Open Bisimulation for Quantum Processes

Yuxin Deng[1] and Yuan Feng[2]

[1] Shanghai Jiao Tong University
and Chinese Academy of Sciences, China

[2] University of Technology, Sydney, Australia
and Tsinghua University, China

UTS:QCIS
QUANTUM COMPUTATION & INTELLIGENT SYSTEMS

Outline

1. Motivation
2. Basic definitions
3. Equivalences for quantum processes
4. Modal characterisation
5. Summary

Motivation

Motivation

- Quantum protocols may have many more potential bugs than classical protocols, since quantum mechanics is counter-intuitive.

Motivation

- Quantum protocols may have many more potential bugs than classical protocols, since quantum mechanics is counter-intuitive.
- Quantum process algebras to clone the success of classical process algebras.

Quantum process algebras

Quantum process algebras

- QPAlg (Quantum Process Algebra, Jorrand and Lalire, 2004)

Quantum process algebras

- QPAlg (Quantum Process Algebra, Jorrand and Lalire, 2004)
- CQP (Communicating Quantum Processes, Gay and Nagarajan, POPL2005)

Quantum process algebras

- QPAlg (Quantum Process Algebra, Jorrand and Lalire, 2004)
- CQP (Communicating Quantum Processes, Gay and Nagarajan, POPL2005)
- qCCS (quantum CCS, Feng et al, I&C2007, ACM TCL2009, POPL2011)

In this talk, we present

In this talk, we present

- A natural extensional behavioural equivalence between quantum processes in qCCS.

In this talk, we present

- A natural extensional behavioural equivalence between quantum processes in qCCS.
- A notion of open bisimulation which provides both a sound and complete proof methodology for the behavioural equivalence.

In this talk, we present

- A natural extensional behavioural equivalence between quantum processes in qCCS.
- A notion of open bisimulation which provides both a sound and complete proof methodology for the behavioural equivalence.
- A modal characterisation of the behavioural equivalence, by extending the Hennessy-Milner logic to the quantum setting.

Outline

1 Motivation

2 Basic definitions

3 Equivalences for quantum processes

4 Modal characterisation

5 Summary

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.
- 'bra' $\langle\psi|$ stands for the adjoint (dual vector) of $|\psi\rangle$.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.
- 'bra' $\langle\psi|$ stands for the adjoint (dual vector) of $|\psi\rangle$.
- Generally, $A^\dagger$ stands for the adjoint of A, such that

$$(A^\dagger|\psi\rangle, |\phi\rangle) = (|\psi\rangle, A|\phi\rangle).$$

  In particular, $(|\psi\rangle)^\dagger = \langle\psi|$.

Quantum states

Quantum states

- Associated to any quantum system is a Hilbert space known as the state space.

Quantum states

- Associated to any quantum system is a Hilbert space known as the state space.
- The state of a closed quantum system is described by a unit vector, say $|\psi\rangle$, in its state space.

Quantum states(Cont'd)

Quantum states(Cont'd)

- $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$: lies in the state $|\psi_k\rangle$ with probability p_k, $\sum_k p_k = 1$.
  - ρ is a positive operator
  - $\mathrm{tr}(\rho) = 1$

Quantum states(Cont'd)

- $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$: lies in the state $|\psi_k\rangle$ with probability p_k, $\sum_k p_k = 1$.
  - ρ is a positive operator
  - $\mathrm{tr}(\rho) = 1$
- These two conditions characterize exactly the set of density operators.

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$, such that

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$, such that

- $\mathcal{E}$ is trace-preserving. That is, $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ for any positive operator A.

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$, such that

- $\mathcal{E}$ is trace-preserving. That is, $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ for any positive operator A.
- $\mathcal{E}$ is completely positive. That is, for any auxiliary space $\mathcal{H}'$ and any positive operator σ on the tensor Hilbert space $\mathcal{H}' \otimes \mathcal{H}$, $(\mathcal{I}_{\mathcal{H}'} \otimes \mathcal{E})(\sigma)$ is also a positive operator on $\mathcal{H}' \otimes \mathcal{H}$.

Quantum dynamics

Quantum dynamics

- The evolution of a quantum system is described by a super-operator

$$\rho' = \mathcal{E}(\rho)$$

Quantum dynamics

- The evolution of a quantum system is described by a super-operator

$$\rho' = \mathcal{E}(\rho)$$

- Kraus representation theorem: A map $\mathcal{E}$ is a super-operator if and only if

$$\mathcal{E}(A) = \sum_{i=1}^{d} E_i A E_i^\dagger$$

for some set of matrices $\{E_i, i = 1, \ldots, d\}$ with $\sum_i E_i^\dagger E_i = I$.

Quantum measurements

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

- If we measure ρ by the observable A, then we obtain the result k with probability

$$p_k = \mathrm{tr}(P_k \rho)$$

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

- If we measure ρ by the observable A, then we obtain the result k with probability

$$p_k = \mathrm{tr}(P_k \rho)$$

- The measurement disturbs the system, leaving it in a state $P_k \rho P_k / p_k$ determined by the outcome.

Syntax of qCCS

The syntax of qCCS:

$$\mathbf{nil} \mid \mathit{pref}.P \mid P + Q \mid P \| Q \mid P \backslash L \mid \mathbf{if}\ b\ \mathbf{then}\ P \mid A(\tilde{q}; \tilde{x})$$

where

$$\mathit{pref} ::= \tau \mid c?x \mid c!e \mid \mathsf{c}?q \mid \mathsf{c}!q \mid \mathcal{E}[\widetilde{q}] \mid M[\widetilde{q}; x]$$

Further requirements

Further requirements

- $c?x.d!x.d!x.0$

Further requirements

- $c?x.d!x.d!x.0$

$\not\Rightarrow$ $c?r.d!r.d!r.0$

Further requirements

- $c?x.d!x.d!x.0$

$\not\Rightarrow$ $c?r.d!r.d!r.0$

- Quantum no-cloning theorem!

Syntax of qCCS, cont'd

For a process to be legal, we require that

Syntax of qCCS, cont'd

For a process to be legal, we require that

1. $q \notin qv(P)$ `in the process` $\mathtt{c}!q.P$;

Syntax of qCCS, cont'd

For a process to be legal, we require that

1. $q \notin qv(P)$ `in the process` $\mathtt{c}!q.P$;
2. $qv(P) \cap qv(Q) = \emptyset$ `in the process` $P \,||\, Q$.

Operational Semantics of qCCS

Suppose P is a closed quantum process. A pair of the form

$$\langle P, \rho \rangle$$

is called a configuration, where ρ is a density operator. The set of configurations is denoted by Con. We sometimes let $\mathcal{C}, \mathcal{D}, \ldots$ range over Con to ease notations.

Operational Semantics of qCCS

Let

$$\begin{aligned} Act \;=\; & \{\tau\} \cup \{c?v, c!v \mid c \text{ classical channel}, v \text{ real number}\} \cup \\ & \{\mathrm{c}?r, \mathrm{c}!r \mid \mathrm{c} \text{ quantum channel}, r \text{ quantum variable}\}, \end{aligned}$$

and $D(Con)$ be the set of finite-support probability distributions over Con.

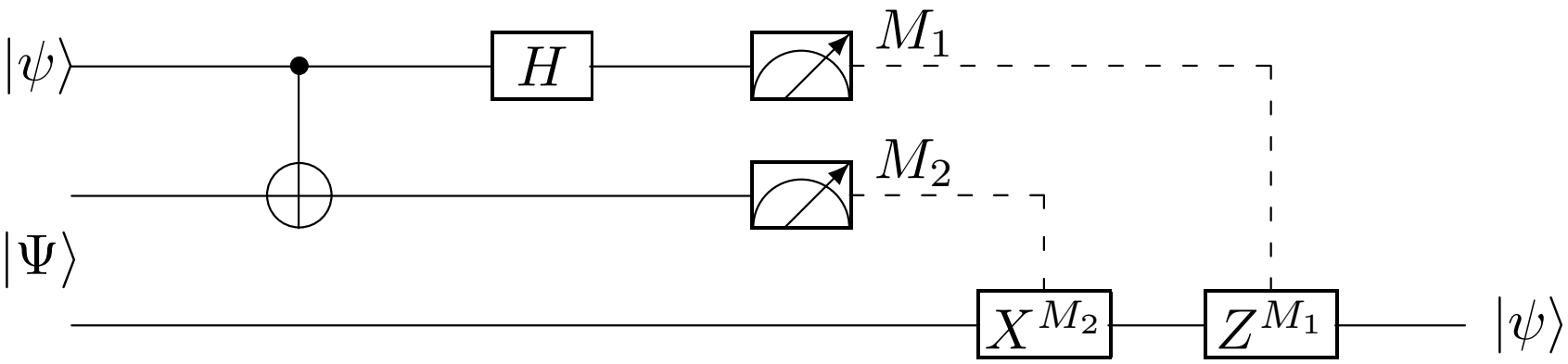
The semantics of qCCS is given by the probabilistic labeled transition system $(Con, Act, \rightarrow)$, where $\rightarrow \subseteq Con \times Act \times D(Con)$ is the smallest relation satisfying some rules.

An example: Teleportation

Quantum teleportation [Bennett, Brassard, Crepeau, Jozsa, Peres, and Wootters, PRL 1993] is one of the most important protocols in quantum information theory which makes use of a maximally entangled state to teleport an unknown quantum state by sending only *classical* information.

It serves as a key ingredient in many other quantum communication protocols.

An example: Teleportation



Let

$$\begin{aligned} \mathit{Alice} &:= \mathit{CNot}[q, q_1].H[q].M[q, q_1; x].c!x.\mathbf{nil} \\ \mathit{Bob} &:= c?x.U_x[q_2].\mathbf{nil} \\ \mathit{Telep} &:= (\mathit{Alice} \| \mathit{Bob}) \backslash \{c\} \end{aligned}$$

Here $M = \sum_{i=0}^{3} \lambda_i |\tilde{i}\rangle\langle\tilde{i}|$, and

$$\begin{aligned} U_x[q_2].\mathbf{nil} := {} & \mathbf{if}\ x = \lambda_0\ \mathbf{then}\ \sigma_0[q_2].\mathbf{nil} + \mathbf{if}\ x = \lambda_1\ \mathbf{then}\ \sigma_1[q_2].\mathbf{nil} \\ & + \mathbf{if}\ x = \lambda_2\ \mathbf{then}\ \sigma_3[q_2].\mathbf{nil} + \mathbf{if}\ x = \lambda_3\ \mathbf{then}\ \sigma_2[q_2].\mathbf{nil}. \end{aligned}$$

$$\langle Telep,\ [(\alpha|0\rangle+\beta|1\rangle)\otimes\tfrac{1}{\sqrt{2}}(|00\rangle+|11\rangle)]\rangle$$

$\downarrow \tau$

$$\langle (H[q].M[q,q_1;x].c!x.\mathbf{nil}\|Bob)\backslash\{c\},\ [\tfrac{1}{\sqrt{2}}(\alpha(|000\rangle+|011\rangle)+\beta(|110\rangle+|101\rangle))]\rangle$$

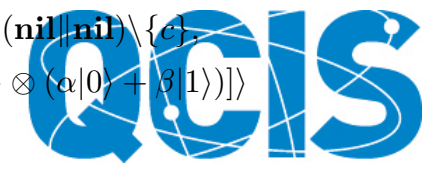
$\downarrow \tau$

$$\langle (M[q,q_1;x].c!x.\mathbf{nil}\|Bob)\backslash\{c\},\ [\tfrac{1}{2}(\alpha(|000\rangle+|100\rangle+|011\rangle+|111\rangle)+\beta(|010\rangle-|110\rangle+|001\rangle-|101\rangle))]\rangle$$

$\downarrow \tau$

1/4 1/4 1/4 1/4

$\langle (c!\lambda_0.\mathbf{nil}\|Bob)\backslash\{c\}, [\alpha\|000\rangle+\beta\|001\rangle]\rangle$	$\langle (c!\lambda_1.\mathbf{nil}\|Bob)\backslash\{c\}, [\alpha\|011\rangle+\beta\|010\rangle]\rangle$	$\langle (c!\lambda_2.\mathbf{nil}\|Bob)\backslash\{c\}, [\alpha\|100\rangle-\beta\|101\rangle]\rangle$	$\langle (c!\lambda_3.\mathbf{nil}\|Bob)\backslash\{c\}, [\alpha\|111\rangle-\beta\|110\rangle]\rangle$
$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$
$\langle (\mathbf{nil}\|\sigma_0[q_2].\mathbf{nil})\backslash\{c\}, [\|00\rangle\otimes(\alpha\|0\rangle+\beta\|1\rangle)]\rangle$	$\langle (\mathbf{nil}\|\sigma_1[q_2].\mathbf{nil})\backslash\{c\}, [\|01\rangle\otimes(\alpha\|1\rangle+\beta\|0\rangle)]\rangle$	$\langle (\mathbf{nil}\|\sigma_3[q_2].\mathbf{nil})\backslash\{c\}, [\|10\rangle\otimes(\alpha\|0\rangle-\beta\|1\rangle)]\rangle$	$\langle (\mathbf{nil}\|\sigma_2[q_2].\mathbf{nil})\backslash\{c\}, [\|11\rangle\otimes(\alpha\|1\rangle-\beta\|0\rangle)]\rangle$
$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$	$\downarrow \tau$
$\langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\}, [\|00\rangle\otimes(\alpha\|0\rangle+\beta\|1\rangle)]\rangle$	$\langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\}, [\|01\rangle\otimes(\alpha\|0\rangle+\beta\|1\rangle)]\rangle$	$\langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\}, [\|10\rangle\otimes(\alpha\|0\rangle+\beta\|1\rangle)]\rangle$	$\langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\}, [\|11\rangle\otimes(\alpha\|0\rangle+\beta\|1\rangle)]\rangle$



Outline

1 Motivation

2 Basic definitions

3 Equivalences for quantum processes

4 Modal characterisation

5 Summary

Lifted relation

Let $\mathcal{R} \subseteq S \times \mathit{Dist}(S)$ be a relation from states to distributions in a pLTS. Then $\mathcal{R}^\circ \subseteq \mathit{Dist}(S) \times \mathit{Dist}(S)$ is the smallest relation that satisfies the two rules:

Lifted relation

Let $\mathcal{R} \subseteq S \times \mathit{Dist}(S)$ be a relation from states to distributions in a pLTS. Then $\mathcal{R}^\circ \subseteq \mathit{Dist}(S) \times \mathit{Dist}(S)$ is the smallest relation that satisfies the two rules:

1. $s \mathcal{R} \Theta$ `implies` $\overline{s}\, \mathcal{R}^\circ\, \Theta$;

Lifted relation

Let $\mathcal{R} \subseteq S \times Dist(S)$ be a relation from states to distributions in a pLTS. Then $\mathcal{R}^\circ \subseteq Dist(S) \times Dist(S)$ is the smallest relation that satisfies the two rules:

1. $s \mathcal{R} \Theta$ implies $\overline{s}\ \mathcal{R}^\circ\ \Theta$;
2. $\Delta_i\ \mathcal{R}^\circ\ \Theta_i$ for all $i \in I$ implies

$$(\sum_{i \in I} p_i \cdot \Delta_i)\ \mathcal{R}^\circ\ (\sum_{i \in I} p_i \cdot \Theta_i)$$

for any $p_i \in [0,1]$ with $\sum_{i \in I} p_i = 1$, where I is a countable index set.

Weak transitions

Weak transitions

- We write $s \xrightarrow{\hat{\tau}} \Delta$ if either $s \xrightarrow{\tau} \Delta$ or $\Delta = \overline{s}$.

Weak transitions

- We write $s \xrightarrow{\hat{\tau}} \Delta$ if either $s \xrightarrow{\tau} \Delta$ or $\Delta = \overline{s}$.
- We define weak transitions $\stackrel{\hat{a}}{\Longrightarrow}$ by letting $\stackrel{\hat{\tau}}{\Longrightarrow}$ be the reflexive and transitive closure of $\xrightarrow{\hat{\tau}}$ and writing $\Delta \stackrel{\hat{a}}{\Longrightarrow} \Theta$ for $a \in \mathrm{Act}$ whenever

$$\Delta \stackrel{\hat{\tau}}{\Longrightarrow} \xrightarrow{a} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta.$$

Four criteria to judge equivalence

A relation $\mathcal{R}$ is

Four criteria to judge equivalence

A relation $\mathcal{R}$ is

- barb-preserving if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that $\mathcal{C} \Downarrow_c^{\geq p}$ iff $\mathcal{D} \Downarrow_c^{\geq p}$ for any $p \in [0,1]$ and any classical channel c, where $\mathcal{C} \Downarrow_c^{\geq p}$ holds if $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with

$$\sum\{\Delta(\mathcal{C}') \mid \mathcal{C}' \xrightarrow{c!v} \text{ for some } v\} \geq p;$$

Four criteria to judge equivalence

A relation $\mathcal{R}$ is

- barb-preserving if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that $\mathcal{C} \Downarrow_c^{\geq p}$ iff $\mathcal{D} \Downarrow_c^{\geq p}$ for any $p \in [0,1]$ and any classical channel c, where $\mathcal{C} \Downarrow_c^{\geq p}$ holds if $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with

$$\sum\{\Delta(\mathcal{C}') \mid \mathcal{C}' \xrightarrow{c!v} \text{ for some } v\} \geq p;$$

- reduction-closed if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies
  - whenever $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$, there exists Θ such that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \, \mathcal{R}^\circ \, \Theta$,
  - whenever $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$, there exists Δ such that $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ and $\Delta \, \mathcal{R}^\circ \, \Theta$;

Four criteria to judge equivalence, cont.

- compositional if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $(\mathcal{C}||R)\mathcal{R}(\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$,

Four criteria to judge equivalence, cont.

- compositional if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $(\mathcal{C}||R)\mathcal{R}(\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$,
- closed under super-operator application, if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $\mathcal{E}(\mathcal{C})\mathcal{R}\mathcal{E}(\mathcal{D})$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$.

Reduction barbed congruence

Let `reduction barbed congruence`, written $\approx_r$, be the largest relation over configurations which is

- `barb-preserving`,
- `reduction-closed`,
- `compositional`,
- `closed under super-operator application`,

Reduction barbed congruence

Let `reduction barbed congruence`, written $\approx_r$, be the largest relation over configurations which is

- `barb-preserving`,
- `reduction-closed`,
- `compositional`,
- `closed under super-operator application`,
- `and furthermore, if` $\mathcal{C} \approx_r \mathcal{D}$ `then` $qv(\mathcal{C}) = qv(\mathcal{D})$ `and` $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$.

Open bisimulation

A relation $\mathcal{R} \subseteq \mathit{Con} \times \mathit{Con}$ is an `open simulation` if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that

- $qv(\mathcal{C}) = qv(\mathcal{D})$, and $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$,
- for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$, whenever $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, there is some Θ with $\mathcal{E}(\mathcal{D}) \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \, \mathcal{R}^{\circ} \, \Theta$.

A relation $\mathcal{R}$ is an `open bisimulation` if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are open simulations. We let $\approx_o$ be the largest open bisimulation.

Theorem : Congruence

Theorem : Congruence

- The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.

Theorem : Congruence

- The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.
- $\mathcal{C} \approx_o \mathcal{D}$ if and only if $\mathcal{C} \approx_r \mathcal{D}$.

Outline

1 Motivation

2 Basic definitions

3 Equivalences for quantum processes

4 Modal characterisation

5 Summary

Modal characterisation

The class $\mathcal{L}$ of modal formulae over Act, ranged over by ϕ, is defined by the following grammar:

$$\begin{array}{lcl} \phi & := & E_{\tilde{q}}^{\geq p} \mid \bigwedge_{i \in I} \phi_i \mid \langle \alpha \rangle \psi \mid \neg \phi \mid \mathcal{E}.\phi \\ \psi & := & \bigoplus_{i \in I} p_i \cdot \phi_i \end{array}$$

where $\alpha \in \mathrm{Act}_\tau$, $\mathcal{E}$ is a super-operator, and E is a projector associated with a certain subspace of $\mathcal{H}_{\tilde{q}}$.

We call ϕ a `configuration formula` and ψ a `distribution formula`.

The satisfaction relation $\models \subseteq Con \times \mathcal{L}$ is defined by, say,

The satisfaction relation $\models \subseteq Con \times \mathcal{L}$ is defined by, say,

- $\langle P, \rho \rangle \models E_{\tilde{q}}^{\geq p}$ if $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$.

The satisfaction relation $\models \subseteq Con \times \mathcal{L}$ is defined by, say,

- $\langle P, \rho \rangle \models E_{\tilde{q}}^{\geq p}$ if $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$.
- $\mathcal{C} \models \mathcal{E}.\phi$ if $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ and $\mathcal{E}(\mathcal{C}) \models \phi$.

The satisfaction relation $\models \subseteq Con \times \mathcal{L}$ is defined by, say,

- $\langle P, \rho \rangle \models E_{\tilde{q}}^{\geq p}$ if $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$.
- $\mathcal{C} \models \mathcal{E}.\phi$ if $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ and $\mathcal{E}(\mathcal{C}) \models \phi$.
- $\Delta \models \bigoplus_{i \in I} p_i \cdot \phi_i$ if there are Δ_i, $i \in I$, such that $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$, and for all $\mathcal{D} \in \lceil \Delta_i \rceil$, $\mathcal{D} \models \phi_i$.

A logical equivalence

We write $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ if $\mathcal{C} \models \phi \Leftrightarrow \mathcal{D} \models \phi$ for all $\phi \in \mathcal{L}$.

Theorem

$\mathcal{C} \approx_r \mathcal{D}$ if and only if $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$.

Outline

1 Motivation

2 Basic definitions

3 Equivalences for quantum processes

4 Modal characterisation

5 Summary

Summary

Summary

- A natural extensional behavioural equivalence between quantum processes.

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.
- A modal characterisation of the behavioural equivalence.

Topic for further studies

Topic for further studies

- Can we get rid of the application of an arbitrary super-operator in the definition of bisimulation?

Topic for further studies

- Can we get rid of the application of an arbitrary super-operator in the definition of bisimulation?
- Apply the open bisimulation to analyze the security of quantum cryptographic protocols such as BB84 quantum key distribution protocol.

Thank you!