An Introduction to Quantum Process Algebras

Part 2: Quantum Representations and Bisimulations

Fabio Gadducci Lorenzo Ceragioli **Giuseppe Lomurno** Gabriele Tedeschi

17 November 2026

QCOMICAL School 2026

Where we left off

Yesterday

- lqCCS: value-passing CCS $+$ quantum operations $+$ linear types
- Semantics: an (NP)LTS of configurations $\langle |\psi\rangle , P\rangle$
- Equivalence: probabilistic testing
- Lesson: non-deterministic tests inspect qubits without measuring them
- Fix: only deterministic tests

Today's plan

1. Quantum toolkit: density operators and superoperators
2. Configuration semantics, revisited
3. Bisimulation in a nutshell
4. When bisimilarity fails physics
5. Schedulers via tags, and scheduled bisimilarity
6. Quantum distributions and labelled bisimilarity
7. Angelic vs demonic scheduling, and a look ahead
8. Case study: the quantum coin flip

1. Quantum Toolkit

Mixtures of Quantum States

A state is a unit vector $|\psi\rangle$ (a *pure* state). But protocols produce *random* states, e.g. $|0\rangle$ with probability $1/3$ and $|+\rangle$ with probability $2/3$: $\Delta = \frac{1}{3} \bullet |0\rangle \oplus \frac{2}{3} \bullet |+\rangle \in \mathcal{D}(\mathcal{H})$

Mixtures of Quantum States

A state is a unit vector $|\psi\rangle$ (a *pure* state). But protocols produce *random* states, e.g. $|0\rangle$ with probability $1/3$ and $|+\rangle$ with probability $2/3$: $\Delta = \frac{1}{3} \bullet |0\rangle \oplus \frac{2}{3} \bullet |+\rangle \in \mathcal{D}(\mathcal{H})$

Density operator

A distribution of pure states Δ is represented by the matrix

$$\rho_\Delta = \sum_{|\psi\rangle} \Delta(|\psi\rangle)\ |\psi\rangle\langle\psi| \qquad \text{e.g. } \tfrac{1}{3}|0\rangle\langle 0| + \tfrac{2}{3}|+\rangle\langle +| = \tfrac{1}{3}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \tfrac{1}{3}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \tfrac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Positive semidefinite, with $\mathsf{tr}(\rho)$ the total probability (*mass*): $\mathcal{DO}(\mathcal{H})$ has trace 1, $\mathcal{DO}^{\leq}(\mathcal{H})$ trace ≤ 1 (*partial* density operators)

Different Mixtures, Same Density Operator

$$\tfrac{1}{2}\left|0\right\rangle\!\left\langle 0\right| + \tfrac{1}{2}\left|1\right\rangle\!\left\langle 1\right| = \tfrac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \tfrac{1}{2}\mathbb{I} = \tfrac{1}{4}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \tfrac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \tfrac{1}{2}\left|+\right\rangle\!\left\langle +\right| + \tfrac{1}{2}\left|-\right\rangle\!\left\langle -\right|$$

Different Mixtures, Same Density Operator

$$\tfrac{1}{2}\left|0\right\rangle\!\left\langle 0\right| + \tfrac{1}{2}\left|1\right\rangle\!\left\langle 1\right| = \tfrac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \tfrac{1}{2}\mathbb{I} = \tfrac{1}{4}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + \tfrac{1}{4}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix} = \tfrac{1}{2}\left|+\right\rangle\!\left\langle +\right| + \tfrac{1}{2}\left|-\right\rangle\!\left\langle -\right|$$

The encoding is **not injective**

Fact (indistinguishability)

Two distributions of pure states Δ, Θ cannot be told apart by *any* physical observer whenever $\rho_\Delta = \rho_\Theta$

Different Mixtures, Same Density Operator

$$\tfrac{1}{2}\,|0\rangle\langle 0| + \tfrac{1}{2}\,|1\rangle\langle 1| = \tfrac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \tfrac{1}{2}\mathbb{I} = \tfrac{1}{4}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + \tfrac{1}{4}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix} = \tfrac{1}{2}\,|+\rangle\langle +| + \tfrac{1}{2}\,|-\rangle\langle -|$$

The encoding is **not injective**

Fact (indistinguishability)

Two distributions of pure states Δ, Θ cannot be told apart by *any* physical observer whenever $\rho_\Delta = \rho_\Theta$

A source of $|0\rangle$ / $|1\rangle$ and a source of $|+\rangle$ / $|-\rangle$ (fair coins) are the *same* source

Measurements only ever reveal the density operator

Desideratum: our equivalence must identify such systems

Composite Systems and Partial Trace

Density operators compose with $\otimes$, and describe *parts* of a system

Partial trace

Given ρ^{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, the state of A alone is $\rho^A = \mathrm{tr}_B(\rho^{AB})$, where

$$\mathrm{tr}_B\left(|\psi\rangle\langle\psi'| \otimes |\phi\rangle\langle\phi'|\right) = |\psi\rangle\langle\psi'| \cdot \langle\phi'|\phi\rangle$$

and extended by linearity

Composite Systems and Partial Trace

Density operators compose with $\otimes$, and describe *parts* of a system

Partial trace

Given ρ^{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, the state of A alone is $\rho^A = \mathrm{tr}_B(\rho^{AB})$, where

$$\mathrm{tr}_B\left(|\psi\rangle\langle\psi'| \otimes |\phi\rangle\langle\phi'|\right) = |\psi\rangle\langle\psi'| \cdot \langle\phi'|\phi\rangle$$

and extended by linearity

Separable states: we get the actual part

$$\mathrm{tr}_{q_2}(|00\rangle\langle 00|) = |0\rangle\langle 0|$$

Entangled states: we get a mixture

$$\mathrm{tr}_{q_2}(|\Phi^+\rangle\langle\Phi^+|) = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{1}{2}\mathbb{I}$$

with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Later: the partial trace tells us what the *environment* of a process can see

Superoperators

The evolution of (mixed) states is described by superoperators

Kraus representation

$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \qquad \text{with} \qquad \sum_i E_i^\dagger E_i \sqsubseteq \mathbb{I}$

- *trace-preserving* if $\sum_i E_i^\dagger E_i = \mathbb{I}$: the set $\mathcal{SO}(\mathcal{H})$
- *trace non-increasing* in general: the set $\mathcal{SO}^{\leq}(\mathcal{H}) \supseteq \mathcal{SO}(\mathcal{H})$

Superoperators

The evolution of (mixed) states is described by superoperators

Kraus representation

$\mathcal{E}(\rho) = \sum_i E_i \, \rho \, E_i^\dagger \qquad$ with $\qquad \sum_i E_i^\dagger E_i \sqsubseteq \mathbb{I}$

- *trace-preserving* if $\sum_i E_i^\dagger E_i = \mathbb{I}$: the set $\mathcal{SO}(\mathcal{H})$
- *trace non-increasing* in general: the set $\mathcal{SO}^{\leq}(\mathcal{H}) \supseteq \mathcal{SO}(\mathcal{H})$

Unitaries: $\{U\}$, i.e. $\rho \mapsto U\rho U^\dagger \quad$ (e.g. H, X, $CNOT$)

Noise: bit flip with probability p, i.e. $\{\sqrt{1-p}\,\mathbb{I}, \sqrt{p}\,X\}$

Reset: $Set_\sigma(\rho) = \mathsf{tr}(\rho)\,\sigma$

Local action on qubits $\tilde{q}$ of a bigger state: $\mathcal{E}^{\tilde{q}} = \mathcal{E} \otimes \mathbb{I}$ (up to reordering)

Measurements

A measurement is a set $\mathcal{M} = \{M_m\}_m$ with $\sum_m M_m^\dagger M_m = \mathbb{I}$

- outcome m with probability $p_m = \mathrm{tr}\left(M_m \rho M_m^\dagger\right)$
- the state collapses to $M_m \rho M_m^\dagger / p_m$

Measurements

A measurement is a set $\mathcal{M} = \{M_m\}_m$ with $\sum_m M_m^\dagger M_m = \mathbb{I}$

- outcome m with probability $p_m = \mathrm{tr}\left(M_m \rho M_m^\dagger\right)$
- the state collapses to $M_m \rho M_m^\dagger / p_m$

One object for both

Each $\mathcal{M}_m$, with $\mathcal{M}_m(\rho) = M_m \rho M_m^\dagger$, is a trace non-increasing superoperator: the trace conveys the probability, the density operator is the state

Measurements

A measurement is a set $\mathcal{M} = \{M_m\}_m$ with $\sum_m M_m^\dagger M_m = \mathbb{I}$

- outcome m with probability $p_m = \mathrm{tr}\left(M_m \rho M_m^\dagger\right)$
- the state collapses to $M_m \rho M_m^\dagger / p_m$

One object for both

Each $\mathcal{M}_m$, with $\mathcal{M}_m(\rho) = M_m \rho M_m^\dagger$, is a trace non-increasing superoperator: the trace conveys the probability, the density operator is the state

Example: $\mathcal{M}_{01} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on $|+\rangle\langle +|$

$$\mathcal{M}_0(|+\rangle\langle +|) = \tfrac{1}{2}|0\rangle\langle 0| \qquad \mathcal{M}_1(|+\rangle\langle +|) = \tfrac{1}{2}|1\rangle\langle 1|$$

We use $\mathcal{M}_{01}$, $\mathcal{M}_{\pm}$, $\mathcal{M}_{\pm i}$ (the three bases) and $\mathcal{M}_{\mathrm{bit}}$: a measurement on no qubits, i.e. a fair coin

2. Configuration Semantics

lqCCS

$$P ::= \mathbf{0}_{\tilde{e}} \mid \alpha.P \mid \textbf{if } e \textbf{ then } P \textbf{ else } P \mid P + P \mid P \parallel P \mid P \setminus c$$

$$\alpha ::= \tau \mid c?x \mid c!e \mid \mathcal{E}(\tilde{e}) \mid \mathcal{M}(\tilde{e} \triangleright x)$$

$\mathcal{E}$: any trace-preserving superoperator (unitaries, noise, resets, ...)

$\mathcal{M}(\tilde{e} \triangleright x)$: measure the qubits $\tilde{e}$, store the outcome in x

$\mathbf{0}_{\tilde{e}}$: terminate, *discarding* the qubits $\tilde{e}$ (they become unreachable)

lqCCS

$$P ::= \mathbf{0}_{\tilde{e}} \mid \alpha.P \mid \textbf{if } e \textbf{ then } P \textbf{ else } P \mid P + P \mid P \parallel P \mid P \setminus c$$

$$\alpha ::= \tau \mid c?x \mid c!e \mid \mathcal{E}(\tilde{e}) \mid \mathcal{M}(\tilde{e} \triangleright x)$$

$\mathcal{E}$: any trace-preserving superoperator (unitaries, noise, resets, ...)

$\mathcal{M}(\tilde{e} \triangleright x)$: measure the qubits $\tilde{e}$, store the outcome in x

$\mathbf{0}_{\tilde{e}}$: terminate, *discarding* the qubits $\tilde{e}$ (they become unreachable)

Linear typing $\Sigma \vdash P$

P owns exactly the qubits in Σ

- parallel processes own disjoint qubits (no-cloning)
- each qubit is sent or discarded

Configurations

A configuration $\langle \rho, P \rangle$ pairs

- a global quantum state $\rho \in \mathcal{DO}(\mathcal{H}_{\Sigma_\rho})$
- a well-typed process $\Sigma_P \vdash P$ with $\Sigma_P \subseteq \Sigma_\rho$

The qubits in $\Sigma_\rho \setminus \Sigma_P$ form the environment: not owned by P, available to the outside world

Configurations

A configuration $\langle \rho, P \rangle$ pairs

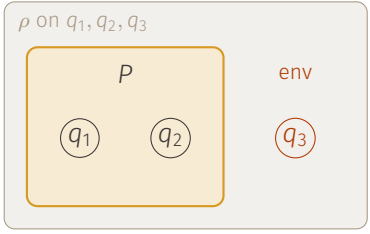
- a global quantum state $\rho \in \mathcal{DO}(\mathcal{H}_{\Sigma_\rho})$
- a well-typed process $\Sigma_P \vdash P$ with $\Sigma_P \subseteq \Sigma_\rho$

The qubits in $\Sigma_\rho \setminus \Sigma_P$ form the environment: not owned by P, available to the outside world

The semantics is a **probabilistic LTS**

$$\longrightarrow \subseteq \mathit{Conf} \times \mathit{Act} \times \mathcal{D}(\mathit{Conf})$$

with $\mathit{Act} \ni \tau, c!v, c?v$



Operational Semantics: Quantum and Communication

$$\frac{}{\langle \rho, \tau.\, P\rangle \xrightarrow{\tau} 1 \bullet \langle \rho, P\rangle}\ \textsc{Tau} \qquad \frac{}{\langle \rho, \mathcal{E}(\tilde{q}).\, P\rangle \xrightarrow{\tau} 1 \bullet \left\langle \mathcal{E}^{\tilde{q}}(\rho), P\right\rangle}\ \textsc{Sop}$$

$$\frac{}{\langle \rho, \mathcal{M}(\tilde{q} \rhd x).\, P\rangle \xrightarrow{\tau} \sum_m \mathrm{tr}\left(\mathcal{M}_m^{\tilde{q}}(\rho)\right) \bullet \left\langle \frac{\mathcal{M}_m^{\tilde{q}}(\rho)}{\mathrm{tr}\left(\mathcal{M}_m^{\tilde{q}}(\rho)\right)}, P[^m/_x]\right\rangle}\ \textsc{Meas}$$

$$\frac{e \Downarrow v}{\langle \rho, c!e.\, P\rangle \xrightarrow{c!v} 1 \bullet \langle \rho, P\rangle}\ \textsc{Send} \qquad \frac{c : \widehat{\mathcal{Q}} \Rightarrow v \in \Sigma_\rho \setminus \Sigma_P}{\langle \rho, c?x.\, P\rangle \xrightarrow{c?v} 1 \bullet \langle \rho, P[^v/_x]\rangle}\ \textsc{Recv}$$

Probabilities are the result of measurements

An open quantum reception must take a qubit from the environment

Operational Semantics: Choice and Parallelism

$$\frac{\langle \rho, P \rangle \xrightarrow{\mu} \Delta}{\langle \rho, P + Q \rangle \xrightarrow{\mu} \Delta} \textsc{SumL} \qquad \frac{e \Downarrow tt \quad \langle \rho, P \rangle \xrightarrow{\mu} \Delta}{\langle \rho, \textsf{if } e \textsf{ then } P \textsf{ else } Q \rangle \xrightarrow{\mu} \Delta} \textsc{IteT}$$

$$\frac{\langle \rho, P \rangle \xrightarrow{\mu} \Delta \quad \mu \notin \{c?v \mid v \in \Sigma_Q\}}{\langle \rho, P \parallel Q \rangle \xrightarrow{\mu} \Delta \parallel Q} \textsc{ParL} \qquad \frac{\langle \rho, P \rangle \xrightarrow{\mu} \Delta \quad \mu \notin \{c!v, c?v\}}{\langle \rho, P \setminus c \rangle \xrightarrow{\mu} \Delta \setminus c} \textsc{Restr}$$

$$\frac{\langle \rho, P \rangle \xrightarrow{c!v} 1 \bullet \langle \rho, P' \rangle \quad \langle \rho, Q \rangle \xrightarrow{c?v} 1 \bullet \langle \rho, Q' \rangle}{\langle \rho, P \parallel Q \rangle \xrightarrow{\tau} 1 \bullet \langle \rho, P' \parallel Q' \rangle} \textsc{SynchL}$$

$\Delta \parallel Q$ puts Q in parallel with every configuration in the support of Δ

Example: a Quantum Lottery

Initial state $|0\rangle\langle 0|$

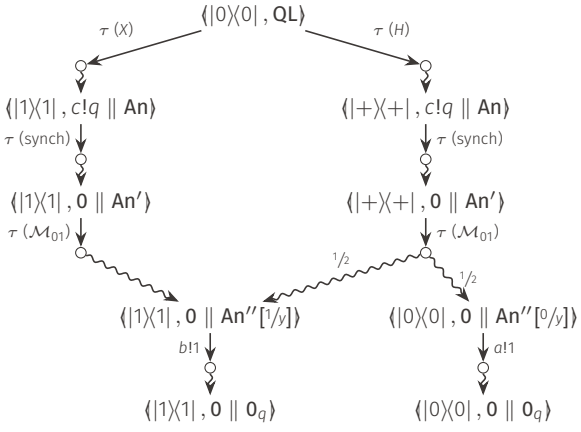
$$\mathsf{QL} = \mathsf{Pr} \parallel \mathsf{An}$$

$$\mathsf{Pr} = X(q).\, c!q.\, \mathbf{0} + H(q).\, c!q.\, \mathbf{0}$$

$$\mathsf{An} = c?x.\, \underbrace{\mathcal{M}_{01}(x \rhd y).\, \mathsf{An}''}_{\mathsf{An}'}$$

$$\mathsf{An}'' = \text{if } y = 0 \text{ then } a!1.\, \mathbf{0}_x \text{ else } b!1.\, \mathbf{0}_x$$

(moves of $c!q$ towards the environment are omitted)



3. Bisimulation in a Nutshell

Strong Bisimulation

Definition

A symmetric relation $\mathcal{R}$ on processes is a *bisimulation* if $P \mathcal{R} Q$ and $P \xrightarrow{\mu} P'$ imply $Q \xrightarrow{\mu} Q'$ for some Q' with $P' \mathcal{R} Q'$.
Bisimilarity $\sim$ is the largest bisimulation

A *coinductive* proof technique: exhibit a relation, check that it is closed under moves

It observes *when* choices are made, not only the traces

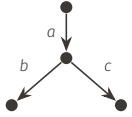
Strong Bisimulation

Definition

A symmetric relation $\mathcal{R}$ on processes is a *bisimulation* if $P \mathcal{R} Q$ and $P \xrightarrow{\mu} P'$ imply $Q \xrightarrow{\mu} Q'$ for some Q' with $P' \mathcal{R} Q'$.
Bisimilarity $\sim$ is the largest bisimulation

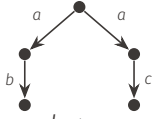
A *coinductive* proof technique: exhibit a relation, check that it is closed under moves

It observes *when* choices are made, not only the traces



$a.(b + c)$

$\not\sim$



$a.b + a.c$

Same traces, yet not bisimilar: on the right the choice is taken *before a*

Probabilistic Systems: Two Views

State-based

Relate configurations

$C \mathcal{R} D$ and $C \xrightarrow{\mu} \Delta$ imply $D \xrightarrow{\mu} \Theta$ with Δ and Θ related by the lifted relation

Distribution-based

Relate (sub)distributions of configurations

A distribution moves *as a whole*

Probabilistic Systems: Two Views

State-based

Relate configurations

$C \mathrel{\mathcal{R}} D$ and $C \xrightarrow{\mu} \Delta$ imply $D \xrightarrow{\mu} \Theta$ with Δ and Θ related by the lifted relation

Distribution-based

Relate (sub)distributions of configurations

A distribution moves *as a whole*

Quantum calculi need the second view: we want

$$\tfrac{1}{2} \cdot \langle |0\rangle\langle 0| , P\rangle \oplus \tfrac{1}{2} \cdot \langle |1\rangle\langle 1| , P\rangle \quad \text{equivalent to} \quad \tfrac{1}{2} \cdot \langle |+\rangle\langle +| , P\rangle \oplus \tfrac{1}{2} \cdot \langle |-\rangle\langle -| , P\rangle$$

although no configuration on the left matches any on the right

Lifting Transitions to Distributions

Subdistributions $\mathcal{D}^{\leq}(Conf)$: mass $|\Delta| = \sum_C \Delta(C) \leq 1$, with ϵ the empty one

Lifting

$$\frac{\forall i.\ C_i \xrightarrow{\mu} \Delta_i,\ \text{or } \Delta_i = \epsilon \text{ if } C_i \text{ cannot move with } \mu}{\sum_i p_i \cdot C_i \xrightarrow{\mu}_{\bullet} \sum_i p_i \cdot \Delta_i}$$

Every element moves with the same *label* μ

Elements that cannot do μ *vanish*: the mass drops

Each element picks its own transition, independently of the others

Lifting Transitions to Distributions

Subdistributions $\mathcal{D}^{\leq}(Conf)$: mass $|\Delta| = \sum_C \Delta(C) \leq 1$, with ϵ the empty one

Lifting

$$\frac{\forall i.\, C_i \xrightarrow{\mu} \Delta_i, \text{ or } \Delta_i = \epsilon \text{ if } C_i \text{ cannot move with } \mu}{\sum_i p_i \cdot C_i \overset{\mu}{\rightarrowtail}_{\bullet} \sum_i p_i \cdot \Delta_i}$$

Every element moves with the same *label* μ

Elements that cannot do μ *vanish*: the mass drops

Each element picks its own transition, independently of the others

$$\frac{1}{2} \cdot \langle |0\rangle\langle 0|, a!1\rangle \oplus \frac{1}{2} \cdot \langle |1\rangle\langle 1|, b!1\rangle \overset{a!1}{\rightarrowtail}_{\bullet} \frac{1}{2} \cdot \langle |0\rangle\langle 0|, \mathbf{0}\rangle$$

Saturated Bisimilarity: Let the Observers Decide

What should be observable in a quantum system?

Saturated Bisimilarity: Let the Observers Decide

What should be observable in a quantum system? **Let other processes find out!**

- the only primitive observation: the *mass* of a distribution
- everything else is probed by *contexts* $B[\cdot] ::= [\cdot] \mid [\cdot] \parallel R$ (typed: R may own environment qubits)

Saturated Bisimilarity: Let the Observers Decide

What should be observable in a quantum system? **Let other processes find out!**

- the only primitive observation: the *mass* of a distribution
- everything else is probed by *contexts* $B[\cdot] ::= [\cdot] \mid [\cdot] \parallel R$ (typed: R may own environment qubits)

Unscheduled saturated bisimilarity $\simeq_\bullet$

A well-typed relation $\mathcal{R}$ on subdistributions is a *saturated bisimulation* if $\Delta\ \mathcal{R}\ \Theta$ implies $|\Delta| = |\Theta|$ and, for every context $B[\cdot]$,

- $B[\Delta] \overset{\tau}{\rightarrowtail}_\bullet \Delta'$ implies $B[\Theta] \overset{\tau}{\rightarrowtail}_\bullet \Theta'$ for some Θ' with $\Delta'\ \mathcal{R}\ \Theta'$
- and symmetrically

Closed under parallel contexts by construction

4. When Bisimilarity Fails Physics

The Qubit Sources, Again

Two fair sources, sending one qubit on channel c

$$\Delta_{01} = \tfrac{1}{2} \cdot \langle |0\rangle\langle 0| \, , c!q \rangle \oplus \tfrac{1}{2} \cdot \langle |1\rangle\langle 1| \, , c!q \rangle \qquad \Delta_{\pm} = \tfrac{1}{2} \cdot \langle |+\rangle\langle +| \, , c!q \rangle \oplus \tfrac{1}{2} \cdot \langle |-\rangle\langle -| \, , c!q \rangle$$

Quantum theory: both send $\frac{1}{2}\mathbb{I}$, so Δ_{01} and $\Delta_{\pm}$ **must** be equivalent

The Qubit Sources, Again

Two fair sources, sending one qubit on channel c

$$\Delta_{01} = \tfrac{1}{2} \cdot \langle |0\rangle\langle 0| , c!q \rangle \oplus \tfrac{1}{2} \cdot \langle |1\rangle\langle 1| , c!q \rangle \qquad \Delta_{\pm} = \tfrac{1}{2} \cdot \langle |+\rangle\langle +| , c!q \rangle \oplus \tfrac{1}{2} \cdot \langle |-\rangle\langle -| , c!q \rangle$$

Quantum theory: both send $\frac{1}{2}\mathbb{I}$, so Δ_{01} and $\Delta_{\pm}$ **must** be equivalent

The observer

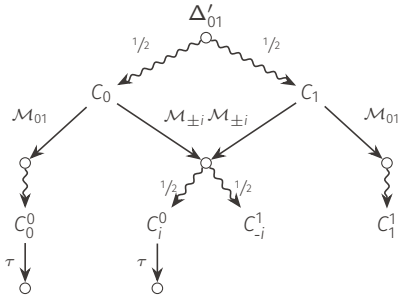
$$B[\cdot] = [\cdot] \parallel c?x.\,(P + Q) \qquad \begin{array}{l} P = \mathcal{M}_{01}(x \rhd y).\,R \\ Q = \mathcal{M}_{\pm i}(x \rhd y).\,R \end{array} \qquad R = (\textsf{if } y = 0 \textsf{ then } \tau \textsf{ else } \mathbf{0}) \parallel \mathbf{0}_x$$

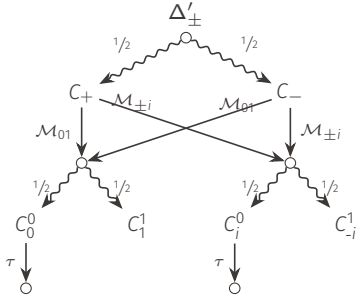
Receives the qubit, then chooses *one* of two measurements

R performs a last τ only if $y = 0$: the final mass changes according to y

Mixing Choices Across the Distribution

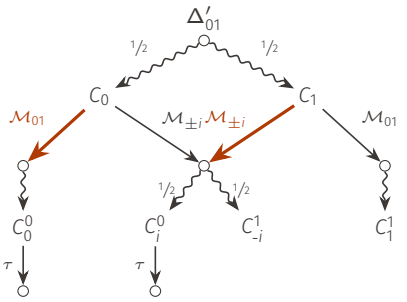
After the synchronisation, $\Delta'_{01} = \frac{1}{2} \cdot C_0 \oplus \frac{1}{2} \cdot C_1$ and $\Delta'_{\pm} = \frac{1}{2} \cdot C_+ \oplus \frac{1}{2} \cdot C_-$, with $C_\psi = \langle |\psi\rangle\langle\psi| \, , P + Q \rangle$ and $C^n_\psi = \langle |\psi\rangle\langle\psi| \, , R[^n/_y] \rangle$

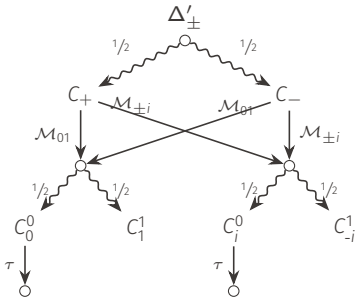




Mixing Choices Across the Distribution

After the synchronisation, $\Delta'_{01} = \frac{1}{2} \cdot C_0 \oplus \frac{1}{2} \cdot C_1$ and $\Delta'_{\pm} = \frac{1}{2} \cdot C_+ \oplus \frac{1}{2} \cdot C_-$, with $C_\psi = \langle |\psi\rangle\langle\psi| \, , P + Q \rangle$ and $C^n_\psi = \langle |\psi\rangle\langle\psi| \, , R[^n/_y] \rangle$

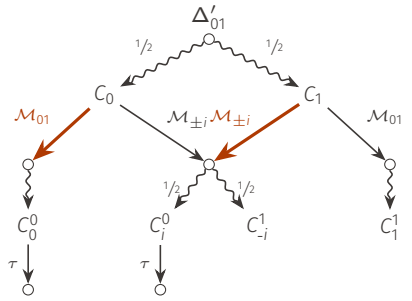


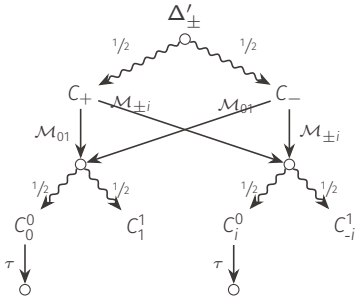


Δ'_{01} picks $\mathcal{M}_{01}$ on C_0 and $\mathcal{M}_{\pm i}$ on C_1: final mass $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$

Mixing Choices Across the Distribution

After the synchronisation, $\Delta'_{01} = \frac{1}{2} \cdot C_0 \oplus \frac{1}{2} \cdot C_1$ and $\Delta'_{\pm} = \frac{1}{2} \cdot C_+ \oplus \frac{1}{2} \cdot C_-$, with $C_\psi = \langle |\psi\rangle\langle\psi| \,, P + Q \rangle$ and $C^n_\psi = \langle |\psi\rangle\langle\psi| \,, R[^n/_y] \rangle$





Δ'_{01} picks $\mathcal{M}_{01}$ on C_0 and $\mathcal{M}_{\pm i}$ on C_1: final mass $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$

$\Delta'_{\pm}$: *every* combination of choices gives final mass $\frac{1}{2}$ $\Rightarrow$ $\Delta_{01} \not\sim_\bullet \Delta_{\pm}$

Choosing $\mathcal{M}_{01}$ on $|0\rangle$ and $\mathcal{M}_{\pm i}$ on $|1\rangle$
means *knowing* the state of the qubit
without measuring it

Is it the Observer's Fault?

Yesterday the culprit was the non-deterministic *test*. Now a physical scenario: Alice and Bob share $|\Phi^+\rangle$ on q_1, q_2, then move apart

$$\mathsf{A}_{01} = \mathcal{M}_{01}(q_1 \rhd x).\,\mathbf{0}_{q_1} \qquad \mathsf{A}_{\pm} = \mathcal{M}_{\pm}(q_1 \rhd x).\,\mathbf{0}_{q_1}$$
$$\mathsf{B} = \left(\mathcal{M}_{01}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right) + \left(\mathcal{M}_{\pm i}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right)$$

Is it the Observer's Fault?

Yesterday the culprit was the non-deterministic *test*. Now a physical scenario: Alice and Bob share $|\Phi^+\rangle$ on q_1, q_2, then move apart

$$\mathsf{A}_{01} = \mathcal{M}_{01}(q_1 \rhd x).\,\mathbf{0}_{q_1} \qquad \mathsf{A}_{\pm} = \mathcal{M}_{\pm}(q_1 \rhd x).\,\mathbf{0}_{q_1}$$
$$\mathsf{B} = \left(\mathcal{M}_{01}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right) + \left(\mathcal{M}_{\pm i}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right)$$

No-signalling

Bob's statistics cannot depend on Alice's basis, otherwise she could send a bit *faster than light*. We expect $\langle |\Phi^+\rangle\langle\Phi^+|\,, \mathsf{A}_{01} \parallel \mathsf{B}\rangle \simeq_\bullet \langle |\Phi^+\rangle\langle\Phi^+|\,, \mathsf{A}_{\pm} \parallel \mathsf{B}\rangle$

Is it the Observer's Fault?

Yesterday the culprit was the non-deterministic *test*. Now a physical scenario: Alice and Bob share $|\Phi^+\rangle$ on q_1, q_2, then move apart

$$\mathsf{A}_{01} = \mathcal{M}_{01}(q_1 \rhd x).\,\mathbf{0}_{q_1} \qquad \mathsf{A}_{\pm} = \mathcal{M}_{\pm}(q_1 \rhd x).\,\mathbf{0}_{q_1}$$
$$\mathsf{B} = \left(\mathcal{M}_{01}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right) + \left(\mathcal{M}_{\pm i}(q_2 \rhd y).\,c!y.\,\mathbf{0}_{q_2}\right)$$

No-signalling

Bob's statistics cannot depend on Alice's basis, otherwise she could send a bit *faster than light*. We expect $\langle |\Phi^+\rangle\langle\Phi^+|\,, \mathsf{A}_{01} \parallel \mathsf{B}\rangle \simeq_\bullet \langle |\Phi^+\rangle\langle\Phi^+|\,, \mathsf{A}_{\pm} \parallel \mathsf{B}\rangle$

Note: the non-determinism is now *inside the system*, not in the observer

Faster than Light

After Alice measures

$$\Delta = \tfrac{1}{2} \cdot \langle |00\rangle\langle 00| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \tfrac{1}{2} \cdot \langle |11\rangle\langle 11| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$

$$\Theta = \tfrac{1}{2} \cdot \langle |{+}{+}\rangle\langle {+}{+}| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \tfrac{1}{2} \cdot \langle |{-}{-}\rangle\langle {-}{-}| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$

Faster than Light

After Alice measures

$$\Delta = \frac{1}{2} \cdot \langle |00\rangle\langle 00| \, , \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \frac{1}{2} \cdot \langle |11\rangle\langle 11| \, , \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$
$$\Theta = \frac{1}{2} \cdot \langle |{+}{+}\rangle\langle {+}{+}| \, , \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \frac{1}{2} \cdot \langle |{-}{-}\rangle\langle {-}{-}| \, , \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$

In Δ, Bob picks $\mathcal{M}_{01}$ on the $|00\rangle\langle 00|$ element and $\mathcal{M}_{\pm i}$ on the $|11\rangle\langle 11|$ element: he sends 0 with probability $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$

In Θ, every combination sends 0 with probability $\frac{1}{2}$

Faster than Light

After Alice measures

$$\Delta = \tfrac{1}{2} \cdot \langle |00\rangle\langle 00| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \tfrac{1}{2} \cdot \langle |11\rangle\langle 11| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$
$$\Theta = \tfrac{1}{2} \cdot \langle |{+}{+}\rangle\langle {+}{+}| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle \oplus \tfrac{1}{2} \cdot \langle |{-}{-}\rangle\langle {-}{-}| \,, \mathbf{0}_{q_1} \parallel \mathrm{B} \rangle$$

In Δ, Bob picks $\mathcal{M}_{01}$ on the $|00\rangle\langle 00|$ element and $\mathcal{M}_{\pm i}$ on the $|11\rangle\langle 11|$ element: he sends 0 with probability $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$

In Θ, every combination sends 0 with probability $\frac{1}{2}$

A *deterministic* observer suffices

$$B[\cdot] = [\cdot] \parallel c?z.\, \textbf{if } z = 0 \textbf{ then } \tau \textbf{ else } \mathbf{0} \qquad \text{final mass } \tfrac{3}{4} \text{ vs } \tfrac{1}{2}$$

$\simeq_\bullet$ lets Bob read Alice's basis instantaneously

Diagnosis

The culprit: non-determinism resolved separately for each element of a distribution, i.e. *depending on the unknown quantum state*

Diagnosis

The culprit: non-determinism resolved separately for each element of a distribution, i.e. *depending on the unknown quantum state*

It shows up in observers (qubit sources) *and* inside systems (faster than light)

Diagnosis

The culprit: non-determinism resolved separately for each element of a distribution, i.e. *depending on the unknown quantum state*

It shows up in observers (qubit sources) *and* inside systems (faster than light)

Restricting the observers only (e.g. deterministic tests) is not enough

Moreover, treating observers differently from processes breaks compositionality: an observer composed in parallel *becomes* part of a system

Diagnosis

The culprit: non-determinism resolved separately for each element of a distribution, i.e. *depending on the unknown quantum state*

It shows up in observers (qubit sources) *and* inside systems (faster than light)

Restricting the observers only (e.g. deterministic tests) is not enough

Moreover, treating observers differently from processes breaks compositionality: an observer composed in parallel *becomes* part of a system

We need one discipline for *all* non-deterministic choices

Diagnosis

The culprit: non-determinism resolved separately for each element of a distribution, i.e. *depending on the unknown quantum state*

It shows up in observers (qubit sources) *and* inside systems (faster than light)

Restricting the observers only (e.g. deterministic tests) is not enough

Moreover, treating observers differently from processes breaks compositionality: an observer composed in parallel *becomes* part of a system

We need one discipline for *all* non-deterministic choices

Schedulers

5. Schedulers via Tags

Admissible Schedulers

Probabilistic security had the same problem (Chatzikokolakis & Palamidessi, 2007)

A scheduler resolving non-determinism can *see* secret data and leak it for free

Solution: *name* the choices syntactically; the scheduler picks names, not states

Admissible Schedulers

Probabilistic security had the same problem (Chatzikokolakis & Palamidessi, 2007)

A scheduler resolving non-determinism can *see* secret data and leak it for free

Solution: *name* the choices syntactically; the scheduler picks names, not states

For lqCCS, the “secret” is the quantum state

- every non-deterministic choice carries a **tag**
- a **scheduler** selects a tag, using only classical, syntactic information
- all the elements of a distribution must follow the *same* scheduler

Tagged lqCCS

$$\alpha ::= t{:}\,\tau \mid (t, t'){:}\,\tau \mid t{:}\,c?x \mid t{:}\,c!e \mid t{:}\,\mathcal{E}(\tilde{e}) \mid t{:}\,\mathcal{M}(\tilde{e} \rhd x) \qquad s ::= t \mid (t, t')$$

The pLTS becomes $\longrightarrow \subseteq \mathit{Conf} \times \mathit{Act} \times \mathit{Sched} \times \mathcal{D}(\mathit{Conf})$, written $\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta$

Tagged lqCCS

$$\alpha ::= t{:}\,\tau \mid (t,t'){:}\,\tau \mid t{:}\,c?x \mid t{:}\,c!e \mid t{:}\,\mathcal{E}(\tilde{e}) \mid t{:}\,\mathcal{M}(\tilde{e} \rhd x) \qquad s ::= t \mid (t,t')$$

The pLTS becomes $\longrightarrow \subseteq \mathit{Conf} \times \mathit{Act} \times \mathit{Sched} \times \mathcal{D}(\mathit{Conf})$, written $\langle \rho, P\rangle \xrightarrow{\mu}_s \Delta$

$$\frac{}{\langle \rho, t{:}\,\mathcal{M}(\tilde{q} \rhd x).\, P\rangle \xrightarrow{\tau}_t \sum_m \mathrm{tr}\left(\mathcal{M}^{\tilde{q}}_m(\rho)\right) \cdot \left\langle \frac{\mathcal{M}^{\tilde{q}}_m(\rho)}{\mathrm{tr}\left(\mathcal{M}^{\tilde{q}}_m(\rho)\right)}, P[^m/_x] \right\rangle}\ \textsc{Meas} \qquad \frac{\langle \rho, P\rangle \xrightarrow{\mu}_s \Delta}{\langle \rho, P + Q\rangle \xrightarrow{\mu}_s \Delta}\ \textsc{SumL}$$

$$\frac{\langle \rho, P\rangle \xrightarrow{c!v}_t 1 \cdot \langle \rho, P'\rangle \quad \langle \rho, Q\rangle \xrightarrow{c?v}_{t'} 1 \cdot \langle \rho, Q'\rangle}{\langle \rho, P \parallel Q\rangle \xrightarrow{\tau}_{(t,t')} 1 \cdot \langle \rho, P' \parallel Q'\rangle}\ \textsc{SynchL} \qquad \frac{\langle \rho, P\rangle \xrightarrow{\mu}_s \Delta \quad \cdots}{\langle \rho, P \parallel Q\rangle \xrightarrow{\mu}_s \Delta \parallel Q}\ \textsc{ParL}$$

The other rules just carry the tag along

Deterministic Tagging

Deterministic process

For every state and scheduler s, there is at most one transition $\xrightarrow{\mu}_s$, except for inputs: $\xrightarrow{c?v}_s$ for every value v the environment may send

- *internal* non-determinism ($+$, interleaving) is resolved by the scheduler
- *external* non-determinism (which value arrives) is left to the environment
- **Assumption**: all processes are deterministically tagged

Deterministic Tagging

Deterministic process

For every state and scheduler s, there is at most one transition $\xrightarrow{\mu}_s$, except for inputs: $\xrightarrow{c?v}_s$ for every value v the environment may send

- *internal* non-determinism ($+$, interleaving) is resolved by the scheduler
- *external* non-determinism (which value arrives) is left to the environment
- **Assumption**: all processes are deterministically tagged

$t_1 : a!0 + t_2 : a!1$	✓ the scheduler picks the branch
$t_1 : a!0 + t_1 : a!1$	✗ two different moves with the same name
$t : c?x.\, P$	✓ one move per received value
if $y = 0$ **then** $t_5 : a!1$ **else** $t_5 : b!1$	✓ branches decided by classical data

Scheduled Lifting

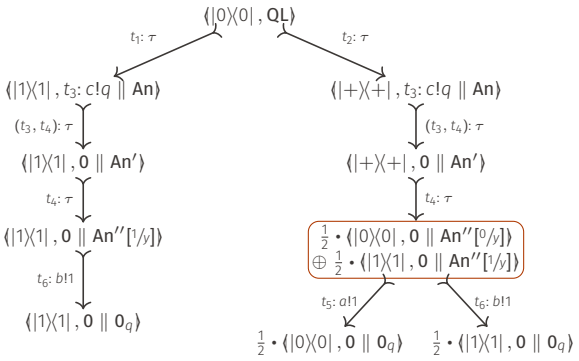
Every element of the distribution follows the same scheduler

Scheduled lifting

$$\frac{\forall i.\, C_i \xrightarrow{\mu}_s \Delta_i, \text{ or } \Delta_i = \epsilon \text{ if } C_i \text{ has no such move}}{\sum_i p_i \bullet C_i \;\rightarrowtail^{\mu}_s\; \sum_i p_i \bullet \Delta_i}$$

The Quantum Lottery, Tagged and Lifted

$$\begin{aligned}
\mathsf{Pr} &= t_1\colon X(q).\, t_3\colon c!q \\
&\quad + t_2\colon H(q).\, t_3\colon c!q \\
\mathsf{An} &= t_4\colon c?x.\, t_4\colon \mathcal{M}_{01}(x \rhd y).\, \mathsf{An}'' \\
\mathsf{An}'' &= \mathsf{if}\ y = 0 \\
&\quad \mathsf{then}\ t_5\colon a!1.\, \mathbf{0}_x \\
&\quad \mathsf{else}\ t_6\colon b!1.\, \mathbf{0}_x
\end{aligned}$$



A distribution is now a *state* of an LTS: with t_5 only the $|0\rangle$ element moves; the other vanishes (mass $\frac{1}{2}$)

Contexts Must Play by the Rules Too

Compatible context

$B[\cdot] = [\cdot] \parallel R$ is compatible with Δ if

- the types match: R only owns qubits of the environment of Δ
- R uses *fresh* tags: $Tag(R) \cap Tag(\Delta) = \emptyset$

Contexts Must Play by the Rules Too

Compatible context

$B[\cdot] = [\cdot] \parallel R$ is compatible with Δ if

- the types match: R only owns qubits of the environment of Δ
- R uses *fresh* tags: $Tag(R) \cap Tag(\Delta) = \emptyset$

Fresh tags preserve determinism: if P and R are deterministic with disjoint tags, then $P \parallel R$ is deterministic

Contexts and processes obey *the same* scheduler discipline

A context put in parallel is just another component of the system

6. Scheduled Bisimilarity

Scheduled Saturated Bisimilarity

Definition

A well-typed relation $\mathcal{R}$ on subdistributions is a *scheduled saturated bisimulation* if $\Delta\ \mathcal{R}\ \Theta$ implies $|\Delta| = |\Theta|$ and, for every compatible context $B[\cdot]$ and every scheduler s,

- $B[\Delta] \overset{\tau}{\rightarrowtail}_s \Delta'$ implies $B[\Theta] \overset{\tau}{\rightarrowtail}_s \Theta'$ for some Θ' with $\Delta'\ \mathcal{R}\ \Theta'$
- and symmetrically

$\simeq$ is the largest scheduled saturated bisimulation

Scheduled Saturated Bisimilarity

Definition

A well-typed relation $\mathcal{R}$ on subdistributions is a *scheduled saturated bisimulation* if $\Delta\ \mathcal{R}\ \Theta$ implies $|\Delta| = |\Theta|$ and, for every compatible context $B[\cdot]$ and every scheduler s,

- $B[\Delta] \overset{\tau}{\rightarrowtail}_s \Delta'$ implies $B[\Theta] \overset{\tau}{\rightarrowtail}_s \Theta'$ for some Θ' with $\Delta'\ \mathcal{R}\ \Theta'$
- and symmetrically

$\simeq$ is the largest scheduled saturated bisimulation

Same shape as before: only the transitions have changed

The move with scheduler s must be matched *by the same* s (more on this later)

Still closed under parallel contexts by construction

The Qubit Sources, Fixed

The observer, now tagged, with $R = (\textbf{if } y = 0 \textbf{ then } t_4{:}\,\tau \textbf{ else } 0) \parallel \mathbf{0}_x$

$$B[\cdot] = [\cdot] \parallel t_1{:}\, c?x.\, \left(t_2{:}\, \mathcal{M}_{01}(x \rhd y).\, R + t_3{:}\, \mathcal{M}_{\pm i}(x \rhd y).\, R\right)$$

The Qubit Sources, Fixed

The observer, now tagged, with $R = (\textbf{if } y = 0 \textbf{ then } t_4{:}\,\tau \textbf{ else } 0) \parallel \mathbf{0}_x$

$$B[\cdot] = [\cdot] \parallel t_1{:}\, c?x.\, \big(t_2{:}\, \mathcal{M}_{01}(x \rhd y).\, R + t_3{:}\, \mathcal{M}_{\pm i}(x \rhd y).\, R\big)$$

After the synchronisation, the *whole* distribution follows t_2 or t_3

scheduler	Δ'_{01} (final mass)	$\Delta'_{\pm}$ (final mass)
t_2 $(\mathcal{M}_{01})$	$\frac{1}{2}$	$\frac{1}{2}$
t_3 $(\mathcal{M}_{\pm i})$	$\frac{1}{2}$	$\frac{1}{2}$

The Qubit Sources, Fixed

The observer, now tagged, with $R = (\textbf{if } y = 0 \textbf{ then } t_4{:}\,\tau \textbf{ else } 0) \parallel \mathbf{0}_x$

$$B[\cdot] = [\cdot] \parallel t_1{:}\, c?x.\, \big(t_2{:}\, \mathcal{M}_{01}(x \rhd y).\, R + t_3{:}\, \mathcal{M}_{\pm i}(x \rhd y).\, R\big)$$

After the synchronisation, the *whole* distribution follows t_2 or t_3

scheduler	Δ'_{01} (final mass)	$\Delta'_{\pm}$ (final mass)
t_2 $(\mathcal{M}_{01})$	$\frac{1}{2}$	$\frac{1}{2}$
t_3 $(\mathcal{M}_{\pm i})$	$\frac{1}{2}$	$\frac{1}{2}$

In fact, tagging the sources with t_0, $\Delta_{01} \;\simeq\; 1 \bullet \big\langle \frac{1}{2}\mathbb{I}, t_0{:}\, c!q \big\rangle \;\simeq\; \Delta_{\pm}$

Lifting Quantum Indistinguishability

Theorem

If $\sum_i p_i \cdot \rho_i = \sum_j q_j \cdot \sigma_j$ then $\sum_i p_i \bullet \langle \rho_i, P \rangle \simeq \sum_j q_j \bullet \langle \sigma_j, P \rangle$

The same process on indistinguishable mixtures is indistinguishable

Two ingredients: *linearity* of superoperators and measurements, and *schedulers*, which forbid per-element choices

Fails for $\simeq_\bullet$: the qubit sources are a counterexample

Lifting Quantum Indistinguishability

Theorem

If $\sum_i p_i \cdot \rho_i = \sum_j q_j \cdot \sigma_j$ then $\sum_i p_i \bullet \langle \rho_i, P \rangle \simeq \sum_j q_j \bullet \langle \sigma_j, P \rangle$

The same process on indistinguishable mixtures is indistinguishable

Two ingredients: *linearity* of superoperators and measurements, and *schedulers*, which forbid per-element choices

Fails for $\simeq_\bullet$: the qubit sources are a counterexample

Theorem (linearity)

If $\Delta_i \simeq \Theta_i$ for all i, then $\sum_i p_i \bullet \Delta_i \simeq \sum_i p_i \bullet \Theta_i$

No Signalling, Restored

Tags: Alice $t_0 : \mathcal{M}(q_1 \triangleright x)$, Bob $t_1 : \mathcal{M}_{01}(q_2 \triangleright y) \ldots + t_2 : \mathcal{M}_{\pm i}(q_2 \triangleright y) \ldots$. Probability that Bob sends 0:

schedulers		$\mathsf{A}_{01} \parallel \mathsf{B}$	$\mathsf{A}_{\pm} \parallel \mathsf{B}$
t_0 then t_1	(Alice, then Bob $\mathcal{M}_{01}$)	$\frac{1}{2}$	$\frac{1}{2}$
t_0 then t_2	(Alice, then Bob $\mathcal{M}_{\pm i}$)	$\frac{1}{2}$	$\frac{1}{2}$
t_1 then t_0	(Bob $\mathcal{M}_{01}$, then Alice)	$\frac{1}{2}$	$\frac{1}{2}$
t_2 then t_0	(Bob $\mathcal{M}_{\pm i}$, then Alice)	$\frac{1}{2}$	$\frac{1}{2}$

Bob can no longer choose his basis per element: the $\frac{3}{4}$ strategy is gone, and

$$\left\langle \left| \Phi^+ \right\rangle\!\left\langle \Phi^+ \right| , \mathsf{A}_{01} \parallel \mathsf{B} \right\rangle \simeq \left\langle \left| \Phi^+ \right\rangle\!\left\langle \Phi^+ \right| , \mathsf{A}_{\pm} \parallel \mathsf{B} \right\rangle$$

Where We Stand

$\simeq$ is the right notion

- ✓ respects quantum indistinguishability
- ✓ respects no-signalling
- ✓ linear
- ✓ closed under parallel composition
- ✓ intuitive: no observer can tell the difference

but hard to use

- ✗ quantifies over *all* contexts
- ✗ proofs by hand are painful
- ✗ no direct algorithm

Where We Want to Stand

The classical recipe:

1. find the *atomic* observations a context can make
2. define a *labelled* bisimilarity on them
3. prove that the two coincide

7. Quantum Distributions

Weights Beyond Probabilities

Probabilities: $\langle [0,1], 0, + \rangle$, a *partial* commutative monoid (sum defined if ≤ 1)

$$\Delta \in \mathcal{D}^{\leq}(S) \quad \text{a finite map } S \to [0,1] \text{ with } \sum_s \Delta(s) \leq 1$$

Weights Beyond Probabilities

Probabilities: $\langle [0,1], 0, + \rangle$, a *partial* commutative monoid (sum defined if ≤ 1)

$$\Delta \in \mathcal{D}^{\leq}(S) \quad \text{a finite map } S \to [0,1] \text{ with } \textstyle\sum_s \Delta(s) \leq 1$$

Partial density operators: $\langle \mathcal{DO}^{\leq}(\mathcal{H}), \mathbb{O}, + \rangle$, also a partial commutative monoid (sum defined if trace ≤ 1)

Quantum distribution

$$\mathcal{Q}_\Sigma(S) = \left\{ \mathfrak{D} : S \to \mathcal{DO}^{\leq}(\mathcal{H}_\Sigma) \;\middle|\; \lceil \mathfrak{D} \rceil \text{ finite and } \textstyle\sum_s \mathrm{tr}(\mathfrak{D}(s)) \leq 1 \right\}$$

Same notation: $\rho \bullet s$, $\oplus$, ϵ

$\mathcal{Q}_\emptyset(S) \cong \mathcal{D}^{\leq}(S)$: 1×1 density operators *are* probabilities

Quantum Distributions of Processes

States are now $\mathfrak{D} \in \mathcal{Q}_\Sigma(Proc)$: the weight of P carries *both* the quantum state and its probability

$$\sum_i p_i \bullet \langle \rho_i, P_i \rangle \quad \rightsquigarrow \quad \sum_i p_i \, \rho_i \bullet P_i$$

Quantum Distributions of Processes

States are now $\mathfrak{D} \in \mathcal{Q}_\Sigma(Proc)$: the weight of P carries *both* the quantum state and its probability

$$\sum_i p_i \bullet \langle \rho_i, P_i \rangle \quad \rightsquigarrow \quad \sum_i p_i \, \rho_i \bullet P_i$$

Elements with the same process merge by summing their weights

$$\tfrac{1}{2} |0\rangle\langle 0| \bullet P \oplus \tfrac{1}{2} |1\rangle\langle 1| \bullet P \;=\; \tfrac{1}{2}\mathbb{I} \bullet P \;=\; \tfrac{1}{2} |+\rangle\langle +| \bullet P \oplus \tfrac{1}{2} |-\rangle\langle -| \bullet P$$

Quantum Distributions of Processes

States are now $\mathfrak{D} \in \mathcal{Q}_\Sigma(Proc)$: the weight of P carries *both* the quantum state and its probability

$$\sum_i p_i \cdot \langle \rho_i, P_i \rangle \quad \rightsquigarrow \quad \sum_i p_i \, \rho_i \cdot P_i$$

Elements with the same process merge by summing their weights

$$\tfrac{1}{2} |0\rangle\langle 0| \cdot P \oplus \tfrac{1}{2} |1\rangle\langle 1| \cdot P \;=\; \tfrac{1}{2}\mathbb{I} \cdot P \;=\; \tfrac{1}{2} |+\rangle\langle +| \cdot P \oplus \tfrac{1}{2} |-\rangle\langle -| \cdot P$$

Indistinguishable mixtures are equal by construction

Quantum Distribution Semantics

$$\frac{}{\rho \bullet t\colon \mathcal{E}(\tilde{q}).\, P \xrightarrow{\tau}\!\!\gg_t \mathcal{E}^{\tilde{q}}(\rho) \bullet P}\ \textsc{Sop} \qquad \frac{}{\rho \bullet t\colon \mathcal{M}(\tilde{q} \rhd x).\, P \xrightarrow{\tau}\!\!\gg_t \sum_m \mathcal{M}_m^{\tilde{q}}(\rho) \bullet P[^m/_x]}\ \textsc{Meas}$$

$$\frac{\mathfrak{D} \xrightarrow{\mu}\!\!\gg_s \mathfrak{D}'}{\mathfrak{D} \rightarrowtail^{\mu}\!\!\gg_s \mathfrak{D}'}\ \textsc{Id} \qquad \frac{\mathfrak{D} \text{ has no } \xrightarrow{\mu}\!\!\gg_s}{\mathfrak{D} \rightarrowtail^{\mu}\!\!\gg_s \epsilon}\ \textsc{Not} \qquad \frac{\mathfrak{D} \rightarrowtail^{\mu}\!\!\gg_s \mathfrak{D}' \quad \mathfrak{T} \rightarrowtail^{\mu}\!\!\gg_s \mathfrak{T}'}{\mathfrak{D} \oplus \mathfrak{T} \rightarrowtail^{\mu}\!\!\gg_s \mathfrak{D}' \oplus \mathfrak{T}'}\ \textsc{Conv}$$

- the other rules mirror the configuration semantics
- Meas: no normalisation, the unnormalised branch is the weight
- Conv: the components move *together*, with the same s and μ

Quantum Distribution Semantics

$$\frac{}{\rho \bullet t\colon \mathcal{E}(\tilde{q}).\, P \xrightarrow{\tau}\!\!\!\!\rightarrow_t \mathcal{E}^{\tilde{q}}(\rho) \bullet P}\ \textsc{Sop} \qquad \frac{}{\rho \bullet t\colon \mathcal{M}(\tilde{q} \rhd x).\, P \xrightarrow{\tau}\!\!\!\!\rightarrow_t \sum_m \mathcal{M}_m^{\tilde{q}}(\rho) \bullet P[^m/_x]}\ \textsc{Meas}$$

$$\frac{\mathfrak{D} \xrightarrow{\mu}\!\!\!\!\rightarrow_s \mathfrak{D}'}{\mathfrak{D} \succ\!\!\succ^{\mu}\!\!\!\!\rightarrow_s \mathfrak{D}'}\ \textsc{Id} \qquad \frac{\mathfrak{D} \text{ has no } \xrightarrow{\mu}\!\!\!\!\rightarrow_s}{\mathfrak{D} \succ\!\!\succ^{\mu}\!\!\!\!\rightarrow_s \epsilon}\ \textsc{Not} \qquad \frac{\mathfrak{D} \succ\!\!\succ^{\mu}\!\!\!\!\rightarrow_s \mathfrak{D}' \quad \mathfrak{T} \succ\!\!\succ^{\mu}\!\!\!\!\rightarrow_s \mathfrak{T}'}{\mathfrak{D} \oplus \mathfrak{T} \succ\!\!\succ^{\mu}\!\!\!\!\rightarrow_s \mathfrak{D}' \oplus \mathfrak{T}'}\ \textsc{Conv}$$

- the other rules mirror the configuration semantics
- Meas: no normalisation, the unnormalised branch is the weight
- Conv: the components move *together*, with the same s and μ

Example: $P = t_0\colon \mathcal{M}_{01}(q \rhd x).\, t_0\colon c!q$

$$|+\rangle\langle+| \bullet P \succ\!\!\succ^{\tau}\!\!\!\!\rightarrow_{t_0} \tfrac{1}{2}\,|0\rangle\langle 0| \bullet t_0\colon c!q \oplus \tfrac{1}{2}\,|1\rangle\langle 1| \bullet t_0\colon c!q = \tfrac{1}{2}\mathbb{I} \bullet t_0\colon c!q \succ\!\!\succ^{c!q}\!\!\!\!\rightarrow_{t_0} \tfrac{1}{2}\mathbb{I} \bullet \mathbf{0}$$

8. Labelled Bisimilarity

What Can a Context See Right Away?

The mass of $\mathfrak{D}$ is now a density operator: $|\mathfrak{D}| = \sum_P \mathfrak{D}(P)$

What Can a Context See Right Away?

The mass of $\mathfrak{D}$ is now a density operator: $|\mathfrak{D}| = \sum_P \mathfrak{D}(P)$

Environment

If $\mathfrak{D}$ has type (Σ, Σ') (processes own Σ'), its environment is

$$env(\mathfrak{D}) = \mathrm{tr}_{\Sigma'}\left(\,|\mathfrak{D}|\,\right)$$

the state of the qubits that *no process owns*

A context can measure environment qubits immediately: bisimilar distributions need the same environment

No environment qubits: $env(\mathfrak{D})$ is a number, the probability mass, as before

What Can a Context See Right Away?

The mass of $\mathfrak{D}$ is now a density operator: $|\mathfrak{D}| = \sum_P \mathfrak{D}(P)$

Environment

If $\mathfrak{D}$ has type (Σ, Σ') (processes own Σ'), its environment is

$$env(\mathfrak{D}) = \mathrm{tr}_{\Sigma'}\left(\,|\mathfrak{D}|\,\right)$$

the state of the qubits that *no process owns*

A context can measure environment qubits immediately: bisimilar distributions need the same environment

No environment qubits: $env(\mathfrak{D})$ is a number, the probability mass, as before

Example: $\Sigma_P = \{q_1\}$ $env(\frac{1}{2}\,|00\rangle\langle 00| \bullet P \oplus \frac{1}{2}\,|11\rangle\langle 11| \bullet P) = \frac{1}{2}\mathbb{I}$ on q_2

Labelled Scheduled Bisimilarity

Definition

A relation $\mathcal{R}$ on quantum distributions is a *labelled scheduled bisimulation* if it is

1. **well-typed**: related distributions have the same type
2. **transition-closed**: for all s and μ, $\mathfrak{D}\ \mathcal{R}\ \mathfrak{T}$ and $\mathfrak{D} \overset{\mu}{\rightarrowtail\!\!\!\!\twoheadrightarrow}_s \mathfrak{D}'$ imply $\mathfrak{T} \overset{\mu}{\rightarrowtail\!\!\!\!\twoheadrightarrow}_s \mathfrak{T}'$ with $\mathfrak{D}'\ \mathcal{R}\ \mathfrak{T}'$, and vice versa
3. **environment-preserving**: $\mathfrak{D}\ \mathcal{R}\ \mathfrak{T}$ implies $env(\mathfrak{D}) = env(\mathfrak{T})$
4. **closed under compatible superoperators**: $\mathfrak{D}\ \mathcal{R}\ \mathfrak{T}$ implies $\mathcal{E}(\mathfrak{D})\ \mathcal{R}\ \mathcal{E}(\mathfrak{T})$ for every $\mathcal{E}$ acting on environment qubits

$\sim$ is the largest labelled scheduled bisimulation

Visible labels $c!v$, $c?v$ replace the contexts interacting on c; condition 4: a context can *modify* environment qubits before handing them over

Example: Measuring and Forgetting

$$P = t\colon \mathcal{M}_{01}(q \rhd x).\, R' \qquad R = t\colon Set_{\frac{1}{2}\mathbb{I}}(q).\, R' \qquad R' = t\colon c!q \parallel t'\colon d!1$$

P looks at x but does nothing with it: on $|+\rangle\langle+|$ it should behave as a reset to $\frac{1}{2}\mathbb{I}$

Example: Measuring and Forgetting

$$P = t\colon \mathcal{M}_{01}(q \rhd x).\, R' \qquad R = t\colon Set_{\frac{1}{2}\mathbb{I}}(q).\, R' \qquad R' = t\colon c!q \parallel t'\colon d!1$$

P looks at x but does nothing with it: on $|+\rangle\langle+|$ it should behave as a reset to $\frac{1}{2}\mathbb{I}$

$$|+\rangle\langle+| \bullet P \xrightarrow{\tau}\!\!\!\!\rightarrow_t \tfrac{1}{2}\,|0\rangle\langle 0| \bullet R' \oplus \tfrac{1}{2}\,|1\rangle\langle 1| \bullet R' \;=\; \tfrac{1}{2}\mathbb{I} \bullet R'$$

$$|+\rangle\langle+| \bullet R \xrightarrow{\tau}\!\!\!\!\rightarrow_t \tfrac{1}{2}\mathbb{I} \bullet R'$$

Example: Measuring and Forgetting

$$P = t\colon \mathcal{M}_{01}(q \rhd x).\, R' \qquad R = t\colon Set_{\frac{1}{2}\mathbb{I}}(q).\, R' \qquad R' = t\colon c!q \parallel t'\colon d!1$$

P looks at x but does nothing with it: on $|+\rangle\langle+|$ it should behave as a reset to $\frac{1}{2}\mathbb{I}$

$$|+\rangle\langle+| \bullet P \xrightarrow{\tau}\!\!\!\!\rightarrow_t \tfrac{1}{2}\,|0\rangle\langle 0| \bullet R' \oplus \tfrac{1}{2}\,|1\rangle\langle 1| \bullet R' \;=\; \tfrac{1}{2}\mathbb{I} \bullet R'$$

$$|+\rangle\langle+| \bullet R \xrightarrow{\tau}\!\!\!\!\rightarrow_t \tfrac{1}{2}\mathbb{I} \bullet R'$$

After one step both sides reach the *same* quantum distribution

$\mathcal{R} = \{(|+\rangle\langle+| \bullet P, |+\rangle\langle+| \bullet R)\} \cup Id$ is a labelled scheduled bisimulation

Hence $|+\rangle\langle+| \bullet P \sim |+\rangle\langle+| \bullet R$: P does not leak its outcome

Full Abstraction

Theorem

For any ρ, σ, P, Q

$$1 \bullet \langle \rho, P \rangle \simeq 1 \bullet \langle \sigma, Q \rangle \quad \text{if and only if} \quad \rho \bullet P \sim \sigma \bullet Q$$

Full Abstraction

Theorem

For any ρ, σ, P, Q

$$1 \bullet \langle \rho, P \rangle \simeq 1 \bullet \langle \sigma, Q \rangle \quad \text{if and only if} \quad \rho \bullet P \sim \sigma \bullet Q$$

The labelled bisimilarity has *exactly* the discriminating power of all admissible observers

$\sim$ is a congruence for $\|$: verify components in isolation, then compose

Coinductive proofs without contexts: exhibit a relation, check four conditions

Quantum indistinguishability holds by construction

Do We Really Need Superoperator Closure?

$$P = t\colon c?x.\, t\colon \mathcal{M}_{01}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x \qquad Q = t\colon c?x.\, t\colon \mathcal{M}_{\pm}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x$$

with an environment qubit q in state $|i\rangle\langle i|$

Do We Really Need Superoperator Closure?

$$P = t\colon c?x.\, t\colon \mathcal{M}_{01}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x \qquad Q = t\colon c?x.\, t\colon \mathcal{M}_{\pm}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x$$

with an environment qubit q in state $|i\rangle\langle i|$

- without condition 4: both receive q and send 0 or 1 with probability $\frac{1}{2}$: equated

Do We Really Need Superoperator Closure?

$$P = t\colon c?x.\, t\colon \mathcal{M}_{01}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x \qquad Q = t\colon c?x.\, t\colon \mathcal{M}_{\pm}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x$$

with an environment qubit q in state $|i\rangle\langle i|$

- without condition 4: both receive q and send 0 or 1 with probability $\frac{1}{2}$: equated
- but a context can first apply $U = HS^\dagger$, with $U|i\rangle = |0\rangle$
  - P then always sends 0
  - Q sends 0 or 1 with probability $\frac{1}{2}$

Do We Really Need Superoperator Closure?

$$P = t\colon c?x.\, t\colon \mathcal{M}_{01}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x \qquad Q = t\colon c?x.\, t\colon \mathcal{M}_{\pm}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x$$

with an environment qubit q in state $|i\rangle\langle i|$

- without condition 4: both receive q and send 0 or 1 with probability $\frac{1}{2}$: equated
- but a context can first apply $U = HS^\dagger$, with $U|i\rangle = |0\rangle$
  - P then always sends 0
  - Q sends 0 or 1 with probability $\frac{1}{2}$
- closure under environment superoperators catches exactly this

Do We Really Need Superoperator Closure?

$$P = t\colon c?x.\, t\colon \mathcal{M}_{01}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x \qquad Q = t\colon c?x.\, t\colon \mathcal{M}_{\pm}(x \rhd y).\, t\colon c!y.\, \mathbf{0}_x$$

with an environment qubit q in state $|i\rangle\langle i|$

- without condition 4: both receive q and send 0 or 1 with probability $\frac{1}{2}$: equated
- but a context can first apply $U = HS^\dagger$, with $U|i\rangle = |0\rangle$
  - P then always sends 0
  - Q sends 0 or 1 with probability $\frac{1}{2}$
- closure under environment superoperators catches exactly this

Price: infinitely many superoperators to consider

Towards Decision Procedures

Closure is needed only for processes that *receive qubits from the environment*

Input-restricted processes $Proc_g$

No unrestricted input on quantum channels

Ground bisimilarity $\sim_g$

Well-typed, transition-closed, environment-preserving (no superoperator closure)

Ground Bisimilarity Suffices

Theorem

For $P, Q \in Proc_g$: $\quad 1 \bullet \langle \rho, P \rangle \simeq 1 \bullet \langle \sigma, Q \rangle$ iff $\rho \bullet P \sim_g \sigma \bullet Q$

Ground Bisimilarity Suffices

Theorem

For $P, Q \in Proc_g$: $\quad 1 \bullet \langle \rho, P \rangle \simeq 1 \bullet \langle \sigma, Q \rangle$ iff $\rho \bullet P \sim_g \sigma \bullet Q$

Finite LTS of quantum distributions + partition refinement: **decidable**

Many protocols are in $Proc_g$

This is what QUARC implements ▶ TOMORROW

9. Angelic vs Demonic Scheduling

Who Matches Whom?

When Δ moves with scheduler s, how may Θ answer?

Demonic

- Θ must answer with the *same* s
- an adversary fixes the sequence of choices; both systems must survive it

Angelic

- Θ may answer with *any* s'
- tags only say which moves are *feasible*
- the names themselves are irrelevant

Demonic: Names Matter

$$1 \bullet \langle \rho, t_0 : c!1 \rangle \qquad \text{vs} \qquad 1 \bullet \langle \rho, t_1 : c!1 \rangle$$

Demonic: not equivalent, t_0 is enabled only on the left

Angelic: equivalent, t_0 on the left is matched by t_1 on the right

Demonic: Names Matter

$$1 \bullet \langle \rho, t_0 : c!1 \rangle \qquad \text{vs} \qquad 1 \bullet \langle \rho, t_1 : c!1 \rangle$$

Demonic: not equivalent, t_0 is enabled only on the left

Angelic: equivalent, t_0 on the left is matched by t_1 on the right

Consequences for the modeller

- specification and implementation must be tagged *consistently*
- the tagging is part of the model: it states which choices are “the same”
- angelic scheduling relieves the modeller of guessing the right tags

Angelic: the Price

Mixing breaks. With $\Delta = 1 \bullet \langle \rho, t_0 : c!1 \rangle$ and $\Theta = 1 \bullet \langle \rho, t_1 : c!1 \rangle$

- Δ and Θ are angelically equivalent, yet
- $\frac{1}{2} \bullet \Delta \oplus \frac{1}{2} \bullet \Delta$ can output with mass 1 (scheduler t_0)
- $\frac{1}{2} \bullet \Delta \oplus \frac{1}{2} \bullet \Theta$ reaches only mass $\frac{1}{2}$, whatever the scheduler

so angelic equivalence is not linear

Angelic: the Price

Mixing breaks. With $\Delta = 1 \bullet \langle \rho, t_0 \colon c!1 \rangle$ and $\Theta = 1 \bullet \langle \rho, t_1 \colon c!1 \rangle$

- Δ and Θ are angelically equivalent, yet
- $\frac{1}{2} \bullet \Delta \oplus \frac{1}{2} \bullet \Delta$ can output with mass 1 (scheduler t_0)
- $\frac{1}{2} \bullet \Delta \oplus \frac{1}{2} \bullet \Theta$ reaches only mass $\frac{1}{2}$, whatever the scheduler

so angelic equivalence is not linear

Labels are not enough. Tags inside classical branches matter

$$t_0 \colon c?b.\ \textsf{if}\ b = 0\ \textsf{then}\ t_1 \colon \tau\ \textsf{else}\ t_1 \colon \tau \quad \text{vs} \quad t_0 \colon c?b.\ \textsf{if}\ b = 0\ \textsf{then}\ t_1 \colon \tau\ \textsf{else}\ t_2 \colon \tau$$

Angelically equal step by step, but a context sending a *random* bit splits the right one across two tags

Demonic or Angelic?

	demonic	angelic
discriminating power	finer	coarser
independent of tag names	✗	✓
linear	✓	✗
labelled characterisation	✓	open

Demonic or Angelic?

	demonic	angelic
discriminating power	finer	coarser
independent of tag names	✗	✓
linear	✓	✗
labelled characterisation	✓	open

Demonic: robust and compositional, but the tagging is part of the specification

Angelic: closer to intuition for modellers, but harder to reason about

In between: schedulers allowed to branch on *classical* data (measurement outcomes, received values) are a natural next step

10. Looking Ahead

Beyond Strong Bisimilarity

Work in progress Strong bisimilarity counts every τ: specifications must be padded, e.g. $\mathsf{FairCoin} = \mathcal{M}_{\mathsf{bit}}(\triangleright x).\, \tau^8.\, (a!x \parallel b!x \parallel \mathit{cheat}!0)$

Beyond Strong Bisimilarity

Work in progress Strong bisimilarity counts every τ: specifications must be padded, e.g. **FairCoin** $= \mathcal{M}_{\text{bit}}(\triangleright x).\, \tau^8.\, (a!x \parallel b!x \parallel \mathit{cheat}!0)$

Desirable: a weak or branching bisimilarity, skipping *inert* internal steps

$$t.\, \tau.\, t' : a!1 \;\approx\; t' : a!1 \qquad \text{but} \qquad t.\, \tau.\, t' : a!1 + t'' : b!1 \;\not\approx\; t' : a!1 + t'' : b!1$$

Beyond Strong Bisimilarity

Work in progress Strong bisimilarity counts every τ: specifications must be padded, e.g. **FairCoin** $= \mathcal{M}_{\text{bit}}(\triangleright x).\, \tau^8.\, (a!x \parallel b!x \parallel \mathit{cheat}!0)$

Desirable: a weak or branching bisimilarity, skipping *inert* internal steps

$$t\colon \tau.\, t'\colon a!1 \;\approx\; t'\colon a!1 \qquad \text{but} \qquad t\colon \tau.\, t'\colon a!1 + t''\colon b!1 \;\not\approx\; t'\colon a!1 + t''\colon b!1$$

Needs formal development

- which scheduler matches a *sequence* of τ moves?
- divergence and loss of mass along τ paths
- does it stay a congruence, and does indistinguishability still lift?
- does a labelled characterisation exist?

Quantifying over Inputs

Work in progress $\sim_g$ fixes the input: $\rho \bullet P \sim_g \rho \bullet Q$ for *one* ρ

Teleportation, secret sharing, authentication: correct for *every* input,
$\forall \rho.\ \rho \bullet P \sim_g \rho \bullet Q$: infinitely many LTSs to compare

Quantifying over Inputs

Work in progress $\sim_g$ fixes the input: $\rho \bullet P \sim_g \rho \bullet Q$ for *one* ρ

Teleportation, secret sharing, authentication: correct for *every* input,
$\forall \rho.\ \rho \bullet P \sim_g \rho \bullet Q$: infinitely many LTSs to compare

Idea: weights become superoperators, again a PCM $\langle \mathcal{SO}^{\leq}(\mathcal{H}_\Sigma), 0, + \rangle$

Superoperator distributions $\mathcal{S}_\Sigma(Proc)$

The weight of P is *what has been done to the unknown input* to reach P

$$\frac{\forall i.\ P_i \xrightarrow{\mu}_s \sum_j \mathcal{E}_{ij} \bullet P_{ij}}{\sum_i \mathcal{F}_i \bullet P_i \rightarrowtail\!\!\!\!\!\!\rightarrow^{\mu}_s \sum_{i,j} \mathcal{E}_{ij} \circ \mathcal{F}_i \bullet P_{ij}} \qquad \text{from } \mathcal{I}d \bullet P$$

Quantifying over Inputs

Work in progress $\sim_g$ fixes the input: $\rho \bullet P \sim_g \rho \bullet Q$ for *one* ρ

Teleportation, secret sharing, authentication: correct for *every* input,
$\forall \rho.\ \rho \bullet P \sim_g \rho \bullet Q$: infinitely many LTSs to compare

Idea: weights become superoperators, again a PCM $\langle \mathcal{SO}^{\leq}(\mathcal{H}_\Sigma), 0, + \rangle$

Superoperator distributions $\mathcal{S}_\Sigma(Proc)$

The weight of P is *what has been done to the unknown input* to reach P

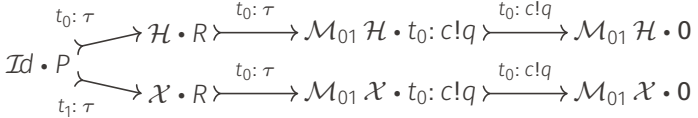
$$\frac{\forall i.\ P_i \xrightarrow{\mu}_s \sum_j \mathcal{E}_{ij} \bullet P_{ij}}{\sum_i \mathcal{F}_i \bullet P_i \rightarrowtail\!\!\!\!\!\rightarrow^{\mu}_s \sum_{i,j} \mathcal{E}_{ij} \circ \mathcal{F}_i \bullet P_{ij}} \qquad \text{from } \mathcal{I}d \bullet P$$

Instantiation $\mathfrak{D}[\rho] = \sum_i \mathcal{E}_i(\rho) \bullet P_i$: symbolic LTS $\mapsto$ ground LTS for ρ

Example: a Symbolic Lottery

$P = t_0\colon H(q).\, R + t_1\colon X(q).\, R \qquad R = t_0\colon \mathcal{M}_{01}(q \rhd x).\, t_0\colon c!q$

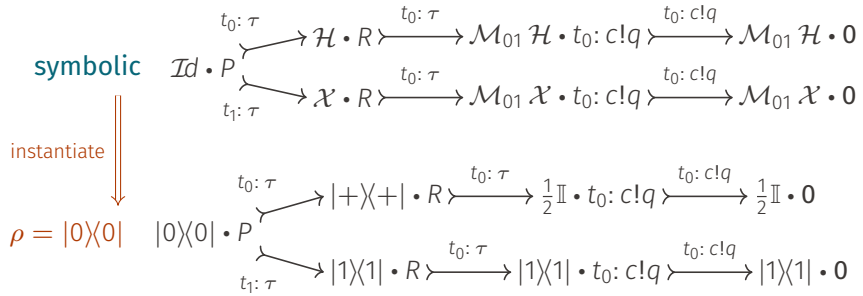
symbolic



$\mathcal{M}_0\mathcal{H} \bullet t_0\colon c!q \oplus \mathcal{M}_1\mathcal{H} \bullet t_0\colon c!q = \mathcal{M}_{01}\,\mathcal{H} \bullet t_0\colon c!q$, with $\mathcal{M}_{01} = \{|0\rangle\langle 0|\,, |1\rangle\langle 1|\}$

Example: a Symbolic Lottery

$P = t_0\colon H(q).\, R + t_1\colon X(q).\, R \qquad R = t_0\colon \mathcal{M}_{01}(q \rhd x).\, t_0\colon c!q$



$\mathcal{M}_0\mathcal{H} \bullet t_0\colon c!q \oplus \mathcal{M}_1\mathcal{H} \bullet t_0\colon c!q = \mathcal{M}_{01}\,\mathcal{H} \bullet t_0\colon c!q$, with $\mathcal{M}_{01} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

Instantiating every node with $|0\rangle\langle 0|$ gives exactly the ground LTS

Symbolic Bisimilarity

Same conditions as $\sim_g$, but $env(\mathfrak{D}) = \mathsf{tr}_{\Sigma'} \circ |\mathfrak{D}|$ is now a *superoperator*

Theorem (full abstraction)

$$\mathfrak{D} \sim_{\mathcal{S}} \mathfrak{T} \quad \text{iff} \quad \forall \rho.\, \mathfrak{D}[\rho] \sim_g \mathfrak{T}[\rho]$$

Symbolic Bisimilarity

Same conditions as $\sim_g$, but $env(\mathfrak{D}) = \mathrm{tr}_{\Sigma'} \circ |\mathfrak{D}|$ is now a *superoperator*

Theorem (full abstraction)

$$\mathfrak{D} \sim_{\mathcal{S}} \mathfrak{T} \quad \text{iff} \quad \forall \rho.\, \mathfrak{D}[\rho] \sim_g \mathfrak{T}[\rho]$$

Example: $P = \mathcal{M}_{\pm}(q \rhd x).\, c!x.\, \mathbf{0}_q$ vs $Q = \mathcal{M}_{01}(q \rhd x).\, c!x.\, \mathbf{0}_q$

- on $|i\rangle\langle i|$ both are a fair coin: ground bisimilar
- after $c!0$: $env(\mathcal{M}_+ \bullet \mathbf{0}_q)$ has Kraus $\{\langle +|\}$, $env(\mathcal{M}_0 \bullet \mathbf{0}_q)$ has $\{\langle 0|\}$: $P \not\sim_{\mathcal{S}} Q$
- witness: on $|1\rangle\langle 1|$, P outputs 0 half of the time, Q never

Symbolic Bisimilarity

Same conditions as $\sim_g$, but $env(\mathfrak{D}) = \mathrm{tr}_{\Sigma'} \circ |\mathfrak{D}|$ is now a *superoperator*

Theorem (full abstraction)

$$\mathfrak{D} \sim_{\mathcal{S}} \mathfrak{T} \quad \text{iff} \quad \forall \rho.\, \mathfrak{D}[\rho] \sim_g \mathfrak{T}[\rho]$$

Example: $P = \mathcal{M}_{\pm}(q \rhd x).\, c!x.\, \mathbf{0}_q$ vs $Q = \mathcal{M}_{01}(q \rhd x).\, c!x.\, \mathbf{0}_q$

- on $|i\rangle\langle i|$ both are a fair coin: ground bisimilar
- after $c!0$: $env(\mathcal{M}_+ \bullet \mathbf{0}_q)$ has Kraus $\{\langle +|\}$, $env(\mathcal{M}_0 \bullet \mathbf{0}_q)$ has $\{\langle 0|\}$: $P \not\sim_{\mathcal{S}} Q$
- witness: on $|1\rangle\langle 1|$, P outputs 0 half of the time, Q never

Decidable: finite symbolic LTS, superoperators compared via Choi matrices, then partition refinement

Open: schedulers that remember classical outcomes, efficient representations

11. Case Study: Quantum Coin Flip

Quantum Coin Flip

Alice and Bob, who do not trust each other, toss a coin remotely. Bob wins if he guesses Alice's secret basis

$$
\begin{aligned}
&\textbf{Alice} ::= \mathcal{M}_{\text{bit}}(\triangleright s).\\
&\quad \textbf{if } s = 0 \textbf{ then } H(q).\, \mathcal{M}_{01}(q \triangleright w)\\
&\quad\quad \textbf{else } I(q).\, \mathcal{M}_{\pm}(q \triangleright w).\\
&\quad \mathit{AtoB}!q.\, \mathit{guess}?g.\\
&\quad \mathit{witness}!w.\, \mathit{secret}!s.\\
&\quad a!(g = s)
\end{aligned}
\qquad
\begin{aligned}
&\textbf{Bob} ::= \mathit{AtoB}?x.\, \mathcal{M}_{\text{bit}}(\triangleright g).\\
&\quad \textbf{if } g = 0 \textbf{ then } \mathcal{M}_{\pm}(x \triangleright p)\\
&\quad\quad \textbf{else } \mathcal{M}_{01}(x \triangleright p).\\
&\quad \mathit{guess}!g.\, \mathit{witness}?w.\, \mathit{secret}?s.\\
&\quad \big(b!(g = s) \parallel \mathit{cheat}!(g \neq s \wedge p \neq w) \parallel \mathbf{0}_x\big)
\end{aligned}
$$

$$\textbf{QCF} ::= (\textbf{Alice} \parallel \textbf{Bob}) \setminus \{\mathit{AtoB}, \mathit{guess}, \mathit{secret}, \mathit{witness}\} \qquad q \text{ starts in } |0\rangle$$

Alice encodes a random bit w in basis s; Bob measures in the basis opposite to his guess. If he guessed wrong, his outcome p must match Alice's witness w, otherwise she cheated (tags omitted)

Correctness and Confidentiality

Correctness: the protocol behaves as a fair coin

$$\mathsf{QCF} \simeq \mathcal{M}_{\mathsf{bit}}(\triangleright x).\, \tau^{8}.\, (a!x \parallel b!x \parallel \mathit{cheat}!0)$$

Correctness and Confidentiality

Correctness: the protocol behaves as a fair coin

$$\mathsf{QCF} \;\simeq\; \mathcal{M}_{\mathsf{bit}}(\triangleright x).\, \tau^{8}.\, (a!x \parallel b!x \parallel \mathit{cheat}!0)$$

Confidentiality: Bob cannot learn s from the qubit. Take Alice before revealing

$$\mathsf{Alice}_0 = H(q).\, \mathcal{M}_{01}(q \triangleright w).\, \mathit{AtoB}!q \qquad \mathsf{Alice}_1 = I(q).\, \mathcal{M}_{\pm}(q \triangleright w).\, \mathit{AtoB}!q$$

From $|0\rangle$, both reach $\frac{1}{2}\mathbb{I} \bullet \mathit{AtoB}!q$: $\mathsf{Alice}_0 \simeq \mathsf{Alice}_1$

It is the qubit-source example in disguise

With $\simeq_\bullet$ they are distinguished: we would wrongly conclude that Bob can cheat

Attacks as Equivalences

$$\textbf{Alison} ::= \mathcal{M}_{\text{bit}}(\triangleright s).\ \ldots(\text{as Alice})\ldots \\ \quad AtoB!q.\, guess?g.\, witness!w. \\ \quad (secret!(1-g) \parallel a!0)$$

$$\textbf{Alix} ::= H(q).\, CNOT(q, q').\, AtoB!q.\, guess?g. \\ \quad \textbf{if } g = 0 \textbf{ then } \mathcal{M}_{\pm}(q' \triangleright w) \textbf{ else } \mathcal{M}_{01}(q' \triangleright w). \\ \quad witness!w.\, (secret!(1-g) \parallel a!0)$$

Attacks as Equivalences

$$\textsf{Alison} ::= \mathcal{M}_{\text{bit}}(\triangleright s).\ \ldots(\text{as Alice})\ldots \\ \quad AtoB!q.\, guess?g.\, witness!w. \\ \quad (secret!(1-g) \parallel a!0)$$

$$\textsf{Alix} ::= H(q).\, CNOT(q, q').\, AtoB!q.\, guess?g. \\ \quad \textbf{if } g = 0 \textbf{ then } \mathcal{M}_{\pm}(q' \triangleright w) \textbf{ else } \mathcal{M}_{01}(q' \triangleright w). \\ \quad witness!w.\, (secret!(1-g) \parallel a!0)$$

Alison lies about the basis: Bob catches her with probability $\frac{1}{4}$

$$(\textsf{Alison} \parallel \textsf{Bob}) \setminus \ldots \ \simeq\ \mathcal{M}_{3/4}(\triangleright x).\, \tau^8.\, (a!0 \parallel b!0 \parallel cheat!x)$$

Attacks as Equivalences

$$\textsf{Alison} ::= \mathcal{M}_{\text{bit}}(\triangleright s).\ \ldots(\text{as Alice})\ldots \\ \quad AtoB!q.\, guess?g.\, witness!w. \\ \quad (secret!(1-g) \parallel a!0)$$

$$\textsf{Alix} ::= H(q).\, CNOT(q, q').\, AtoB!q.\, guess?g. \\ \quad \textsf{if } g = 0 \textsf{ then } \mathcal{M}_{\pm}(q' \triangleright w) \textsf{ else } \mathcal{M}_{01}(q' \triangleright w). \\ \quad witness!w.\, (secret!(1-g) \parallel a!0)$$

Alison lies about the basis: Bob catches her with probability $\frac{1}{4}$

$$(\textsf{Alison} \parallel \textsf{Bob}) \setminus \ldots \ \simeq\ \mathcal{M}_{3/4}(\triangleright x).\, \tau^8.\, (a!0 \parallel b!0 \parallel cheat!x)$$

Alix uses entanglement to forge a valid witness: she always wins, undetected

$$(\textsf{Alix} \parallel \textsf{Bob}) \setminus \ldots \ \simeq\ \tau^9.\, (a!0 \parallel b!0 \parallel cheat!0)$$

Attacks as Equivalences

$$\textsf{Alison} ::= \mathcal{M}_{\text{bit}}(\triangleright s).\ \ldots(\text{as Alice})\ldots \\ \quad AtoB!q.\, guess?g.\, witness!w. \\ \quad (secret!(1-g) \parallel a!0)$$

$$\textsf{Alix} ::= H(q).\, CNOT(q, q').\, AtoB!q.\, guess?g. \\ \quad \textsf{if } g = 0 \textsf{ then } \mathcal{M}_{\pm}(q' \triangleright w) \textsf{ else } \mathcal{M}_{01}(q' \triangleright w). \\ \quad witness!w.\, (secret!(1-g) \parallel a!0)$$

Alison lies about the basis: Bob catches her with probability $\frac{1}{4}$

$$(\textsf{Alison} \parallel \textsf{Bob}) \setminus \ldots \simeq \mathcal{M}_{3/4}(\triangleright x).\, \tau^8.\, (a!0 \parallel b!0 \parallel cheat!x)$$

Alix uses entanglement to forge a valid witness: she always wins, undetected

$$(\textsf{Alix} \parallel \textsf{Bob}) \setminus \ldots \simeq \tau^9.\, (a!0 \parallel b!0 \parallel cheat!0)$$

Only Alice has a winning strategy, as expected. We will check all of this with QUARC

▶ TOMORROW

12. Wrap-up

Summary

	respects QM	congr. ($\|\|$)	no contexts	decidable
$\simeq_\bullet$ unscheduled saturated	✗	✓	✗	✗
$\simeq$ scheduled saturated	✓	✓	✗	✗
$\sim$ labelled, quantum distrib.	✓	✓	✓	✗
$\sim_g$ ground, on $Proc_g$	✓	✓	✓	✓

Summary

	respects QM	congr. ($\|\|$)	no contexts	decidable
$\simeq_\bullet$ unscheduled saturated	✗	✓	✗	✗
$\simeq$ scheduled saturated	✓	✓	✗	✗
$\sim$ labelled, quantum distrib.	✓	✓	✓	✗
$\sim_g$ ground, on $Proc_g$	✓	✓	✓	✓

Non-determinism resolved per element of a distribution lets observers peek at qubits

Schedulers via tags: choices by name, uniformly for processes and observers

Quantum distributions make indistinguishable mixtures equal

Labelled bisimilarity = saturated bisimilarity, decidable for input-restricted processes

Pointers

- L. Ceragioli, F. Gadducci, G. Lomurno, G. Tedeschi. *Quantum Bisimilarity Is a Congruence Under Physically Admissible Schedulers*. APLAS 2024
- L. Ceragioli, F. Gadducci, G. Lomurno, G. Tedeschi. *Verification of Quantum Protocols Adopting Physically Admissible Schedulers*. ACM TQC 2026
- K. Chatzikokolakis, C. Palamidessi. *Making Random Choices Invisible to the Scheduler*. CONCUR 2007
- K. Chatzikokolakis, G. Norman, D. Parker. *Bisimulation for Demonic Schedulers*. FoSSaCS 2009
- F. Bonchi, F. Gadducci, G. V. Monreale. *A General Theory of Barbs, Contexts, and Labels*. ACM TOCL 2014
- Y. Feng, R. Duan, M. Ying. *Bisimulation for Quantum Processes*. ACM TOPLAS 2012
- Y. Deng. *Bisimulations for Probabilistic and Quantum Processes*. CONCUR 2018

Questions?

github.com/glomurno/QUARC