Observational equivalence using scheduler for quantum processes

K. Yasuda / T. Kubota / Y. Kakutani

Dept. of Computer Science
University of Tokyo

Outline

1. Introduction
2. Quantum process calculus qCCS
3. Open bisimulation on qCCS
4. Our equivalence relation
   - Observational equivalence
   - Scheduler / Strategy
5. Conclusion

Introduction

Introduction | Quantum process calculi

Quantum communication protocols

- Quantum key distribution: BB84, B92, …
- Quantum bit commitment
- Quantum oblivious transfer

Quantum process calculi

» To analyze/verify quantum processes formally

» QPAlg, CQP, qCCS, …

Introduction | Formal verification

Formal verification of quantum protocols

Model $\approx$ Spec.

Equivalence

Equivalence between processes

- (Weak) **bisimulation**
- Barbed congruence

Not bisimilar but **intuitively** equivalent processes

Example:

- Sends $|0\rangle$ or $|1\rangle$ with the same prob.
- Sends $|+\rangle$ or $|-\rangle$ with the same prob.

» The **same density matrix** expresses these qubits:

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$$

» Used in Shor & Preskill's security proof of BB84 [SP'00]

Introduction | Motivation

Not bisimilar but **intuitively** equivalent processes

Example: [KKKKS'12]

- Measures a qubit $|+\rangle\langle+|$ and ...

$$|+\rangle\langle+| \xrightarrow{1/2} |0\rangle\langle 0|$$

$$|+\rangle\langle+| \xrightarrow{1/2} |1\rangle\langle 1|$$

- Applies $\mathcal{E}$ to a qubit $|+\rangle\langle+|$ and ...
  - » $\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$

$$|+\rangle\langle+| \longrightarrow \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

To define more intuitive equivalence

qCCS [FDY'12]

Existing notions of equivalence:

- (Weak) bisimulation [FDY'12]
- (Weak) open bisimulation [DF'12]
- Reduction barbed congruence [DF'12]

Quantum process calculus qCCS

Quantum process calculus qCCS | Syntax

Quantum processes (classical constructs)

$$
\begin{array}{rcll}
P, Q & ::= & \mathbf{nil} & \\
& | & c?x.P & \text{Receive classical data} \\
& | & c!e.P & \text{Send classical data} \\
& | & P + Q & \text{Nondeterministic choice} \\
& | & P \,||\, Q & \text{Parallel composition} \\
& | & \mathbf{if}\ b\ \mathbf{then}\ P & \\
& \vdots & &
\end{array}
$$

Quantum process calculus qCCS | Syntax

Quantum processes (quantum constructs)

$$
\begin{array}{lll}
\vdots & & \\
\mid & \mathsf{c}?q.P & \text{Receive qubit} \\
\mid & \mathsf{c}!q.P & \text{Send qubit} \\
\mid & \mathcal{E}[\tilde{q}].P & \text{Applying super-operator} \\
\mid & M[\tilde{q}; x].P & \text{Measurement} \\
\vdots & &
\end{array}
$$

Quantum process calculus qCCS | Semantics

State of a process: *configuration* $C = \langle P, \rho \rangle$

» P : quantum process

» ρ : quantum state (density operator)

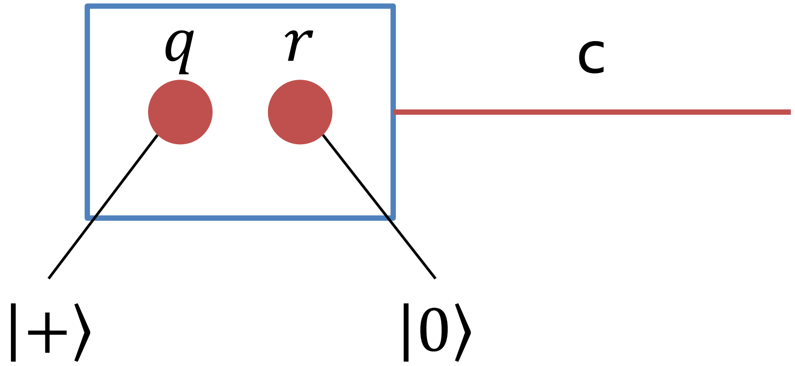
Operational semantics: labeled transition system

Labels:

- $c?v$ / $c!v$:
  receive/send data v using c
- $\mathrm{c}?q$ / $\mathrm{c}!q$:
  receive/send **qubit** q using c
- τ :
  internal transition (cannot be observed)

Example:

$$\left\langle \mathcal{CNOT}[q,r].\mathrm{c}!r.P, |+\rangle\langle+|_q \otimes |0\rangle\langle 0|_r \otimes \rho_E \right\rangle$$

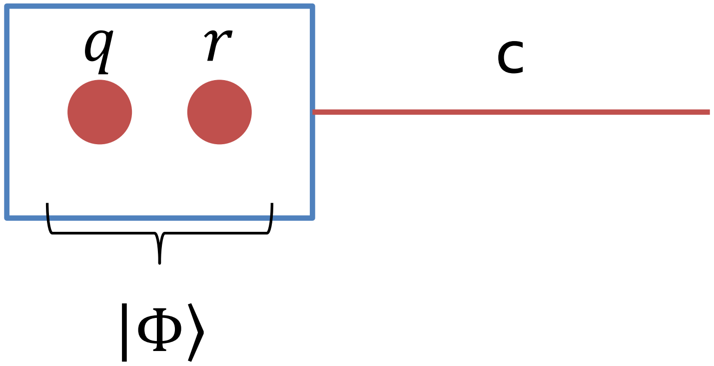


Quantum process calculus qCCS | Semantics

Example:

$$\left\langle \mathcal{CNOT}[q,r].\mathsf{c}!r.P, |+\rangle\langle +|_q \otimes |0\rangle\langle 0|_r \otimes \rho_E \right\rangle$$

$$\xrightarrow{\tau} \left\langle \mathsf{c}!r.P, |\Phi\rangle\langle\Phi|_{qr} \otimes \rho_E \right\rangle$$

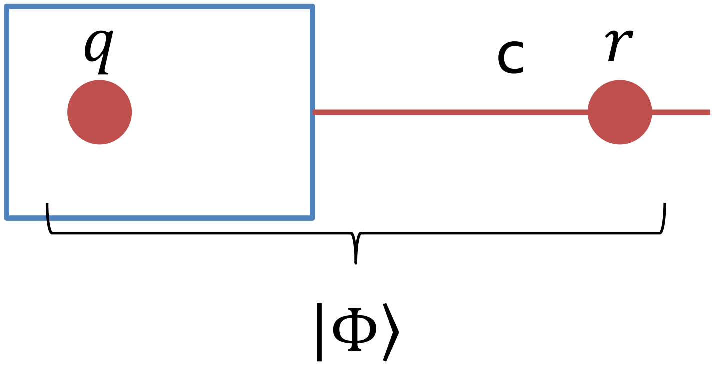


Example:

$$\left\langle \mathcal{CNOT}[q,r].\mathsf{c}!r.P, |+\rangle\langle+|_q \otimes |0\rangle\langle 0|_r \otimes \rho_E \right\rangle$$

$$\xrightarrow{\tau} \left\langle \mathsf{c}!r.P, |\Phi\rangle\langle\Phi|_{qr} \otimes \rho_E \right\rangle$$

$$\xrightarrow{\mathsf{c}!r} \left\langle P, |\Phi\rangle\langle\Phi|_{qr} \otimes \rho_E \right\rangle$$



Quantum process calculus qCCS | Semantics

Example:

$$\left\langle M[q;x].A(x), |+\rangle\langle +|_q \otimes \rho_E \right\rangle \xrightarrow{\tau} \begin{cases} \xrightarrow{1/2} \left\langle A(0), |0\rangle\langle 0|_q \otimes \rho_E \right\rangle \\ \xrightarrow{1/2} \left\langle A(1), |1\rangle\langle 1|_q \otimes \rho_E \right\rangle \end{cases}$$

Probabilistic transition

Open bisimulation on qCCS

Open bisimulation on qCCS | Definition

$\mathcal{R}$ is a *(weak) open bisimulation* if $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle \Longrightarrow$

- P and Q hold the same quantum variables
  - » $qv(P) = qv(Q)$
- Their environment (states associated with the qubits that P and Q do not hold) are the same
  - » $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$
- For any super-operator $\mathcal{E}$ acting on the environment, whenever $\langle P, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \mu$ there is some ν s.t. $\langle Q, \mathcal{E}(\sigma)\rangle \stackrel{\hat{\alpha}}{\Longrightarrow} \nu$
- (Symmetric condition)

Adding/removing τ transitions

$\approx_o$: largest open bisimulation

Open bisimulation on qCCS | Example

Intuitively equivalent processes [KKKKS'12]

- Measures a qubit $|+\rangle\langle+|$ and …

$$
\begin{tikzcd}
 & {|0\rangle\langle 0|} \\
{|+\rangle\langle+|} \arrow[ur, "1/2"] \arrow[dr, "1/2"'] & \\
 & {|1\rangle\langle 1|}
\end{tikzcd}
$$

- Applies $\mathcal{E}$ to a qubit $|+\rangle\langle+|$ and …
  - » $\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$

$$|+\rangle\langle+| \longrightarrow \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|$$

Open bisimulation on qCCS | Example

Intuitively equivalent processes

$$\left\langle M[q;x].\boxed{(c!0 + d!0)}, |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

$$\left\langle \mathcal{E}[q].\boxed{(c!0 + d!0)}, |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

» M: projective measurement $\{|0\rangle, |1\rangle\}$

» $\mathcal{E}$: super-operator

$$\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$$

Not open bisimilar

Our equivalence relation

Our equivalence relation | Informal definition

When are two processes *equivalent*?

They are observed the same by any attackers

- Observable actions = Receiving/sending data
- Attackers = Processes

They <u>use the same channels</u> with the same prob. whenever they <u>run parallel with any other process</u>

Our equivalence relation | Related notions

- Barbed congruence
  - Defined in qCCS [DF'12]
  - Coincides with $\approx_o$ [DF'12]
- Testing equivalence
  - Not defined in quantum process calculi

Our equivalence relation | Informal definition

When are two processes *equivalent*?

They are observed the same by any attackers

- Observable actions = Receiving/sending data
- Attackers = Processes

They use the same channels with the same **prob.** whenever they run parallel with any other process

Our equivalence relation | Solving nondeterminism

Processes have **nondeterministic** transitions

$$\begin{tikzcd}[column sep=tiny]
& \langle a!0 \mid\mid a?x.b!0 \mid\mid a?x.c!0, \rho\rangle \arrow[dl, "\tau"] \arrow[dr, "\tau"] & \\
\langle \mathbf{nil} \mid\mid b!0 \mid\mid a?x.c!0, \rho\rangle \arrow[d, "b!0"] & & \langle \mathbf{nil} \mid\mid a?x.b!0 \mid\mid c!0, \rho\rangle \arrow[d, "c!0"] \\
{} & & {}
\end{tikzcd}$$

Probabilities of using each channel?

Our equivalence relation | Solving nondeterminism

Schedulers solve nondeterminism

Scheduler F: configuration → next transition

$$
\begin{tikzcd}
& \langle a!0 \;||\; a?x.b!0 \;||\; a?x.c!0, \rho \rangle \arrow[dl, "\tau", "F"', red] \arrow[dr, "\tau"] & \\
\langle \mathbf{nil} \;||\; b!0 \;||\; a?x.c!0, \rho \rangle \arrow[d, "b!0", "F"', red] & & \langle \mathbf{nil} \;||\; a?x.b!0 \;||\; c!0, \rho \rangle \arrow[d, "c!0", "F"', red] \\
{} & & {}
\end{tikzcd}
$$

Our equivalence relation | Informal definition

When are two processes *equivalent*?

They are observed the same by any attackers

- Observable actions = Receiving/sending data
- Attackers = Processes

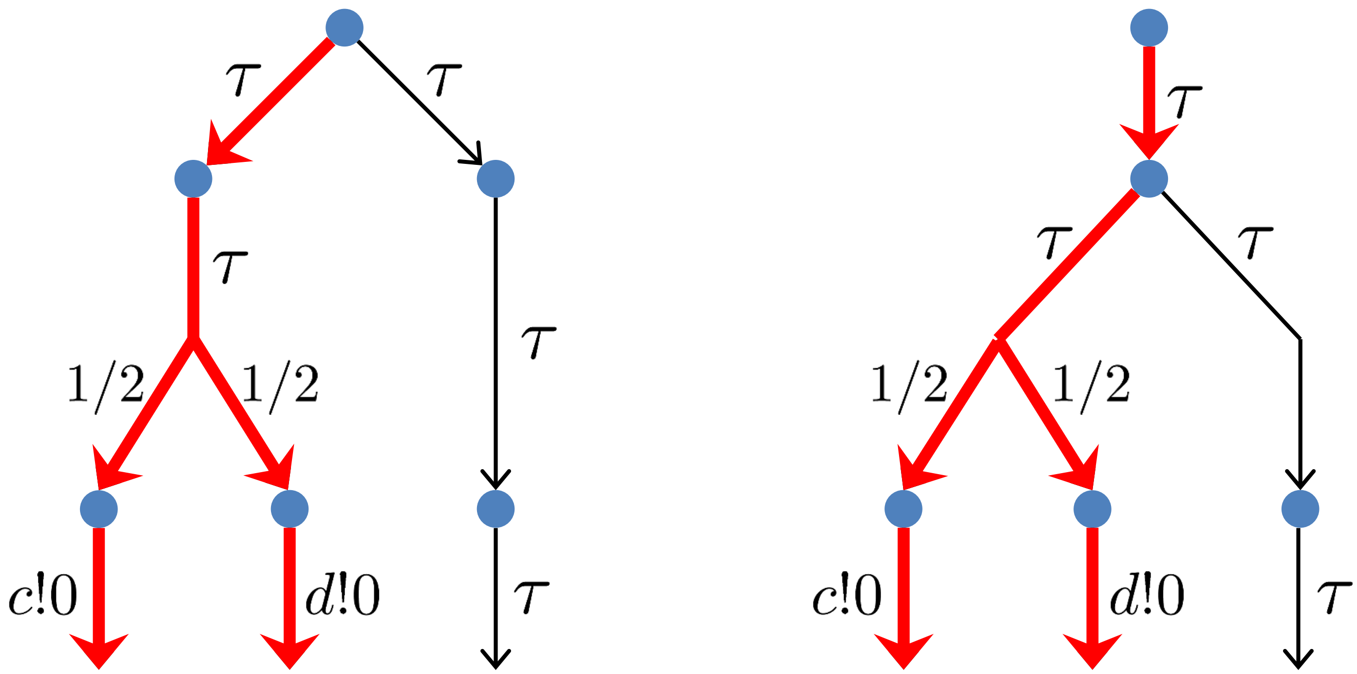
They use the same channels with the same prob. whenever they run parallel with any other process

Observational equivalence | Definition

$\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are *observationally equivalent*
($\langle P, \rho \rangle \approx_{oe} \langle Q, \sigma \rangle$) if

- P and Q hold the same quantum variables
- Their **Attacker** nt are the same
- For any process R and scheduler F,
  there exists a scheduler F' s.t. for any channel c,
  if $\langle P || R, \rho \rangle$ uses c w.p. p according to F,
  then $\langle Q || R, \sigma \rangle$ also uses c w.p. p according to F'
- (Symmetric condition)

Observational equivalence | Sketch



Run parallel with any process R

Observational equivalence | Example

Not bisimilar but intuitively equivalent processes

$$\left\langle M[q;x].(c!0 + d!0), |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

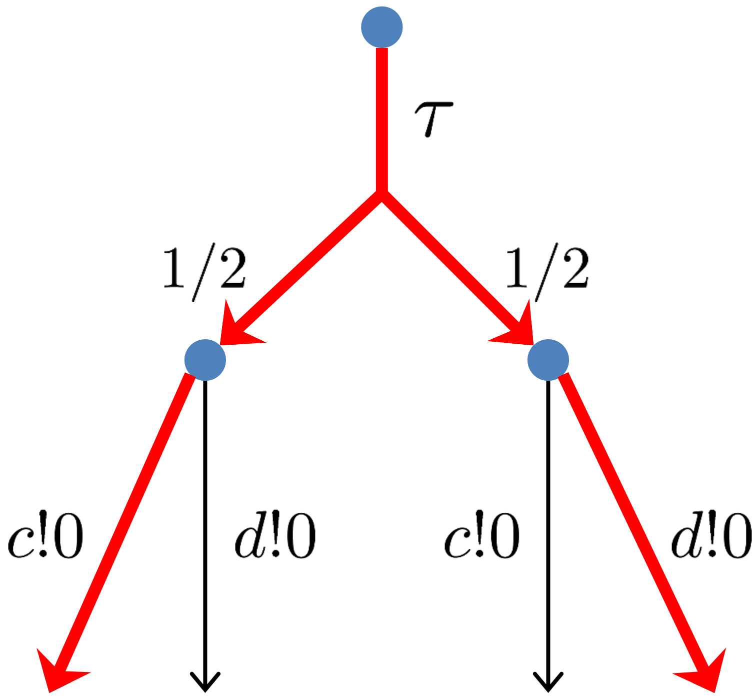
$$\left\langle \mathcal{E}[q].(c!0 + d!0), |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

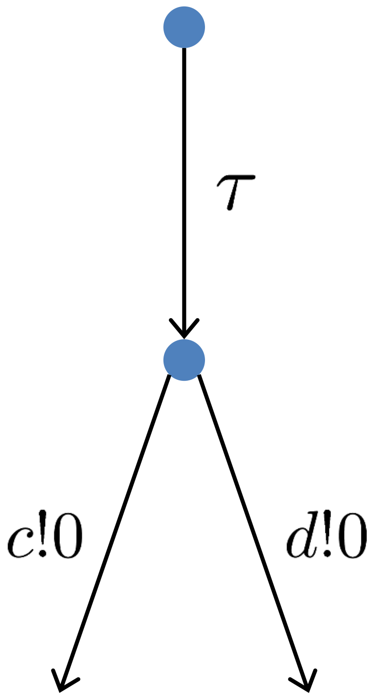
- M: projective measurement $\{|0\rangle, |1\rangle\}$
- $\mathcal{E}$: super-operator

$$\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$$

Not observationally equivalent

Observational equivalence | Example

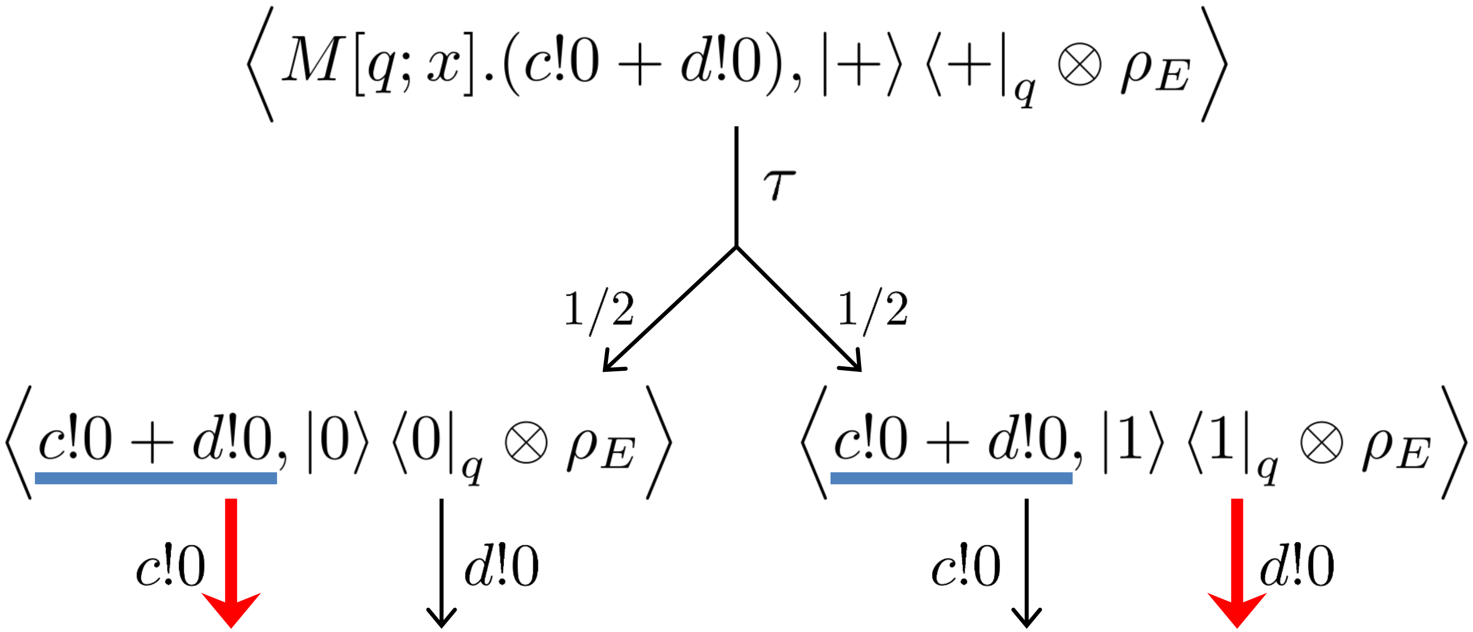




No schedulers

Observational equivalence | Example

Schedulers can choose **different** transitions after measurement



Processes are the same

$\Longrightarrow$ Schedulers should choose the same transitions

Observational equivalence | Strategy

Strategies: schedulers with this limitation

Strategy F: configuration → next transition

$$\left\langle M[q;x].(c!0 + d!0), |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

$$\Big\downarrow \tau$$

$$\swarrow 1/2 \qquad 1/2 \searrow$$

$$\left\langle c!0 + d!0, |0\rangle\langle 0|_q \otimes \rho_E \right\rangle \qquad \left\langle c!0 + d!0, |1\rangle\langle 1|_q \otimes \rho_E \right\rangle$$

$$c!0 \downarrow \quad \downarrow d!0 \qquad\qquad c!0 \downarrow \quad \cancel{\downarrow d!0}$$

Not allowed

Observational equivalence | Strategy

$\langle P, \rho \rangle, \langle Q, \sigma \rangle$ are *observationally equivalent* ***with strategies*** ($\langle P, \rho \rangle \approx_{oe}^{st} \langle Q, \sigma \rangle$) if

- P and Q hold the same quantum variables
- Their environment are the same
- For any process R and **strategy** F,
  there exists a **strategy** F' s.t. for any channel c,
  if $\langle P || R, \rho \rangle$ uses c w.p. p according to F,
  then $\langle Q || R, \sigma \rangle$ also uses c w.p. p according to F'
- (Symmetric condition)

Observational equivalence | Example

Not bisimilar but intuitively equivalent processes

$$\left\langle M[q;x].(c!0 + d!0), |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

$$\left\langle \mathcal{E}[q].(c!0 + d!0), |+\rangle\langle+|_q \otimes \rho_E \right\rangle$$

- M: projective measurement $\{|0\rangle, |1\rangle\}$
- $\mathcal{E}$: super-operator

$$\mathcal{E}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$$

Not observationally equivalent

Observationally equivalent with strategies

Observational equivalence | Comparing with others

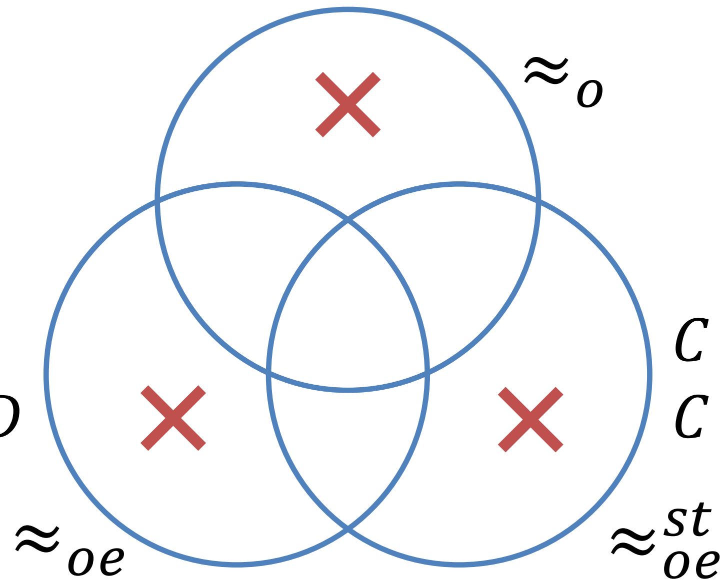
Relation among $\approx_o, \approx_{oe}, \approx_{oe}^{st}$?

$\approx_o \subseteq \approx_{oe} \subseteq \approx_{oe}^{st}$?

Observational equivalence | Comparing with others

$\approx_o, \approx_{oe}, \approx_{oe}^{st}$ are **incomparable**

$C \approx_o D$ but $C \not\approx_{oe} D, C \not\approx_{oe}^{st} D$



$C \approx_{oe} D$ but
$C \not\approx_o D,\ C \not\approx_{oe}^{st} D$

$C \approx_{oe}^{st} D$ but
$C \not\approx_o D,\ C \not\approx_{oe} D$

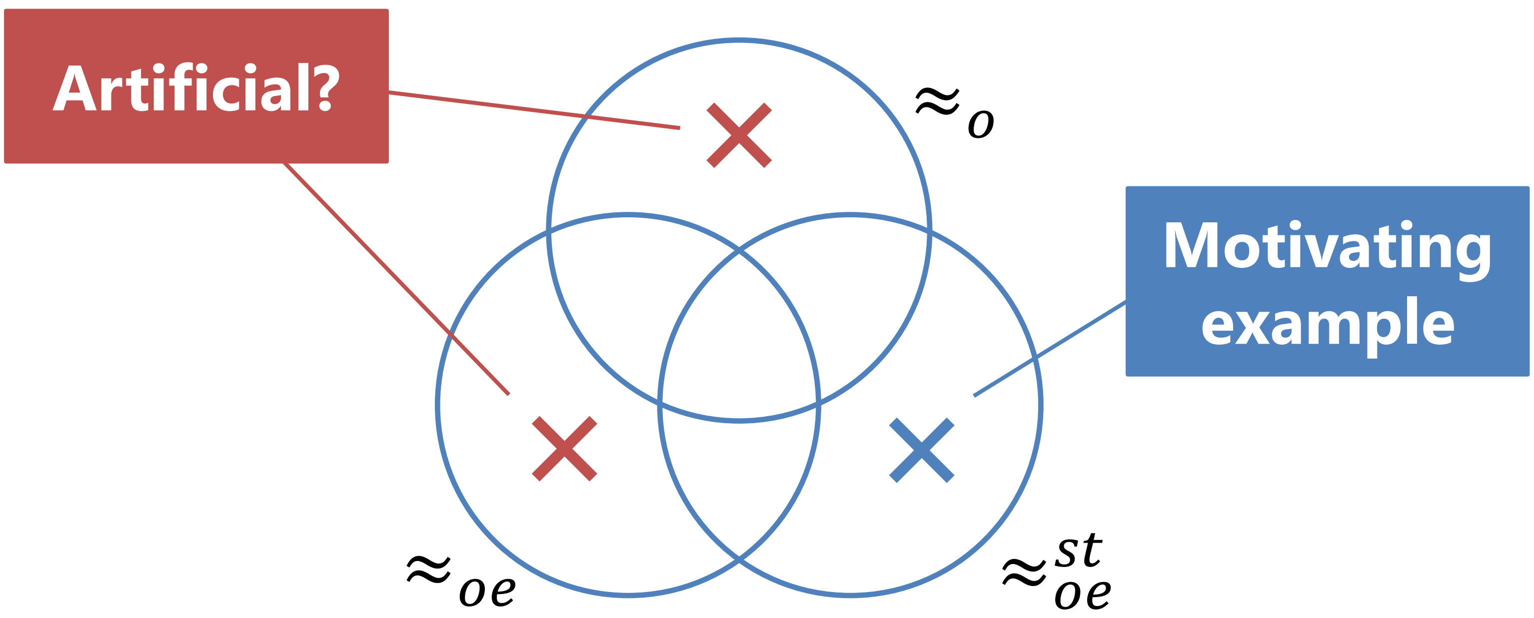
Conclusion

Conclusion | Summary

- Introduce qCCS and open bisimulation $\approx_o$
- Define observational equivalence
  - With schedulers: $\approx_{oe}$
  - With strategies: $\approx_{oe}^{st}$
- Show motivating examples are $\approx_{oe}^{st}$
- Show $\approx_o, \approx_{oe}, \approx_{oe}^{st}$ are incomparable

Conclusion | Future work

- Formalize our "intuition"
  - » Is observational equivalence really "intuitive"?



Conclusion | Future work

- Check congruence property
  - Congruence for parallel compositions holds:

$$P \approx_{oe}^{st} Q \Longrightarrow P||R \approx_{oe}^{st} Q||R$$

  - Does congruence for other constructs hold?

Conclusion

» Summary

- Define observational equivalence
  - With schedulers $\approx_{oe}$
  - With strategies $\approx_{oe}^{st}$
- Show motivating examples are $\approx_{oe}^{st}$
- Show $\approx_{o}, \approx_{oe}, \approx_{oe}^{st}$ are incomparable

» Future work

- Formalize our “intuition”
- Check congruence property