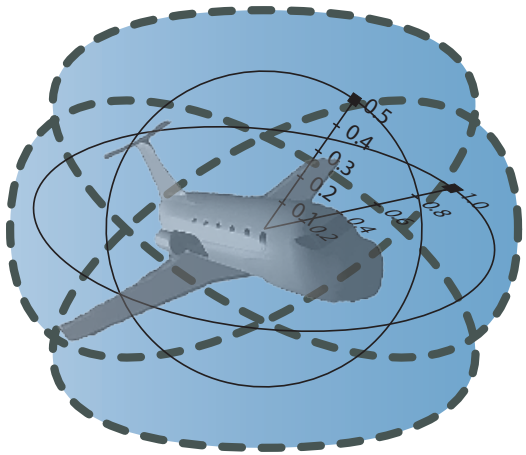
18: Winning & Proving Hybrid Games

15-424: Foundations of Cyber-Physical Systems

André Platzer

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

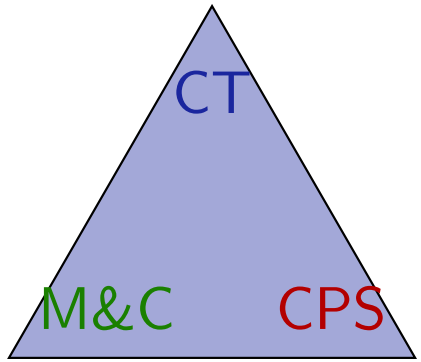


Outline

Outline

Learning Objectives
Winning & Proving Hybrid Games

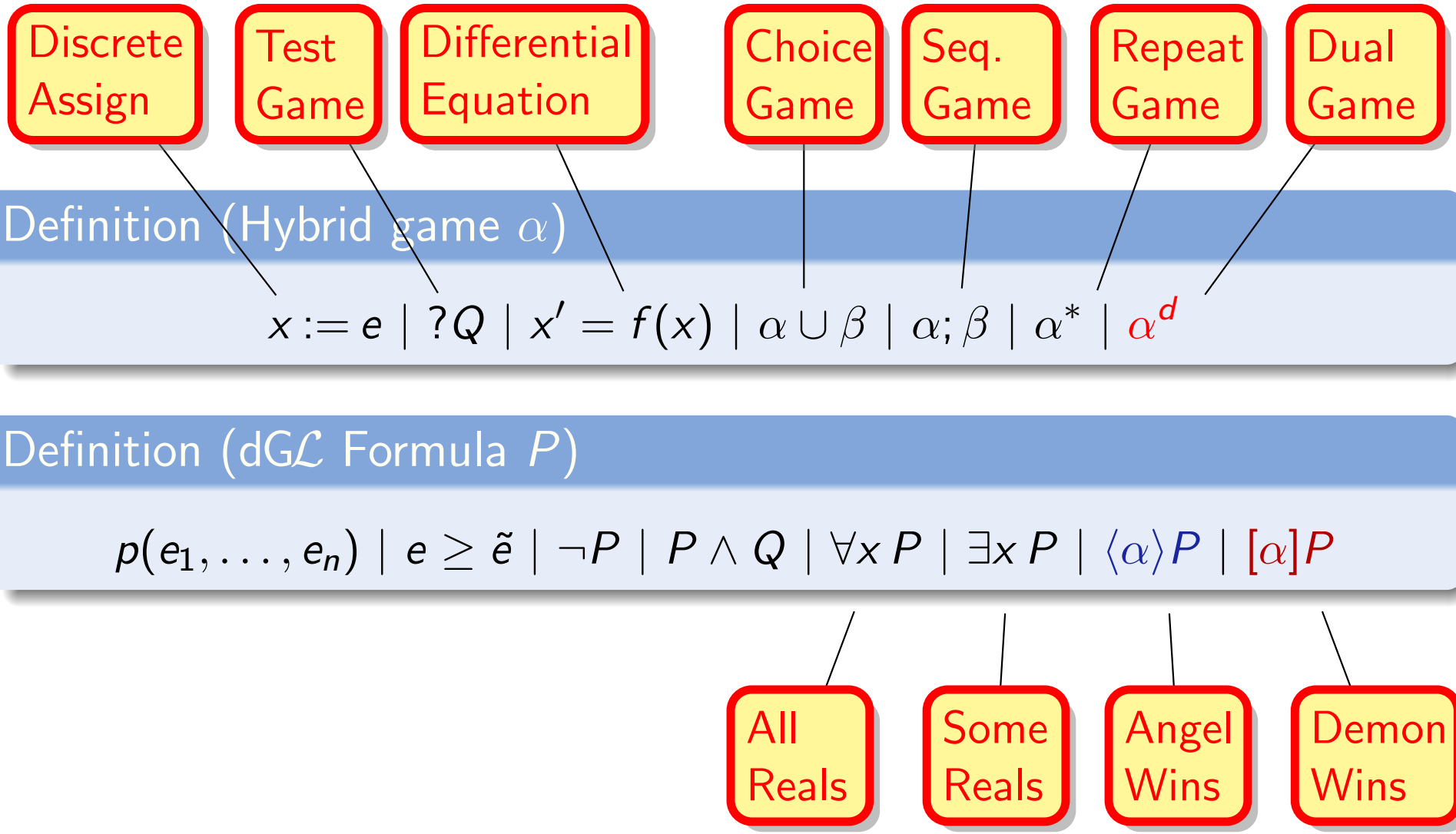
rigorous reasoning for adversarial dynamics
compositional reasoning from compositional semantics
modular addition of adversarial dynamics
axiomatization of dG$\mathcal{L}$



analytical & semantical interaction
of discrete+continuous+adversarial
adversarial repetitions
fixpoints

CPS semantics
align semantics&reasoning
operational CPS effects

Differential Game Logic: Syntax



TOCL'15

Differential Game Logic: Denotational Semantics

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

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

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

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

Outline

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

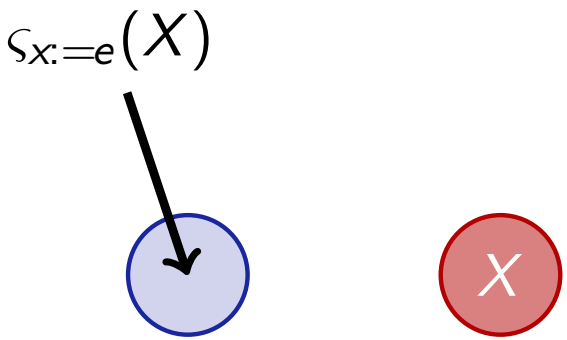
$$\langle^d\rangle\ \langle\alpha^d\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

TOCL'15

Hybrid Game Axioms

Axiom (Assignment) TOCL'15

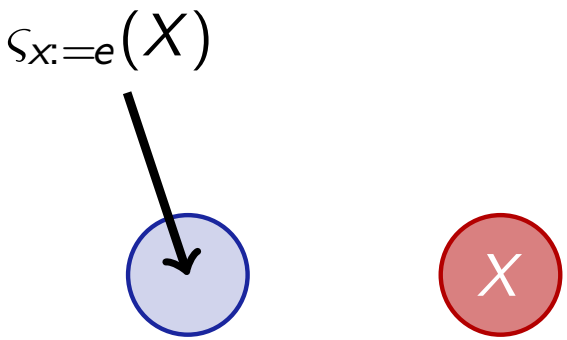
$\langle := \rangle \quad \langle x := e \rangle p(x) \leftrightarrow$



Hybrid Game Axioms

Axiom (Assignment) TOCL'15

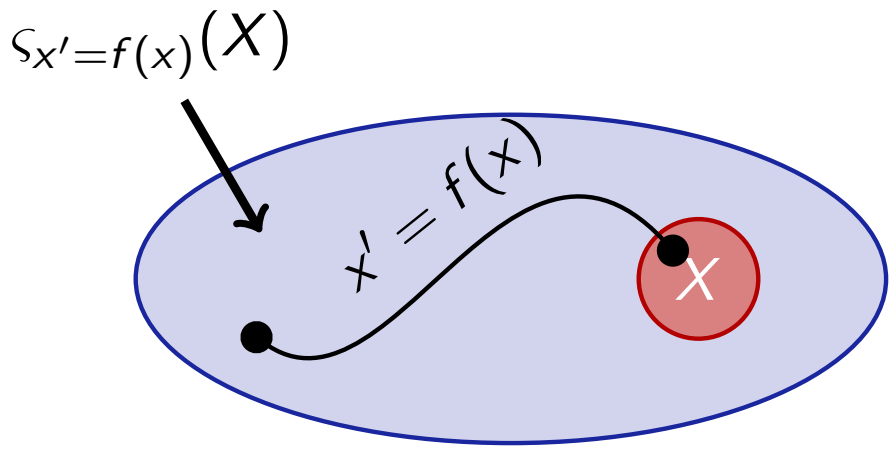
$\langle := \rangle \quad \langle x := e \rangle p(x) \leftrightarrow p(e)$



Hybrid Game Axioms

Axiom (Differential Equation) TOCL'15

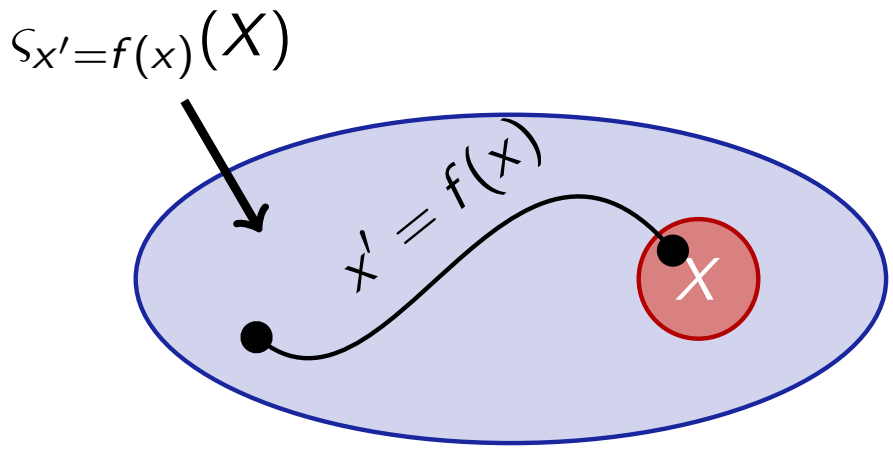
$\langle' \rangle \quad \langle x' = f(x) \rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Differential Equation) TOCL'15

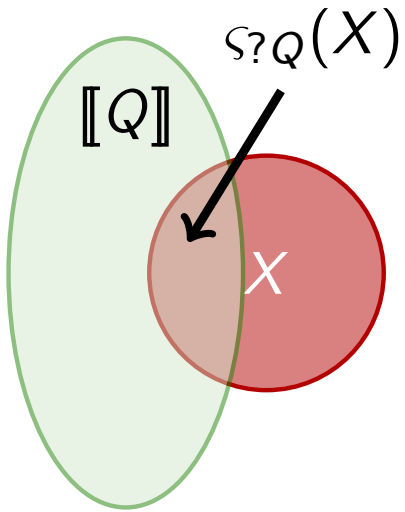
$\langle' \rangle \quad \langle x' = f(x) \rangle P \leftrightarrow \exists t \geq 0 \, \langle x := y(t) \rangle P$



Hybrid Game Axioms

Axiom (Test) TOCL'15

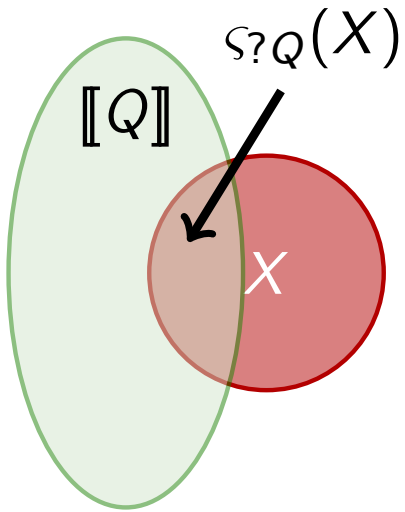
$\langle ? \rangle \quad \langle ?Q \rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Test) TOCL'15

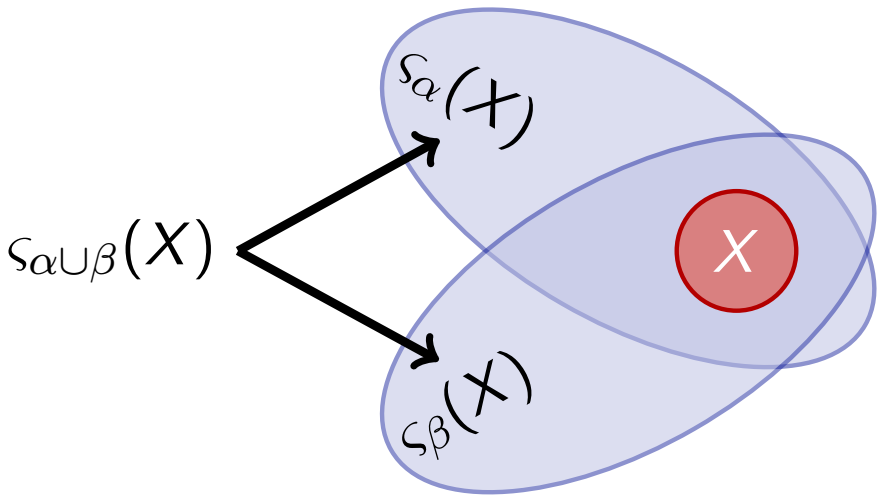
$\langle ? \rangle \quad \langle ?Q \rangle P \leftrightarrow (Q \wedge P)$



Hybrid Game Axioms

Axiom (Choice Game) TOCL'15

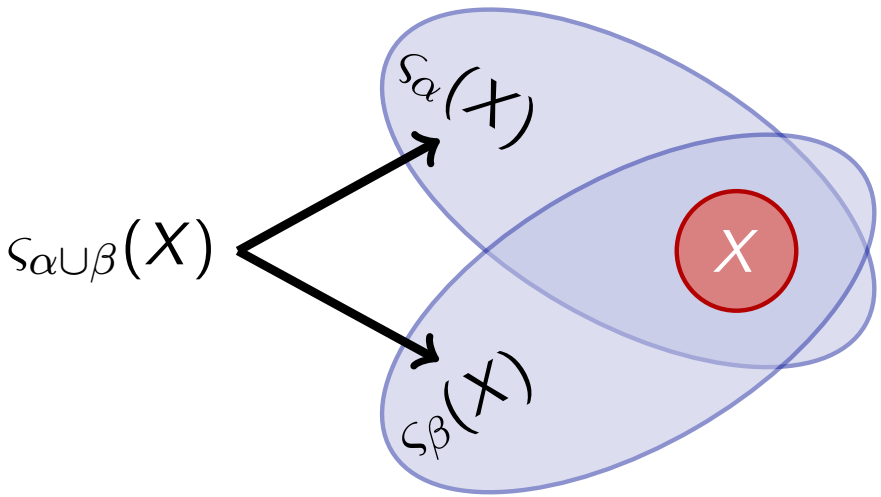
$\langle\cup\rangle \quad \langle\alpha \cup \beta\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Choice Game) TOCL'15

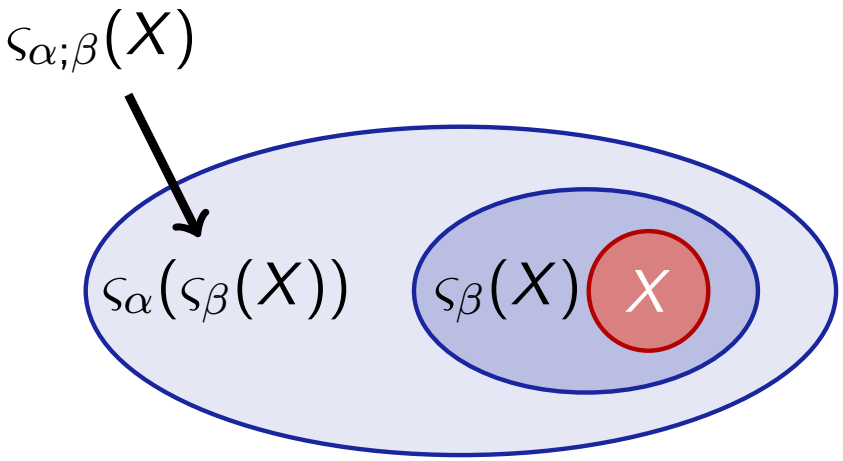
$\langle\cup\rangle$ $\langle\alpha \cup \beta\rangle P \leftrightarrow \langle\alpha\rangle P \vee \langle\beta\rangle P$



Hybrid Game Axioms

Axiom (Sequential Game) TOCL'15

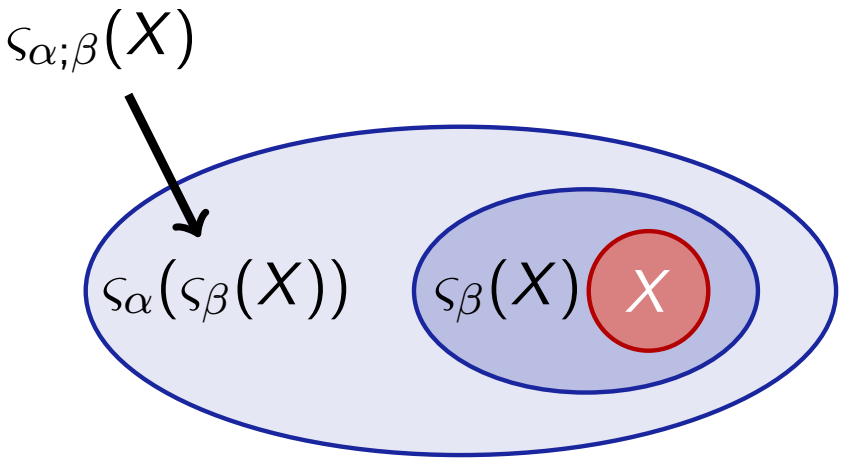
$\langle;\rangle \quad \langle\alpha;\beta\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Sequential Game) TOCL'15

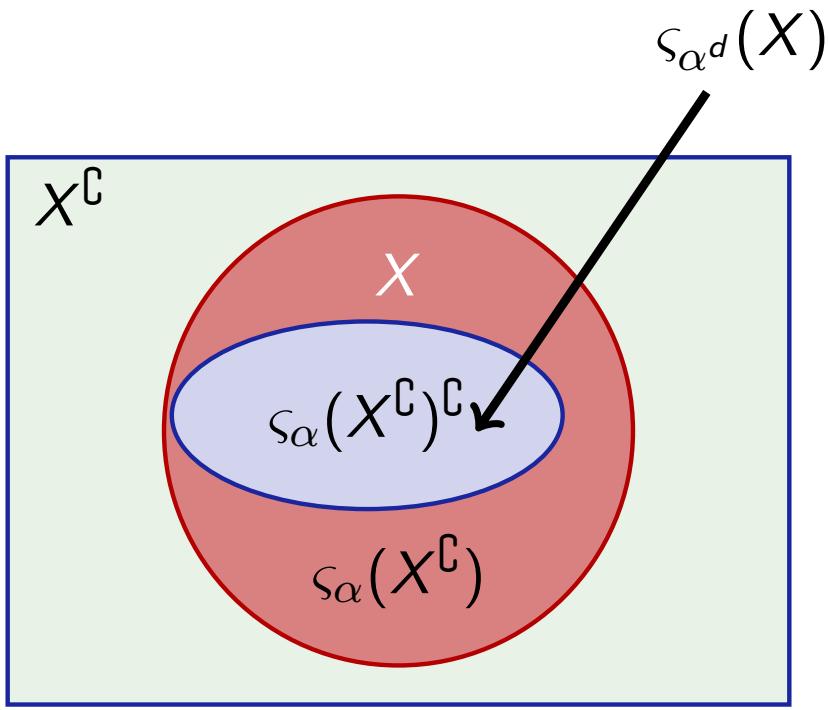
$\langle;\rangle \quad \langle\alpha;\beta\rangle P \leftrightarrow \langle\alpha\rangle\langle\beta\rangle P$



Hybrid Game Axioms

Axiom (Dual Game) TOCL'15

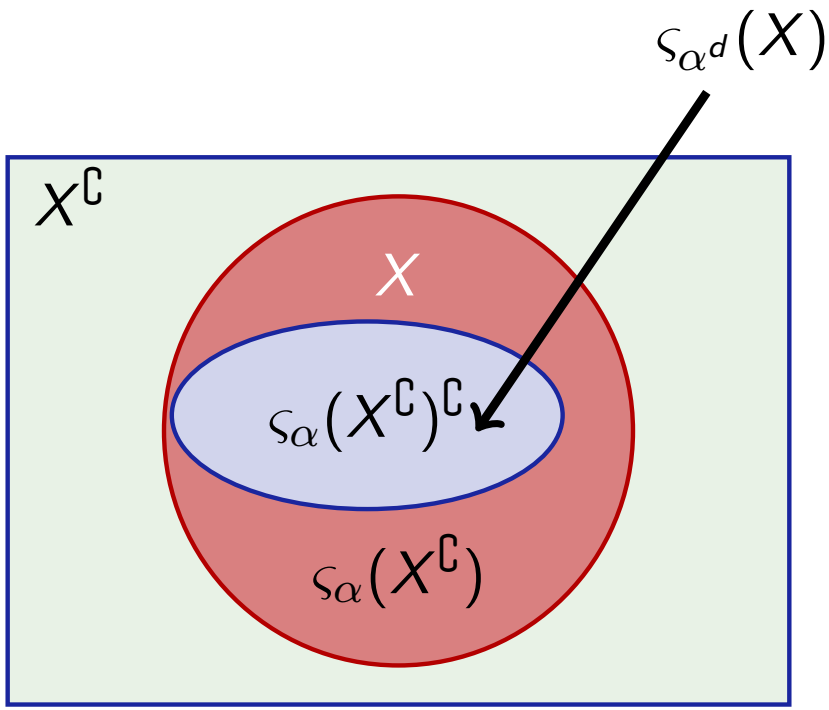
$\langle^d\rangle \quad \langle\alpha^d\rangle P \leftrightarrow$



Hybrid Game Axioms

Axiom (Dual Game) TOCL'15

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



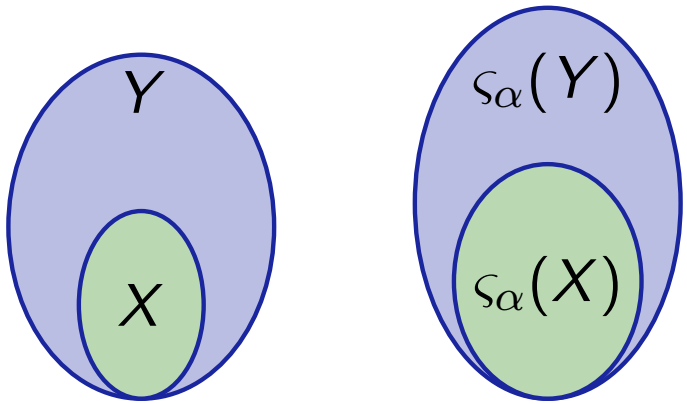
Consistency & Determinacy & Monotonicity

Theorem (Consistency & determinacy)

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

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. $\vDash \neg\langle\alpha\rangle\neg\phi \leftrightarrow [\alpha]\phi$.

Corollary (Axiom: Determinacy)

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

Lemma (Monotonicity)

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

Corollary (Rule: Monotonicity)

M $$\frac{P \to Q}{\langle\alpha\rangle P \to \langle\alpha\rangle Q}$$

Outline

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

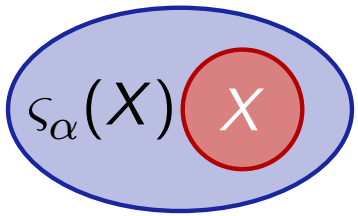
Definition (Hybrid game α)

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

Semantics of Repetition

Definition (Hybrid game α)

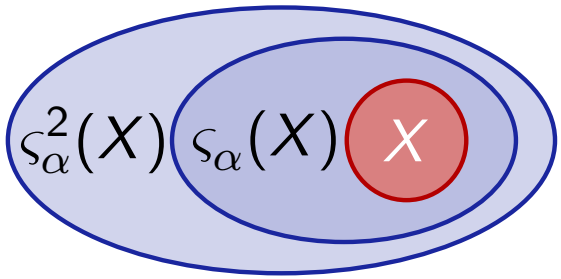
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



Semantics of Repetition

Definition (Hybrid game α)

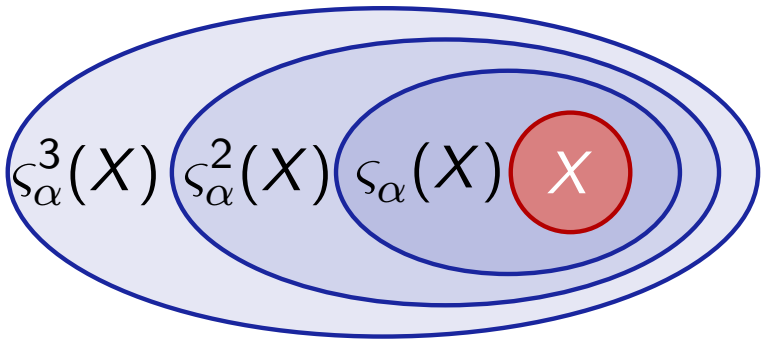
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



Semantics of Repetition

Definition (Hybrid game α)

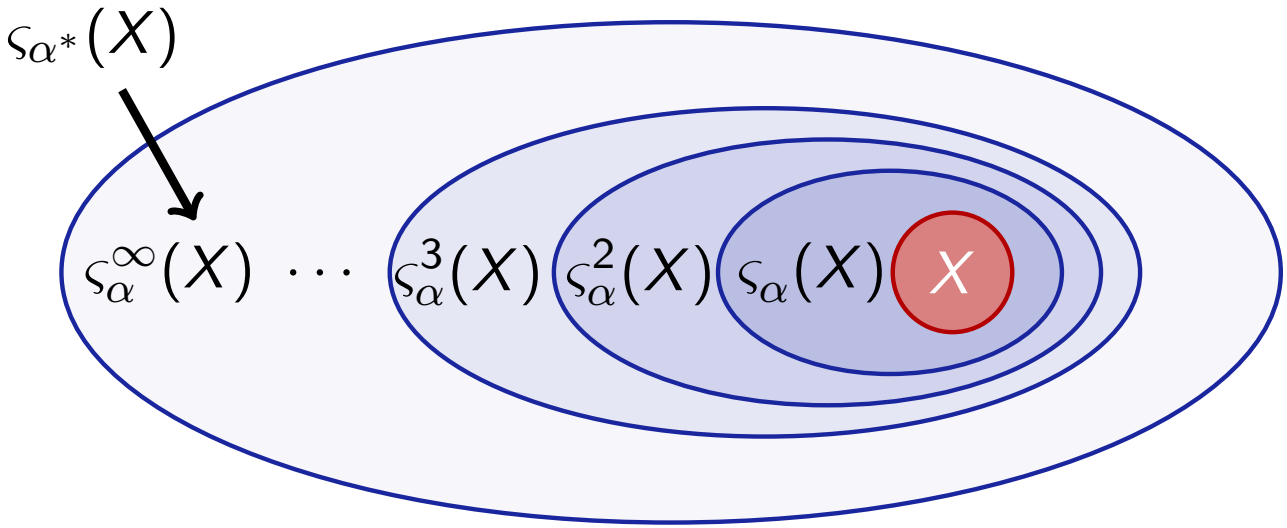
$\varsigma_{\alpha^*}(X) = \bigcup_{\kappa<\infty} \varsigma_\alpha^\kappa(X)$



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.

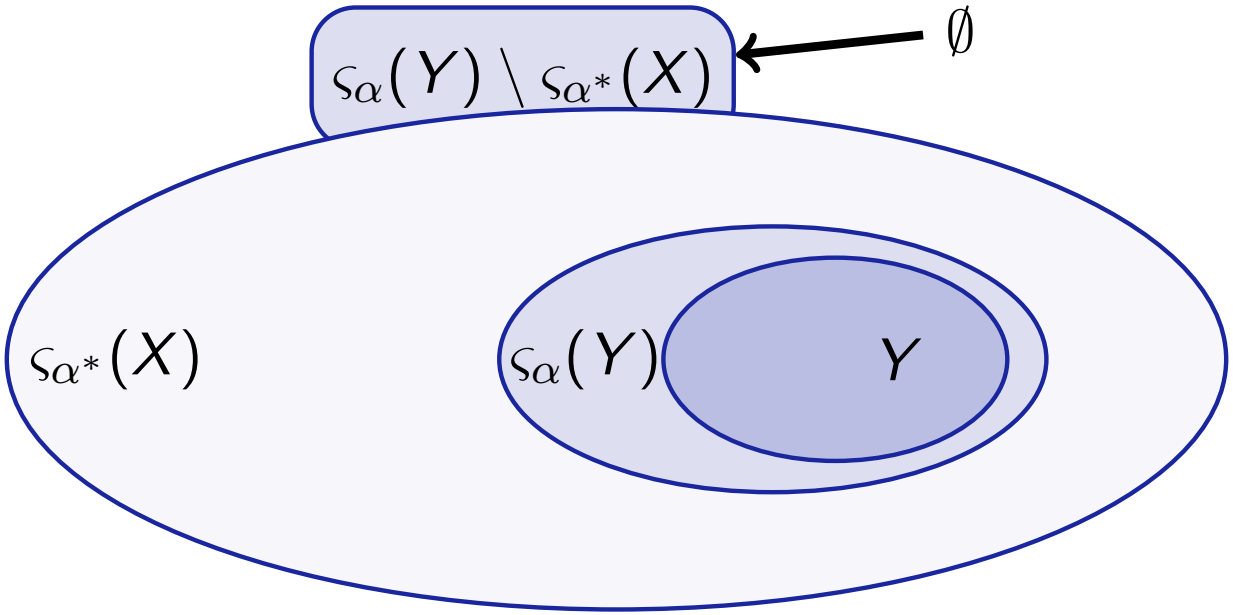
— Bertrand Russell

+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)

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

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

- 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)

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

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

- 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)

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

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

- 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)

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

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

- 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: $\varsigma_{?Q^d}(\llbracket \neg Q \rrbracket) = \varsigma_{?Q}(\llbracket \neg Q \rrbracket^{\complement})^{\complement} = (\llbracket Q \rrbracket \cap \llbracket Q \rrbracket)^{\complement} = \llbracket \neg Q \rrbracket \subseteq \llbracket \neg Q \rrbracket$

+1 Argument

Note (+1 argument)

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

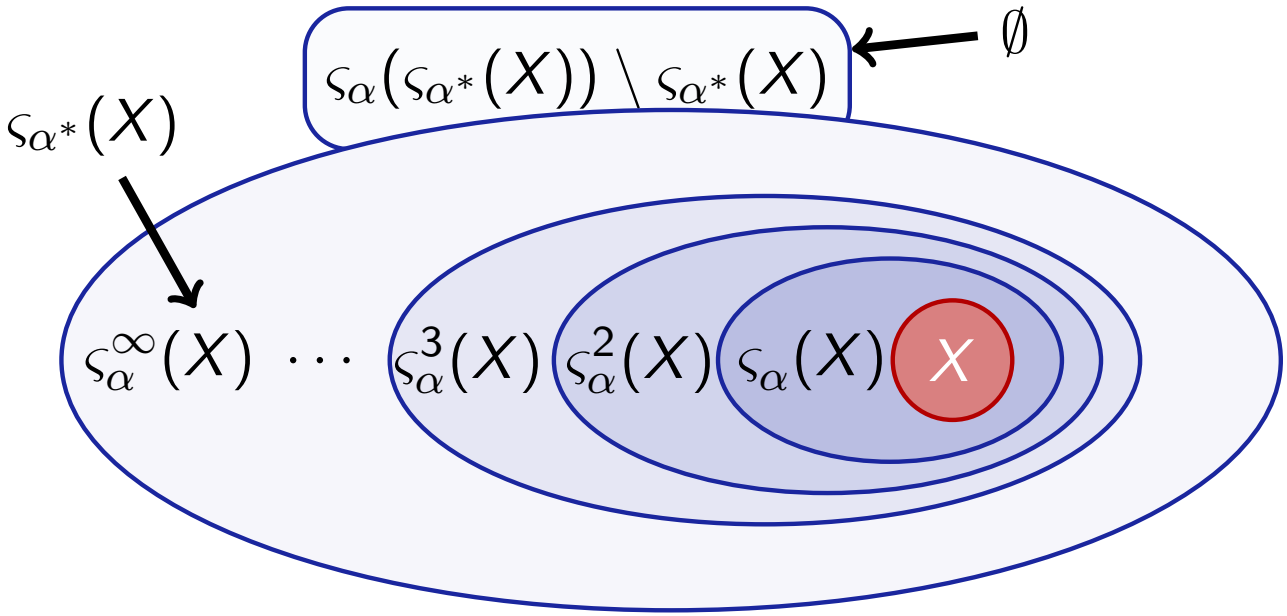
$$Z \overset{\text{def}}{=} \varsigma_{\alpha^*}(X) \text{ then } \varsigma_{\alpha}(Z) \subseteq \varsigma_{\alpha^*}(X) = Z$$

- 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)

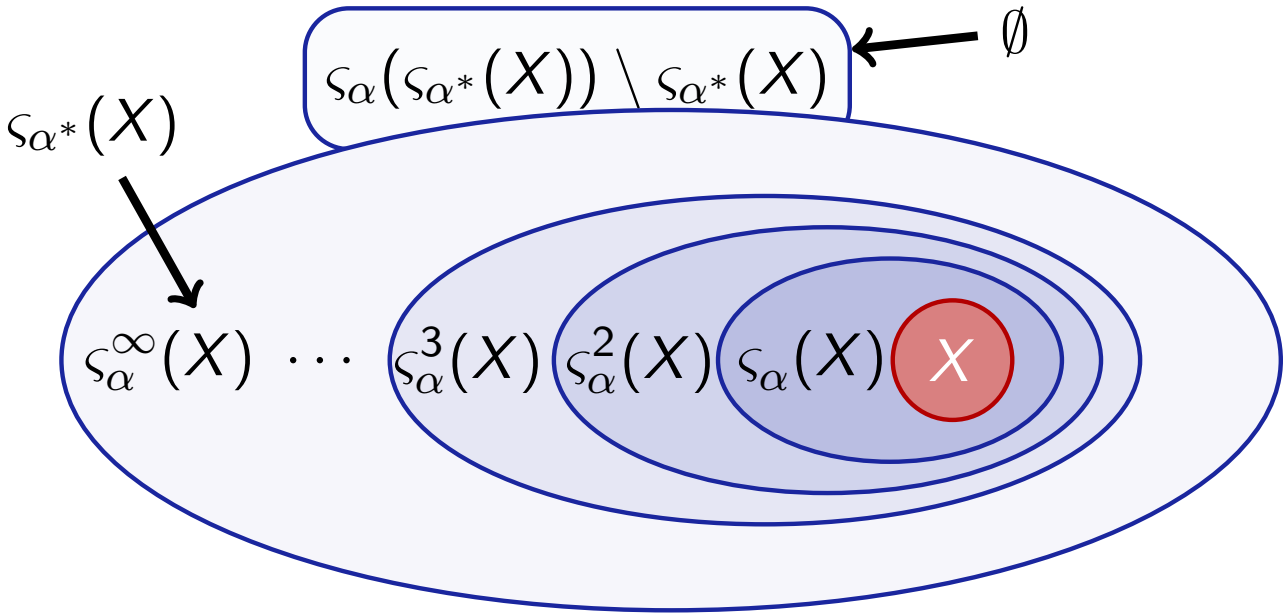
$X \cup \varsigma_\alpha(Z) \subseteq Z$ for the winning region $Z \overset{\text{def}}{=} \varsigma_{\alpha^*}(X)$



Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

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

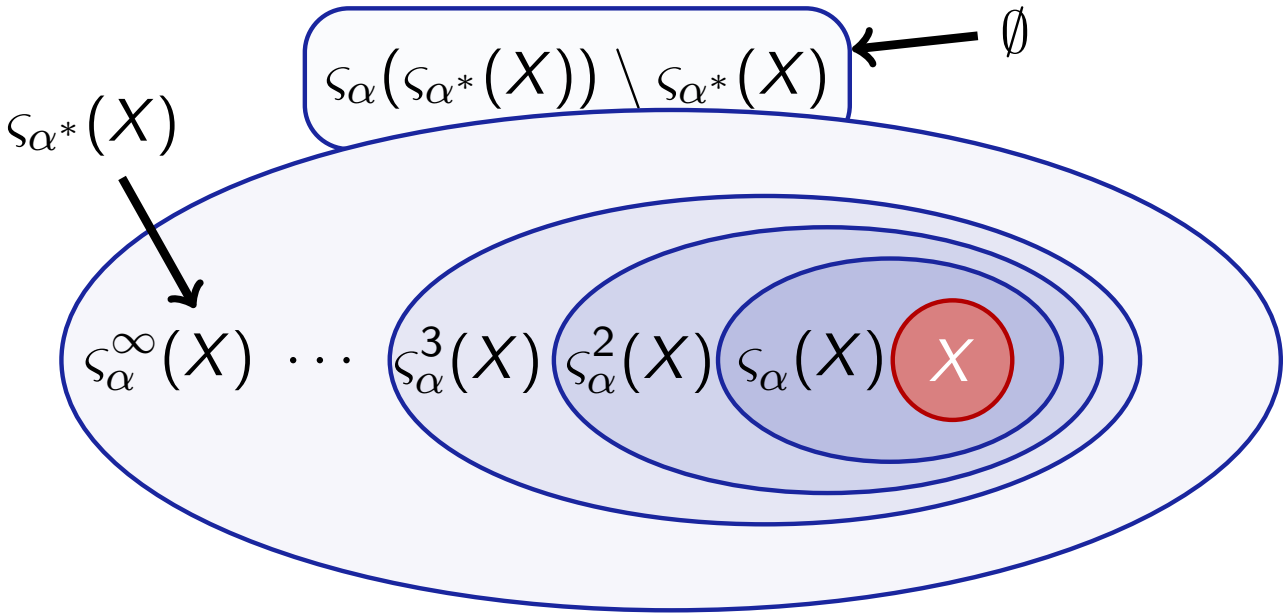


- Which Z is the right one?
- Are there multiple such Z?
- Does such a Z exist?

Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

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

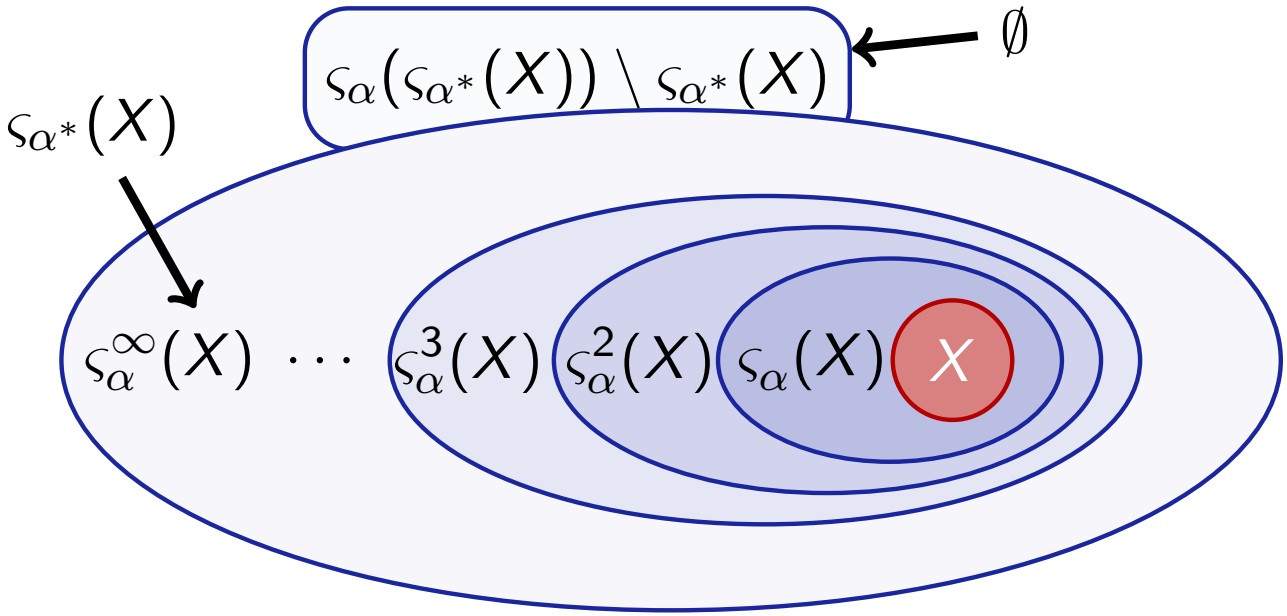


- Which Z is the right one?
- Are there multiple such Z?
- Does such a Z exist?
- Existence: $Z = \mathcal{S}$

Fixpoints and Pre-Fixpoints

Definition (Pre-fixpoint)

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



- 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.

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

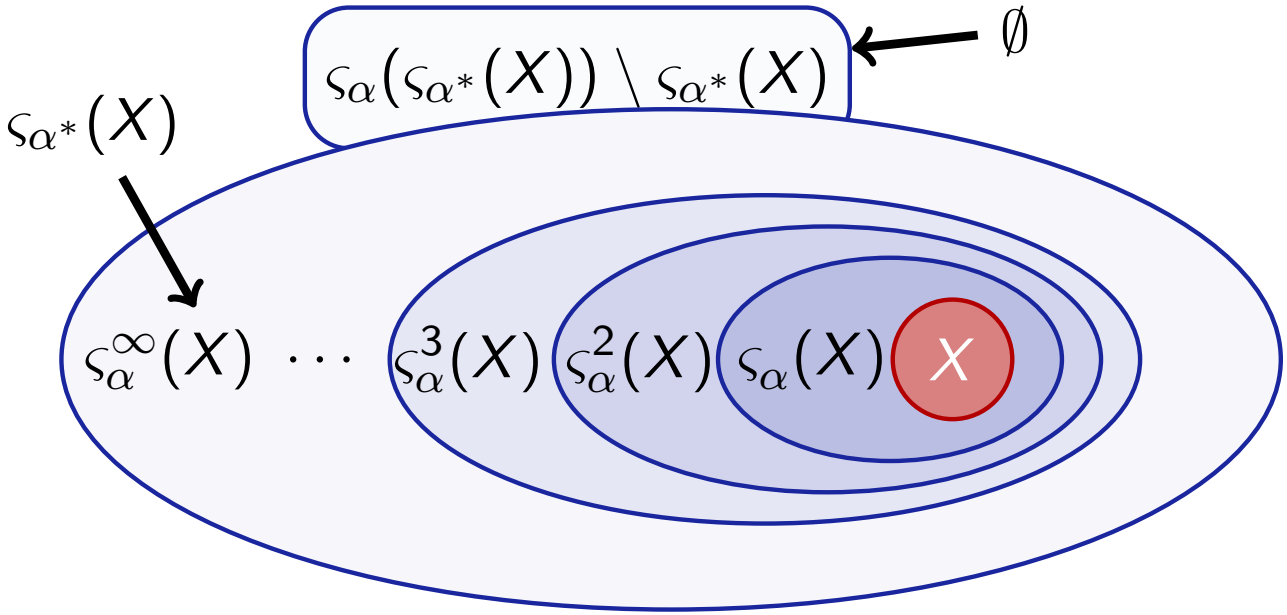
□

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)

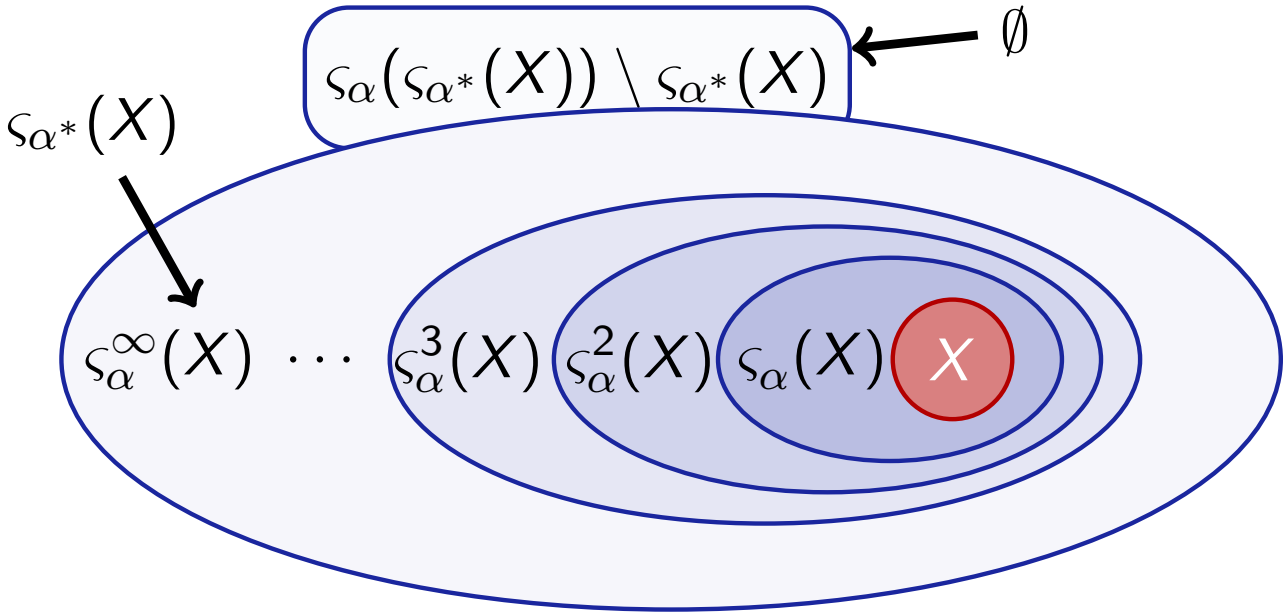
$$\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} \,:\, X \cup \varsigma_\alpha(Z) \subseteq Z\}$$



Semantics of Repetition

Definition (Hybrid game α)

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



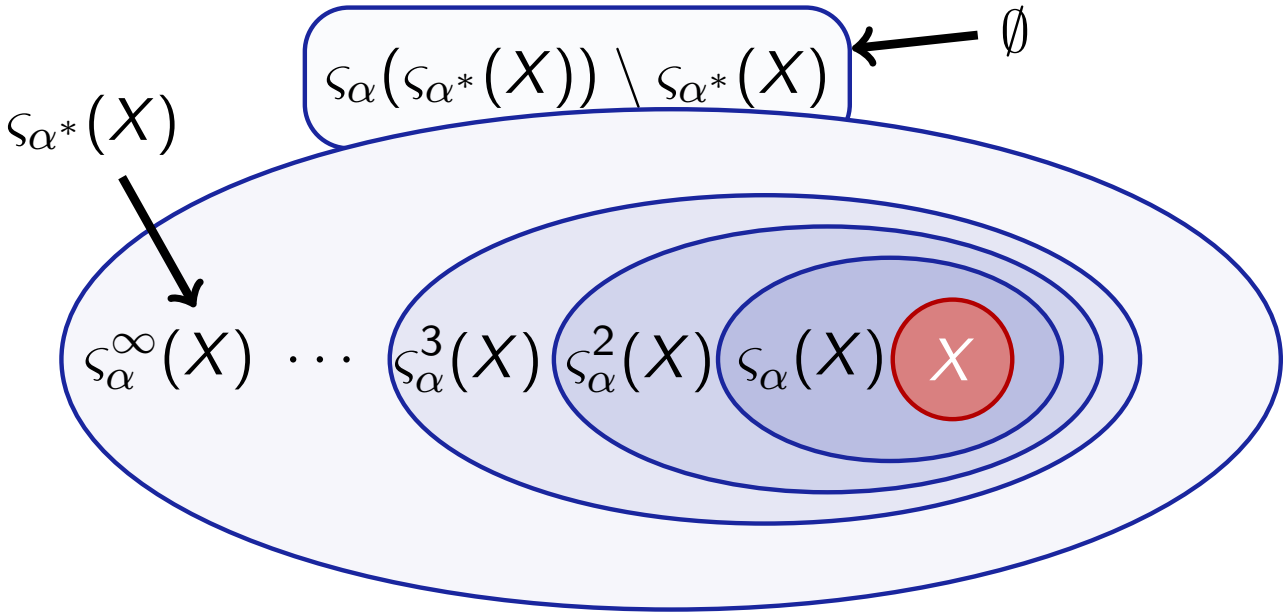
$X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$

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

Semantics of Repetition

Definition (Hybrid game α)

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



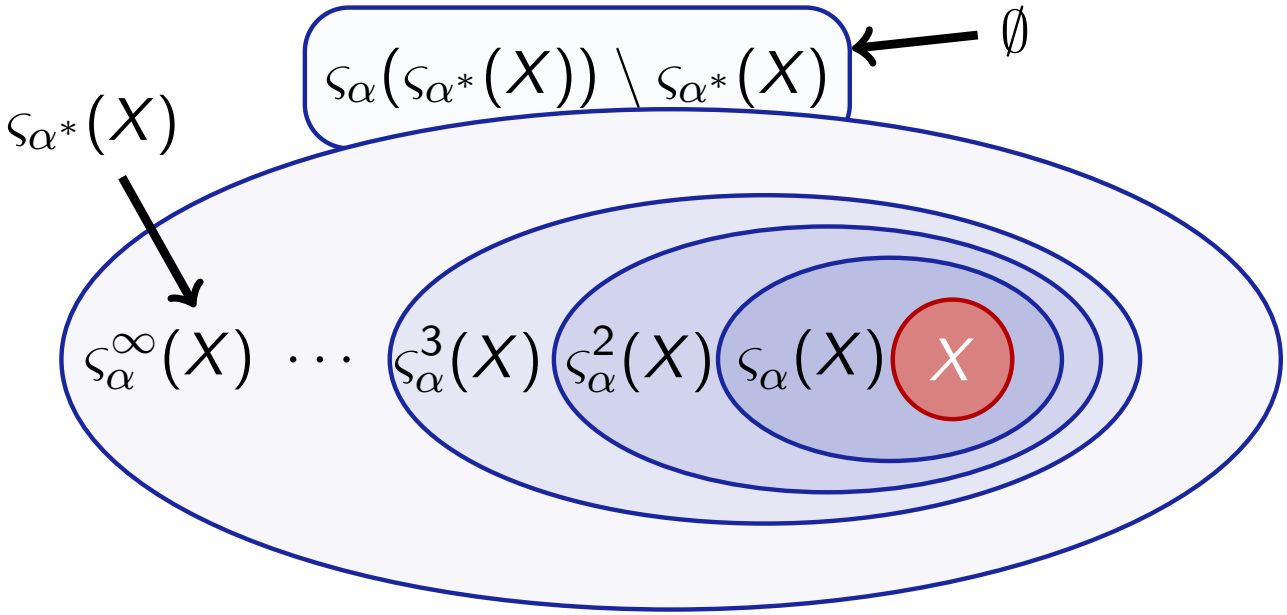
$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ $\varsigma_{\alpha^*}(X)$ intersection of solution

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

Semantics of Repetition

Definition (Hybrid game α)

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



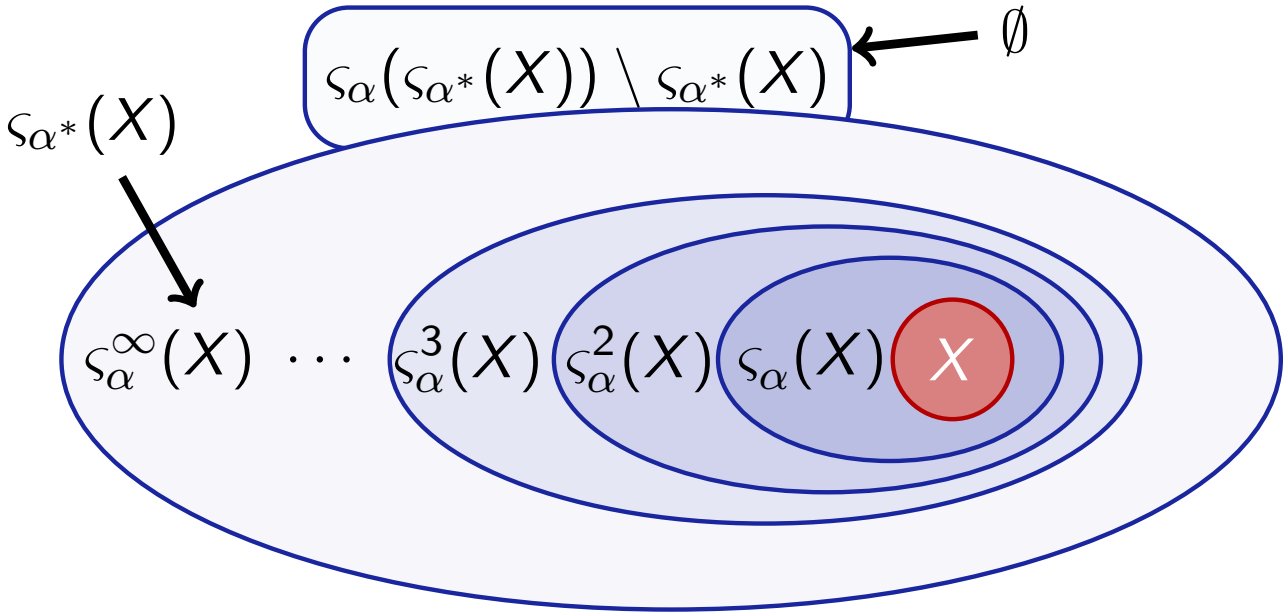
$Z \overset{\text{def}}{=} X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) \subseteq \varsigma_{\alpha^*}(X)$ $\varsigma_{\alpha^*}(X)$ intersection of solution

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

Semantics of Repetition

Definition (Hybrid game α)

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



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

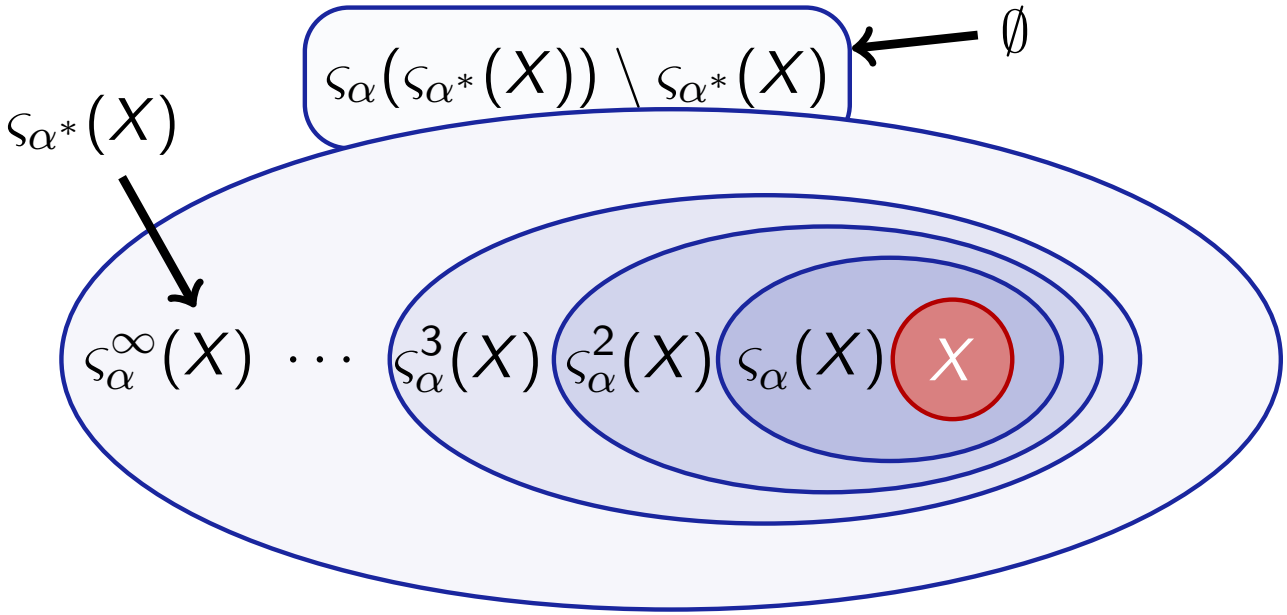
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

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

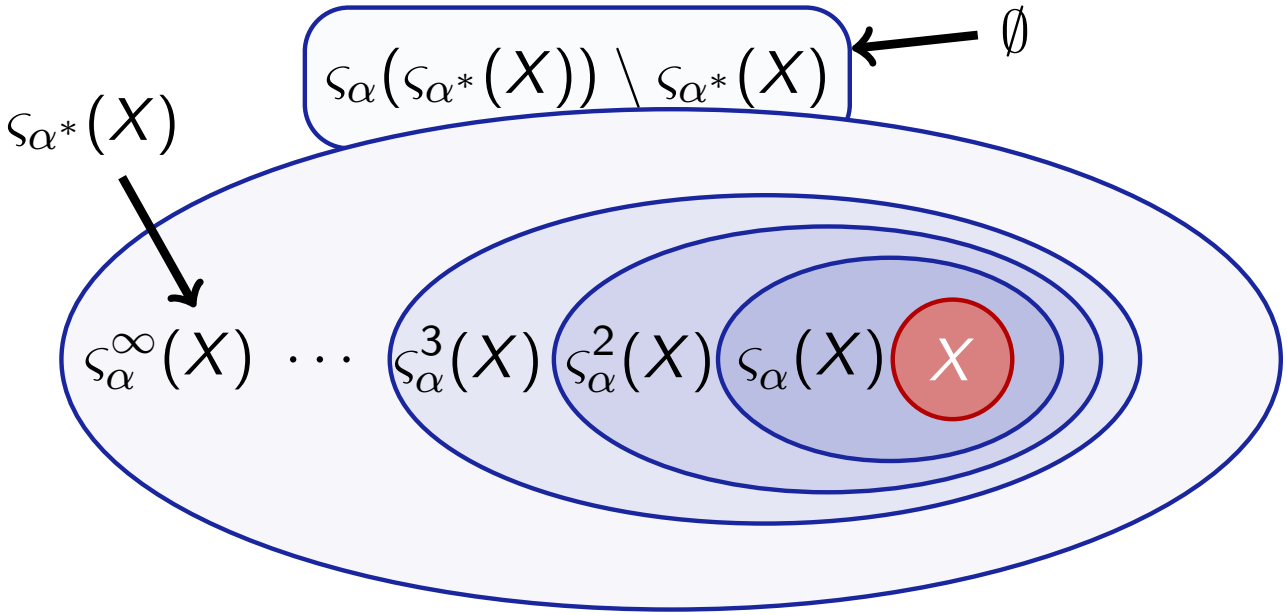
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

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

Semantics of Repetition

Definition (Hybrid game α)

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



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

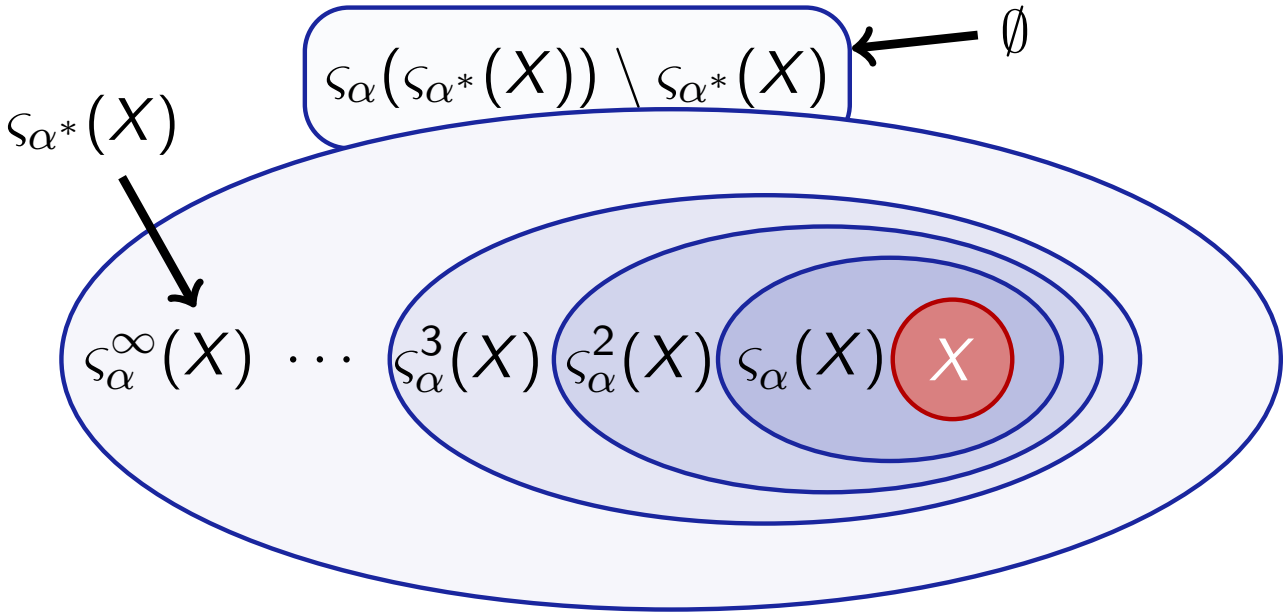
$X \cup \varsigma_\alpha(Z) \subseteq X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X)) = Z$ by mon since $Z \subseteq \varsigma_{\alpha^*}(X)$

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

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

Proofs for Loops

Definition (Hybrid game α)

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

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

Proofs for Loops

Definition (Hybrid game α)

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

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

Corollary (Axiom: Iteration)

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

Proofs for Loops

Definition (Hybrid game α)

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

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

Corollary (Axiom: Iteration)

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

Proofs for Loops

Definition (Hybrid game α)

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

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

Corollary (Axiom: Iteration)

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

Corollary (Rule: Least Fixpoint)

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

Proofs for Loops

Definition (Hybrid game α)

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

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

Corollary (Axiom: Iteration)

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

Corollary (Rule: Least Fixpoint)

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

Corollary (Derived Rule: Loop)

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

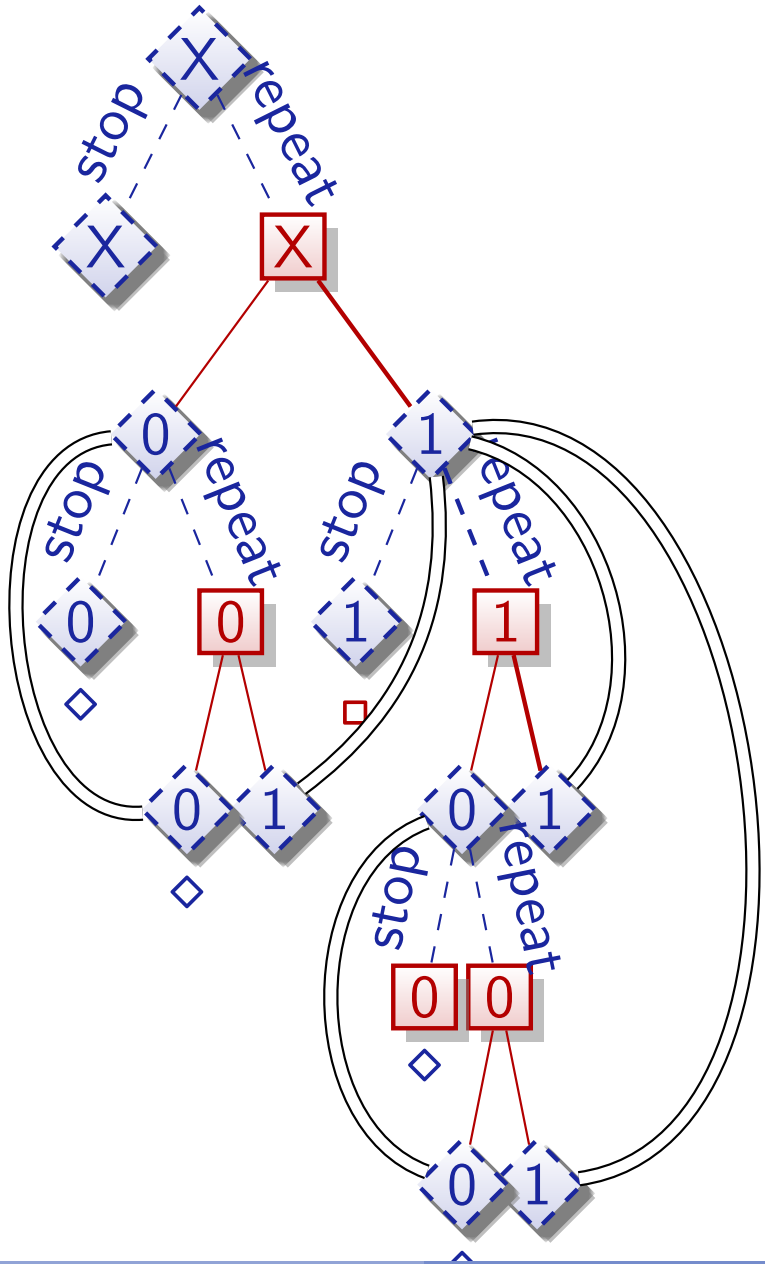
$$\forall\ \frac{p \to Q}{p \to \forall x\, Q} \qquad (x \notin \mathrm{FV}(p))$$

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

TOCL'15

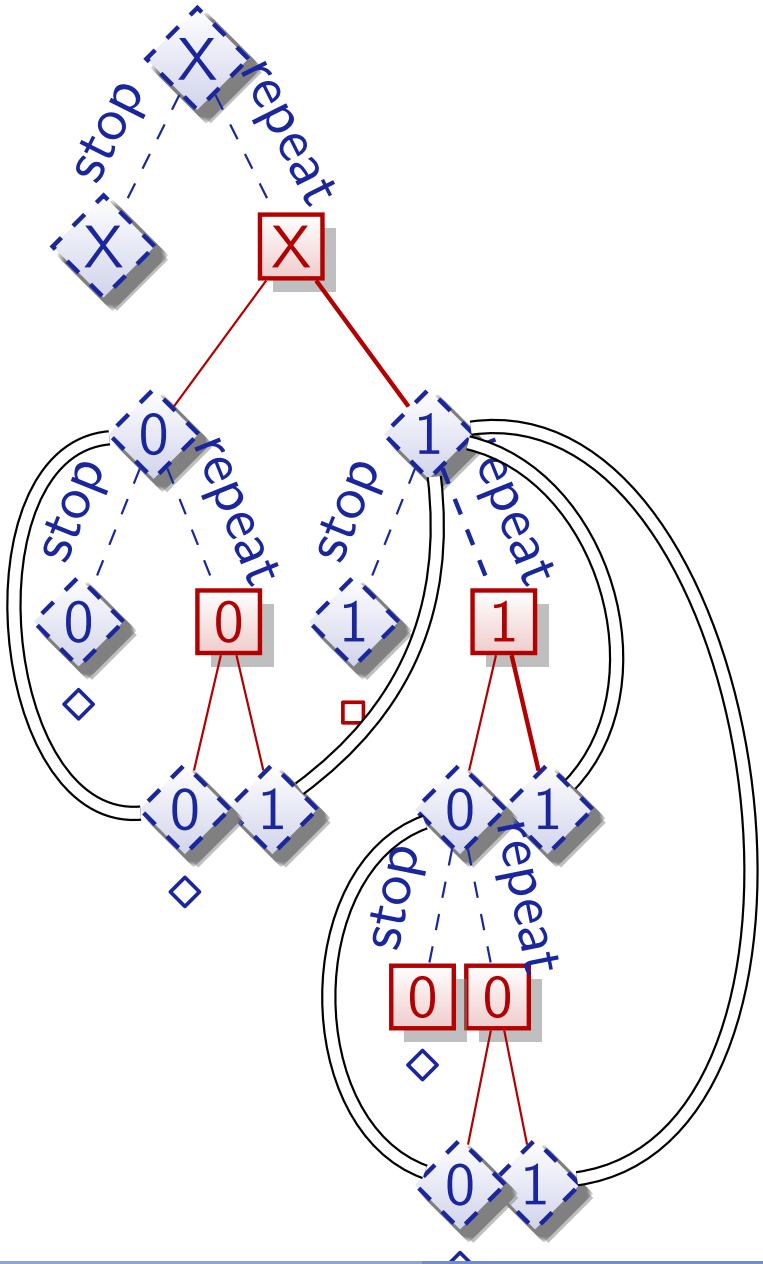
Example Proof: Dual Filibuster

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



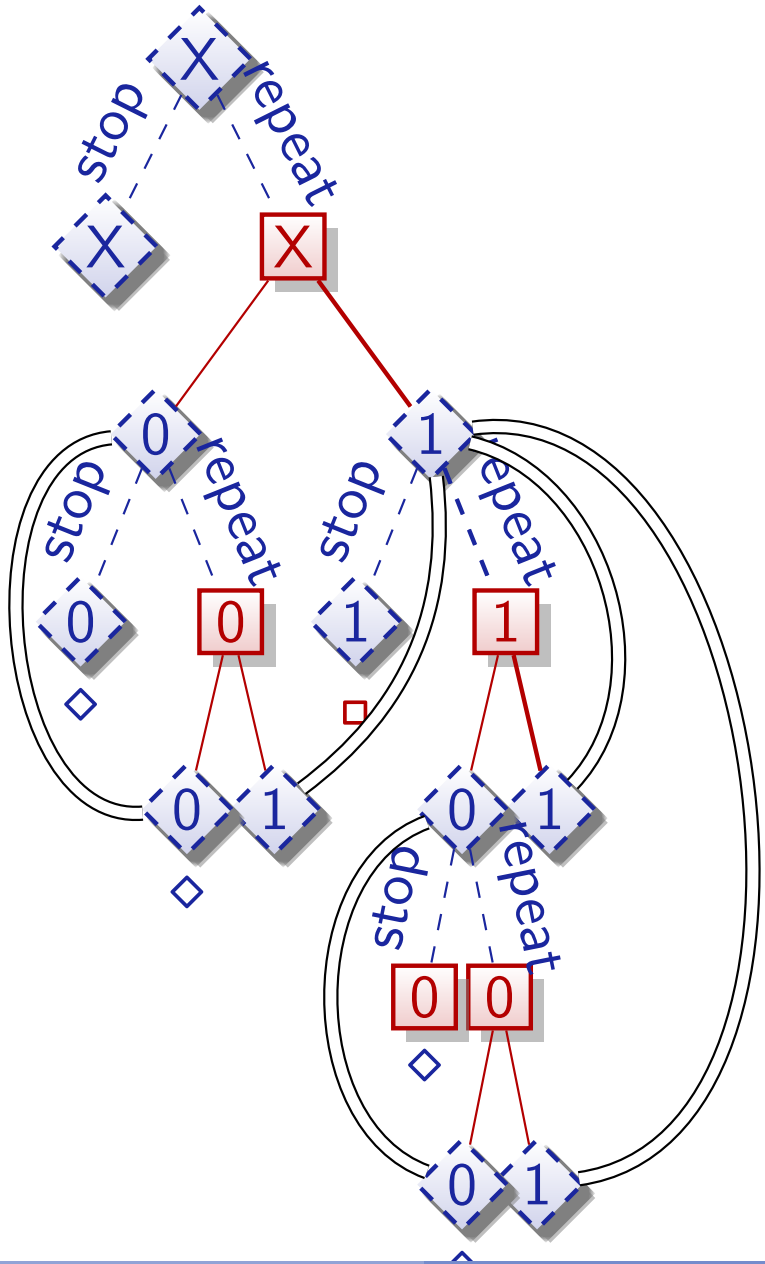
Example Proof: Dual Filibuster

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



Example Proof: Dual Filibuster

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



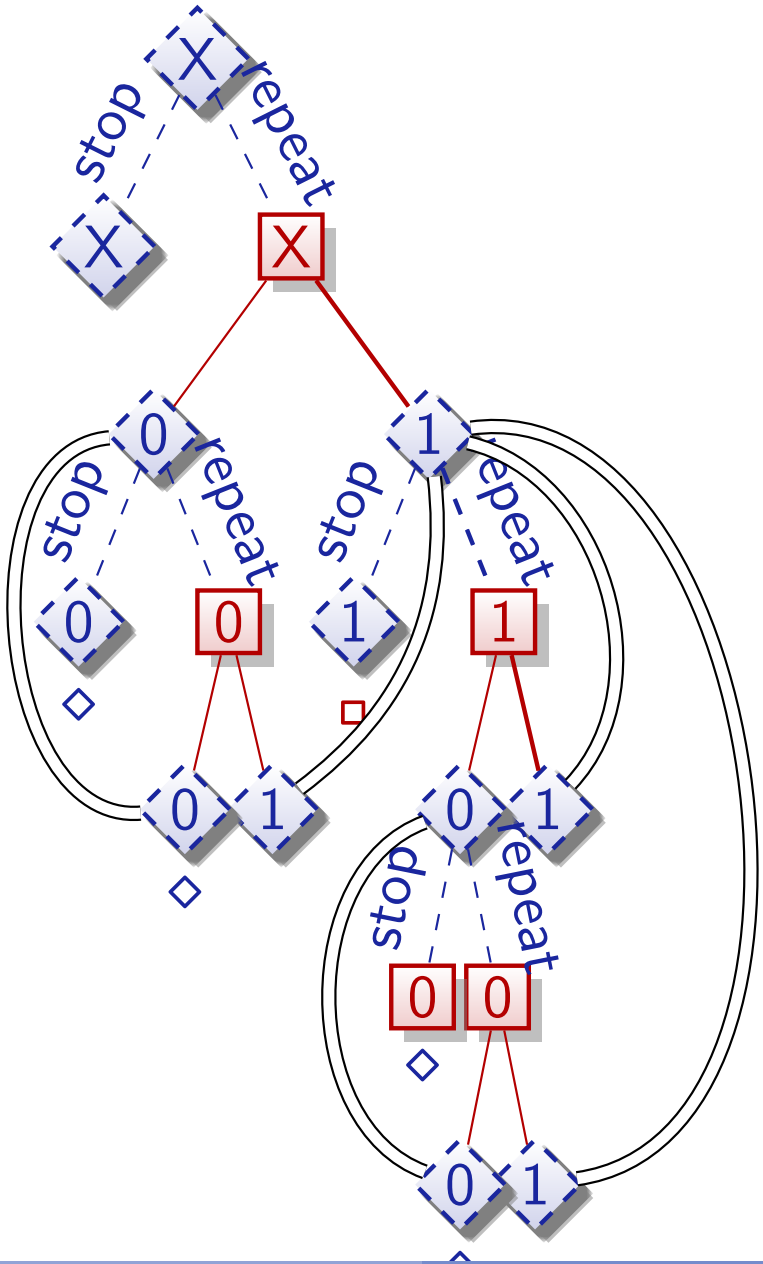
Example Proof: Dual Filibuster

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

$$[\cdot]\ \frac{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle \neg x=0}{x=0 \vdash [x:=0 \cap x:=1]x=0}$$

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

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



Example Proof: Dual Filibuster

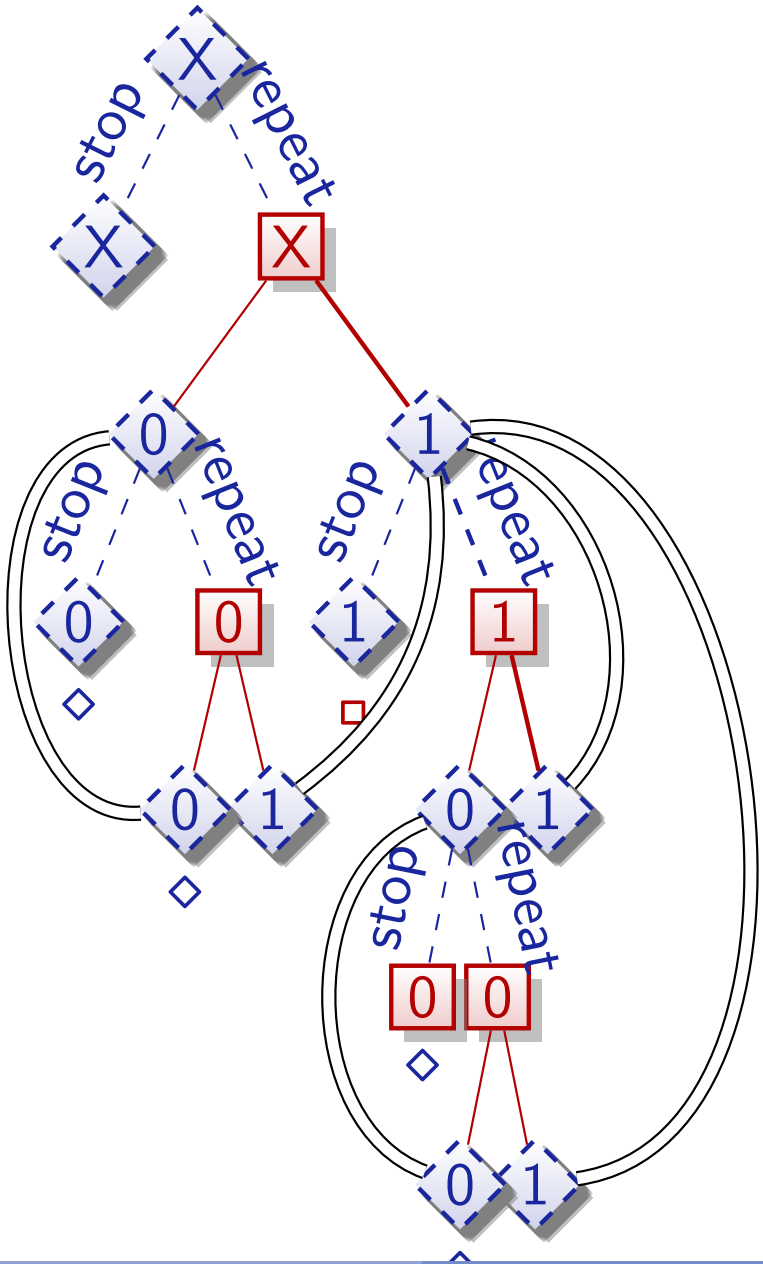
$$\langle\cup\rangle\ \frac{}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}$$

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

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

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

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



Example Proof: Dual Filibuster

$$\langle:=\rangle\ \frac{}{x=0 \vdash \langle x:=0\rangle x=0 \vee \langle x:=1\rangle x=0}$$

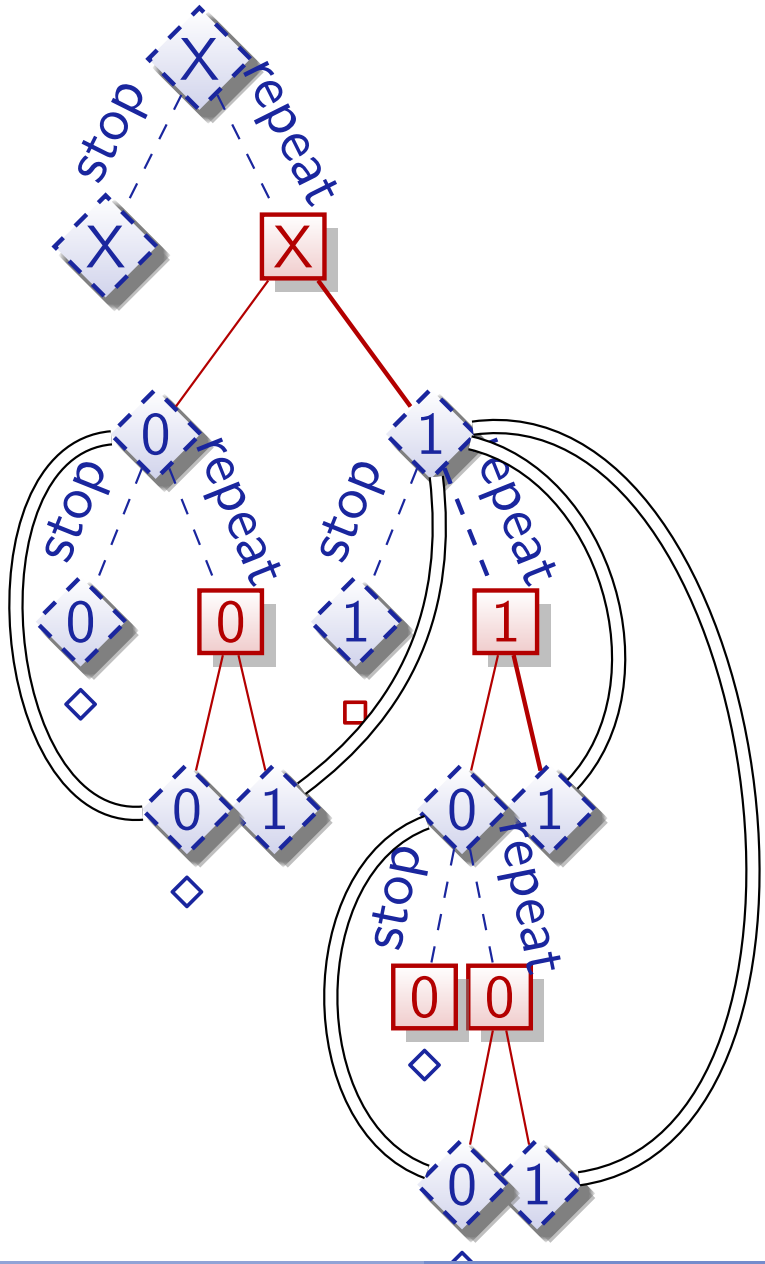
$$\langle\cup\rangle\ \frac{x=0 \vdash \langle x:=0\rangle x=0 \vee \langle x:=1\rangle x=0}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}$$

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

$$[\cdot]\ \frac{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle\neg x=0}{x=0 \vdash [x:=0 \cap x:=1]x=0}$$

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

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



Example Proof: Dual Filibuster

$$\mathbb{R}\ \frac{}{x=0 \vdash 0=0 \vee 1=0}$$

$$\langle:=\rangle\ \frac{x=0 \vdash 0=0 \vee 1=0}{x=0 \vdash \langle x:=0\rangle x=0 \vee \langle x:=1\rangle x=0}$$

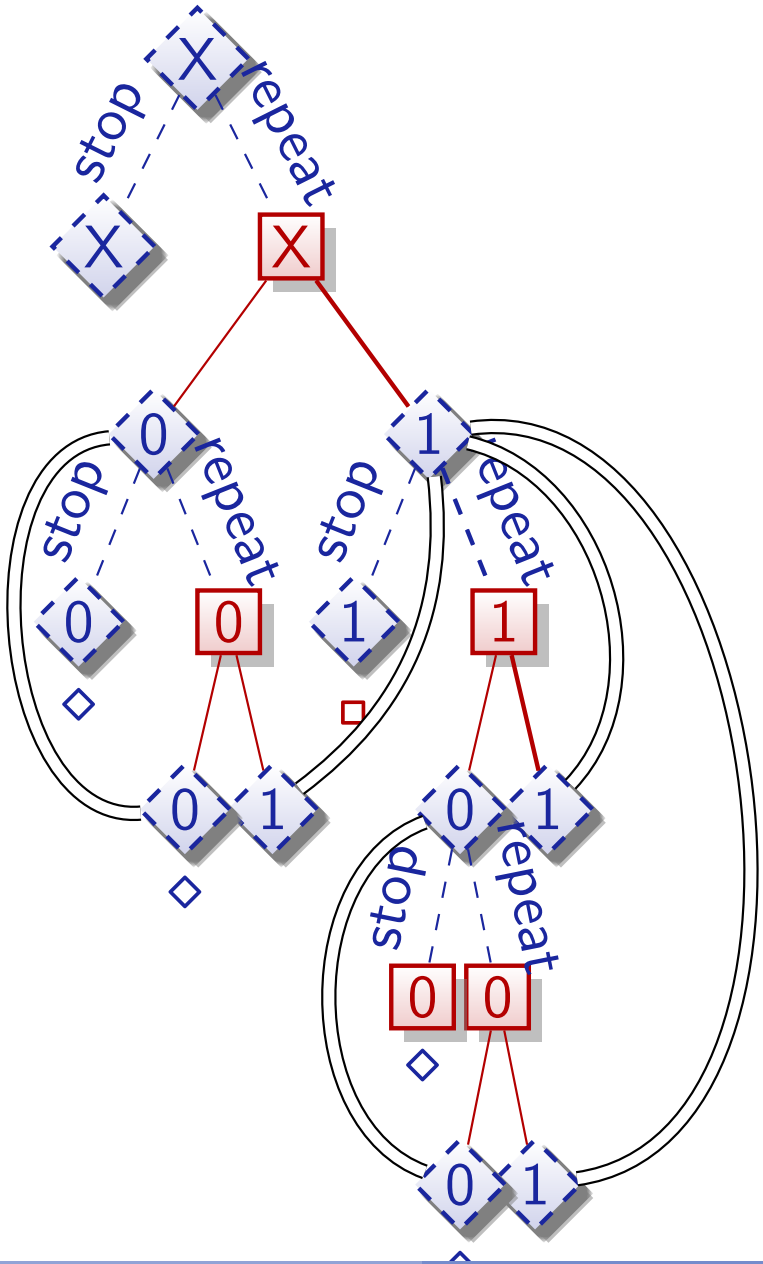
$$\langle\cup\rangle\ \frac{x=0 \vdash \langle x:=0\rangle x=0 \vee \langle x:=1\rangle x=0}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}$$

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

$$[\cdot]\ \frac{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle\neg x=0}{x=0 \vdash [x:=0 \cap x:=1]x=0}$$

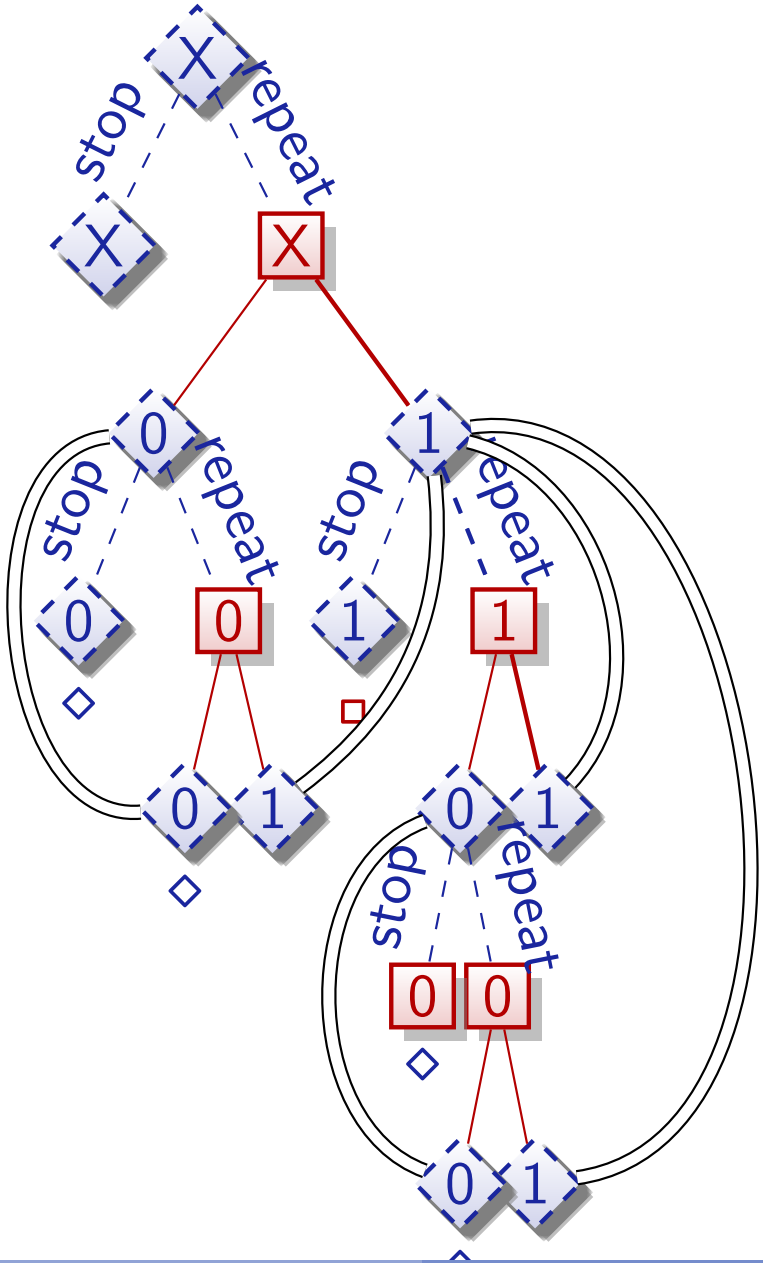
$$\text{ind}\ \frac{x=0 \vdash [x:=0 \cap x:=1]x=0}{x=0 \vdash [(x:=0 \cap x:=1)^*]x=0}$$

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



Example Proof: Dual Filibuster

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



Outline

Differential Game Logic: Denotational Semantics

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

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

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

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

Differential Game Logic: Axiomatization

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

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

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

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

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

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

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

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

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

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

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

$$\forall\ \frac{p \to Q}{p \to \forall x\, Q} \qquad (x \notin \mathsf{FV}(p))$$

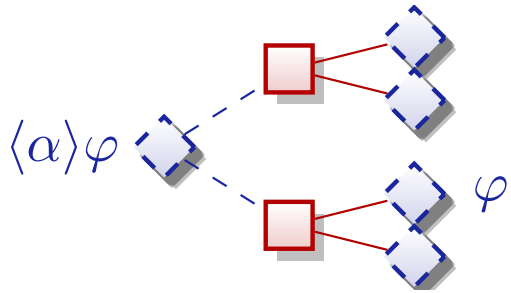
$$\text{US}\ \frac{\varphi}{\varphi^{\psi(\cdot)}_{p(\cdot)}}$$

TOCL'15

Summary

differential game logic

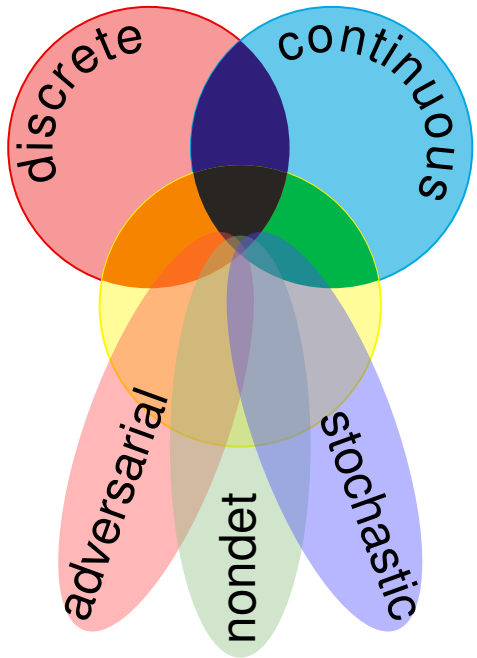
$$\mathsf{dG}\mathcal{L} = \mathsf{GL} + \mathsf{HG} = \mathsf{d}\mathcal{L} + {}^{d}$$



- Axiomatics for hybrid games
- Semantics of game repetition
- Fixpoints

Next lecture

1. Soundness
2. Proofs
3. Separations




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.