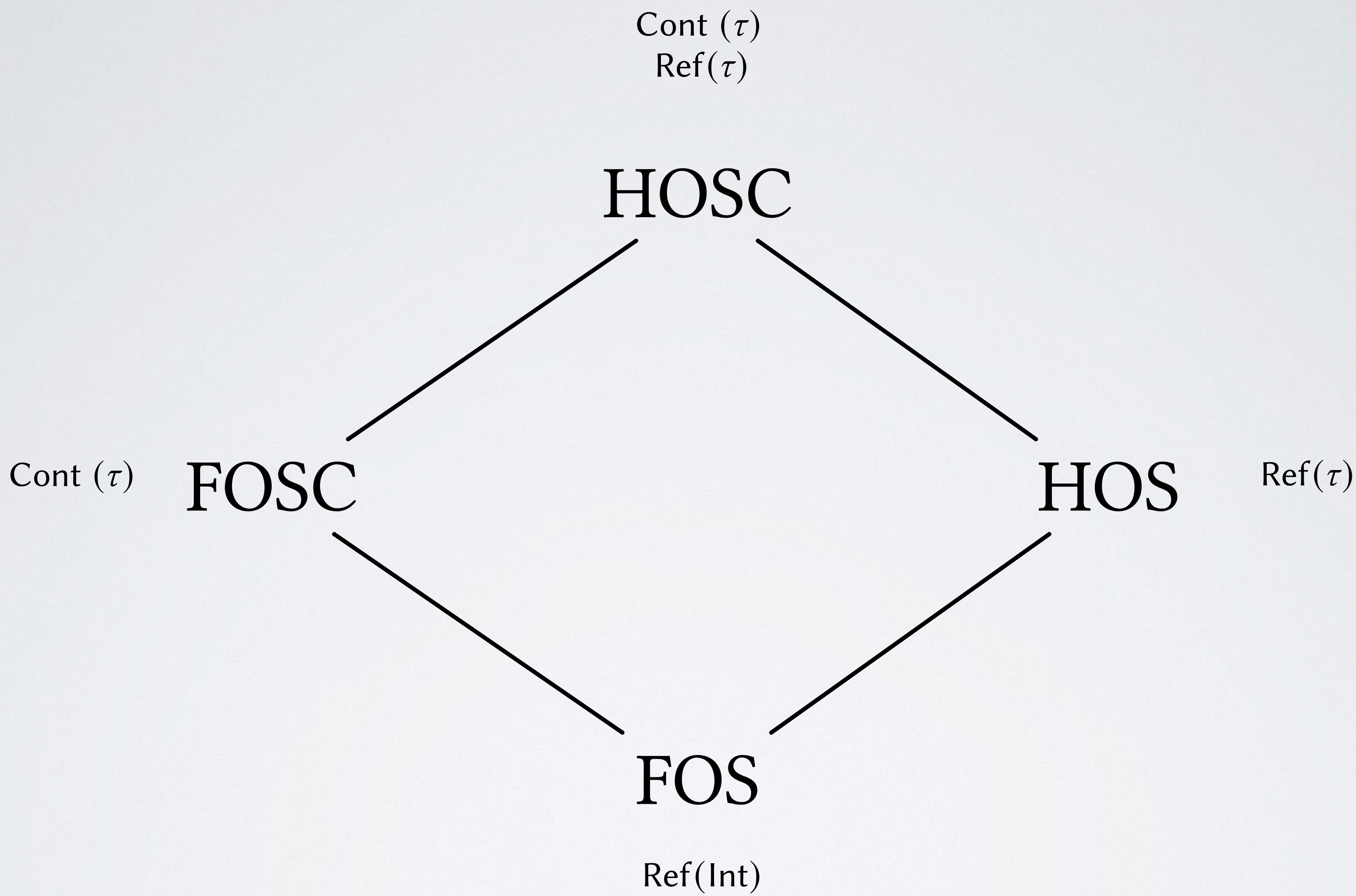
CONTEXTUAL EQUIVALENCE FOR STATE AND CONTROL VIA NESTED DATA

Benedict Bunting
UNIVERSITY OF OXFORD

Andrzej Murawski
UNIVERSITY OF OXFORD



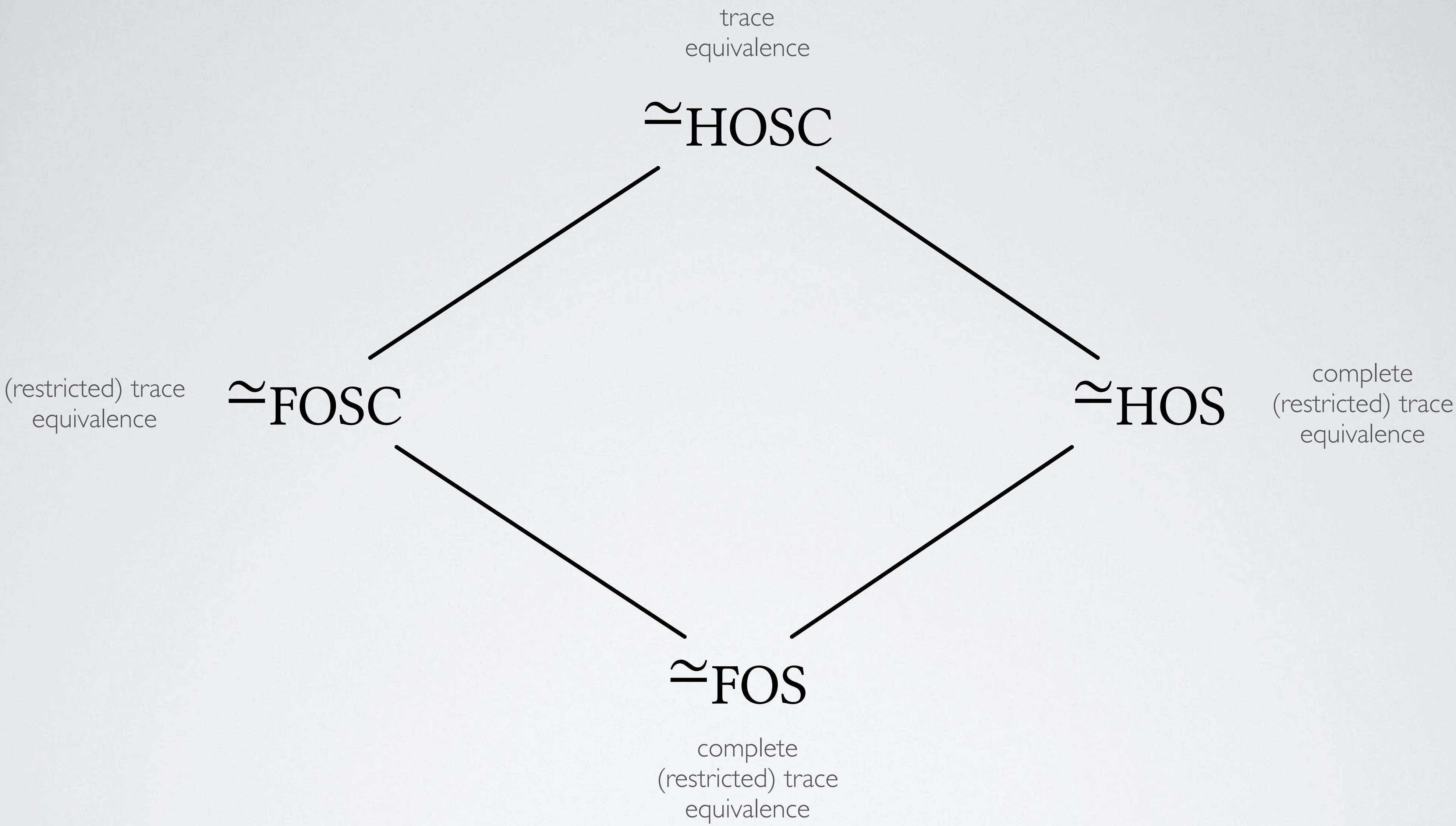
Cont (τ)
Ref(τ)
HOSC
Cont (τ)
FOSC
HOS
Ref(τ)
FOS
Ref(Int)

CONTEXTUAL APPROXIMATION AND EQUIVALENCE

Let $\Gamma \vdash M_1, M_2 : \tau$ be HOSC terms and $X \in \{\text{HOSC, FOSC, HOS, FOS}\}$.

We define $\Gamma \vdash M_1 \lesssim_X M_2$ to hold, when for all X contexts $C[\tau]$ such that $\vdash C[M_1], C[M_2] : \tau'$ for some τ', if $(C[M_1], \emptyset) \Downarrow$ then $(C[M_2], \emptyset) \Downarrow$.

The terms $\Gamma \vdash M_1, M_2 : \tau$ are called *contextually equivalent* (wrt X contexts), written $\Gamma \vdash M_1 \simeq_X M_2$, when $\Gamma \vdash M_1 \lesssim_X M_2$ and $\Gamma \vdash M_2 \lesssim_X M_1$.

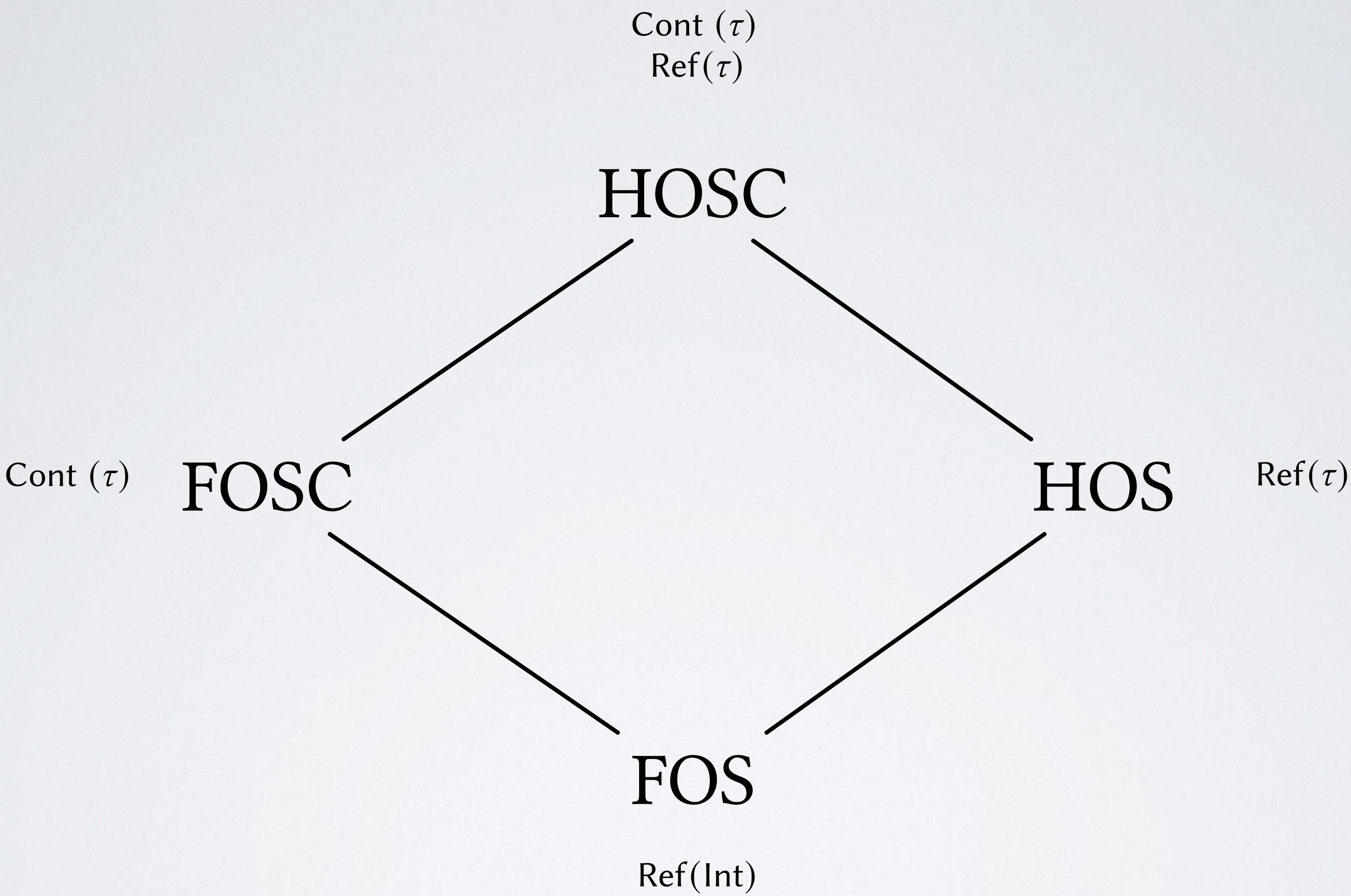


Complete trace models of state and control*

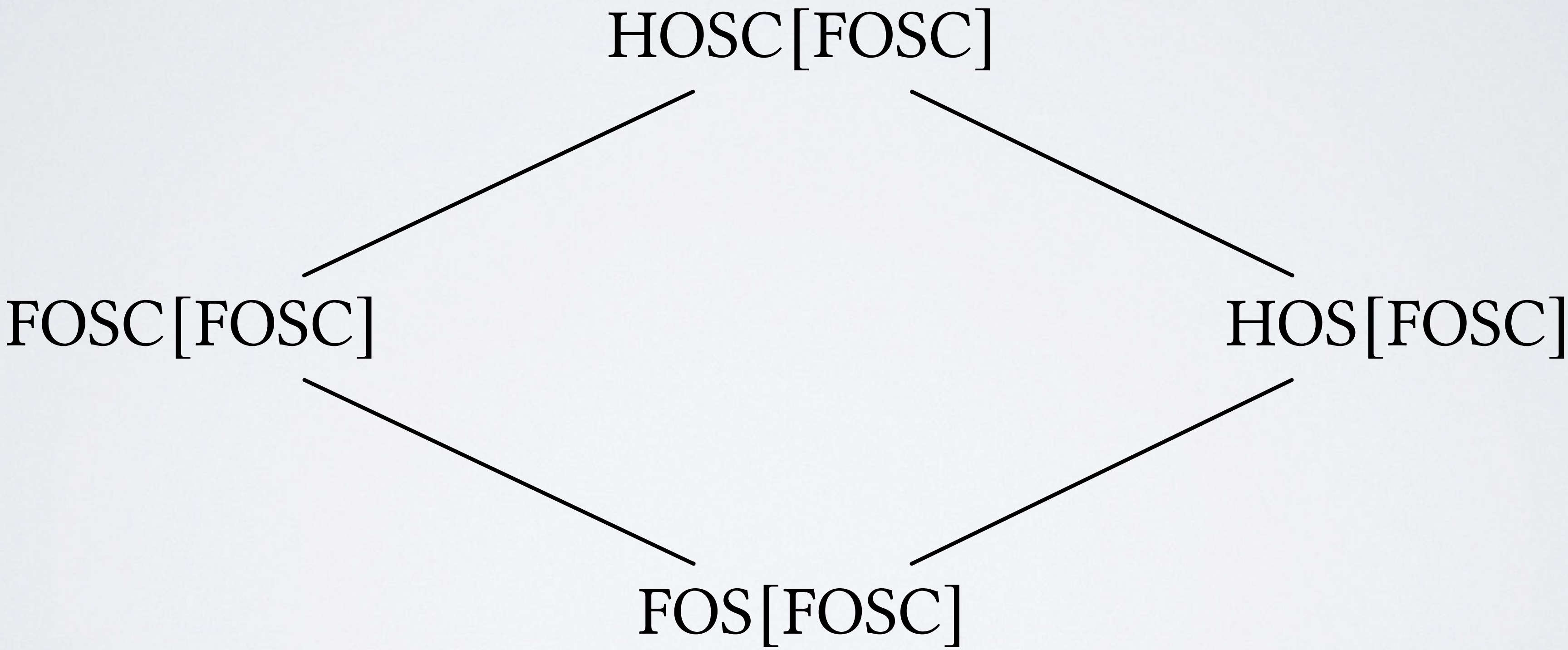
Guilhem Jaber[1] (✉) and Andrzej S. Murawski[2] (✉)

SOURCE OF UNDECIDABILITY

- integer arithmetic
- higher-order recursion (with state)
- general references


Cont (τ)
Ref(τ)
HOSC
Cont (τ)
FOSC
HOS
Ref(τ)
FOS
Ref(Int)

DECIDABILITY STATUS OF X[FOSC]
(FINITE BASE TYPES, NO RECURSION)



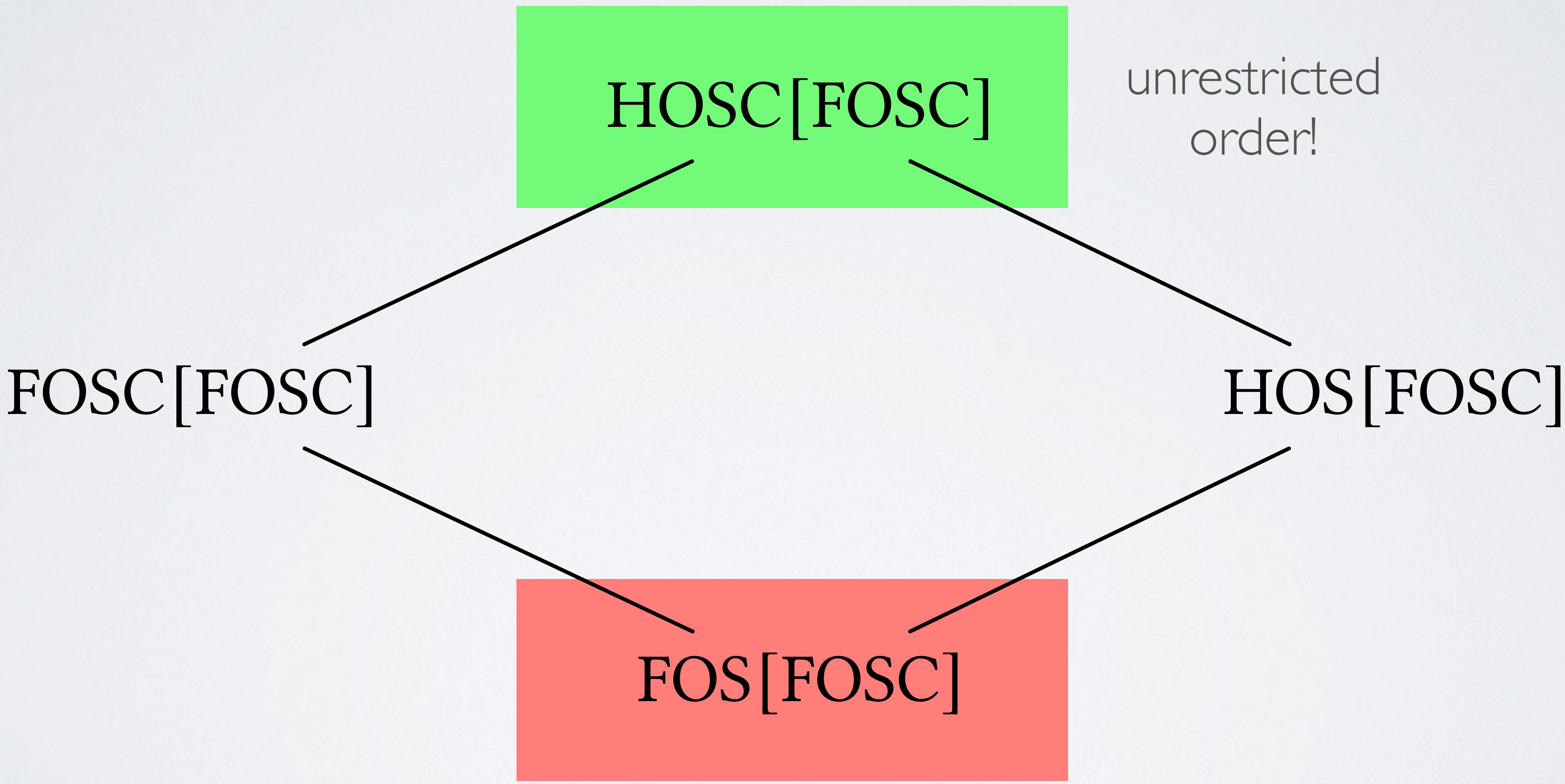
RELATED UNDECIDABILITY RESULTS

- FOS[FOS] is undecidable [M., LICS'03]

$$\mathrm{GOS} = \mathrm{FOS} + \mathrm{Ref}^{i}(\mathrm{Int})$$

- GOS[GOS] is undecidable [M. & Tzevelekos, ICALP'12]
- The undecidability of GOS[GOS] implies that X[GOS] is undecidable for any X.

DECIDABILITY STATUS OF X[FOSC]
(FINITE BASE TYPES, NO RECURSION)



TRACE SEMANTICS

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

AUTOMATA OVER INFINITE ALPHABETS

- Σ is a finite alphabet of *tags*.
- $\mathcal{D}$ is an infinite alphabet of *data values*.
- Automata accept *data words* from $(\Sigma \times \mathcal{D})^*$.

$$(t_1, d_1)(t_2, d_2) \cdots (t_k, d_k)$$

Class memory automata [Björklund & Schwentick, FCT 2007] maintain finite state as well as class memory (a map from a finite subset of $\mathcal{D}$ to a finite set of memories).

$$(t_1, d_1)(t_2, d_2) \cdots (t_k, d_k)(t_{k+1}, d_2)$$

FROM LTS TO CMA

- Lack of recursion means terms do not grow unboundedly and there are finitely many "skeletons".
- But terms also contain function names (introduced by the environment) as well as location names!
- It is not immediate to accommodate γ as class memory.

FROM LTS TO CMA

- Fortunately, traces of FOSC satisfy a visibility condition: function and location names are always introduced in the current scope (P-view).
- P-views for recursion-free FOSC terms are bounded, so we can enumerate the names and refer to their position in the P-view.
- This makes it possible to represent γ as a class memory function!

HEAP

- However, location names must also be updated. For this we need access to whole "scope" (P-view).
- Idea: use a tree-shaped set $\mathcal{D}$ and allow the automaton to access memory not only for one data value but for its ancestors too.
- To achieve this, we use nested data and class memory automata over nested data [Cotton-Barratt, M. & Ong, LATA 2015].

NDCMA

$$(t_1, d_1)(t_1, d_2)(t_2, d_3)(t_3, d_4)(t_4, d_3)$$

$$(q_0, \emptyset) \qquad (q_0,\ d_1^{m_1}) \qquad (q_0,\ d_1^{m_1}\ \ d_2^{m_1}) \qquad (q_1,\ \underset{\underset{\displaystyle d_3^{m_3}}{|}}{d_1^{m_2}}\ \ d_2^{m_1}\ )$$

$$(q_1,\ \ \underset{d_3^{m_3}\ \ \ \ \ \ d_4^{m_4}}{\overset{}{d_1^{m_2}}}\ \ \ d_2^{m_1}\ ) \qquad (q_2,\ \ \underset{d_3^{m_6}\ \ \ \ \ \ d_4^{m_4}}{\overset{}{d_1^{m_5}}}\ \ \ d_2^{m_1}\ )$$

SUMMARY

- The trace semantics of FOSC terms can be faithfully represented using deterministic NDCMA.
- The containment problem for deterministic NDCMA is decidable.
- HOSC[FOSC] is decidable.

DECIDABILITY STATUS OF X[FOSC]
(FINITE BASE TYPES, NO RECURSION)