A Characterisation of Open Bisimilarity using an Intuitionistic Modal Logic

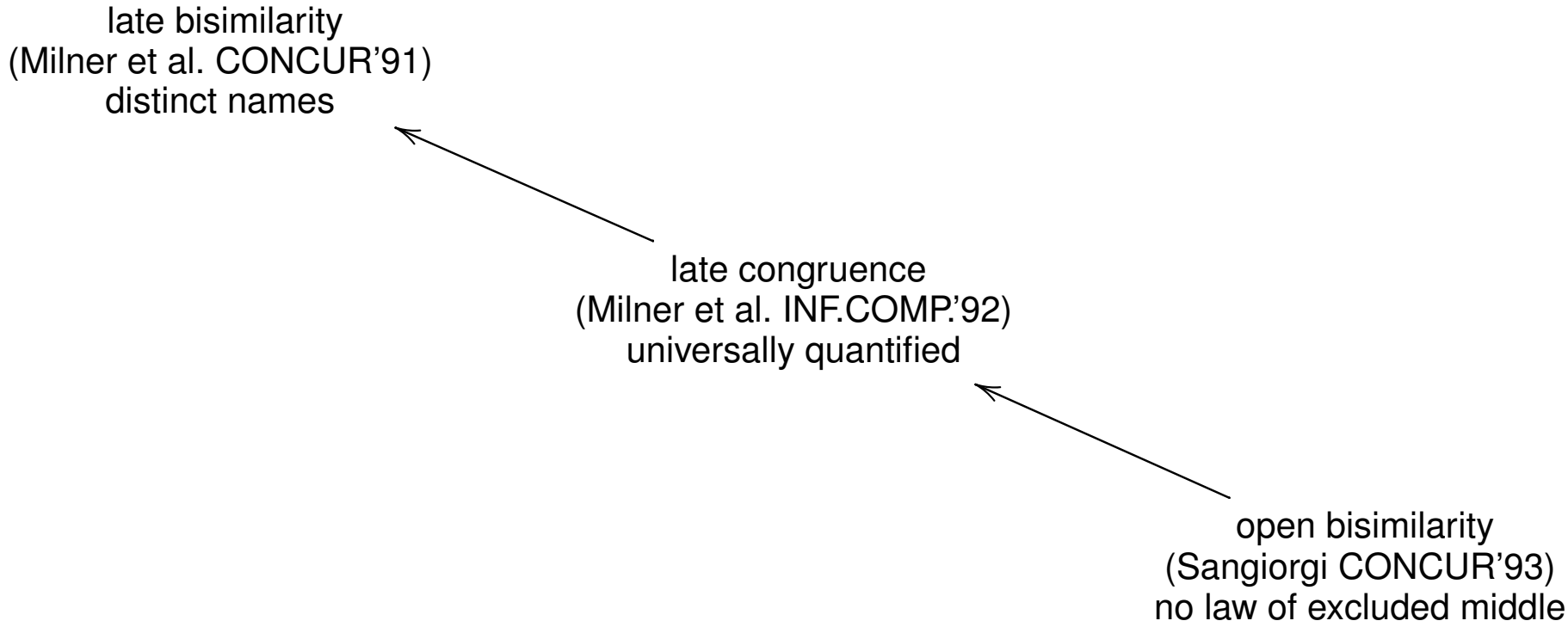
CONCUR 2017, Berlin, Germany

Ki Yung Ahn, Ross Horne and Alwen Tiu

School of Computer Science and Engineering, Nanyang Technological University, Singapore

5-8 September 2017

All you need to know about open bisimilarity



- No distinct name assumption (names are variables).
- Closed by substitutions at every step (variables may be unified later).
- Is automatically a congruence (preserved under input prefixes).
- Still a bisimulation: so robust under unanticipated change of context during runtime.
- Permits a lazy call-by-need instantiation of inputs, which is efficient to automate.

Why no law of excluded middle?

Classically, $\phi \vee \neg\phi$ is a tautology and $\left[\pi\right]\phi = \neg\left\langle\pi\right\rangle\neg\phi$.
Hence for all classical modal logics:

$$\overline{a}b \parallel c(x) \models \left\langle\tau\right\rangle\mathtt{tt} \vee \left[\tau\right]\mathtt{ff}$$

Intuitionistically, "Reachable worlds" are processes accessible by substitutions. E.g.

$$\overline{a}b \parallel c(x) \leq (\overline{a}b \parallel c(x))\{{}^{a}/_{c}\} \qquad \text{and} \qquad \overline{a}b \parallel a(x) \xrightarrow{\tau} 0$$

Closing modalities under all reachable worlds (**intuitionistic heredity**):

$$\overline{a}b \parallel c(x) \not\models \left\langle\tau\right\rangle\mathtt{tt} \vee \left[\tau\right]\mathtt{ff}$$

$\overline{a}b \parallel c(x) \not\models \left\langle\tau\right\rangle\mathtt{tt}$, — no τ-transition in world where a and c are not equal.

$\overline{a}b \parallel c(x) \not\models \left[\tau\right]\mathtt{ff}$, — some τ-transition in world where $a = c$.

For congruences, quantify over all names

For congruences (open bisimilarity and late congruence):

$$[x = y]\tau \qquad \not\sim \qquad 0$$

Distinguishing strategy, in world where $x = y$:

$$([x = y]\tau)\{^{y}/_{x}\} \xrightarrow{\tau} 0 \qquad \text{but} \qquad 0\{^{y}/_{x}\} \not\downarrow_{\tau}$$

Distinguishing formula biased to the left:

$$[x = y]\tau \models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \qquad \text{and} \qquad 0 \not\models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt}$$

Distinguishing formula biased to the right:

$$[x = y]\tau \not\models \big[\tau\big]\mathtt{ff} \qquad \text{and} \qquad 0 \models \big[\tau\big]\mathtt{ff}$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

Distinguishing formula biased to the right:

$$[x = y]\tau \not\models \langle\tau\rangle\mathrm{tt} \qquad \text{and} \qquad 0 \models \langle\tau\rangle\mathrm{tt}$$

Dual formula is **not distinguishing**.

$$[x = y]\tau \not\models \neg\langle\tau\rangle\mathrm{tt} \qquad \text{and} \qquad 0 \not\models \neg\langle\tau\rangle\mathrm{tt}$$

[read as “there is no reachable world in which we can do a τ-transition”]

What is a distinguishing formula biased to the left?

No duality between left and right formulae

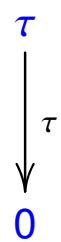
All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

What is a distinguishing formula biased to the left?

Distinguishing strategy (right process leads):

$$[x = y]\tau$$



Since right leads, for formula biased to the left, write **box**:

$$[\tau](\ldots\ldots\ldots\ldots)$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

What is a distinguishing formula biased to the left?

Distinguishing strategy (right process leads):

$[x = y]\tau$ $\xrightarrow{\tau}$ only in worlds where $x = y$

τ $\xrightarrow{\tau}$ 0

Since right leads and left only follows in worlds where $x = y$, write $x = y$ as post-condition:

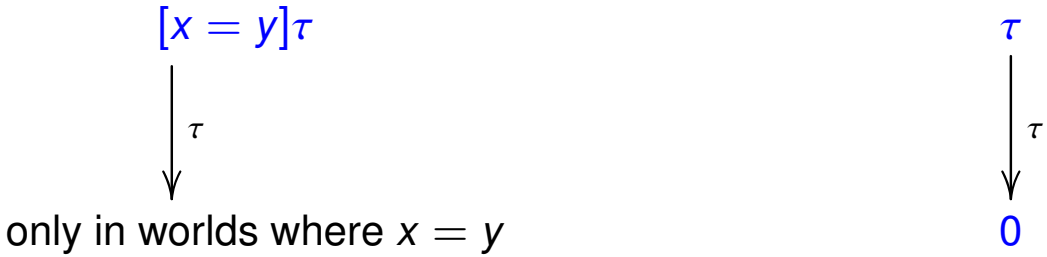
$$\big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt}$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

Distinguishing strategy (right process leads):



Distinguishing formula biased to the left:

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt} \qquad \text{and} \qquad 0 \not\models \big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt}$$

Generating distinguishing formulae algorithmically

Not open bisimilar:

$$\tau + \tau.\tau + \tau.[x = y]\tau \quad \not\sim \quad \tau + \tau.\tau$$

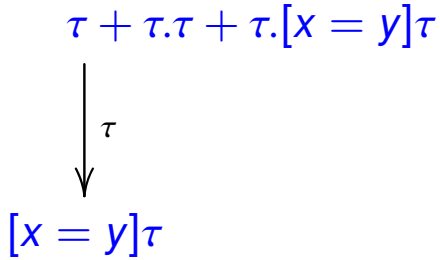
Distinguishing strategy (left process leads first):

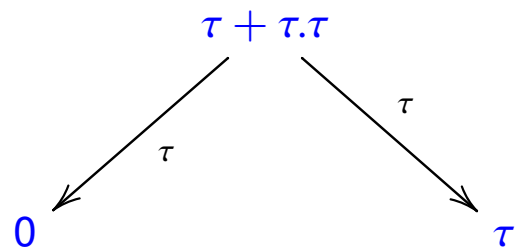
We just saw:

$$[x = y]\tau \not\sim 0 \qquad \text{and} \qquad [x = y]\tau \not\sim \tau$$

Generating distinguishing formulae algorithmically

Distinguishing strategy (left process leads first):





We just saw:

$$[x = y]\tau \models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \qquad 0 \models \big[\tau\big]\mathtt{ff}$$

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt} \qquad \tau \models \big\langle\tau\big\rangle\mathtt{tt}$$

Since left process leads: diamond on left, box on right.

$$\big\langle\tau\big\rangle(\ldots\ldots\ldots\ldots\ldots\ldots) \qquad \big[\tau\big](\ldots\ldots\ldots\ldots\ldots\ldots)$$

Generating distinguishing formulae algorithmically

Distinguishing strategy (left process leads first):

We just saw:

$$[x = y]\tau \models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \qquad 0 \models \big[\tau\big]\mathtt{ff}$$

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt} \qquad \tau \models \big\langle\tau\big\rangle\mathtt{tt}$$

Since left process leads: conjunction on left, disjunction on right.

$$\big\langle\tau\big\rangle\big(\big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \wedge \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt}\big) \qquad \big[\tau\big]\big(\big[\tau\big]\mathtt{ff} \vee \big\langle\tau\big\rangle\mathtt{tt}\big)$$

Generating distinguishing formulae algorithmically

Not open bisimilar:

$$\tau + \tau.\tau + \tau.[x = y]\tau \qquad \not\sim \qquad \tau + \tau.\tau$$

Distinguishing formula biased to left.

$$\tau + \tau.\tau + \tau.[x = y]\tau \models \langle\tau\rangle\big([x = y]\langle\tau\rangle\mathrm{tt} \wedge [\tau]\langle x = y\rangle\mathrm{tt}\big)$$

Distinguishing formula biased to right.

$$\tau + \tau.\tau \models [\tau]\big([\tau]\mathrm{ff} \vee \langle\tau\rangle\mathrm{tt}\big)$$

Only distinguishing if we drop law of excluded middle for name equality. I.e.

$$x = y \text{ or } x \neq y \qquad \text{iff} \qquad \tau + \tau.\tau + \tau.[x = y]\tau \models [\tau]\big([\tau]\mathrm{ff} \vee \langle\tau\rangle\mathrm{tt}\big).$$

[Mechanically proven in intuitionistic proof assistant]

Results for modal logic $\mathcal{OM}$

Theorem (soundness)

If $P \sim Q$ then, for all formulae ϕ, $P \models \phi$ iff $Q \models \phi$.

Proof.

By induction on structure of ϕ. [mechanised] □

Theorem (soundness)

Whenever, for all formulae ϕ, $P \models \phi$ iff $Q \models \phi$, we have that $P \sim Q$.

Proof.

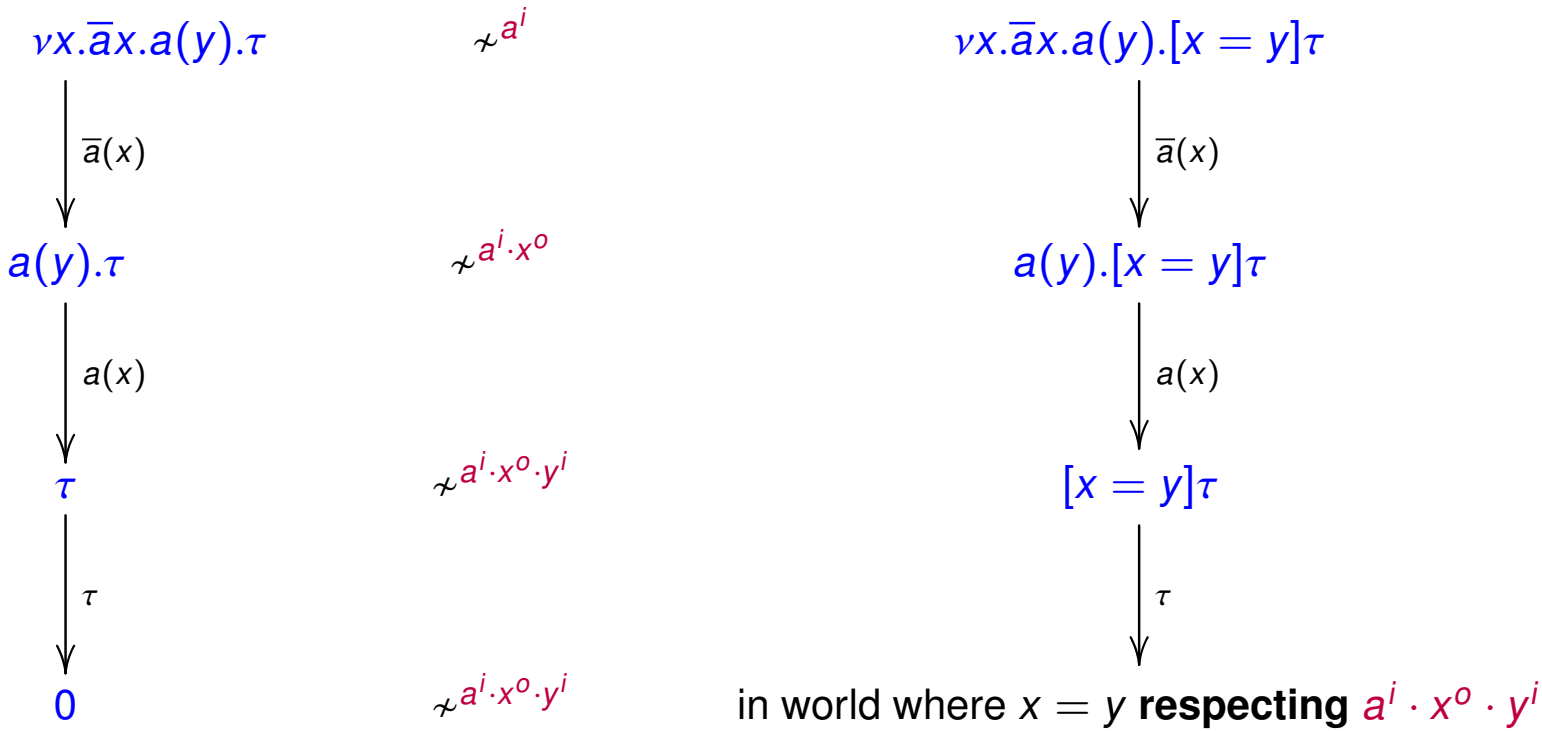
If $P \nsim Q$, by induction on depth of a distinguishing strategy, construct ϕ_L and ϕ_R such that:

- $P \models \phi_L$ and $Q \not\models \phi_L$;
- $P \not\models \phi_R$ and $Q \models \phi_R$.

Proof is constructive, so yields algorithm for generating distinguishing formulae. [implemented] □

Subtleties of $\mathcal{OM}$: respectful substitutions

Distinguishing strategy (left always leading):

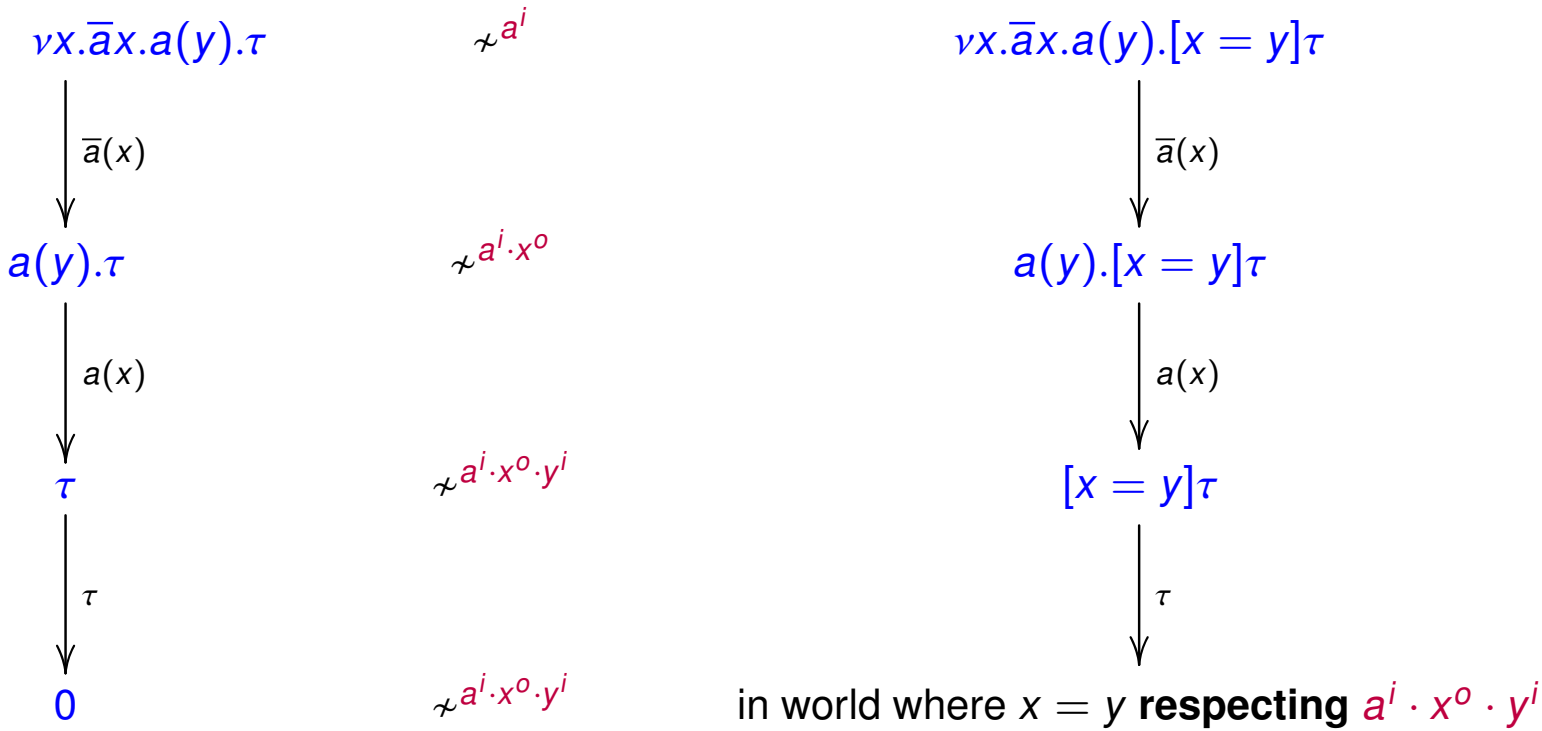


Distinguishing formulae (base case):

$$\tau \models^{a^i \cdot x^o \cdot y^i} \langle\tau\rangle \mathrm{tt} \quad \text{and} \quad [x = y]\tau \models^{a^i \cdot x^o \cdot y^i} [\tau]\langle x = y\rangle \mathrm{tt}$$

Subtleties of $\mathcal{OM}$: respectful substitutions

Distinguishing strategy (left always leading):

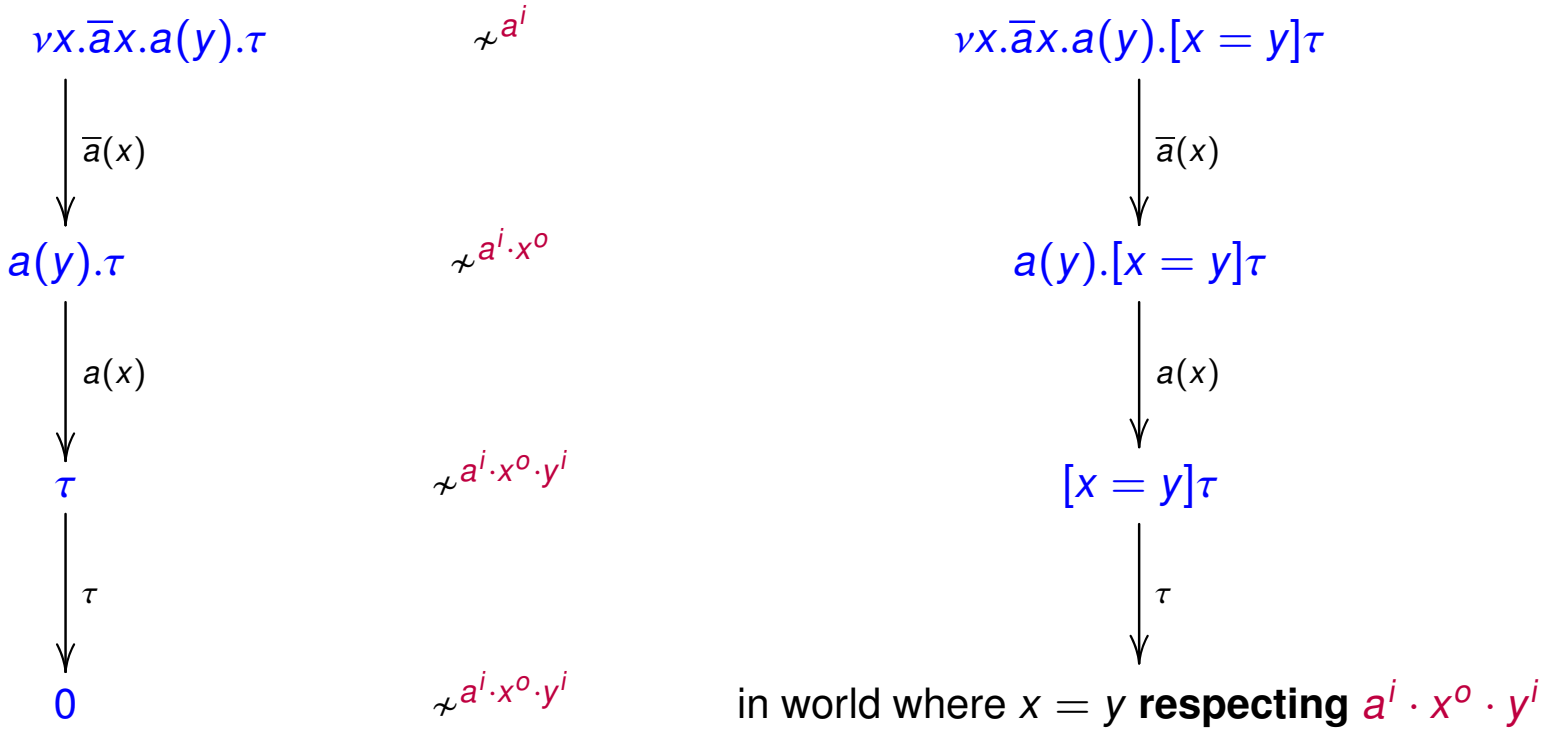


Distinguishing formulae (inductive case):

$$a(y).\tau \models^{a^i \cdot x^o} \langle a(y) \rangle \langle \tau \rangle \mathrm{tt} \quad \text{and} \quad a(y).[x=y]\tau \models^{a^i \cdot x^o} [a(y)][\tau]\langle x=y \rangle \mathrm{tt}$$

Subtleties of $\mathcal{OM}$: respectful substitutions

Distinguishing strategy (left always leading):



Distinguishing formulae:

$\nu x.\overline{a}x.a(y).\tau \models^{a^i} \langle\overline{a}(x)\rangle\langle a(y)\rangle\langle\tau\rangle\mathrm{tt}$ and $\nu x.\overline{a}x.a(y).[x=y]\tau \models^{a^i} [\overline{a}(x)][a(y)][\tau]\langle x=y\rangle\mathrm{tt}$

Subtleties of $\mathcal{OM}$: input modalities

Late modality for diamond:

$$P \models \langle a(z) \rangle \phi \qquad \text{iff} \qquad \exists\, Q.\ P \xrightarrow{a(z)} Q \text{ and } \forall z.\ Q \models \phi.$$

Basic modality for box:

$$P \models [a(z)] \phi \qquad \text{iff} \qquad \forall\, Q.\ P \xrightarrow{a(z)} Q \text{ implies } \forall z.\ Q \models \phi.$$

Modalities have independent interpretations!

In contrast, classical Late modality for box, is de Morgan dual to diamond:

$$P \models [a(x)]^{L} \phi \qquad \text{iff} \qquad \forall\, Q.\ P \xrightarrow{a(x)} Q \text{ implies } \exists x.\ Q \models \phi$$

Subtleties of $\mathcal{OM}$: input modalities

Neither open bisimilar nor late bisimilar:

$$a(x).\tau + a(x) + a(x).[x = a]\tau \quad \not\sim \quad a(x).\tau + a(x)$$

Distinguishing formulae biased to the right:

$$a(x).\tau + a(x) \models \big[a(x)\big]\big(\big\langle\tau\big\rangle\mathtt{tt} \vee \big[\tau\big]\mathtt{ff}\big)$$

However, fails to be distinguishing, both:

- classically, with law of excluded middle;
- intuitionistically, with late box modality.

Intuitionistic with basic box modalities and late diamond modalities.

Conclusion

- $\mathcal{OM}$ is the first modal logic *proven* to **characterise open bisimilarity**.
- $\mathcal{OM}$ is fundamentally an intuitionistic modal logic!
  - **Intuitionistic hereditary**, given by *respectful* substitutions.
  - No **law of excluded middle** (in modal logic and meta-framework).
  - Modalities have **independent** interpretations . . . no **de Morgan dualities**.
- Satisfaction and generation of distinguishing formulae are **implemented**.
- Techniques **general** and known to extend to other calculi and bisimulations.
- Perspectives: open bisimilarity permits efficient **symbolic** decision procedures.
  - especially good for infinite inputs in *cryptographic calculi*.
  - What about *intuitionistic symbolic model checking* (invariant under open bisimilarity)?

A more challenging example!

These processes are late congruent to $\tau + \tau.\tau$.

$$\tau.(\tau + \tau.\tau + \tau.[x = y][w = z]\tau)$$

$$\not\sim$$

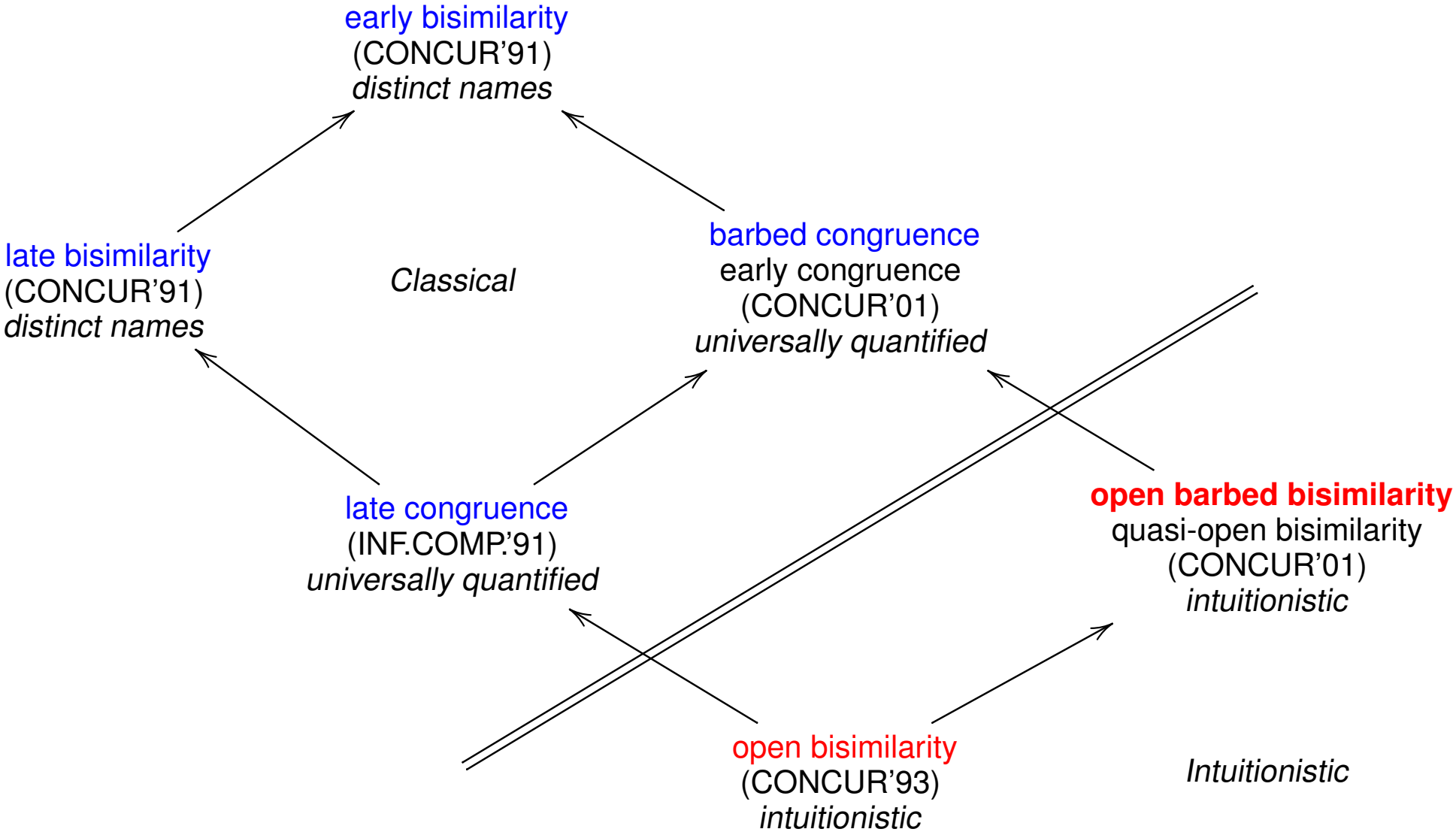
$$\tau.(\tau + \tau.\tau + \tau.[x = y]\tau) + \tau.(\tau + \tau.\tau + \tau.[x = y][w = z]\tau)$$

They are not open bisimilar!

What are the distinguishing strategies?

What are the distinguishing formulae?

Results work for early transition systems



Additional criterion for intuitionistic modal logics:

> *If law of excluded middle is forced we obtain a meaningful classical modal logic (open barbed bisimilarity becomes barbed congruence).*