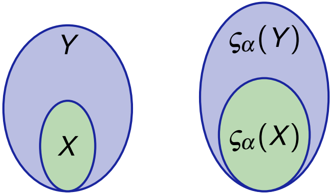
Corollary

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: $[\alpha]P \rightarrow \neg\langle\alpha\rangle\neg P$ *so* $\neg([\alpha]P \wedge \langle\alpha\rangle\neg P)$

Lemma (Monotonicity)

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



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 $\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement \subseteq (\varsigma_\alpha(Y^\complement))^\complement = \varsigma_{\alpha^d}(Y)$.
- $\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathscr{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} \subseteq \varsigma_{\alpha^*}(Y) = \bigcap\{Z \subseteq \mathscr{S} : Y \cup \varsigma_\alpha(Z) \subseteq Z\}$ because $X \subseteq Y$ □

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* $X \subseteq Y$

Theorem (Consistency & determinacy)

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

Corollary (Axiom: Determinacy)

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

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)

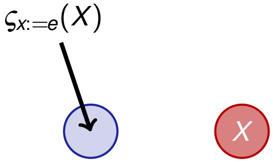
$$\text{M}\ \frac{P \rightarrow Q}{\langle\alpha\rangle P \rightarrow \langle\alpha\rangle Q} \qquad \text{M}[\cdot]\ \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

Outline

Hybrid Game Axioms

Axiom (Assignment) TOCL'15

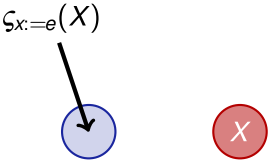
$\langle :=\rangle \quad \langle x := e\rangle p(x) \leftrightarrow$



Hybrid Game Axioms

Axiom (Assignment) TOCL'15

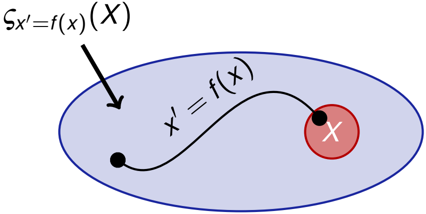
$\langle := \rangle \quad \langle x := e \rangle p(x) \leftrightarrow p(e)$



Hybrid Game Axioms

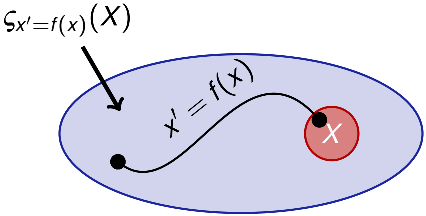
Axiom (Differential Equation) TOCL'15

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



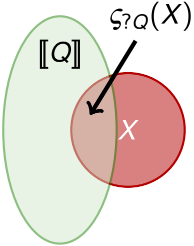
Axiom (Differential Equation) TOCL'15

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



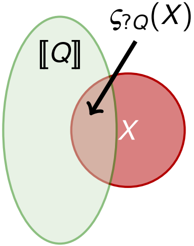
Axiom (Test / Challenge) TOCL'15

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



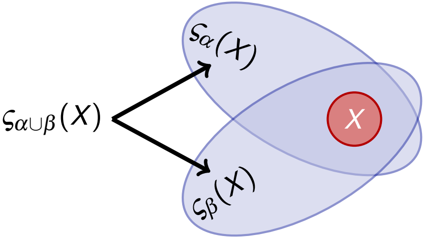
Axiom (Test / Challenge) TOCL'15

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



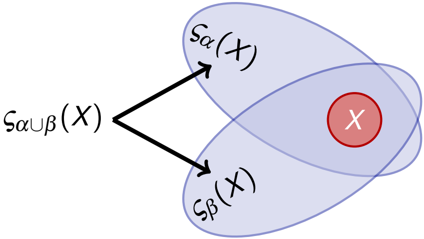
Axiom (Choice Game) TOCL'15

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



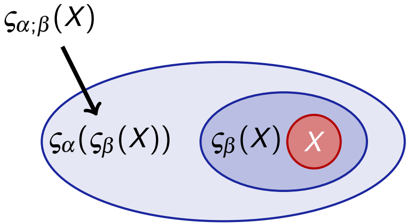
Axiom (Choice Game) TOCL'15

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



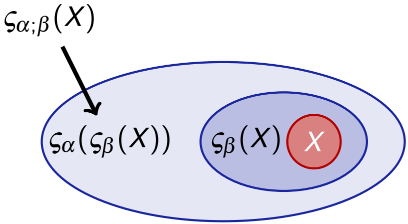
Axiom (Sequential Game) TOCL'15

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



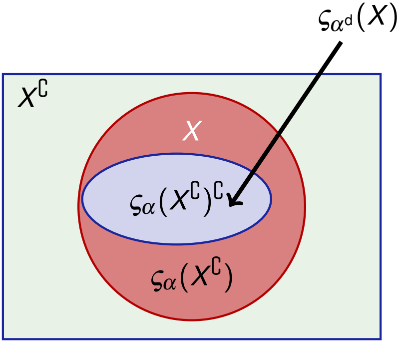
Axiom (Sequential Game) TOCL'15

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



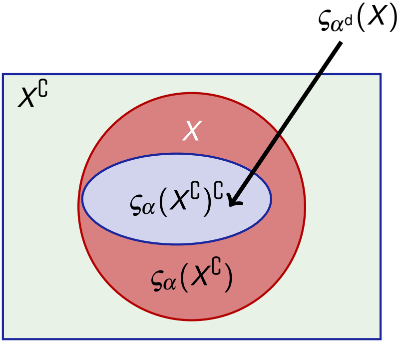
Axiom (Dual Game) — TOCL'15

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



Axiom (Dual Game) TOCL'15

$\langle^d\rangle \quad \langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$



Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

$$\alpha \cap \beta \equiv (\alpha^{\mathrm{d}} \cup \beta^{\mathrm{d}})^{\mathrm{d}}$$

$$\langle^d\rangle \frac{\overline{\vdash \langle(\alpha^{\mathrm{d}} \cup \beta^{\mathrm{d}})^{\mathrm{d}}\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}$$

Example: Demon's Choice Derives by Duality

$\langle^d\rangle \quad \langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$

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

Example: Demon's Choice Derives by Duality

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

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

Example: Demon's Choice Derives by Duality

$$\langle^d\rangle \quad \langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

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

Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

$$
\begin{array}{rl}
 & * \\
\hline
 & \vdash \langle\alpha\rangle P \land \langle\beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P \\
\hline
 & \vdash \neg(\neg\langle\alpha\rangle\neg\neg P \lor \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P \\
\hline
\langle^d\rangle & \vdash \neg(\langle\alpha^{\mathrm{d}}\rangle\neg P \lor \langle\beta^{\mathrm{d}}\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P \\
\hline
\langle\cup\rangle & \vdash \neg\langle\alpha^{\mathrm{d}} \cup \beta^{\mathrm{d}}\rangle\neg P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P \\
\hline
\langle^d\rangle & \vdash \langle(\alpha^{\mathrm{d}} \cup \beta^{\mathrm{d}})^{\mathrm{d}}\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P \\
\hline
 & \vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \land \langle\beta\rangle P
\end{array}
$$

Example: Demon's Choice Derives by Duality

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

Derived axiom:

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

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

Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

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

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

Example: Demon's Choice Derives by Duality

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

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

Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

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

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

Example: Demon's Choice Derives by Duality

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

Example: Demon's Choice Derives by Duality

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

Derived axioms:

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

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

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

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

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

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

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

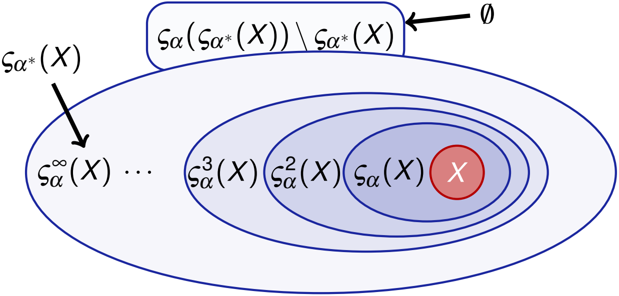
$\langle ; \rangle$ $\langle\alpha;\beta\rangle P \leftrightarrow \langle\alpha\rangle\langle\beta\rangle P$

$\langle^{d}\rangle$ $\langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$

Outline

Definition (Hybrid game α)

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



Proofs for Loops

Definition (Hybrid game α)

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

Proofs for Loops

Definition (Hybrid game α)

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

Proofs for Loops

Definition (Hybrid game α)

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

Lemma (Axiom:)

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

Definition (Hybrid game α)

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

Lemma (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)

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

Lemma (Axiom: Iteration)

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

Lemma (Rule:)

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

Proofs for Loops

Definition (Hybrid game α)

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

Lemma (Axiom: Iteration)

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

Lemma (Rule: Least Fixpoint)

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

Proofs for Loops

Definition (Hybrid game α)

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

Lemma (Axiom: Iteration)

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

Lemma (Rule: Least Fixpoint)

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

Corollary (Derived Rule:)

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

Proofs for Loops

Definition (Hybrid game α)

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

Lemma (Axiom: Iteration)

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

Lemma (Rule: Least Fixpoint)

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

Corollary (Derived Rule: Loop Invariant)

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

Proofs for Loops

Definition (Hybrid game α)

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

Lemma (Axiom: Iteration)

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

Lemma (Rule: Least Fixpoint)

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

Corollary (Derived Rule: Loop Invariant)

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

Proof

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\vdash P \to [\alpha]P}{\vdash P \to P \land [\alpha]P}}{\vdash P \to P \land \neg\langle \alpha \rangle \neg P}\,[\cdot]}{\vdash \neg P \lor \langle \alpha \rangle \neg P \to \neg P}}{\vdash \langle \alpha^* \rangle \neg P \to \neg P}\,\text{FP}}{\vdash P \to \neg\langle \alpha^* \rangle \neg P}}{\vdash P \to [\alpha^*]P}\,[\cdot]$$

Differential Game Logic: Axiomatization

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

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

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

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

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

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

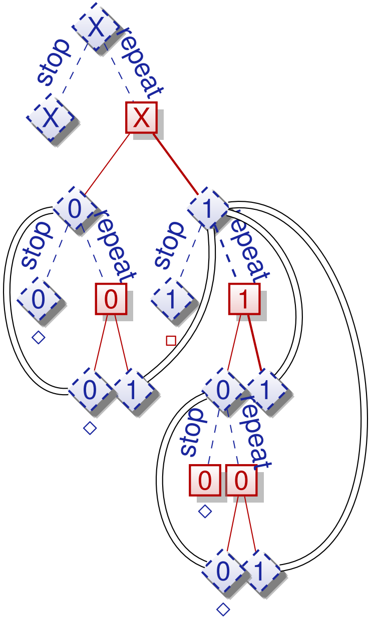
$\langle^*\rangle$ $\langle\alpha^*\rangle P \leftrightarrow P \lor \langle\alpha\rangle\langle\alpha^*\rangle P$

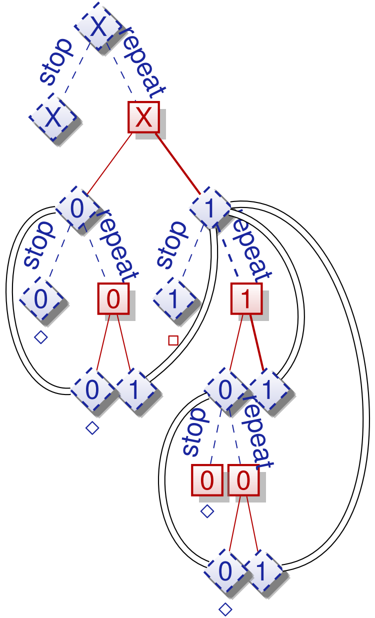
$\langle^d\rangle$ $\langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$

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

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

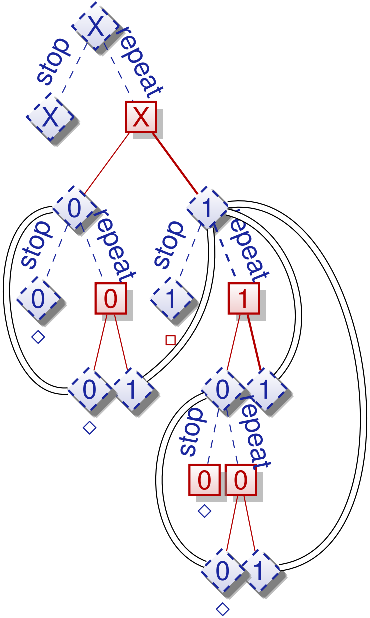
$$\langle^d\rangle \frac{}{x = 0 \vdash \langle (x := 0 \cup x := 1)^\times \rangle x = 0}$$





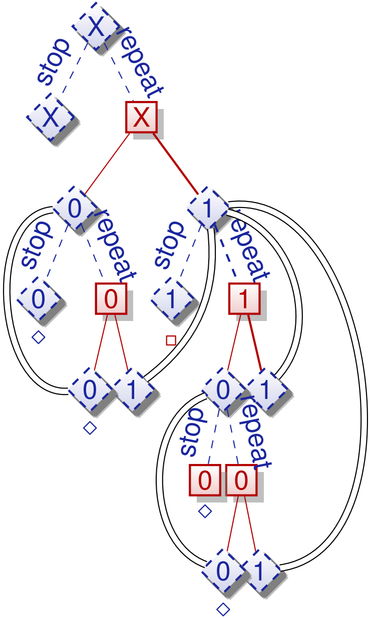
$$\text{ind}\ \dfrac{\dfrac{}{x=0 \vdash [(x:=0 \cap x:=1)^*]x=0}}{x=0 \vdash \langle (x:=0 \cup x:=1)^\times \rangle x=0}\ \langle^d\rangle$$

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



Example Proof: Dual Filibuster

$$
\begin{array}{rl}
\langle^d\rangle & \dfrac{}{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle \neg x=0} \\
[\cdot] & \dfrac{}{x=0 \vdash [x:=0 \cap x:=1]x=0} \\
\text{ind} & \dfrac{}{x=0 \vdash [(x:=0 \cap x:=1)^*]x=0} \\
\langle^d\rangle & \dfrac{}{x=0 \vdash \langle (x:=0 \cup x:=1)^\times \rangle x=0}
\end{array}
$$



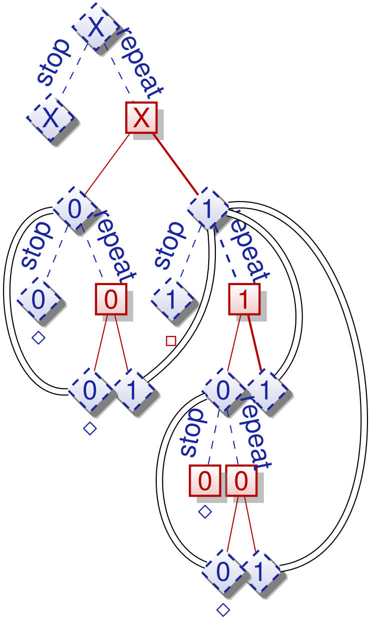
$\langle\cup\rangle$ $x = 0 \vdash \langle x := 0 \cup x := 1\rangle x = 0$

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

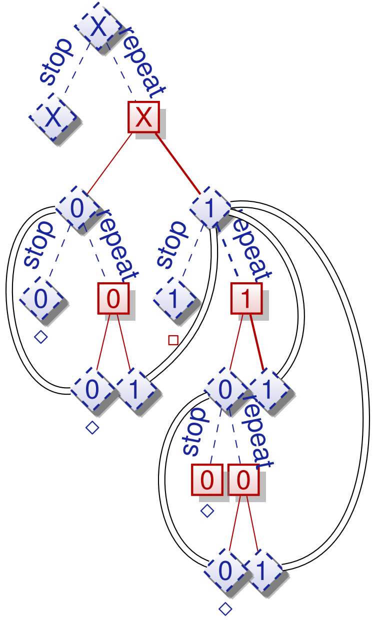
$[\cdot]$ $x = 0 \vdash [x := 0 \cap x := 1] x = 0$

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

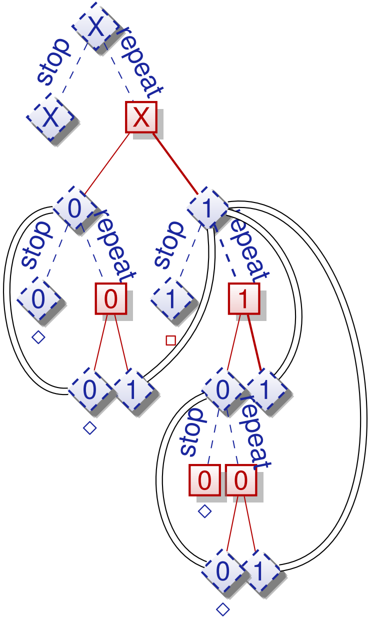
$\langle^d\rangle$ $x = 0 \vdash \langle (x := 0 \cup x := 1)^{\times}\rangle x = 0$



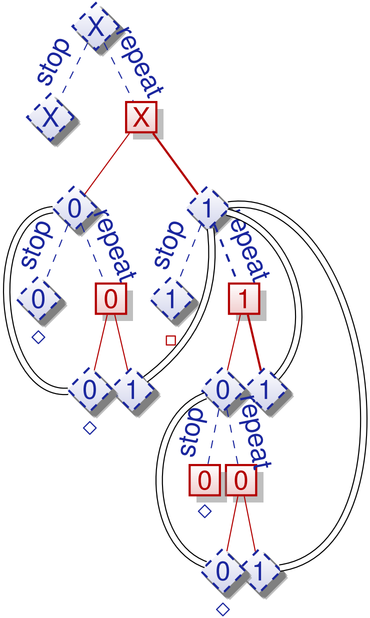
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x=0 \vdash \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0}\langle:=\rangle}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}\langle\cup\rangle}{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle \neg x=0}\langle^d\rangle}{x=0 \vdash [x:=0 \cap x:=1]x=0}[\cdot]}{x=0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



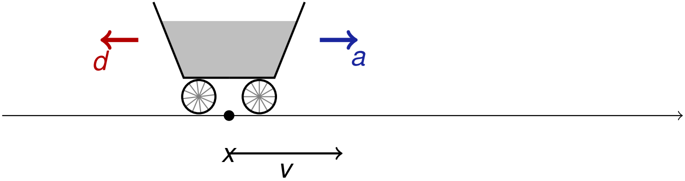
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{x=0 \vdash 0=0 \lor 1=0}\ \mathbb{R}}{x=0 \vdash \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0}\ \langle:=\rangle}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}\ \langle\cup\rangle}{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle\neg x=0}\ \langle^d\rangle}{x=0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



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



Example Proof: Push-around Cart



$$\text{ind}\quad \overline{J \vdash [\big((d := 1 \cap d := -1);(a := 1 \cup a := -1);\{x'=v, v'=a+d\}\big)^*]x \geq 0}$$

$$\dfrac{\dfrac{}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\,[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}\big)^*]x\geq 0}\,\text{ind}$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\overline{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\;[\cap]}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\;[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}\big)^*]x \geq 0}\;\text{ind}
$$

Example Proof: Push-around Cart

$$
\dfrac{
 \dfrac{
  \dfrac{
   \dfrac{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J \lor [d:=-1]\ldots}
   {J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\ \lor\mathrm{R,WR}
  }
  {J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\ [\cap]
 }
 {J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}\ [;]
}
{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}\big)^*]x\geq 0}\ \mathrm{ind}
$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[:=]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \lor [d:=-1]\dots}\,\lor\mathrm{R,WR}}{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[\cap]}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}\big)^*]x \geq 0}\,\mathrm{ind}
$$

Example Proof: Push-around Cart

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J}\;[;]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\;[:=]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \lor [d:=-1]\dots}\;\lor R,WR}{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\;[\cap]}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\;[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}\big)^*]x \geq 0}\;\text{ind}$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [a:=1 \cup a:=-1][\{x'=v, v'=a+1\}]J}[\cup]}{J \vdash [(a:=1 \cup a:=-1);\{x'=v, v'=a+1\}]J}[;]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}[:=]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J \vee [d:=-1]\dots}\vee R,WR}{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}[\cap]}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}]J}[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v, v'=a+d\}\big)^*]x \geq 0}\text{ind}
$$

Example Proof: Push-around Cart

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash [a:=1][\{x'=v,v'=a+1\}]J \land [a:=-1][\{x'=v,v'=a+1\}]J}[:=]}{J \vdash [a:=1 \cup a:=-1][\{x'=v,v'=a+1\}]J}[\cup]}{J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J}[;]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}[:=]}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \lor [d:=-1]\ldots}\lor R,WR}{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}[\cap]}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}[;]}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}\big)^*]x \geq 0}\text{ind}
$$

$$
\begin{array}{ll}
 & J \vdash [\{x' = v, v' = 1+1\}]J \land [\{x' = v, v' = -1+1\}]J \\
\hline
[:=] & J \vdash [a:=1][\{x' = v, v' = a+1\}]J \land [a:=-1][\{x' = v, v' = a+1\}]J \\
\hline
[\cup] & J \vdash [a:=1 \cup a:=-1][\{x' = v, v' = a+1\}]J \\
\hline
[;] & J \vdash [(a:=1 \cup a:=-1); \{x' = v, v' = a+1\}]J \\
\hline
[:=] & J \vdash [d:=1][(a:=1 \cup a:=-1); \{x' = v, v' = a+d\}]J \\
\hline
\lor R, WR & J \vdash [d:=1][(a:=1 \cup a:=-1); \{x' = v, v' = a+d\}]J \lor [d:=-1]\ldots \\
\hline
[\cap] & J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1); \{x' = v, v' = a+d\}]J \\
\hline
[;] & J \vdash [(d:=1 \cap d:=-1); (a:=1 \cup a:=-1); \{x' = v, v' = a+d\}]J \\
\hline
\text{ind} & J \vdash [\big((d:=1 \cap d:=-1); (a:=1 \cup a:=-1); \{x'=v, v'=a+d\}\big)^*]x \geq 0
\end{array}
$$

Example Proof: Push-around Cart

$$
\begin{array}{rl}
 & J \vdash [\{x'=v,v'=1+1\}]J \land [\{x'=v,v'=-1+1\}]J \\
\hline
[:=] & J \vdash [a:=1][\{x'=v,v'=a+1\}]J \land [a:=-1][\{x'=v,v'=a+1\}]J \\
\hline
[\cup] & J \vdash [a:=1 \cup a:=-1][\{x'=v,v'=a+1\}]J \\
\hline
[;] & J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J \\
\hline
[:=] & J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \\
\hline
\lor R,WR & J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \lor [d:=-1]\ldots \\
\hline
[\cap] & J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \\
\hline
[;] & J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \\
\hline
\text{ind} & J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}\big)^*]x \geq 0
\end{array}
$$

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

Example Proof: Push-around Cart

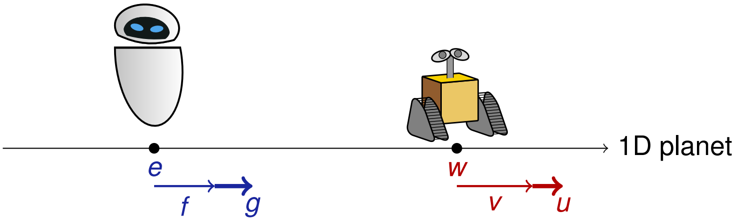
$$
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
J \vdash [\{x'=v,v'=1+1\}]J \land [\{x'=v,v'=-1+1\}]J
}{J \vdash [a:=1][\{x'=v,v'=a+1\}]J \land [a:=-1][\{x'=v,v'=a+1\}]J}\,[:=]
}{J \vdash [a:=1 \cup a:=-1][\{x'=v,v'=a+1\}]J}\,[\cup]
}{J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J}\,[;]
}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[:=]
}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \lor [d:=-1]\ldots}\,\lor R, WR
}{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[\cap]
}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[;]
}{J \vdash [((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\})^*]x \geq 0}\,\text{ind}
$$

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

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

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

Example Proof: WALL·E and EVE Robot Dance



$$
\begin{aligned}
&(w-e)^2 \le 1 \land v = f \rightarrow \\
&\langle ((u := 1 \cap u := -1); \\
&\quad (g := 1 \cup g := -1); \\
&\quad t := 0; \\
&\quad \{w' = v, v' = u, e' = f, f' = g, t' = 1 \,\&\, t \le 1\}^{d} \\
&)^{\times} \rangle \, (w-e)^2 \le 1
\end{aligned}
$$

EVE at e plays Angel's part controlling g

WALL·E at w plays Demon's part controlling u

Outline

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

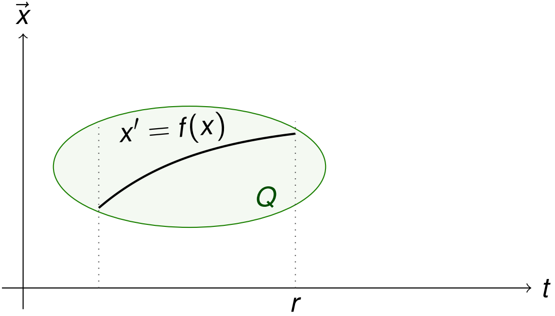
$$\langle^d\rangle \quad \langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

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

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

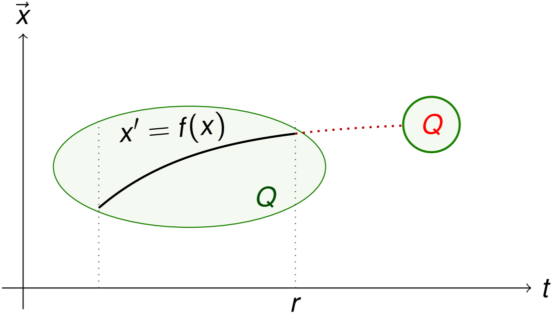
Defining Evolution Domain Constraints

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

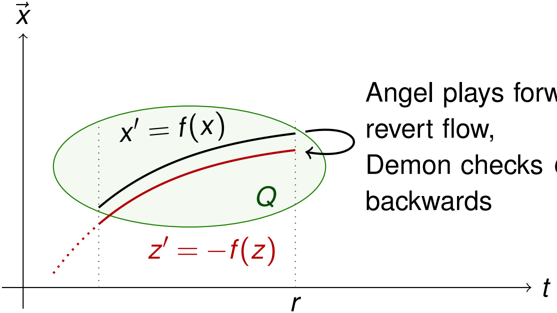


Defining Evolution Domain Constraints

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



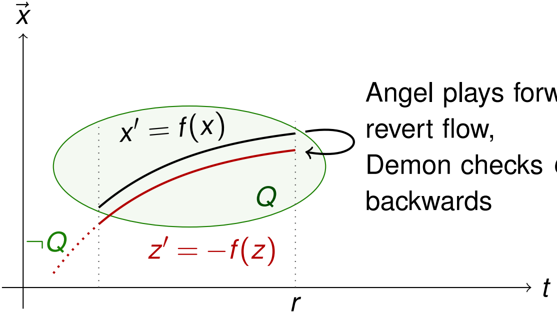
$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); (z := x; z' = -f(z))^{d}; ?(Q(z))$



Angel plays forward revert flow, Demon checks Q backwards

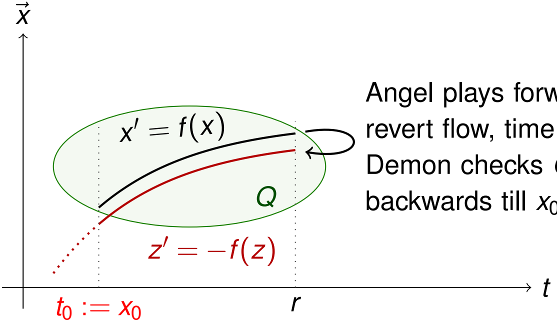
Defining Evolution Domain Constraints

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



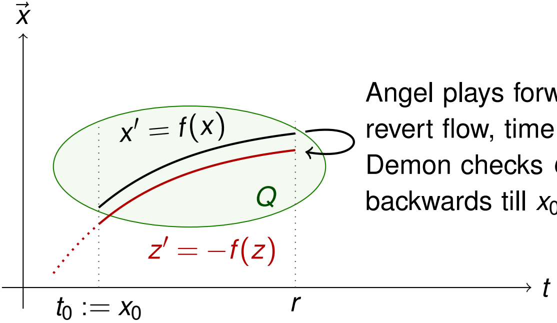
Angel plays forward revert flow, Demon checks Q backwards

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



Angel plays forward
revert flow, time x_0;
Demon checks Q
backwards till x_0

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



Angel plays forward
revert flow, time x_0;
Demon checks Q
backwards till x_0

Lemma

Evolution domains definable by games

Outline

Differential Game Logic: Denotational Semantics

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

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

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

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

$\langle^d\rangle$ $\langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$

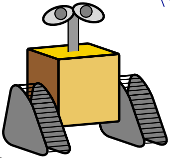
M $\dfrac{P \rightarrow Q}{\langle\alpha\rangle P \rightarrow \langle\alpha\rangle Q}$

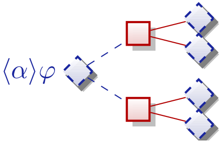
FP $\dfrac{P \vee \langle\alpha\rangle Q \rightarrow Q}{\langle\alpha^*\rangle P \rightarrow Q}$

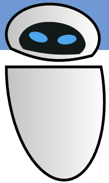
Summary

differential game logic

dGL = GL + HG = dL + ^{d}



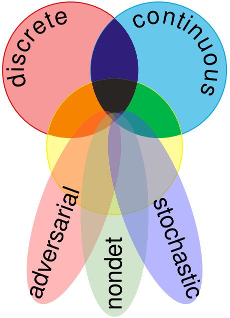




- Axiomatics for hybrid games
- Proving winning strategies

Next chapter

1. Soundness
2. Proofs
3. Separations



André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3, doi:10.1007/978-3-319-63588-0.

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