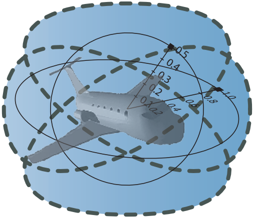
17: Winning Strategies & Regions

15-424: Foundations of Cyber-Physical Systems

André Platzer

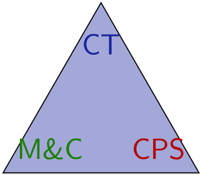
aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

fundamental principles of computational thinking
logical extensions
PL modularity principles
compositional extensions
differential game logic
denotational vs. operational semantics



adversarial dynamics
adversarial semantics

CPS semantics
multi-agent operational-effects
mutual reactions
complementary hybrid systems

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

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

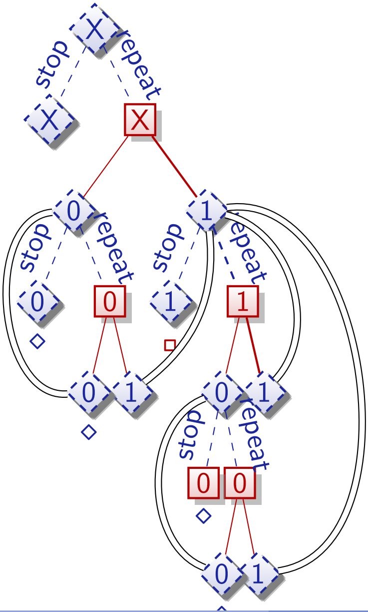
All Reals | Some Reals | Angel Wins | Demon Wins

TOCL'15

Outline

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

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



Differential Game Logic: Denotational Semantics

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

$$
\begin{aligned}
[\![e_1 \geq e_2]\!] &= \{\omega \in \mathcal{S} \ : \ [\![e_1]\!]\omega \geq [\![e_2]\!]\omega\} \\
[\![\neg P]\!] &= ([\![P]\!])^{\complement} \\
[\![P \land Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle\alpha\rangle P]\!] &= \varsigma_\alpha([\![P]\!]) \quad \{\omega \ : \ \nu \in [\![P]\!] \text{ for some } \nu \text{ with } (\omega,\nu) \in [\![\alpha]\!]\} \text{ ???} \\
[\![[\alpha]P]\!] &= \delta_\alpha([\![P]\!])
\end{aligned}
$$

Differential Game Logic: Denotational Semantics

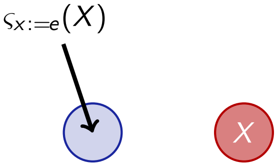
Definition (Hybrid game α: denotational semantics)

$\varsigma_{x:=e}(X) =$

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

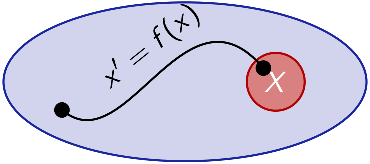
$$\varsigma_{x:=e}(X) = \{\omega \in \mathcal{S} \;:\; \omega_x^{[\![e]\!]\omega} \in X\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

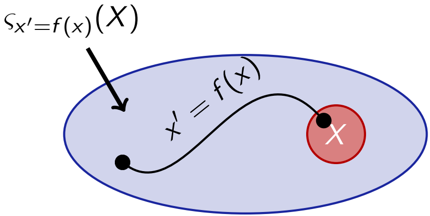
$\varsigma_{x'=f(x)}(X) =$



Differential Game Logic: Denotational Semantics

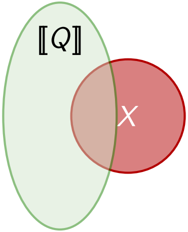
Definition (Hybrid game α: denotational semantics)

$$\varsigma_{x'=f(x)}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(\zeta) \in X, \frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![f(x)]\!]_{\varphi(\zeta)} \text{ for all } \zeta\}$$



Definition (Hybrid game α: denotational semantics)

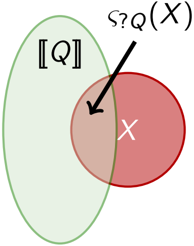
$\varsigma_{?Q}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

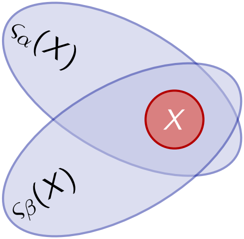
$$\varsigma_{?Q}(X) = [\![Q]\!] \cap X$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

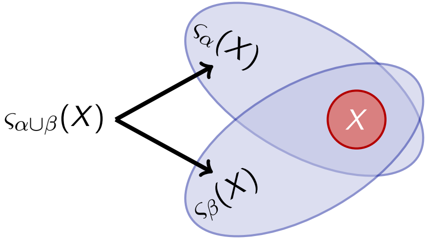
$\varsigma_{\alpha\cup\beta}(X) =$



Differential Game Logic: Denotational Semantics

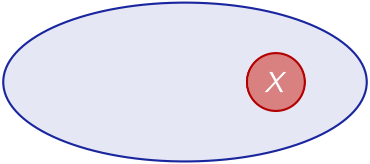
Definition (Hybrid game α: denotational semantics)

$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$



Definition (Hybrid game α: denotational semantics)

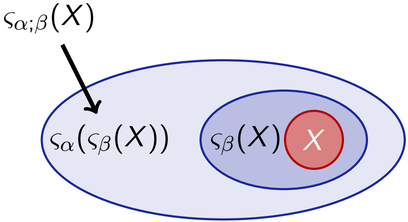
$\varsigma_{\alpha;\beta}(X) =$



Differential Game Logic: Denotational Semantics

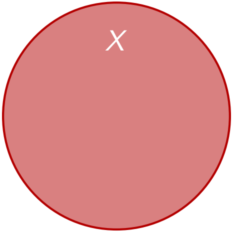
Definition (Hybrid game α: denotational semantics)

$$\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X))$$



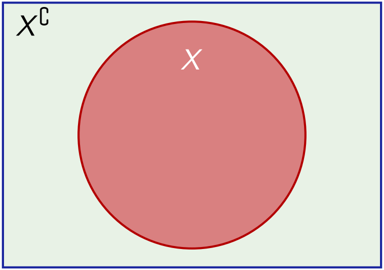
Definition (Hybrid game α: denotational semantics)

$\varsigma_{\alpha^d}(X) =$



Definition (Hybrid game α: denotational semantics)

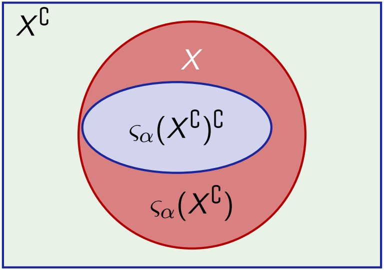
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

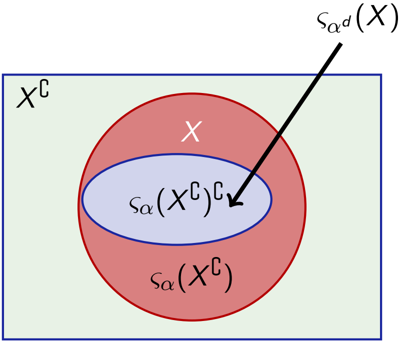
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

$$\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement$$



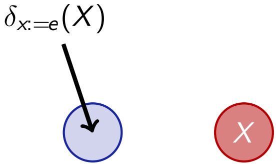
Definition (Hybrid game α: denotational semantics)

$\delta_{x:=e}(X) =$

Differential Game Logic: Denotational Semantics

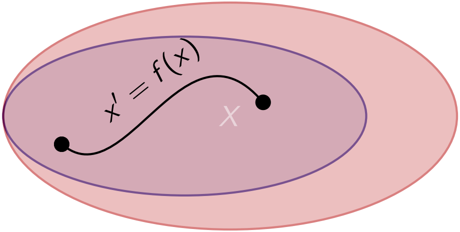
Definition (Hybrid game α: denotational semantics)

$$\delta_{x:=e}(X) = \{\omega \in \mathcal{S} : \omega_x^{[\![e]\!]\omega} \in X\}$$



Definition (Hybrid game α: denotational semantics)

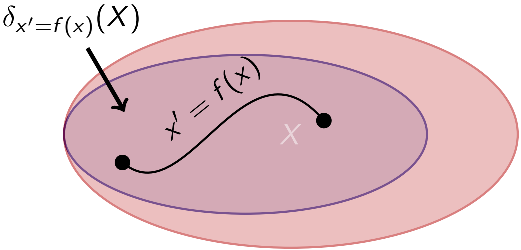
$\delta_{x'=f(x)}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

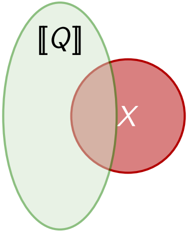
$$\delta_{x'=f(x)}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(\zeta) \in X, \frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![f(x)]\!]\varphi(\zeta) \text{ for all } \zeta\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

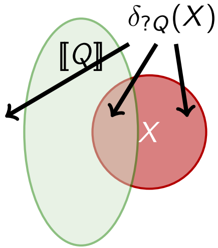
$\delta_{?Q}(X) =$



Differential Game Logic: Denotational Semantics

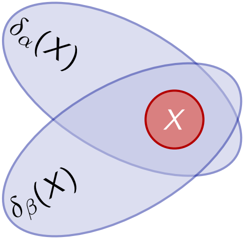
Definition (Hybrid game α: denotational semantics)

$$\delta_{?Q}(X) = [\![Q]\!]^\complement \cup X$$



Definition (Hybrid game α: denotational semantics)

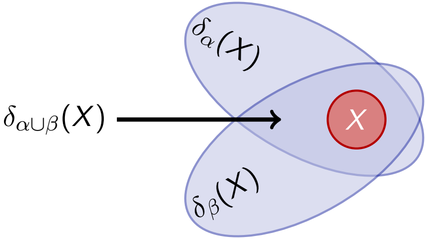
$\delta_{\alpha\cup\beta}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

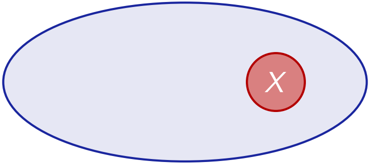
$$\delta_{\alpha\cup\beta}(X) = \delta_\alpha(X) \cap \delta_\beta(X)$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

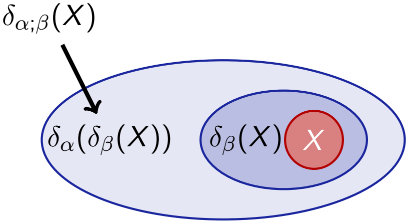
$\delta_{\alpha;\beta}(X) =$



Differential Game Logic: Denotational Semantics

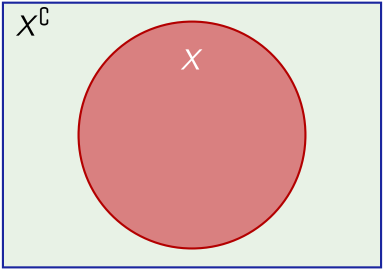
Definition (Hybrid game α: denotational semantics)

$$\delta_{\alpha;\beta}(X) = \delta_\alpha(\delta_\beta(X))$$



Definition (Hybrid game α: denotational semantics)

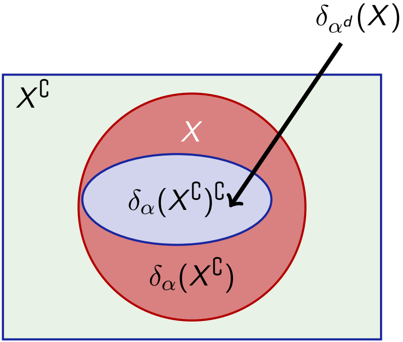
$\delta_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

$$\delta_{\alpha^d}(X) = (\delta_\alpha(X^\complement))^\complement$$



Differential Game Logic: Denotational Semantics

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

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

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

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

Filibusters & The Significance of Finitude

$\overset{<\infty}{\rightsquigarrow}$ true

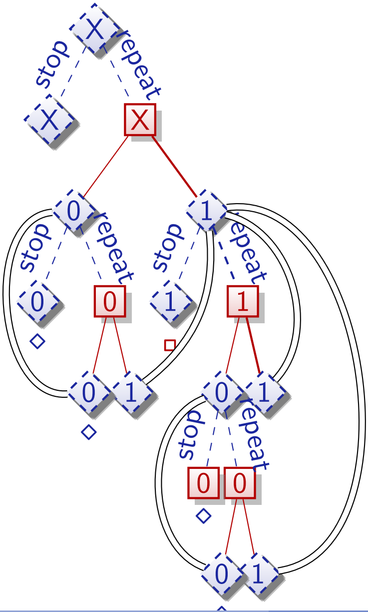
$\langle (x' = 1^d; x := 0)^* \rangle x = 0$

$\langle (x := 0; x' = 1^d)^* \rangle x = 0$

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

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

Well-defined games
can't be postponed forever



Consistency & Determinacy

Theorem (Consistency & determinacy)

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

Corollary (Determinacy: At least one player wins)

$\vDash \neg\langle\alpha\rangle\neg\phi \rightarrow [\alpha]\phi$, *thus* $\vDash \langle\alpha\rangle\neg\phi \lor [\alpha]\phi$.

Corollary (Consistency: At most one player wins)

$\vDash [\alpha]\phi \rightarrow \neg\langle\alpha\rangle\neg\phi$, *thus* $\vDash \neg([\alpha]\phi \land \langle\alpha\rangle\neg\phi)$

Consistency & Determinacy

Theorem (Consistency & determinacy)

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

Corollary (Determinacy: At least one player wins)

$\vDash \neg\langle\alpha\rangle\neg\phi \rightarrow [\alpha]\phi$, *thus* $\vDash \langle\alpha\rangle\neg\phi \vee [\alpha]\phi$.

Corollary (Consistency: At most one player wins)

$\vDash [\alpha]\phi \rightarrow \neg\langle\alpha\rangle\neg\phi$, *thus* $\vDash \neg([\alpha]\phi \wedge \langle\alpha\rangle\neg\phi)$

Proof Sketch.

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

Outline

Semantics of Repetition

Definition (Hybrid game α)

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

Semantics of Repetition

Definition (Hybrid game α)

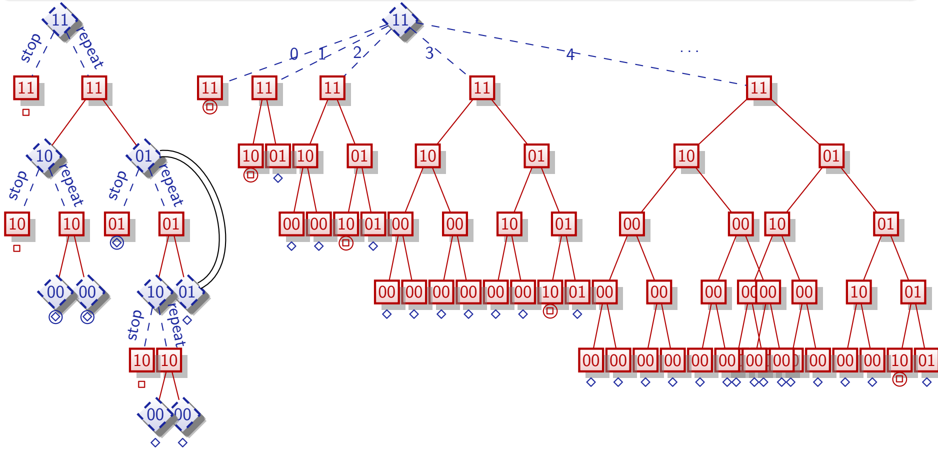
$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_{\alpha^n}(X)$

$$[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!] \quad \text{where } \alpha^{n+1} \equiv \alpha^n;\alpha \quad \alpha^0 \equiv ?\mathit{true}$$

Semantics of Repetition

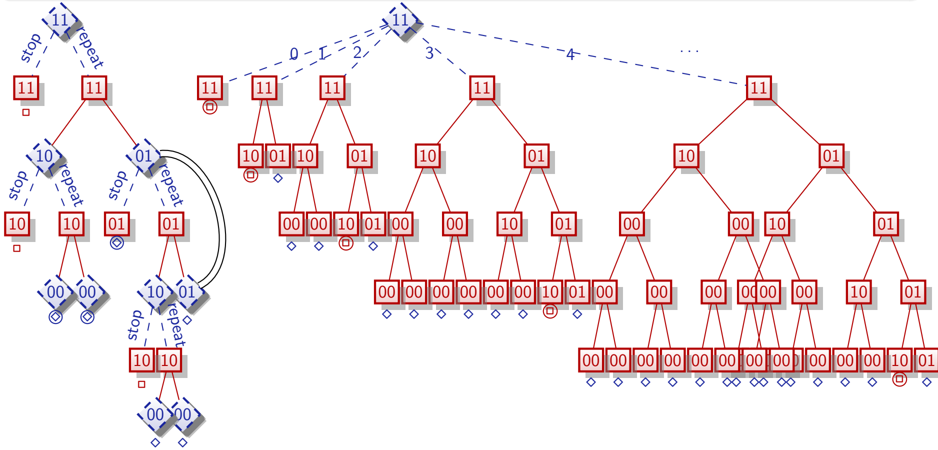
Definition (Hybrid game α)

$$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_{\alpha^n}(X)$$



Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_{\alpha^n}(X)$ — advance notice semantics



+1 Argument

Note (+1 argument)

$$Y \subseteq \varsigma_{\alpha^*}(X) \text{ then } \varsigma_\alpha(Y) \subseteq \varsigma_{\alpha^*}(X)$$

Since $\varsigma_\alpha(Y)$ is just one round away from Y.

Semantics of Repetition

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n(X)$

$$\varsigma_\alpha^0(X) \overset{\text{def}}{=} X$$

$$\varsigma_\alpha^{\kappa+1}(X) \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

Semantics of Repetition

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n(X)$

$$\varsigma_\alpha^0(X) \stackrel{\text{def}}{=} X$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

Example

$\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle\, (0 \le x < 1)$

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n(X)$ ω-semantics

$$\varsigma_\alpha^0(X) \stackrel{\text{def}}{=} X$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

Example

$\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle (0 \le x < 1)$ $\varsigma_\alpha^n([0,1)) = [0,n) \ne \mathbb{R}$

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n(X)$ ω-semantics

$$\varsigma_\alpha^0(X) \stackrel{\text{def}}{=} X$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

$$\varsigma_\alpha^\lambda(X) \stackrel{\text{def}}{=} \bigcup_{\kappa<\lambda} \varsigma_\alpha^\kappa(X) \qquad \lambda \neq 0 \text{ a limit ordinal}$$

Example

$\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle\, (0 \leq x < 1)$ $\quad \varsigma_\alpha^n([0,1)) = [0,n) \neq \mathbb{R}$

$\varsigma_\alpha^\omega([0,1)) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n([0,1)) = [0,\infty) \neq \mathbb{R}$

Semantics of Repetition

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$

$$\varsigma_\alpha^0(X) \stackrel{\text{def}}{=} X$$

$$\varsigma_\alpha^{\kappa+1}(X) \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_\alpha^\kappa(X))$$

$$\varsigma_\alpha^\lambda(X) \stackrel{\text{def}}{=} \bigcup_{\kappa<\lambda} \varsigma_\alpha^\kappa(X) \qquad \lambda \neq 0 \text{ a limit ordinal}$$

Example

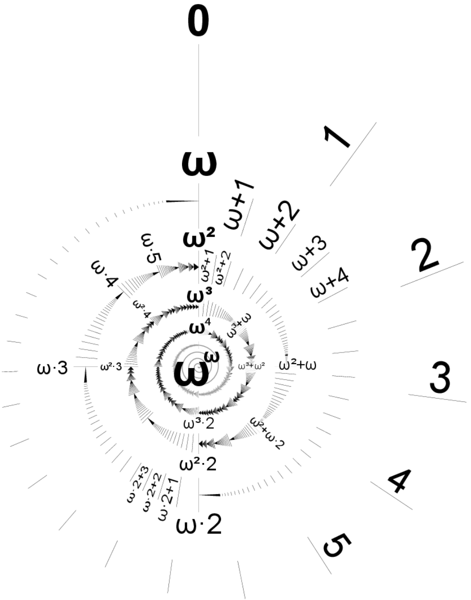
$\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle\, (0 \le x < 1)$ $\qquad \varsigma_\alpha^n([0,1)) = [0,n) \neq \mathbb{R}$

$\varsigma_\alpha^{\omega+1}([0,1)) = \varsigma_\alpha([0,\infty)) = \mathbb{R}$ $\qquad \varsigma_\alpha^\omega([0,1)) = \bigcup_{n\in\mathbb{N}} \varsigma_\alpha^n([0,1)) = [0,\infty) \neq \mathbb{R}$

Strategic Closure Ordinal

Theorem

Hybrid game closure ordinal $\geq \omega_1^{CK}$



Expedition: Ordinal Arithmetic

$$\iota + 0 = \iota$$

$$\iota + (\kappa{+}1) = (\iota + \kappa) + 1 \quad \text{successor } \kappa{+}1$$

$$\iota + \lambda = \bigsqcup_{\kappa<\lambda} \iota + \kappa \quad \text{limit } \lambda$$

$$\iota \cdot 0 = 0$$

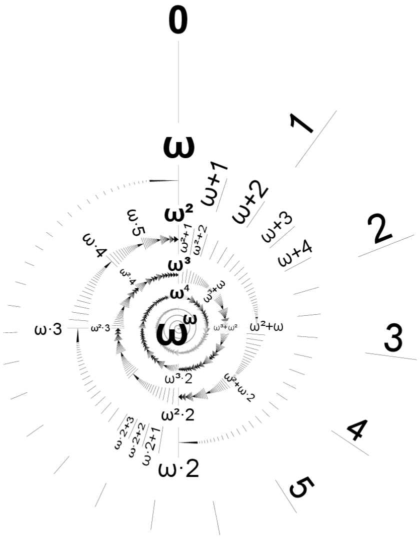
$$\iota \cdot (\kappa{+}1) = (\iota \cdot \kappa) + \iota \quad \text{successor } \kappa{+}1$$

$$\iota \cdot \lambda = \bigsqcup_{\kappa<\lambda} \iota \cdot \kappa \quad \text{limit } \lambda$$

$$\iota^0 = 1$$

$$\iota^{\kappa+1} = \iota^\kappa \cdot \iota \quad \text{successor } \kappa{+}1$$

$$\iota^\lambda = \bigsqcup_{\kappa<\lambda} \iota^\kappa \quad \text{limit } \lambda$$



$$2 \cdot \omega = 4 \cdot \omega \neq \omega \cdot 2 < \omega \cdot 4$$

Monotonicity

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

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

Lemma (Monotonicity)

$\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y)$ *and* $\delta_\alpha(X) \subseteq \delta_\alpha(Y)$ *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 $\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement \subseteq (\varsigma_\alpha(Y^\complement))^\complement = \varsigma_{\alpha^d}(Y)$.

Outline

Differential Game Logic: Denotational Semantics

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

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

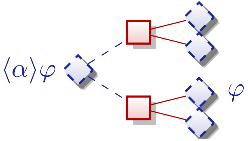
Definition (dG$\mathcal{L}$ Formula P) $[\![\cdot]\!] : \text{Fml} \to \wp(\mathcal{S})$

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

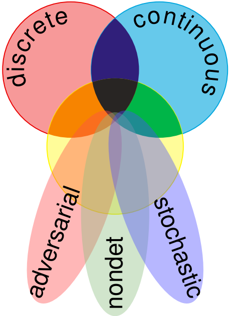
Summary

differential game logic

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



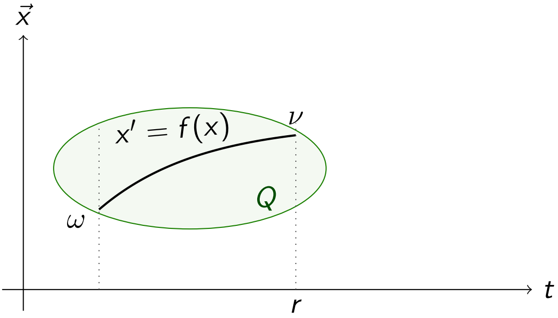
- Semantics for differential game logic
- Simple compositional denotational semantics
- Meaning is a simple function of its pieces
- Outlier: repetition is subtle higher-ordinal iteration
- Monotonicity
- Determinacy



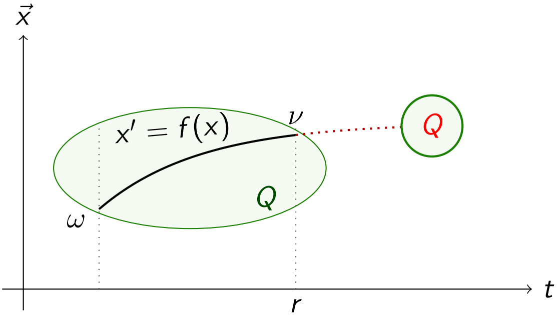
Next lecture

1. Revisit repetition
2. Axiomatics

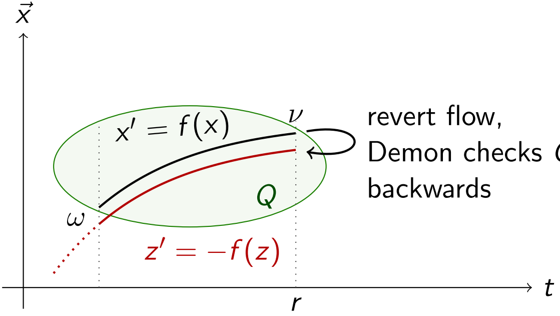
$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); ?(Q)$



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

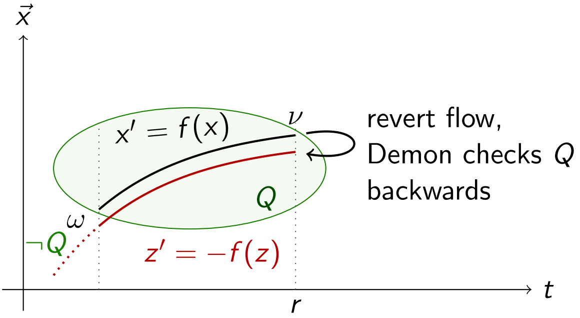


$x' = f(x) \,\&\, Q$ $\qquad$ $x' = f(x); (z := x; z' = -f(z))^d; ?(Q(z))$

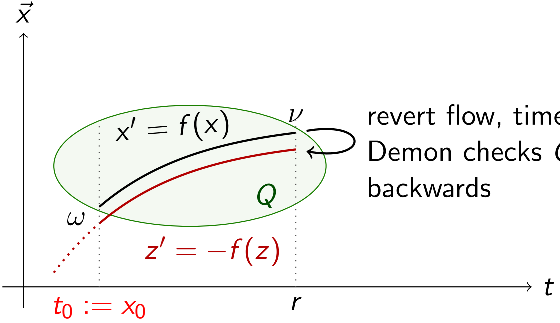


revert flow,
Demon checks Q
backwards

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



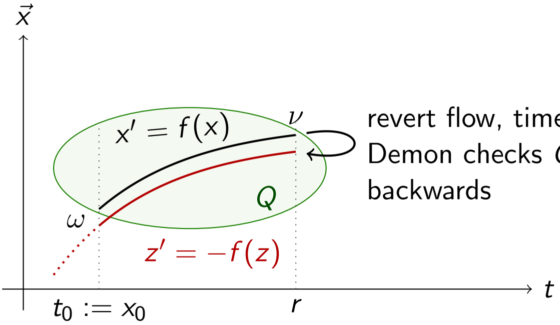
$$x' = f(x) \,\&\, Q \equiv t_0 := x_0; x' = f(x); (z := x; z' = -f(z))^d; ?(z_0 \geq t_0 \rightarrow Q(z))$$



revert flow, time x_0;
Demon checks Q
backwards

"There and Back Again" Game

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



revert flow, time x_0;
Demon checks Q
backwards

Lemma

Evolution domains definable by games

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

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