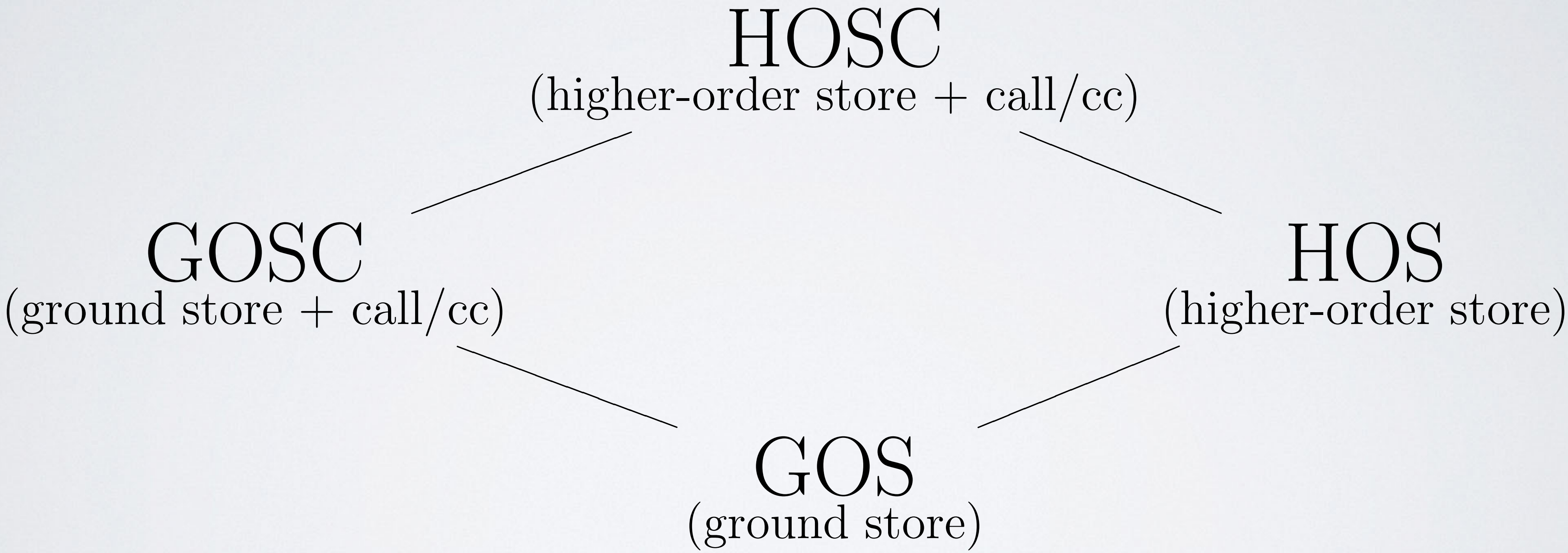
COMPOSITIONAL RELATIONAL REASONING VIA OPERATIONAL GAME SEMANTICS

Guilhem Jaber
NANTES

Andrzej Murawski
OXFORD

HIGHER-ORDER CALL-BY-VALUE LANGUAGES WITH STATE



CONTEXTUAL EQUIVALENCE

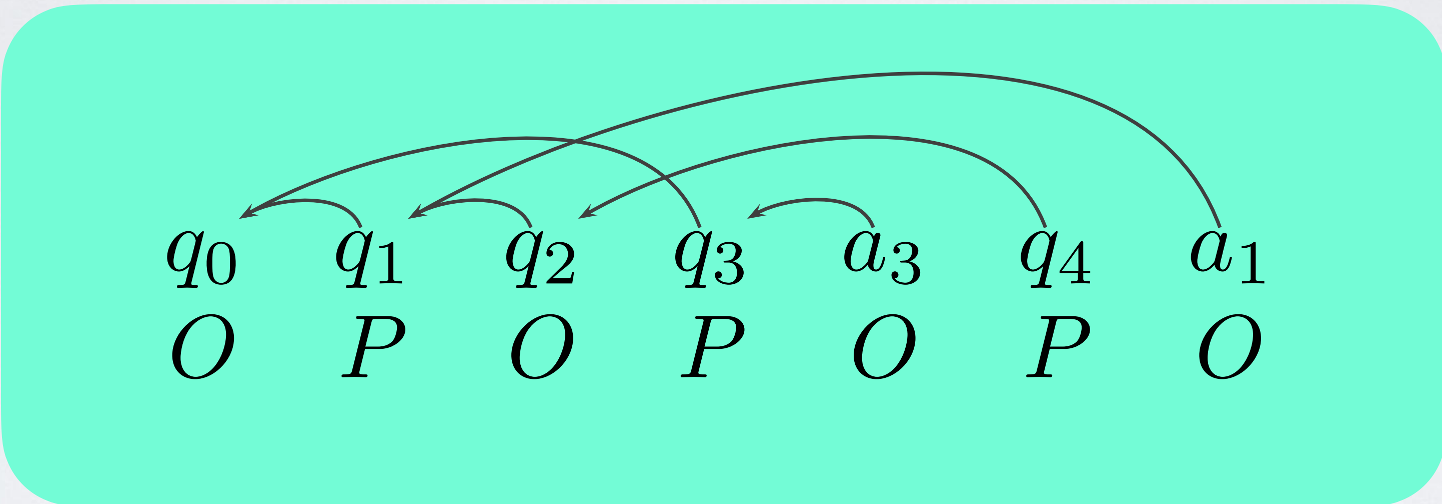
$$\mathbf{x} \in \{\mathrm{HOSC}, \mathrm{GOSC}, \mathrm{HOS}, \mathrm{GOS}\}$$

$$M_1 \cong^{\mathbf{x}} M_2$$

M_1, M_2 cannot be distinguished by $\mathbf{x}$-contexts.

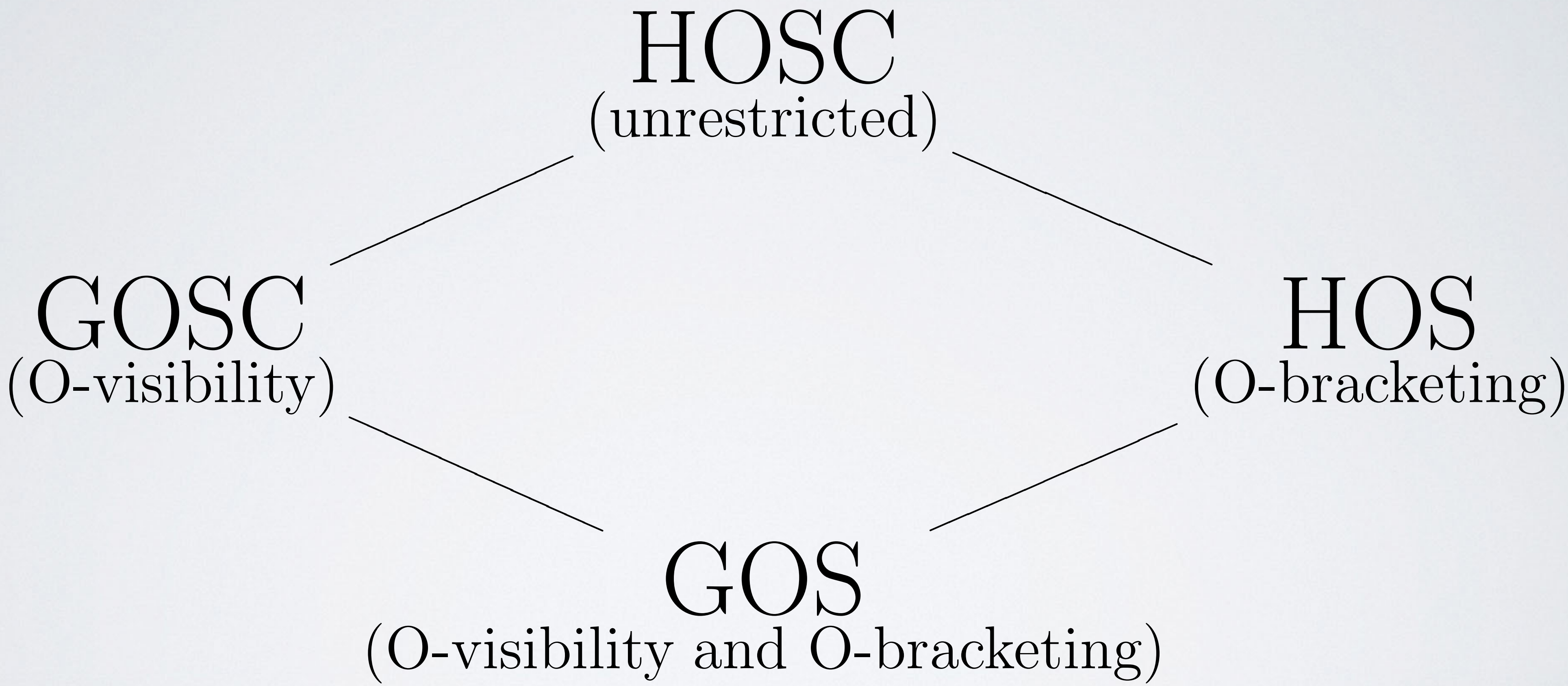
GAME SEMANTICS

- Interaction modelled as an exchange of moves between two players (O-context, P-term)



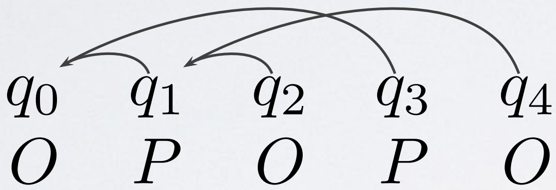
- Constraints on contexts can be expressed as restrictions on the shape of play for O-moves.

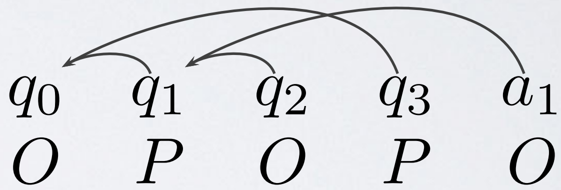
Results from the 1990s: Abramsky, Jagadeesan, Malacaria, Hyland, Ong, Laird, Honda, McCusker



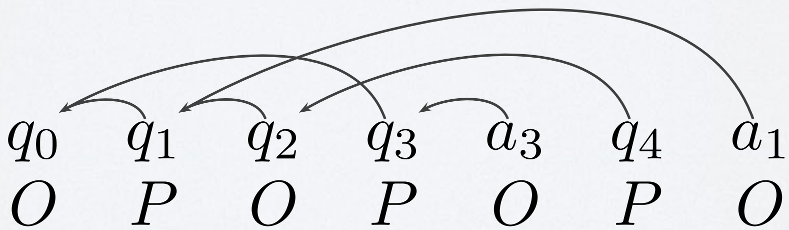
CONSTRAINTS ON O-PLAY

- O-visibility (violation)





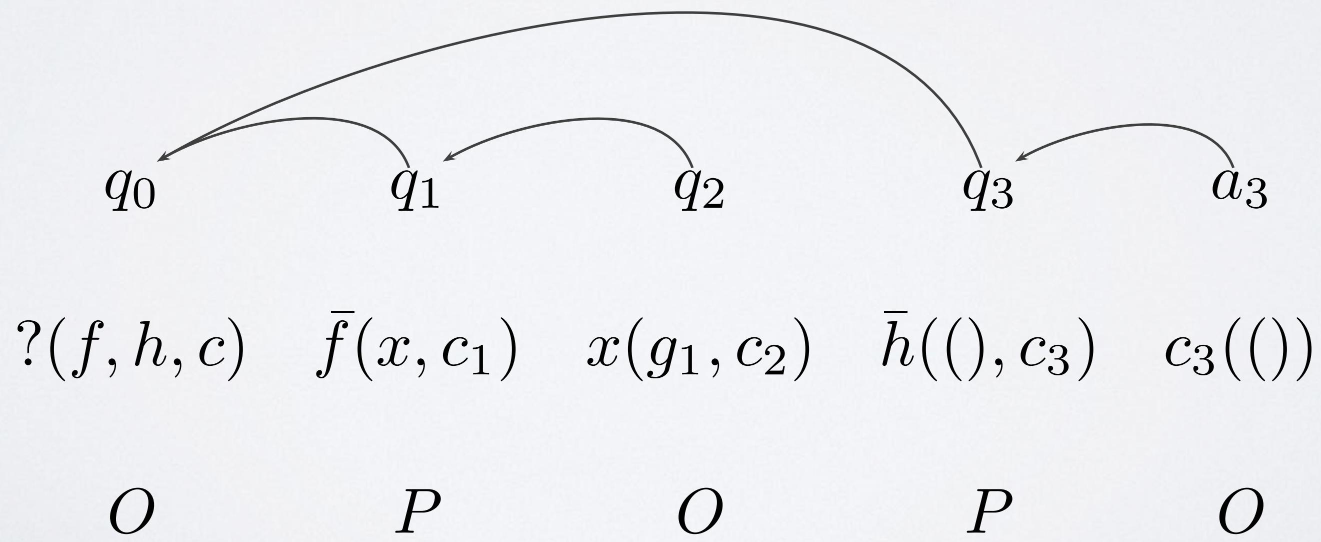
- O-bracketing (violation)



LTS-BASED ACCOUNT

Theorem (Jaber, M. (ESOP'21))**.** Let $\mathbf{Tr}_{\mathbf{x}}(M)$ be the set of traces generated by M in $\mathcal{L}_{\mathbf{x}}$, where $\mathbf{x} \in \{\mathrm{HOSC}, \mathrm{GOSC}, \mathrm{HOS}, \mathrm{GOS}\}$.

$$M_1 \cong^{\mathbf{x}} M_2 \text{ if and only if } \mathbf{Tr}_{\mathbf{x}}(M_1) = \mathbf{Tr}_{\mathbf{x}}(M_2).$$



LTS

$$
\begin{array}{l|lcl}
(P\tau) & \langle M, c, \gamma, \phi, h, H_F, H_C \rangle & \xrightarrow{\tau} & \langle N, c', \gamma, \phi, h', H_F, H_C \rangle \\
& \text{ when } (M, c, h) \to (N, c', h') & & \\
(PA) & \langle V, c, \gamma, \phi, h, H_F, H_C \rangle & \xrightarrow{\bar{c}(A)} & \langle \gamma \cdot \gamma', \phi \uplus \nu(A), h, H_F, H_C, F^{\mathbf{x}}_{PA} \uplus \nu(A), C^{\mathbf{x}}_{PA} \rangle \\
& \text{ when } c : \sigma,\ (A, \gamma') \in \mathbf{AVal}_\sigma(V) & & \\
(PQ) & \langle K[fV], c, \gamma, \phi, h, H_F, H_C \rangle & \xrightarrow{\bar{f}(A,c')} & \langle \gamma \cdot \gamma' \cdot [c' \mapsto (K, c)], \phi \uplus \phi', h, H_F, H_C, F^{\mathbf{x}}_{PQ} \uplus \nu(A), C^{\mathbf{x}}_{PQ} \uplus \{c'\}) \rangle \\
& \text{ when } f : \sigma \to \sigma',\ (A, \gamma') \in \mathbf{AVal}_\sigma(V),\ c' : \sigma' \text{ and } \phi' = \nu(A) \uplus \{c'\} & & \\
(OA) & \langle \gamma, \phi, h, H_F, H_C, Fn, Cn \rangle & \xrightarrow{c(A)} & \langle K[A], c', \gamma, \phi \uplus \nu(A), h, H_F \cdot [\nu(A) \mapsto Fn], H_C \cdot [\nu(A) \mapsto Cn] \rangle \\
& \text{ when } c \in Cn,\ c : \sigma,\ A : \sigma,\ \gamma(c) = (K, c') & & \\
(OQ) & \langle \gamma, \phi, h, H_F, H_C, Fn, Cn \rangle & \xrightarrow{f(A,c)} & \langle VA, c, \gamma, \phi \uplus \phi', h, H_F \cdot [\phi' \mapsto Fn],\ H_C \cdot [\phi' \mapsto Cn] \rangle \\
& \text{ when } f \in Fn,\ f : \sigma \to \sigma',\ A : \sigma,\ c : \sigma',\ \gamma(f) = V \text{ and } \phi' = \nu(A) \uplus \{c\} & &
\end{array}
$$

LTS INSTANTIATION

$\mathbf{x}$	$F^{\mathbf{x}}_{PA}$	$C^{\mathbf{x}}_{PA}$	$F^{\mathbf{x}}_{PQ}$	$C^{\mathbf{x}}_{PQ}$
HOSC	ϕ_{PF}	ϕ_{PC}	ϕ_{PF}	ϕ_{PC}
GOSC	$H_F(c)$	$H_C(c)$	$H_F(f)$	$H_C(f)$
HOS	ϕ_{PF}	$H_C(c)$	ϕ_{PF}	$\emptyset$
GOS	$H_F(c)$	$H_C(c)$	$H_F(f)$	$\emptyset$

TOWARDS KRIPKE NORMAL-FORM BISIMULATIONS

- The LTS can be used off the shelf prove equivalences via trace equivalence and bisimilarity.

- To achieve robustness, we will employ a combination of Kripke-style reasoning about heap invariants (Pitts, Stark, Ahmed, Dreyer, Rossberg, Neis, Birkedal) and normal-form/open bisimulations (Sangiorgi, Stovring, Lassen, Levy, …).

- Uniform treatment of all four languages.

WORLD TRANSITION SYSTEMS

Definition. A ***world transition system*** (WTS) $\mathcal{A}$ is a triple $(\text{Worlds}, \sqsubseteq_{\mathsf{OQ}}, \sqsubseteq_{\mathsf{OA}}, \mathcal{I})$, where Worlds is a set of states (*worlds*), $\sqsubseteq_{\mathsf{OQ}}$, $\sqsubseteq_{\mathsf{OA}}$ are binary reflexive relations on Worlds, and $\mathcal{I} : \text{Worlds} \to \mathcal{P}(\text{Heap} \times \text{Heap})$ is the *invariant assignment* that associates a set of pairs of heaps to any world.

Two accessibility relations

- $w \sqsubseteq_{\mathsf{OQ}} w'$: functions available to O in w are available in w'
- $w \sqsubseteq_{\mathsf{OA}} w'$: continuations available to O in w are available in w'

$\mathcal{A}$-KNFB: $(\mathcal{V}^{\mathbf{x}}_{\mathcal{A}}, \mathcal{K}^{\mathbf{x}}_{\mathcal{A}}, \mathcal{E}^{\mathbf{x}}_{\mathcal{A}})$

- $(V_1, V_2, w, \mathcal{H}) \in \mathcal{V}^{\mathbf{x}}_{\mathcal{A}}$

  $\forall w' \sqsupseteq^*_{\mathsf{OQ}} w.\ \forall A, c \text{ (fresh)}.\ (V_1 A, c, V_2 A, c, w', \mathcal{H}[\nu(A), c \mapsto w']) \in \mathcal{E}^{\mathbf{x}}_{\mathcal{A}}$

- $(K_1, c_1, K_2, c_2, w, \mathcal{H}) \in \mathcal{K}^{\mathbf{x}}_{\mathcal{A}}$

  $\forall w' \sqsupseteq^*_{\mathsf{OA}} w.\ \forall A \text{ (fresh)}.\ (K_1[A], c_1, K_2[A], c_2, w', \mathcal{H}[\nu(A) \mapsto w']) \in \mathcal{E}^{\mathbf{x}}_{\mathcal{A}}$

- $(M_1, c_1, M_2, c_2, w, \mathcal{H}) \in \mathcal{E}^{\mathbf{x}}_{\mathcal{A}}$

  $$\forall (h_1, h_2) \in \mathcal{I}(w).\ P_{Div} \vee P_{PA} \vee P_{PQ}$$

$\mathcal{E}^{\mathbf{x}}_{\mathcal{A}}$

$$P_{Div} \triangleq (M_1, c_1, h_1) \Uparrow \; \wedge \; (M_2, c_2, h_2) \Uparrow$$

$$\begin{aligned}P_{PA} \triangleq \; & \exists V_1, V_2, c, h'_1, h'_2, w'. \\ & (M_1, c_1, h_1) \to^* (V_1, c, h'_1) \; \wedge \; (M_2, c_2, h_2) \to^* (V_2, c, h'_2) \; \wedge \\ & (h'_1, h'_2) \in \mathcal{I}(w') \; \wedge \; (V_1, V_2, w', \mathcal{H}) \in \mathcal{V}^{\mathbf{x}}_{\mathcal{A}} \; \wedge \\ & (w, \mathcal{H}) \sqsubseteq^{\mathbf{x}}_{c} w'\end{aligned}$$

$$\begin{aligned}P_{PQ} \triangleq \; & \exists K_1, V_1, K_2, V_2, c'_1, c'_2, f, w'. \\ & (M_1, c_1, h_1) \to^* (K_1[f V_1], c'_1, h'_1) \; \wedge \; (M_2, c_2, h_2) \to^* (K_2[f V_2], c'_2, h'_2) \; \wedge \\ & (h'_1, h'_2) \in \mathcal{I}(w') \; \wedge \; (V_1, V_2, w', \mathcal{H}) \in \mathcal{V}^{\mathbf{x}}_{\mathcal{A}} \; \wedge \; (K_1, c'_1, K_2, c'_2, w', \mathcal{H}) \in \mathcal{K}^{\mathbf{x}}_{\mathcal{A}} \; \wedge \\ & (w, \mathcal{H}) \sqsubseteq^{\mathbf{x}}_{f} w'\end{aligned}$$

$\sqsubseteq_c^{\mathbf{x}}$ and $\sqsubseteq_f^{\mathbf{x}}$

$\mathbf{x}$	$F_{PA}^{\mathbf{x}}$	$C_{PA}^{\mathbf{x}}$	$F_{PQ}^{\mathbf{x}}$	$C_{PQ}^{\mathbf{x}}$
HOSC	ϕ_{PF}	ϕ_{PC}	ϕ_{PF}	ϕ_{PC}
GOSC	$H_F(c)$	$H_C(c)$	$H_F(f)$	$H_C(f)$
HOS	ϕ_{PF}	$H_C(c)$	ϕ_{PF}	$\emptyset$
GOS	$H_F(c)$	$H_C(c)$	$H_F(f)$	$\emptyset$

$\mathbf{x}$	$(w, \mathcal{H}) \sqsubseteq_c^{\mathbf{x}} w'$	$(w, \mathcal{H}) \sqsubseteq_f^{\mathbf{x}} w'$
HOSC	$w \sqsubseteq_{\mathsf{OQ}} w' \wedge w \sqsubseteq_{\mathsf{OA}} w'$	$w \sqsubseteq_{\mathsf{OQ}} w' \wedge w \sqsubseteq_{\mathsf{OA}} w'$
GOSC	$\mathcal{H}(c) \sqsubseteq_{\mathsf{OQ}} w' \wedge \mathcal{H}(c) \sqsubseteq_{\mathsf{OA}} w'$	$\mathcal{H}(f) \sqsubseteq_{\mathsf{OQ}} w' \wedge \mathcal{H}(f) \sqsubseteq_{\mathsf{OA}} w'$
HOS	$w \sqsubseteq_{\mathsf{OQ}} w' \wedge \mathcal{H}(c) \sqsubseteq_{\mathsf{OA}} w'$	$w \sqsubseteq_{\mathsf{OQ}} w'$
GOS	$\mathcal{H}(c) \sqsubseteq_{\mathsf{OQ}} w' \wedge \mathcal{H}(c) \sqsubseteq_{\mathsf{OA}} w'$	$\mathcal{H}(f) \sqsubseteq_{\mathsf{OQ}} w'$

FULL ABSTRACTION

Theorem (Jaber, M. (LICS'21))**.** Let $\mathbf{x} \in \{\mathrm{HOSC}, \mathrm{GOSC}, \mathrm{HOS}, \mathrm{GOS}\}$.

$$M_1 \cong^{\mathbf{x}} M_2$$

if and only if there exists a WTS $\mathcal{A}$, initial world w_0 such that $(\emptyset, \emptyset) \in \mathcal{I}(w_0)$ and

$$(M_1, c, M_2, c, w_0, [c \mapsto w_0]) \in \mathcal{E}^{\mathbf{x}}_{\mathcal{A}}.$$

Comparison with **Kripke logical relations**:
Dreyer, Neis, Birkedal (ICFP'10, JFP 2012)

	GOSC	HOS
game semantics	O-visibility	O-bracketing
Kripke logical relations	backtracking	private vs public
Kripke nf-bisimulations	$\mathcal{H}(n) \sqsubseteq_{\mathsf{OQ}} w'$ $\mathcal{H}(n) \sqsubseteq_{\mathsf{OA}} w'$	$w \sqsubseteq_{\mathsf{OQ}} w'$ $\mathcal{H}(c) \sqsubseteq_{\mathsf{OA}} w'$ (Q vs A)

SUMMARY

- Relational techniques derived from game models in a uniform fashion
- Soundness and completeness (without biorthogonal closure)
- Abstraction, compositionality, direct style, lightweight quantification
- Scope for automation and generalisation