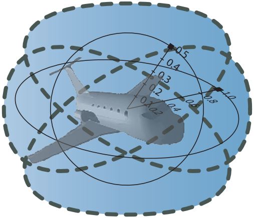
17: Winning Strategies & Regions

15-424: Foundations of Cyber-Physical Systems

André Platzer

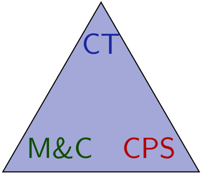
aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



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
adversarial repetitions
fixpoints

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 (dGL 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

Differential Game Logic: Denotational Semantics

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

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

Differential Game Logic: Denotational Semantics

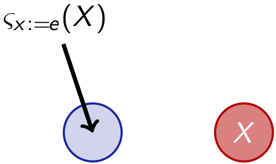
Definition (Hybrid game α: denotational semantics)

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

Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

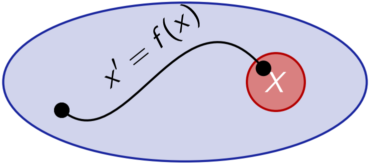
$$\varsigma_{x:=e}(X) = \{\omega \in \mathcal{S} : \omega_x^{\omega[\![e]\!]} \in X\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

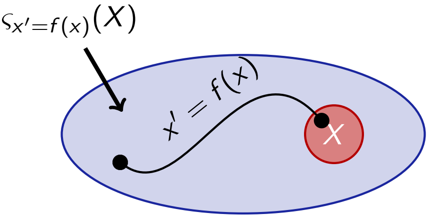
$\varsigma_{x'=f(x)}(X) =$



Differential Game Logic: Denotational Semantics

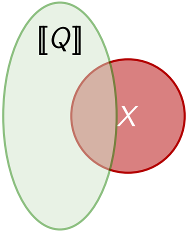
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

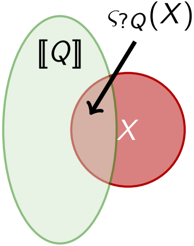
$\varsigma_{?Q}(X) =$



Differential Game Logic: Denotational Semantics

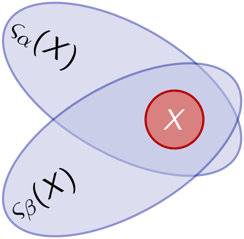
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

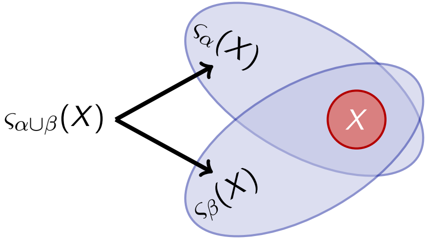
$\varsigma_{\alpha\cup\beta}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

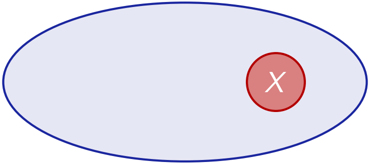
$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

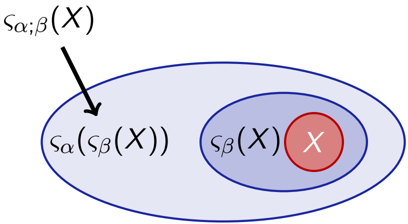
$\varsigma_{\alpha;\beta}(X) =$



Differential Game Logic: Denotational Semantics

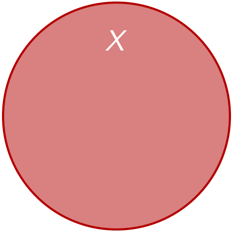
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

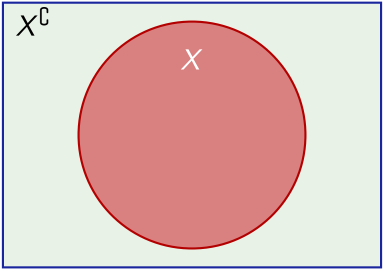
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

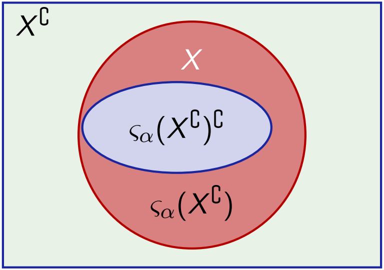
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

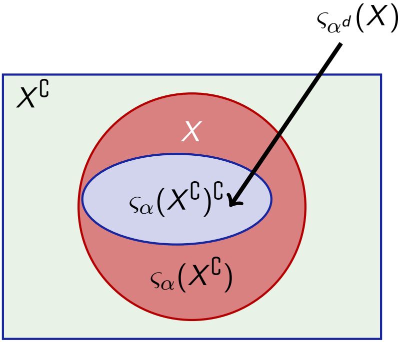
$\varsigma_{\alpha^d}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

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



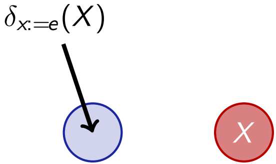
Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

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

Definition (Hybrid game α: denotational semantics)

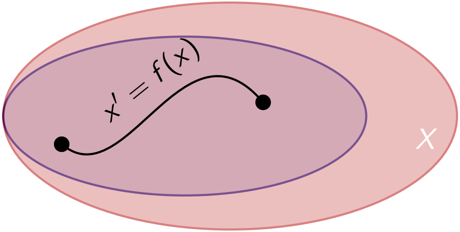
$$\delta_{x:=e}(X) = \{\omega \in \mathcal{S} : \omega_x^{\omega[\![e]\!]} \in X\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

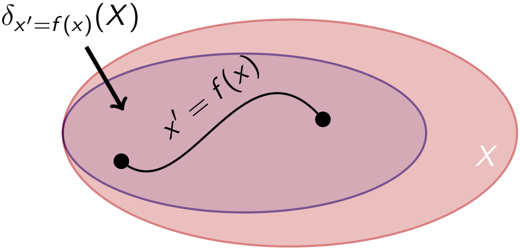
$\delta_{x'=f(x)}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

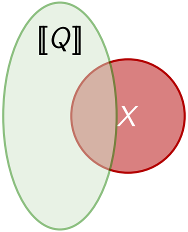
$$\delta_{x'=f(x)}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(z) \in X, \frac{d\,\varphi(t)(x)}{dt}(z) = \varphi(z)[\![f(x)]\!] \text{ for all } z\}$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

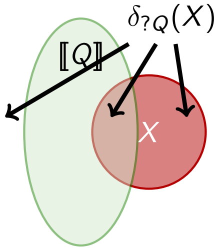
$\delta_{?Q}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

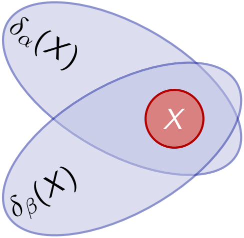
$$\delta_{?Q}(X) = [\![Q]\!]^\complement \cup X$$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

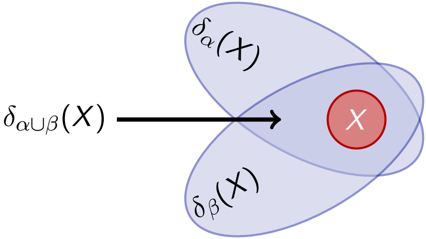
$\delta_{\alpha\cup\beta}(X) =$



Differential Game Logic: Denotational Semantics

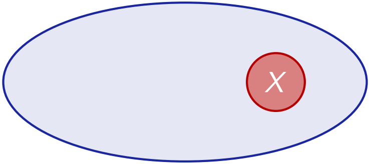
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

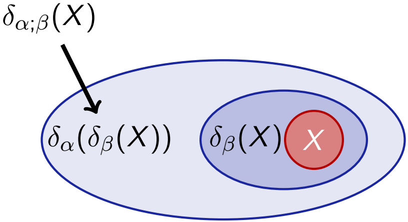
$\delta_{\alpha;\beta}(X) =$



Differential Game Logic: Denotational Semantics

Definition (Hybrid game α: denotational semantics)

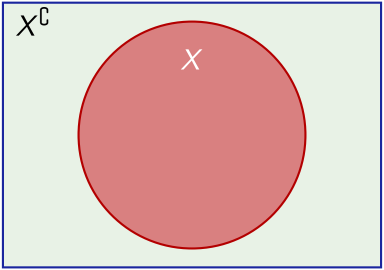
$$\delta_{\alpha;\beta}(X) = \delta_\alpha(\delta_\beta(X))$$



Differential Game Logic: Denotational Semantics

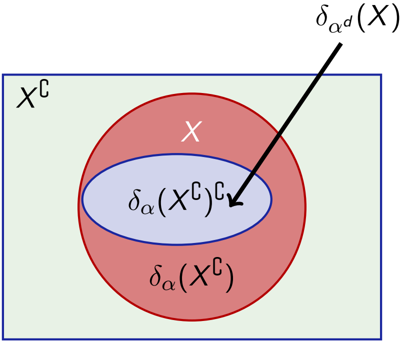
Definition (Hybrid game α: denotational semantics)

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



Definition (Hybrid game α: denotational semantics)

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



Differential Game Logic: Denotational Semantics

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

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

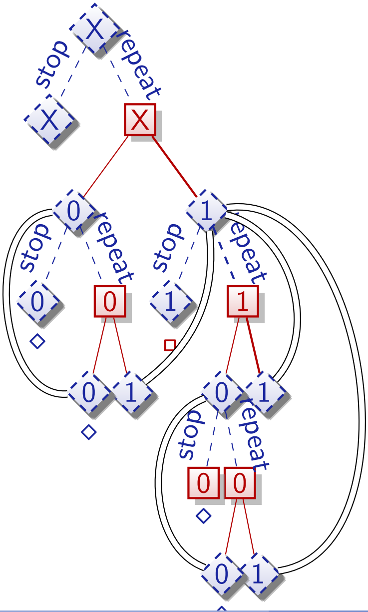
Definition (dGL Formula P) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S})$

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

Outline

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

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



Semantics of Repetition

Definition (Hybrid game α)

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

Semantics of Repetition

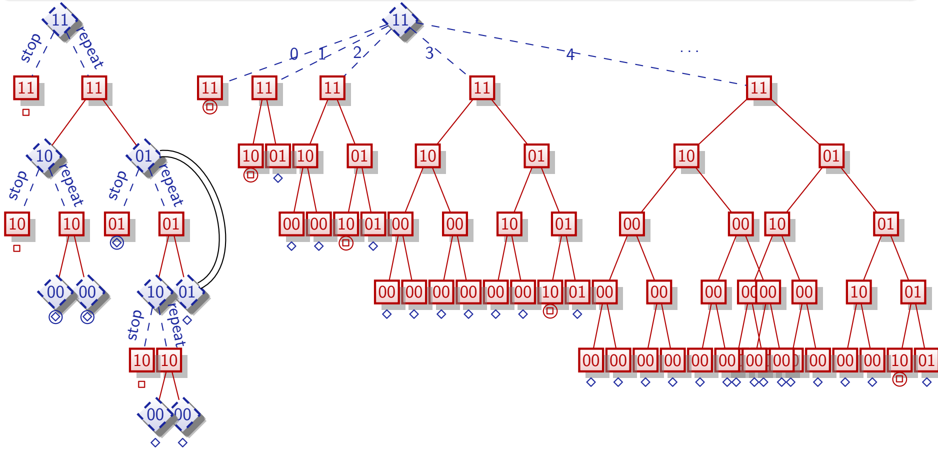
Definition (Hybrid game α)

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

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

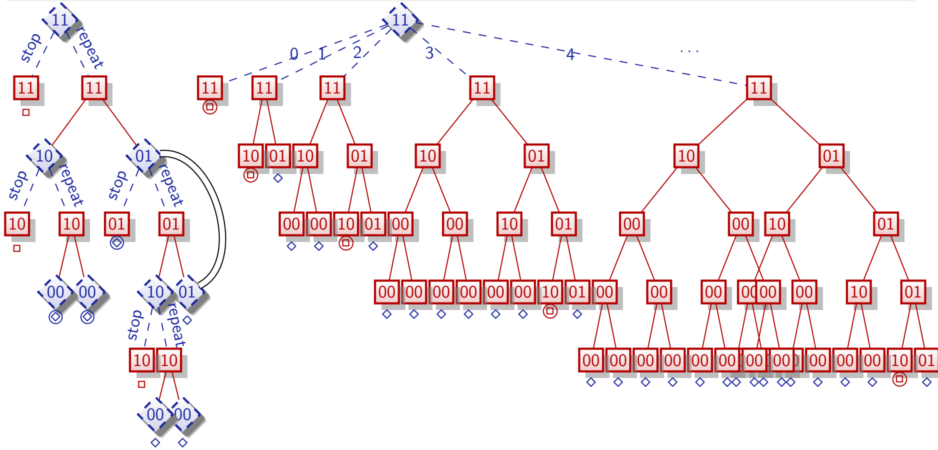
Definition (Hybrid game α)

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



Definition (Hybrid game α)

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

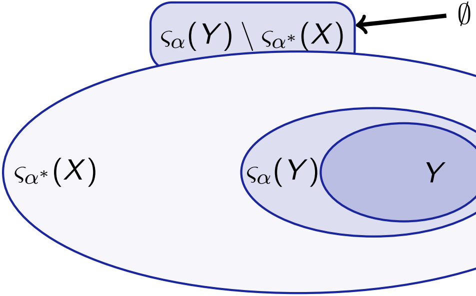


+1 Argument

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)

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

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

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

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

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

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

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

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

Semantics of Repetition

Definition (Hybrid game α)

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

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

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

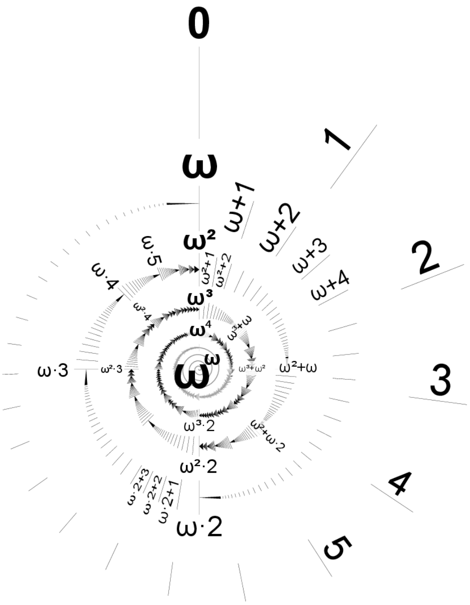
$$\varsigma_\alpha^\lambda(X) \stackrel{\text{def}}{=} \bigcup_{\kappa<\lambda} \varsigma_\alpha^\kappa(X) \qquad \lambda \neq 0 \text{ a limit ordinal}$$

Example

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

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

Strategic Closure Ordinal $\geq \omega_1^{CK}$



Theorem

Hybrid game closure ordinal $>\omega^\omega$

Expedition: Ordinal Arithmetic

$$\iota + 0 = \iota$$

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

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

$$\iota \cdot 0 = 0$$

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

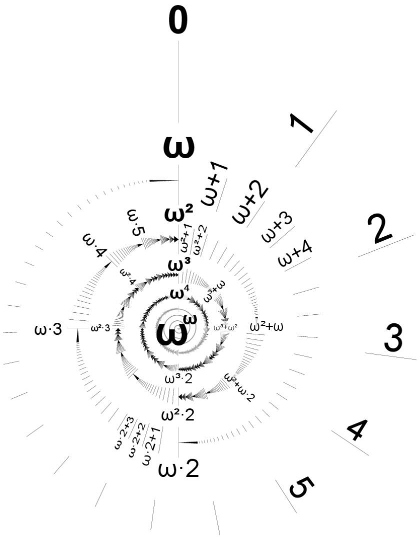
$$\iota \cdot \lambda = \bigsqcup_{\kappa<\lambda} \iota \cdot \kappa \qquad \text{limit } \lambda$$

$$\iota^0 = 1$$

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

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

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



Semantics of Repetition

Definition (Hybrid game α)

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

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

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

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

Semantics of Repetition

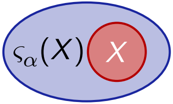
Definition (Hybrid game α)

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

Semantics of Repetition

Definition (Hybrid game α)

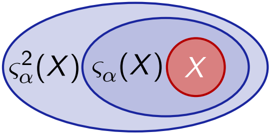
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



Semantics of Repetition

Definition (Hybrid game α)

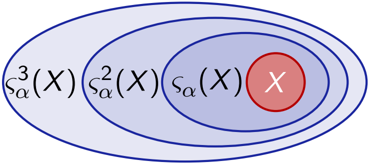
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



Semantics of Repetition

Definition (Hybrid game α)

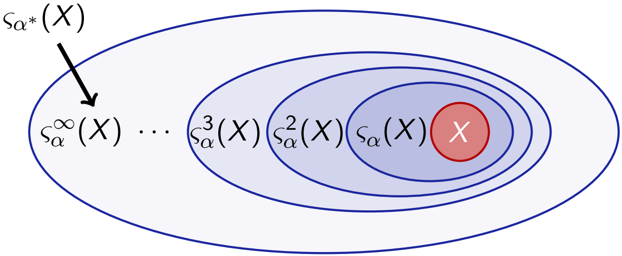
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



Semantics of Repetition

Definition (Hybrid game α)

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



The Power of Implicit Definitions

Implicit Definitions

The advantages of implicit definition over construction are roughly those of theft over honest toil.

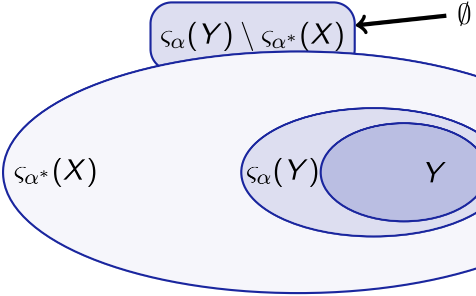
— Bertrand Russell

+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.



+1 Argument

Note (+1 argument)

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

$$Z \overset{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_{\alpha}(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

+1 Argument

Note (+1 argument)

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

$$Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_\alpha(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- Which Z with $\varsigma_\alpha(Z) \subseteq Z$ is the right one?
- Are there multiple such Z?
- Does such a Z exist?

+1 Argument

Note (+1 argument)

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

$$Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_\alpha(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- Which Z with $\varsigma_\alpha(Z) \subseteq Z$ is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \emptyset$

+1 Argument

Note (+1 argument)

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

$$Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_{\alpha}(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- Which Z with $\varsigma_{\alpha}(Z) \subseteq Z$ is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \emptyset$
- No wait, dual tests: $\varsigma_{?Q^d}(\emptyset) = \varsigma_{?Q}(\emptyset^{\complement})^{\complement} = (\llbracket Q \rrbracket \cap \mathcal{S})^{\complement} = \llbracket Q \rrbracket^{\complement} \not\subseteq \emptyset$

+1 Argument

Note (+1 argument)

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

$$Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_{\alpha}(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- Which Z with $\varsigma_{\alpha}(Z) \subseteq Z$ is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \emptyset$
- No wait, dual tests: $\varsigma_{?Q^d}(\emptyset) = \varsigma_{?Q}(\emptyset^{\complement})^{\complement} = ([\![Q]\!] \cap \mathcal{S})^{\complement} = [\![Q]\!]^{\complement} \not\subseteq \emptyset$
- Then: $\varsigma_{?Q^d}([\![\neg Q]\!]) = \varsigma_{?Q}([\![\neg Q]\!]^{\complement})^{\complement} = ([\![Q]\!] \cap [\![Q]\!])^{\complement} = [\![\neg Q]\!] \subseteq [\![\neg Q]\!]$

+1 Argument

Note (+1 argument)

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

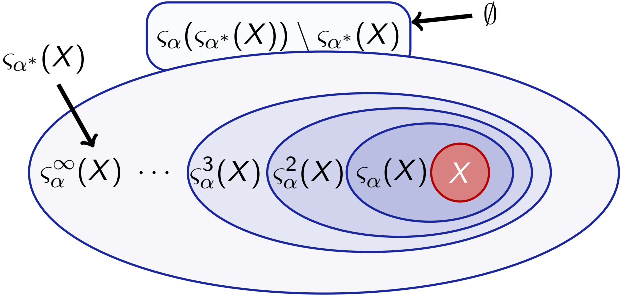
$$Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_{\alpha}(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- Which Z with $\varsigma_{\alpha}(Z) \subseteq Z$ is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \emptyset$
- No wait, dual tests: $\varsigma_{?Q^d}(\emptyset) = \varsigma_{?Q}(\emptyset^{\complement})^{\complement} = (\llbracket Q \rrbracket \cap \mathcal{S})^{\complement} = \llbracket Q \rrbracket^{\complement} \not\subseteq \emptyset$
- Then: $\varsigma_{?Q^d}(\llbracket \neg Q \rrbracket) = \varsigma_{?Q}(\llbracket \neg Q \rrbracket^{\complement})^{\complement} = (\llbracket Q \rrbracket \cap \llbracket Q \rrbracket)^{\complement} = \llbracket \neg Q \rrbracket \subseteq \llbracket \neg Q \rrbracket$
- Still too small: $X \subseteq Z$ since Angel may decide not to repeat

Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

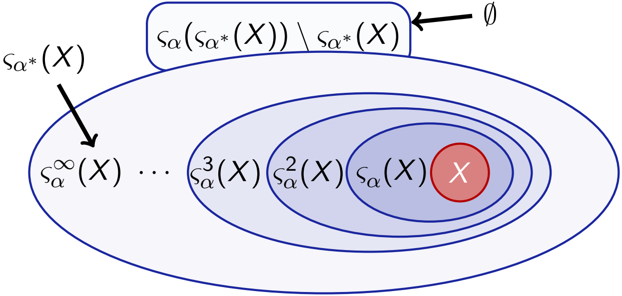
$X \cup \varsigma_\alpha(Z) \subseteq Z$ for the winning region $Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X)$



Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

$X \cup \varsigma_\alpha(Z) \subseteq Z$ for the winning region $Z \overset{\text{def}}{=} \varsigma_{\alpha^*}(X)$

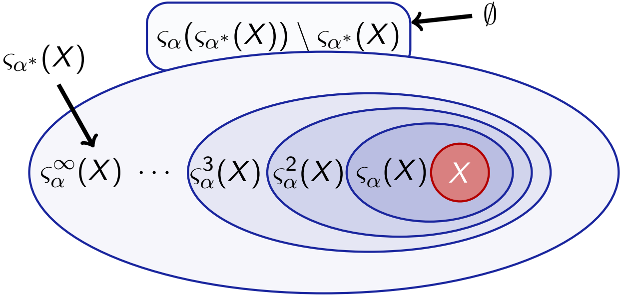


- Which Z is the right one?
- Are there multiple such Z?
- Does such a Z exist?

Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

$X \cup \varsigma_\alpha(Z) \subseteq Z$ for the winning region $Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X)$

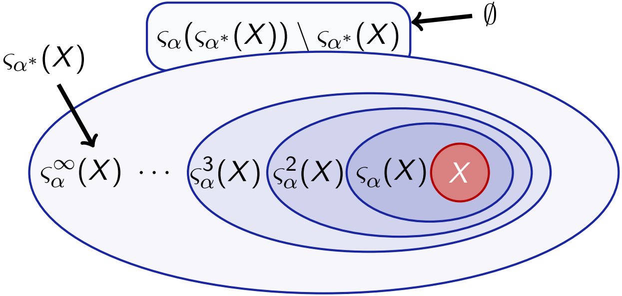


- Which Z is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \mathcal{S}$

Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

$X \cup \varsigma_\alpha(Z) \subseteq Z$ for the winning region $Z \stackrel{\text{def}}{=} \varsigma_{\alpha^*}(X)$



- Which Z is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \mathcal{S}$ but that's too big and independent of α

Comparing (Pre-)Fixpoints

Lemma ( )

$$X \cup \varsigma_\alpha(Y) \subseteq Y$$

$$X \cup \varsigma_\alpha(Z) \subseteq Z$$

are pre-fixpoints, then

Comparing (Pre-)Fixpoints

Lemma (Intersection closure)

$$X \cup \varsigma_\alpha(Y) \subseteq Y$$
$$X \cup \varsigma_\alpha(Z) \subseteq Z$$

are pre-fixpoints, then $Y \cap Z$ *is a smaller pre-fixpoint.*

Comparing (Pre-)Fixpoints

Lemma (Intersection closure)

$$X \cup \varsigma_\alpha(Y) \subseteq Y$$
$$X \cup \varsigma_\alpha(Z) \subseteq Z$$

are pre-fixpoints, then $Y \cap Z$ *is a smaller pre-fixpoint.*

Proof.

$$X \cup \varsigma_\alpha(Y \cap Z) \overset{\text{mon}}{\subseteq} X \cup (\varsigma_\alpha(Y) \cap \varsigma_\alpha(Z)) \overset{\text{above}}{\subseteq} Y \cap Z$$

□

Comparing (Pre-)Fixpoints

Lemma (Intersection closure)

$$X \cup \varsigma_\alpha(Y) \subseteq Y$$
$$X \cup \varsigma_\alpha(Z) \subseteq Z$$

are pre-fixpoints, then $Y \cap Z$ *is a smaller pre-fixpoint.*

Proof.

$$X \cup \varsigma_\alpha(Y \cap Z) \overset{\text{mon}}{\subseteq} X \cup (\varsigma_\alpha(Y) \cap \varsigma_\alpha(Z)) \overset{\text{above}}{\subseteq} Y \cap Z$$

□

Even: The intersection of *any* family of pre-fixpoints is a pre-fixpoint!

Comparing (Pre-)Fixpoints

Lemma (Intersection closure)

$$X \cup \varsigma_\alpha(Y) \subseteq Y$$
$$X \cup \varsigma_\alpha(Z) \subseteq Z$$

are pre-fixpoints, then $Y \cap Z$ *is a smaller pre-fixpoint.*

Proof.

$$X \cup \varsigma_\alpha(Y \cap Z) \overset{\text{mon}}{\subseteq} X \cup (\varsigma_\alpha(Y) \cap \varsigma_\alpha(Z)) \overset{\text{above}}{\subseteq} Y \cap Z$$

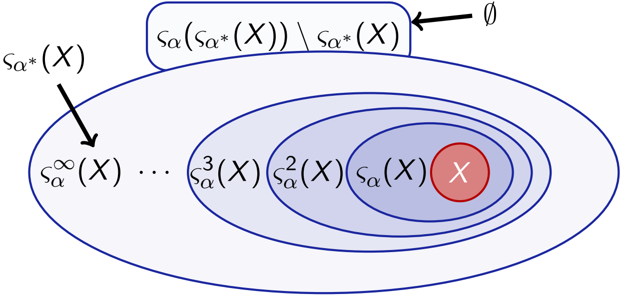
□

Even: The intersection of *any* family of pre-fixpoints is a pre-fixpoint!
So: repetition semantics is the smallest pre-fixpoint (well-founded)

Semantics of Repetition

Definition (Hybrid game α)

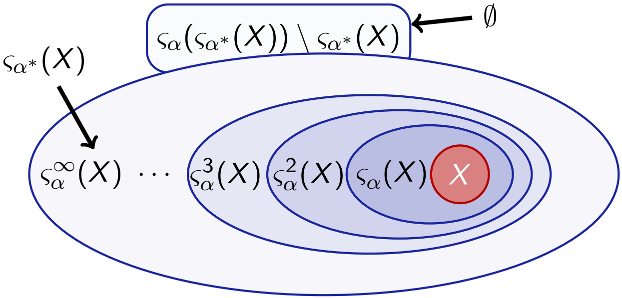
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \ :\ X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Semantics of Repetition

Definition (Hybrid game α)

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



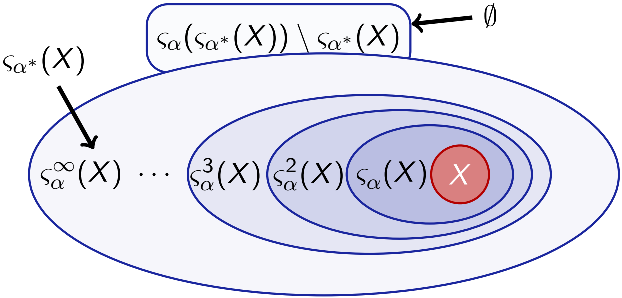
$X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$

$\varsigma_{\alpha^*}(X)$ intersection of solution

Semantics of Repetition

Definition (Hybrid game α)

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



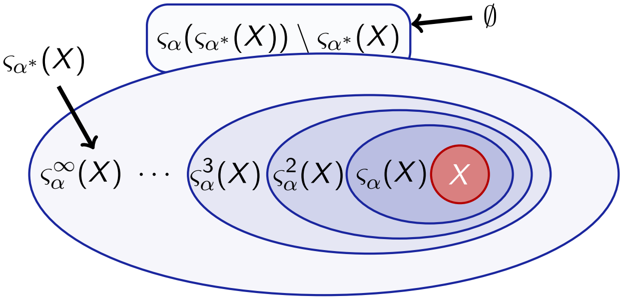
$Z \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

$\varsigma_\alpha(Z) \subseteq \quad \varsigma_\alpha(\varsigma_{\alpha^*}(X))$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

Semantics of Repetition

Definition (Hybrid game α)

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



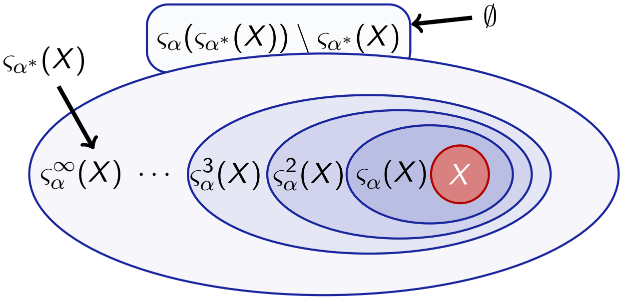
$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

Semantics of Repetition

Definition (Hybrid game α)

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



$Z \stackrel{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

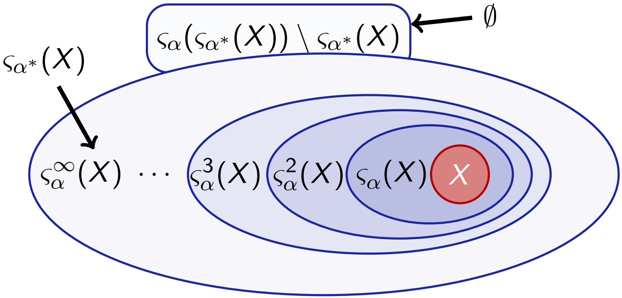
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

$\varsigma_{\alpha^*}(X) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — since $\varsigma_{\alpha^*}(X)$ smallest such Z

Semantics of Repetition

Definition (Hybrid game α)

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



$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

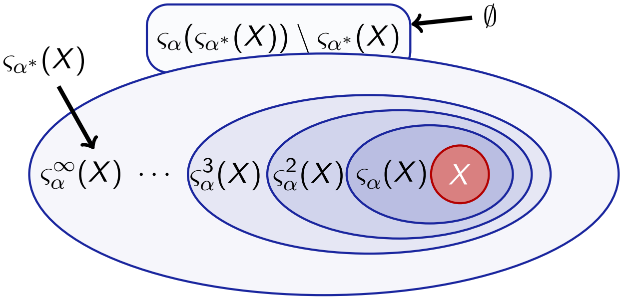
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

$\varsigma_{\alpha^*}(X) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — since $\varsigma_{\alpha^*}(X)$ smallest such Z

Semantics of Repetition

Definition (Hybrid game α)

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



$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

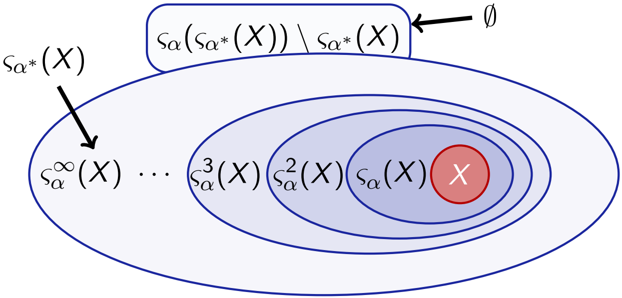
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — since $\varsigma_{\alpha^*}(X)$ smallest such Z

Semantics of Repetition

Definition (Hybrid game α)

$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) = Z\} = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$ by Knaster-Tarski



$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ — $\varsigma_{\alpha^*}(X)$ intersection of solution

$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

$\varsigma_{\alpha^*}(X) = X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ — since $\varsigma_{\alpha^*}(X)$ smallest such Z

Outline

Differential Game Logic: Denotational Semantics

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

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

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: Denotational Semantics

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

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

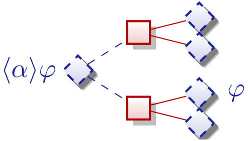
Definition (dGL Formula P) $[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S})$

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

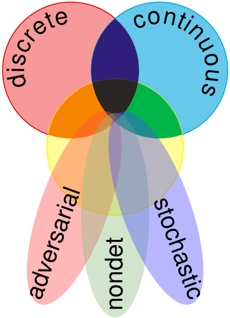
Summary

differential game logic

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



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



Next lecture

1. Axiomatics
2. How to win and prove hybrid games

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.