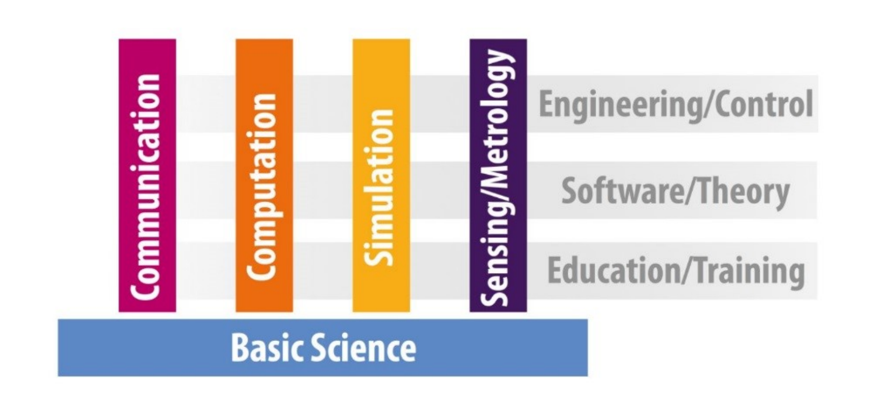
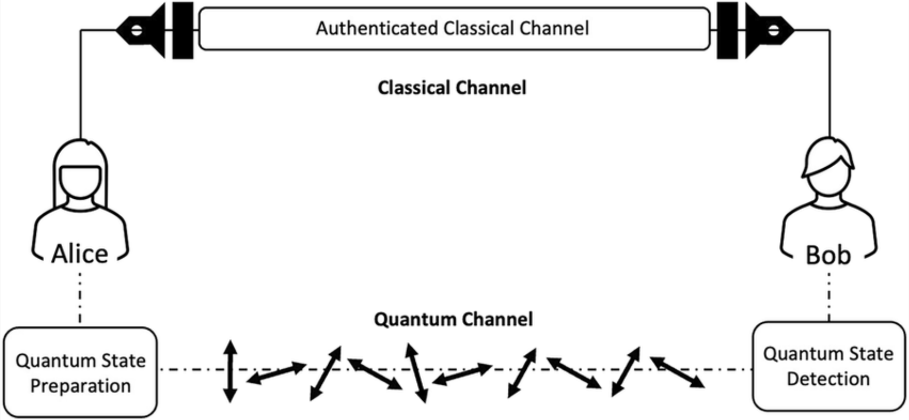
Testing Quantum Processes

L. Ceragioli **F. Gadducci** G. Lomurno G. Tedeschi

Quantum Technologies



Quantum Protocols



Why Quantum Communication

- For Quantum Protocols
  - quantum key distribution; leader-election; superdense-coding
  - security guarantees
  - communication efficiency
- For Implementing Quantum Algorithms
  - speedup over classical counterparts
  - but computers with big registers are difficult
  - distributed computing with the quantum internet

Modeling and Verifying Quantum Distributed Systems

We need:

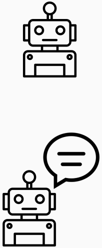
- Description language
- Semantic model
- Technique for checking correctness

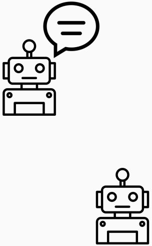
Process algebras have proven successful for modeling and verifying concurrent systems also with probabilities

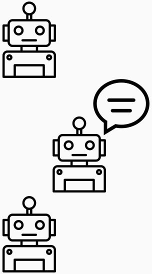
- We use them for modeling quantum concurrent systems
- We compare their behaviour using tests!

Recall — Testing Processes

Modelling and Comparing Concurrent Systems







Concurrent Processes + Communication Primitives + Nondeterministic Choices

Value Passing CCS

A language for concurrent, non-deterministic, communicating systems.

$$P ::= \mathbf{0} \mid \tau.P \mid c!v.P \mid c?x.P \mid P + P \mid P \setminus c \mid P \parallel P \mid \textbf{if } e \textbf{ then } P \textbf{ else } P$$

- $P \parallel Q$ is the parallel composition of P and Q
- $P + Q$ is the non-deterministic composition of P and Q
- $c?x.P$ receives a value on the channel c, $c!v.P$ sends the value v con channel c
- **if** v **then** P **else** Q behaves as P if $v \neq 0$, as Q if $v = 0$.

Operational Semantics

Labelled Transition system $\langle S, Act, \rightarrow \rangle$, with $\rightarrow \subseteq S \times Act \times S$

$$\frac{}{c!v.P \xrightarrow{c!v} P} \qquad \frac{}{c?x.P \xrightarrow{c?v} P[v/x]}$$

$$\frac{P \xrightarrow{\mu} P'}{P + Q \xrightarrow{\mu} P'} \qquad \frac{}{\tau.P \xrightarrow{\tau} P} \qquad \frac{P \xrightarrow{\mu} P' \quad \mu \neq c!v, c?v}{P \setminus c \xrightarrow{\mu} P' \setminus c}$$

$$\frac{P \xrightarrow{\mu} P'}{P \parallel Q \xrightarrow{\mu} P' \parallel Q} \qquad \frac{P \xrightarrow{c!v} P' \quad Q \xrightarrow{c?v} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'} \qquad \frac{n = 0 \quad P \xrightarrow{\alpha} P'}{\textbf{if } n \textbf{ then } P \textbf{ else } Q \xrightarrow{\alpha} P'}$$

Example

$$P = \mathit{start}!0.\mathit{choice}?x.\mathbf{if}\ x\ \mathbf{then}\ \mathit{out}!\mathit{coffee}\ \mathbf{else}\ \mathit{out}!\mathit{tea}$$

$$\begin{tikzcd}
& P \arrow[d, "\mathit{start}!0"'] & \\
& P' \arrow[dl, "\mathit{choice}?0"'] \arrow[dr, "\mathit{choice}?1"] & \\
P''[0/x] \arrow[d, "\mathit{out}!\mathit{coffee}"'] & & P''[1/x] \arrow[d, "\mathit{out}!\mathit{tea}"] \\
\mathbf{0} & & \mathbf{0}
\end{tikzcd}$$

Testing Equivalence in a Nutshell

How to verify that two processes are equivalent? With **Tests**.

Consider:

- The evolution of the processes under the same **test** T
- Tests are like processes with a distinct (successful) termination ω,

$$T ::= \omega \mid \mathbf{0} \mid \tau.T \mid c!v.T \mid c?x.T \mid T + T \mid T \setminus c \mid \textbf{if } e \textbf{ then } T \textbf{ else } T$$

- Processes and tests evolve together $\langle P, T \rangle \xrightarrow{\tau} \langle P_1, T_1 \rangle \xrightarrow{\tau} \ldots$
- Two possible outcomes
    - $\ldots \xrightarrow{\tau} \langle P_n, \omega \rangle$ — **The test is successful**
    - all other cases — **The test fails**

Test Semantics

$$\frac{P \xrightarrow{c!v} P'}{\langle\!|P, c?x.T|\!\rangle \xrightarrow{\tau} \langle\!|P', T[v/x]|\!\rangle} \qquad \frac{e \Downarrow v \quad \langle\!|P|\!\rangle \xrightarrow{c?v} P'}{\langle\!|P, c!e.T|\!\rangle \xrightarrow{\tau} \langle\!|P', T|\!\rangle}$$

$$\frac{P \xrightarrow{\mu} P'}{\langle\!|P, T|\!\rangle \xrightarrow{\mu} \langle\!|P', T|\!\rangle} \qquad \frac{}{\langle\!|P, \tau.T|\!\rangle \xrightarrow{\tau} \langle\!|P, T|\!\rangle}$$

Testing Equivalence

Definition

A process P **may** pass the test T if $\langle P, T\rangle \xrightarrow{\tau}{}^{*} \langle P', \omega\rangle$ for some path.

A process P **must** pass the test T if $\langle P, T\rangle \xrightarrow{\tau}{}^{*} \langle P', \omega\rangle$ for all paths.

$$\begin{tikzcd}
\langle a!0, a?x.\omega\rangle \arrow[d, "\tau"'] \\
\langle \mathbf{0}, \omega\rangle
\end{tikzcd}$$

pass

$$\langle a!0, b?x.\omega\rangle$$

not pass

$$\begin{tikzcd}
 & \langle a!0 + a!1, a?x.\textbf{if } x = 0 \textbf{ then } \omega \textbf{ else } \mathbf{0}\rangle \arrow[dl, "\tau"'] \arrow[dr, "\tau"] & \\
\langle \mathbf{0}, \omega\rangle & & \langle \mathbf{0}, \mathbf{0}\rangle
\end{tikzcd}$$

may pass, not must pass

Definition
Two processes are **may-testing equivalent** if they may pass the same set of tests.

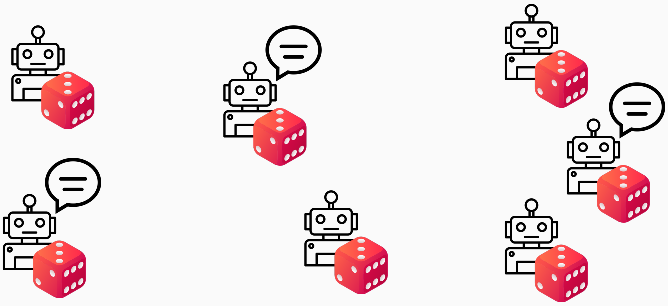
Two processes are **must-testing equivalent** if they must pass the same set of tests.

Two processes are **testing equivalent** if they are may and must testing equivalent.

$$
\begin{tikzcd}
 & c!0 \parallel c!1 \arrow[dl, "c!0"'] \arrow[dr, "c!1"] & & & & c!0.c!1 + c!1.c!0 \arrow[dl, "c!0"'] \arrow[dr, "c!1"] & \\
\mathbf{0} \parallel c!1 \arrow[dr, "c!1"'] & & c!0 \parallel \mathbf{0} \arrow[dl, "c!0"] & \simeq & c!1 \arrow[d, "c!1"'] & & c!0 \arrow[d, "c!0"] \\
 & \mathbf{0} \parallel \mathbf{0} & & & \mathbf{0} & & \mathbf{0}
\end{tikzcd}
$$

Testing Probabilistic Processes

Modeling and Comparing Probabilistic Concurrent Systems



Concurrent Processes	+	Communication Primitives	+	Nondeterministic Choices	+	Random Sources

Probability Distributions

Finite **probability distributions** on X are functions from X to $[0,1]$

$$D(x) = \left\{ \Delta : X \to [0,1] \;\middle|\; \sum_{x \in X} \Delta(x) = 1,\ \lceil \Delta \rceil \text{ is finite} \right\}$$

where $\lceil \Delta \rceil = \{x \in X \mid \Delta(x) \neq 0\}$

Point distribution:

$$\overline{x}(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise} \end{cases} \qquad \ldots \text{we will often write } x \text{ for } \overline{x}$$

Convex combination:

$$(\Delta \ {}_p\!\oplus \Theta)(y) = p(\Delta(y)) + (1-p)(\Theta(y))$$

A Probabilistic Version of CCS

A language for concurrent, non-deterministic, and **probabilistic** communicating systems.

$$P ::= \mathbf{0} \mid \tau.P \mid c!v.P \mid c?x.P \mid P + P \mid P \setminus c \mid P \parallel P \mid \textbf{if } e \textbf{ then } P \textbf{ else } P \mid M_\Delta(x).P$$

- Δ is a probability distribution of natural numbers
- $M_\Delta(x)$ randomly selects an outcome from Δ and associates it to the variable x

e' lievemente diverso perche' c'era un brutto clash di notazione (anche dopo, versione vecchia commentata).

Operational Semantics

Nondeterminist Probabilistic Labelled Transition system (NPLTS) $\langle S, Act, \rightarrow \rangle$, with $\rightarrow \subseteq S \times Act \times D(S)$

$$\frac{}{c!v.P \xrightarrow{c!v} P} \qquad \frac{P \xrightarrow{\mu} \Delta}{P + Q \xrightarrow{\mu} \Delta} \qquad \dots$$

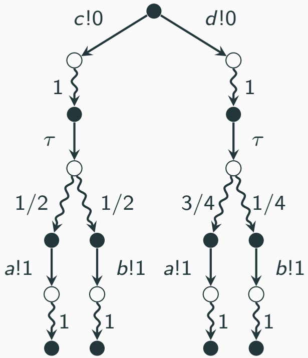
$$\frac{\Delta = \sum_{i \in I} p_i \cdot v_i}{M_\Delta(x).P \xrightarrow{\tau} \sum_{i \in I} p_i \cdot P[{}^{v_i}/_{x}]}$$

Example

$$c!0.M_{\mathrm{fair}}(x).\mathbf{if}\ x\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1$$

$$+$$

$$d!0.M_{\mathrm{unfair}}(x).\mathbf{if}\ x\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1$$



Testing

Distinguishing probabilistic processes

- As before:
  - the evolution of the process P in parallel with a **test** T
  - tests are like processes with a distinct (successful) termination ω
- This time: we must resolve **both non-determinism and probability!**

$$T ::= \mathbf{0} \mid \omega \mid \tau.T \mid c!v.T \mid c?x.T \mid T + T \mid T \setminus c \mid \textbf{if } e \textbf{ then } T \textbf{ else } T \mid M_{\Delta}(x).P$$

Example

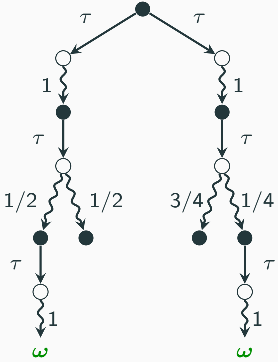
Process

$$P \;:=\; c!0.M_{\mathrm{fair}}(x).\mathbf{if}\ x\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1$$
$$+$$
$$d!0.M_{\mathrm{unfair}}(x).\mathbf{if}\ x\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1$$

Test

$$T \;:=\; c?x.a?y.\omega$$
$$+$$
$$d?x.b?y.\omega$$

The evolution of $\langle P, T\rangle$

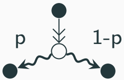


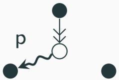
Resolving Non-determinism

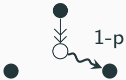
Definition (Resolution though randomized schedulers)
Given an NPTS $(S, \rightarrow)$, a *resolution* R is a PTS $(S, \rightarrow_R)$ such that for every $s \in S$

- if $s \rightarrow_R \Delta$ then there exists probabilities $\{p_i\}_{i \in I}$ and distributions $\{\Delta_i\}_{i \in I}$ such that $\sum_{i \in I} p_i = 1$, $\Delta = \sum_{i \in I} p_i \bullet \Delta_i$ and for each $i \in I$ there is a transition $s \rightarrow \Delta_i$ in the original NPTS.
- if $\nexists \Delta$ such that $s \rightarrow_R \Delta$, then $\nexists \Delta$ such that $s \rightarrow \Delta$ in the original NPTS.

Resolving Probability

From 

to 

or 

Definition (Computation)
Given P_0, T_0 and a resolution R, a computation of length n for $\langle P_0, T_0 \rangle$ is a sequence

$$c = \langle P_0, T_0 \rangle \xrightarrow{\tau}_R \langle P_1, T_1 \rangle, \cdots, \langle P_{n-1}, T_{n-1} \rangle \xrightarrow{\tau}_R \langle P_n, T_n \rangle$$

where, for $i = 1, \ldots, n$, $\langle P_i, T_i \rangle \in \lceil \Delta_i \rceil$ with Δ_i the unique distribution such that $\langle P_{i-1}, T_{i-1} \rangle \xrightarrow{\tau}_R \Delta_i$.

- We say that c is *maximal* if it is not a proper prefix of any other computation
- The *probability* of c is $prob(c) = \prod_{i=1}^{n} \Delta_i(P_i, T_i)$

Success Probability

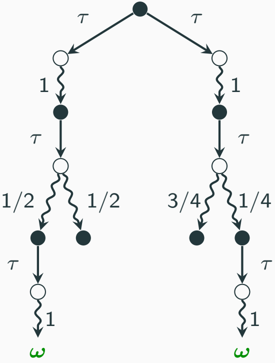
Definition (Success probability)
Given P, T and R,

$$sp_R(\langle\!\langle P, T\rangle\!\rangle) = \sum\nolimits_{c \in Succ_R(\langle\!\langle P,T\rangle\!\rangle)} prob(c)$$

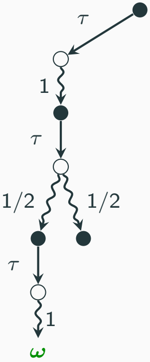
where $Succ_R(\langle\!\langle P, T\rangle\!\rangle)$ is the set of maximal computations in R starting from $\langle\!\langle P, T\rangle\!\rangle$ and containing a success state $\langle\!\langle P', \boldsymbol{\omega}\rangle\!\rangle$.

Example

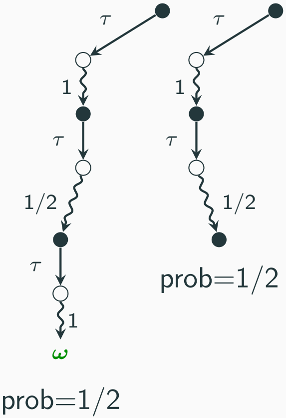
Evolution of $\langle P, T \rangle$



A resolution



Resolution's traces (with probability)



Testing Equivalence

Definition (Testing Equivalence)
$P \sim_{\mathbb{T}} Q$, if for every test T,

- for each resolution R_1, there exists a resolution R_2 such that

$$sp_{R_1}(\langle\!| P, T |\!\rangle) = sp_{R_2}(\langle\!| Q, T |\!\rangle)$$

- for each resolution R_2, there exists a resolution R_1 such that

$$sp_{R_2}(\langle\!| Q, T |\!\rangle) = sp_{R_1}(\langle\!| P, T |\!\rangle)$$

Quantum Background

Hilbert Spaces

A (finite-dimensional) *Hilbert Space* $\mathcal{H}$ is a *complex vector space* with *inner product*.

- Column vector $|\psi\rangle$

$$|\psi\rangle = \begin{pmatrix} 0.6i \\ 0.2 + 0.2i \end{pmatrix}$$

- Conjugate transpose:

$$\langle\psi| = \begin{pmatrix} -0.6i & 0.2 - 0.2i \end{pmatrix}$$

- Dot product between $|\psi\rangle$ and $|\phi\rangle$:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \qquad \langle\psi|\phi\rangle = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} \cdot \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

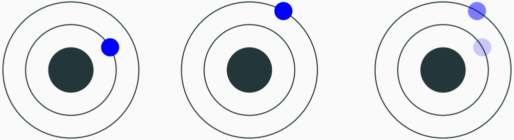
States of a Quantum System

A quantum state $|\phi\rangle$ is a unitary vector in a Hilbert space, i.e. $\langle\phi|\phi\rangle = 1$.

For **bits**: two *classical states* 0 and 1

A **qubit** may be in a *superposition* of the two

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{with amplitudes } \alpha, \beta \in \mathbb{C} \text{ such that } |\alpha|^2 + |\beta|^2 = 1$$



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

Basis

Computational basis: $B_{01} = \{|0\rangle, |1\rangle\}$.

Hadamard basis: $B_{\pm} = \{|+\rangle, |-\rangle\}$ with

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Imaginary basis: $B_{\pm i} = \{|i\rangle, |-i\rangle\}$ with

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$

Programmers use Unitary Transformations to Change the Qubits State

A Couple of Examples

Quantum version of bit flip

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

Basis mapping $B_{01} \Longleftrightarrow B_{\pm}$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$

$$H|+\rangle = |0\rangle$$

$$H|-\rangle = |1\rangle$$

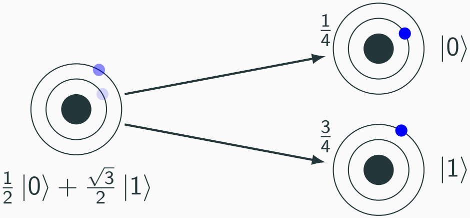
Projective Measurements

Measurement on a given basis: $M_{01}, M_{\pm}$ with a probabilistic result composed by

- the **classical outcome**
- how the **state decays**

For M_{01}, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

- 0 and $|0\rangle$ with probability $|\alpha|^2$
- 1 and $|1\rangle$ with probability $|\beta|^2$



Qubits cannot be observed without affecting their state!

Projective Measurements for our Bases

Our bases are all incompatible!: $M_{01}, M_{\pm}, M_{\pm i}$

- measuring $|\psi\rangle$ in $\{|\psi\rangle, |\phi\rangle\}$ always gives $|\psi\rangle$
- measuring $|\psi\rangle$ in $\{|\psi'\rangle, |\phi'\rangle\}$ always gives $|\psi'\rangle \; {}_{1/2}\!\oplus \; |\phi'\rangle$

$$M_{01}(|+\rangle) = M_{01}(|-\rangle) = M_{01}(|i\rangle) = M_{01}(|-i\rangle) = |0\rangle \; {}_{1/2}\!\oplus \; |1\rangle$$

$$M_{\pm}(|0\rangle) = M_{\pm}(|1\rangle) = M_{\pm}(|i\rangle) = M_{\pm}(|-i\rangle) = |+\rangle \; {}_{1/2}\!\oplus \; |-\rangle$$

$$M_{\pm i}(|0\rangle) = M_{\pm i}(|1\rangle) = M_{\pm i}(|+\rangle) = M_{\pm i}(|-\rangle) = |i\rangle \; {}_{1/2}\!\oplus \; |-i\rangle$$

Composite Quantum Systems

States and transformations composed through *tensor product*, or *kronecker product*.

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$$

$$|+\rangle \otimes |0\rangle = |+0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

A transformation X applied on just the first qubit is $X \otimes I =$

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

No-Cloning Theorem

Theorem. There is no unitary transformation U and state $|\psi\rangle$ such that for every $|\phi\rangle$

$$U(|\phi\rangle \otimes |\psi\rangle) = |\phi\rangle \otimes |\phi\rangle$$

No broadcasting! Aggiungere dopo slide su linearità senza linearità

Entanglement

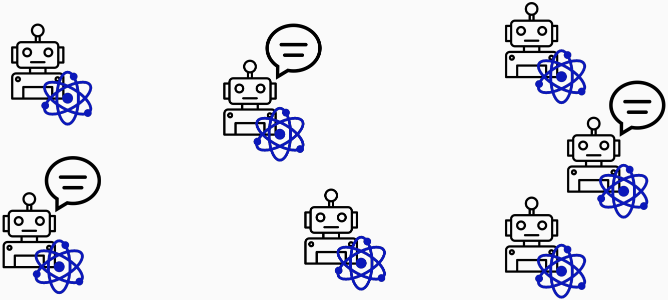
A state that cannot be the product of two smaller states

Definition. $|\psi\rangle$ is entangled iff $\forall\, |\phi_1\rangle, |\phi_2\rangle\,.\, |\psi\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \implies \begin{array}{l} M_{01}(|\Phi^+\rangle) = |00\rangle \ {}_{1/2}{\oplus}\ |11\rangle \\ M_{\pm}(|\Phi^+\rangle) = |{+}{+}\rangle \ {}_{1/2}{\oplus}\ |{-}{-}\rangle \end{array}$$

A Quantum Process Algebra

Modelling and Comparing Quantum Concurrent Systems



Concurrent Processes + Communication Primitives + Nondeterministic Choices + Quantum Capable

lqCCS

$$P ::= \mathbf{0}_{\tilde{q}} \mid \tau.P \mid c!v.P \mid c?x.P \mid P + P \mid P \setminus c \mid P \parallel P \mid \textbf{if } e \textbf{ then } P \textbf{ else } P$$
$$\mid U(\tilde{e}).P \mid M_B(\tilde{e} \triangleright x).P$$

The semantics of $\langle\!| |\psi\rangle , P |\!\rangle \in \mathit{Conf}$ is a **NPLTS**

Nondeterministic **P**robabilistic **L**abelled **T**ransition **S**ystem

$$\langle \mathit{Conf}, \mathit{Act}, \rightarrow \subseteq \mathit{Conf} \times \mathit{Act} \times \mathcal{D}(\mathit{Conf})\rangle$$

Operational Semantics

The classical fragment... is quite standard

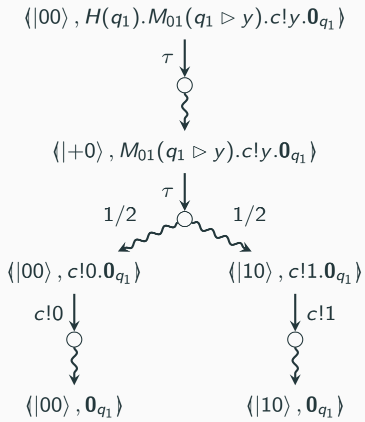
$$\frac{}{\langle\!|\, |\psi\rangle \,, \tau.P \,|\!\rangle \xrightarrow{\tau} \langle\!|\, |\psi\rangle \,, P \,|\!\rangle}\ \textsc{Tau} \qquad \frac{e \Downarrow v}{\langle\!|\, |\psi\rangle \,, c!e.P \,|\!\rangle \xrightarrow{c!v} \langle\!|\, |\psi\rangle \,, P \,|\!\rangle}\ \textsc{Send}$$

Together with the quantum operators

$$\frac{}{\langle\!|\, |\psi\rangle, U(\tilde{q}).P \,|\!\rangle \xrightarrow{\tau} \left\langle\!\left|\, U^{\tilde{q}}|\psi\rangle, P \,\right|\!\right\rangle}\ \textsc{QOp}$$

$$\frac{}{\left\langle\!\left|\, |\psi\rangle, M_{\{b_0,b_1\}}(\tilde{q} \triangleright y).P \,\right|\!\right\rangle \xrightarrow{\tau} \langle\!|\, |\phi_0\rangle \,, P[{}^{0}/_{y}] \,|\!\rangle \;{}_{p_{0,|\psi\rangle}}\!\oplus \langle\!|\, |\phi_1\rangle \,, P[{}^{1}/_{y}] \,|\!\rangle}\ \textsc{QMeas}$$

For Example


$\langle |00\rangle, H(q_1).M_{01}(q_1 \triangleright y).c!y.\mathbf{0}_{q_1} \rangle$
τ
$\langle |{+}0\rangle, M_{01}(q_1 \triangleright y).c!y.\mathbf{0}_{q_1} \rangle$
τ
$1/2$
$1/2$
$\langle |00\rangle, c!0.\mathbf{0}_{q_1} \rangle$
$\langle |10\rangle, c!1.\mathbf{0}_{q_1} \rangle$
$c!0$
$c!1$
$\langle |00\rangle, \mathbf{0}_{q_1} \rangle$
$\langle |10\rangle, \mathbf{0}_{q_1} \rangle$

Linear Type System for Qubits Names

$$\frac{\tilde{q} \in \tilde{\Sigma}}{\Sigma \vdash \langle\!\langle |\psi\rangle , \mathbf{0}_{\tilde{q}} \rangle\!\rangle}\ \textsc{Disc} \qquad \frac{e \in \Sigma \quad \Sigma \setminus \{e\} \vdash P}{\Sigma \vdash \langle\!\langle |\psi\rangle , c!e.P \rangle\!\rangle}\ \textsc{QSend}$$

$$\frac{\Sigma_1 \vdash P \quad \Sigma_2 \vdash Q \quad \Sigma = \Sigma_1 \cup \Sigma_2 \quad \Sigma_1 \cap \Sigma_2 = \emptyset}{\Sigma \vdash \langle\!\langle |\psi\rangle , P \parallel Q \rangle\!\rangle}\ \textsc{Par}$$

- Each qubit is either sent with $c!q$, or explicitly discarded with $\mathbf{0}_q$
- Single ownership implies *no-cloning theorem*

Tests

Tests

Tests $\mathbb{T}_G$ are defined as

$$T \coloneqq \omega \mid \mathbf{0} \mid \textbf{if } e \textbf{ then } T \textbf{ else } T \mid c?x.T \mid c!e.T \mid T + T \mid U(\tilde{e}).T \mid M(\tilde{e} \rhd x).T$$

The semantics of a lqCCS extended configuration $\langle\!\langle |\psi\rangle, P, T \rangle\!\rangle \in TConf$ is a

Non-deterministic **P**robabilistic **T**ransition **S**ystem (**NPTS**)

$$\mathcal{T} = (TConf, \rightarrow \subseteq TConf \times \mathcal{D}(TConf))$$

Testing Equivalence

Definition (Testing Equivalence)
$\langle\!|\,|\psi\rangle, P\,|\!\rangle \sim_{\mathbb{T}} \langle\!|\,|\phi\rangle, Q\,|\!\rangle$, if for every test $T \in \mathbb{T}$,

- for each resolution R_1, there exists a resolution R_2 such that

$$sp_{R_1}(\langle\!|\,|\psi\rangle, P, T\,|\!\rangle) = sp_{R_2}(\langle\!|\,|\phi\rangle, Q, T\,|\!\rangle)$$

- for each resolution R_2, there exists a resolution R_1 such that

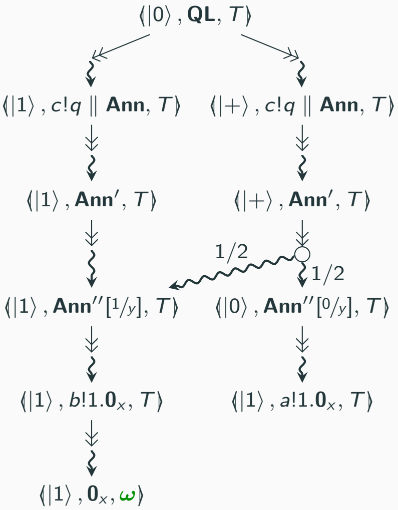
$$sp_{R_2}(\langle\!|\,|\phi\rangle, Q, T\,|\!\rangle) = sp_{R_1}(\langle\!|\,|\psi\rangle, P, T\,|\!\rangle)$$

Example: Quantum Lottery

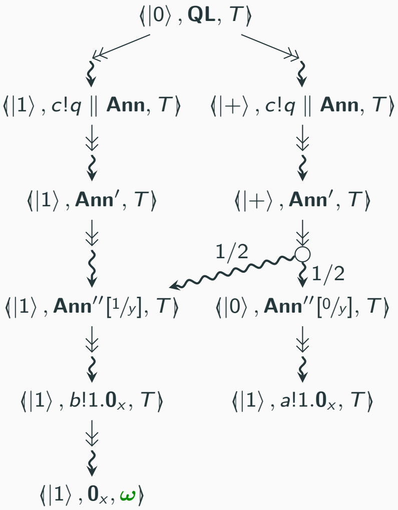
$$
\begin{aligned}
\textbf{State:}\ & |0\rangle \\
\textbf{Process:}\ & \mathbf{QL} = \mathit{Pre} \parallel \mathit{Ann} \\
& \qquad \mathbf{Pre} = (X(q).c!q.\mathbf{0}) + (H(q).c!q.\mathbf{0}) \\
& \qquad \mathbf{Ann} = c?x.M_{01}(x \triangleright y).\mathbf{if}\ y = 0\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x \\
\textbf{Test:}\ & T = b?x.\boldsymbol{\omega}
\end{aligned}
$$

- **Pre** prepares a qubit used as a source of randomness
- **Ann** receives and measure it, and announces the winner, Alice $a!1$ or Bob $b!1$
- The test is successful if Bob wins the lottery

Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)



Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)

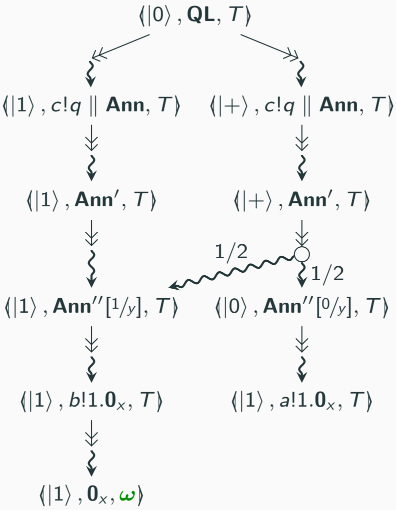


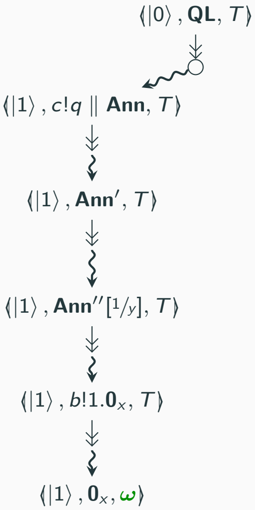
$$\mathbf{Ann} = c?x.M_{01}(x \triangleright y).\mathbf{if}\ y = 0\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x$$

$$\mathbf{Ann'} = M_{01}(x \triangleright y).\mathbf{if}\ y = 0\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x$$

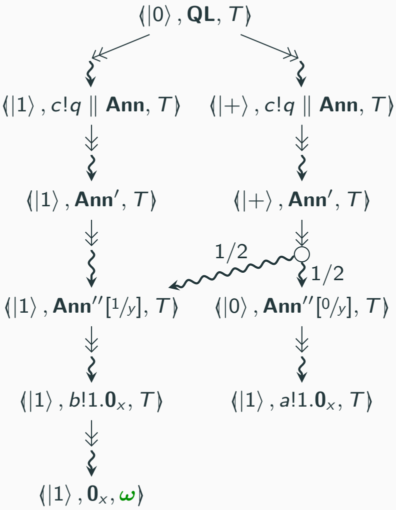
$$\mathbf{Ann''} = \mathbf{if}\ y = 0\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x$$

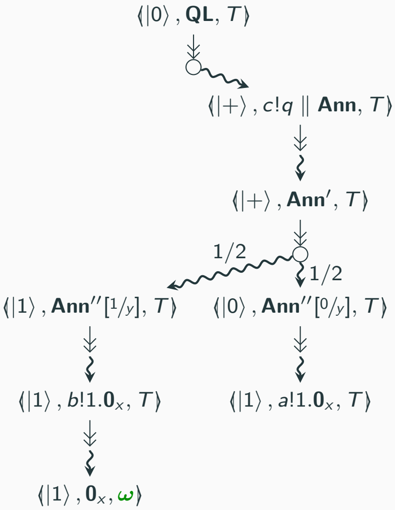
Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)



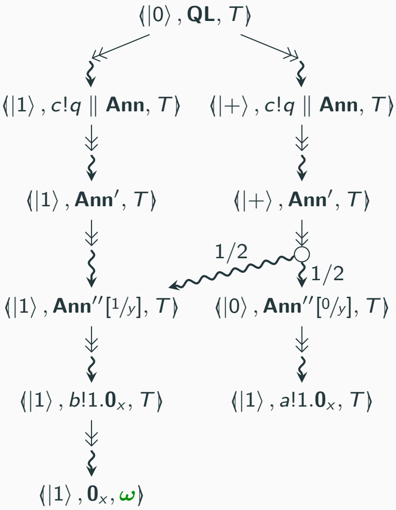


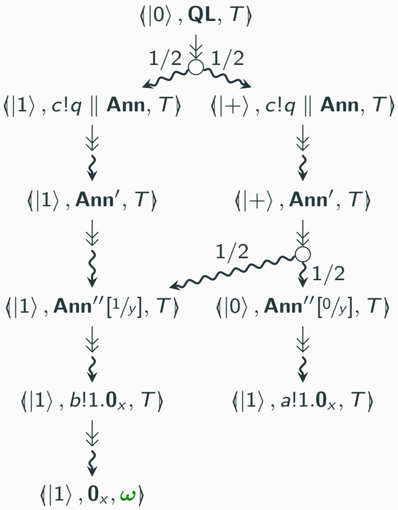
Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)





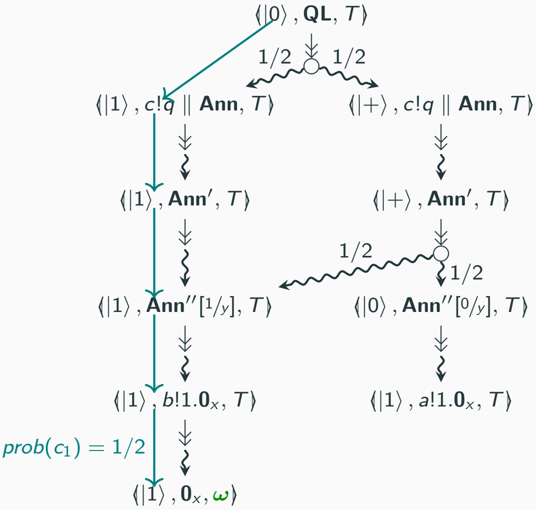
Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)



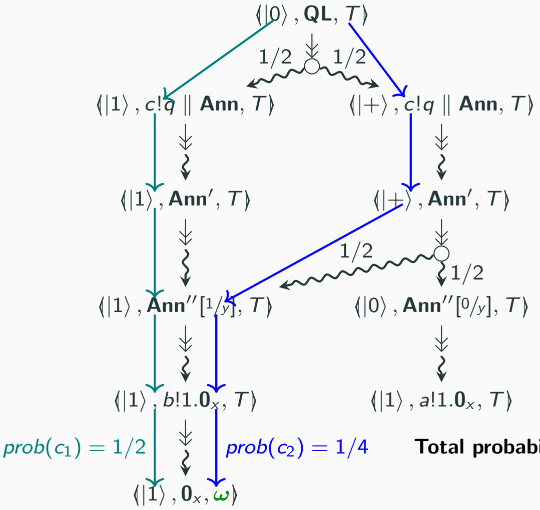


$$
\begin{tikzcd}[column sep=small]
 & \langle\!\langle |0\rangle, \mathbf{QL}, T \rangle\!\rangle \arrow[dl, squiggly, "1/2"'] \arrow[dr, squiggly, "1/2"] & \\
\langle\!\langle |1\rangle, c!q \parallel \mathbf{Ann}, T \rangle\!\rangle \arrow[d, squiggly] & & \langle\!\langle |+\rangle, c!q \parallel \mathbf{Ann}, T \rangle\!\rangle \arrow[d, squiggly] \\
\langle\!\langle |1\rangle, \mathbf{Ann}', T \rangle\!\rangle \arrow[d, squiggly] & & \langle\!\langle |+\rangle, \mathbf{Ann}', T \rangle\!\rangle \arrow[dll, squiggly, "1/2"'] \arrow[d, squiggly, "1/2"] \\
\langle\!\langle |1\rangle, \mathbf{Ann}''[1/y], T \rangle\!\rangle \arrow[d, squiggly] & & \langle\!\langle |0\rangle, \mathbf{Ann}''[0/y], T \rangle\!\rangle \arrow[d, squiggly] \\
\langle\!\langle |1\rangle, b!1.\mathbf{0}_x, T \rangle\!\rangle \arrow[d, squiggly] & & \langle\!\langle |1\rangle, a!1.\mathbf{0}_x, T \rangle\!\rangle \\
\langle\!\langle |1\rangle, \mathbf{0}_x, \boldsymbol{\omega} \rangle\!\rangle & &
\end{tikzcd}
$$

Example: Quantum Lottery Resolution (PTS) and its Computations

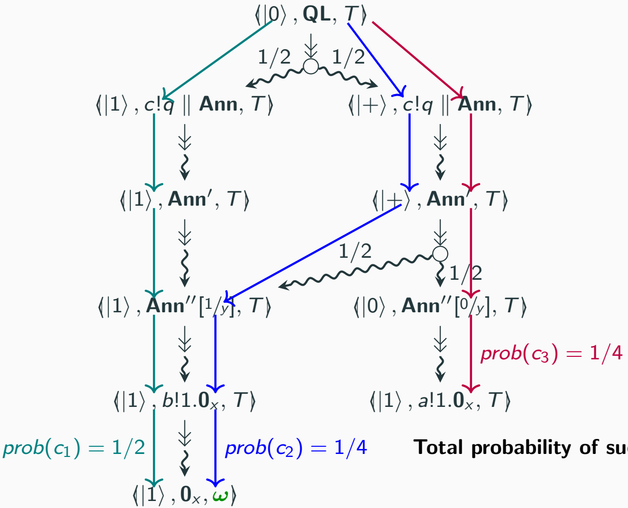


Example: Quantum Lottery Resolution (PTS) and its Computations



Total probability of success $3/4$

Example: Quantum Lottery Resolution (PTS) and its Computations



Total probability of success 3/4

The Problem of Non-deterministic Testing

A Missing Expected Equivalence

Take a pair of non-biased random qubit sources

- the first sends $|0\rangle$ or $|1\rangle$ (both with probability $1/2$)
- the second sends $|+\rangle$ or $|-\rangle$ (both with probability $1/2$)

Quantum theory prescribes that they cannot be distinguished by any observer, as the received qubits behave the same...

But they are distinguished by a non-deterministic test!

Formalizing the Counterexample

The two qubit sources in lqCCS

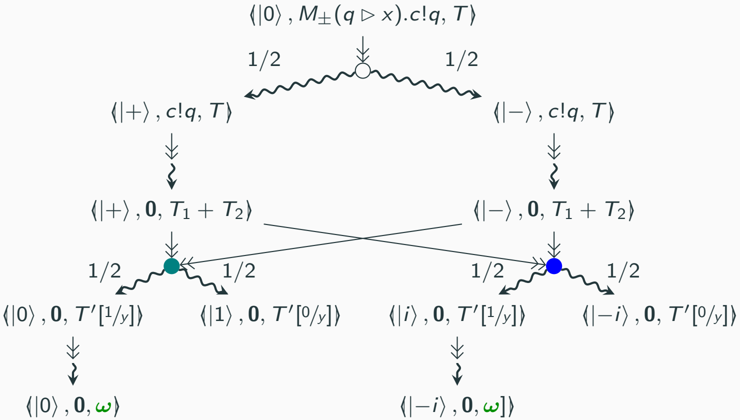
$$C_{01} = \langle |+\rangle, M_{01}(q \triangleright x).c!q \rangle \quad \text{and} \quad C_{\pm} = \langle |0\rangle, M_{\pm}(q \triangleright x).c!q \rangle$$

The distinguishing test $T = c?x.(T_1 + T_2)$ with

$$\begin{aligned} T_1 &= M_{01}(x \triangleright y).\textbf{if } y = 0 \textbf{ then } \omega \textbf{ else } \mathbf{0}, \text{ and} \\ T_2 &= M_{\pm i}(x \triangleright y).\textbf{if } y = 0 \textbf{ then } \omega \textbf{ else } \mathbf{0}. \end{aligned}$$

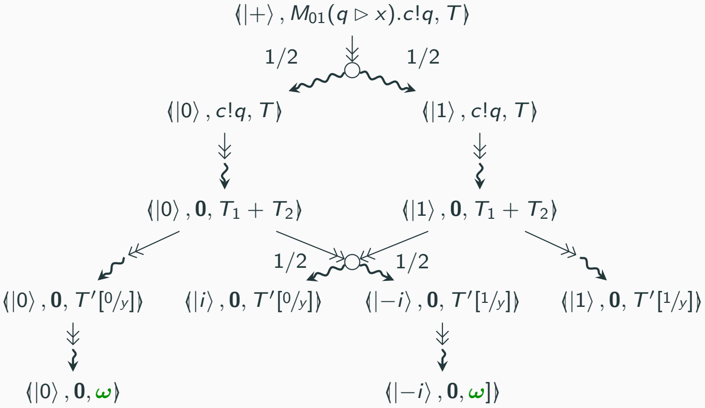
where $M_{\pm i}$ stands for the measurement $\{|i\rangle, |-i\rangle\}$.

Testing the Source of $|+\rangle$ and $|-\rangle$



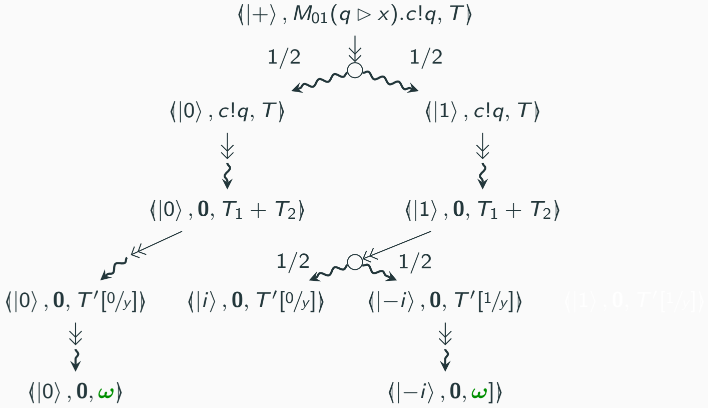
Choosing teal or blue is the same: for any resolution, success probability is $1/2$

Testing the Source of $|0\rangle$ and $|1\rangle$



For this resolution, the probability of success is 3/4!

Testing the Source of $|0\rangle$ and $|1\rangle$



For this resolution, the probability of success is $3/4$!

Why?

$$C_{01} \not\sim_{\mathbb{T}_G} C_{\pm}$$

- The reason of higher success for C_{01} is that we have chosen the measurement based on the quantum state of the received qubit
- But how do we know the state of the received qubit?
- Usually through a measurement... but we did not measure the qubit
- Being capable of inspecting qubits only though measurements is a defining constraint of quantum physics
- That is why in the real world you cannot discriminate these two processes!
- Do deterministic tests solve this problem?

Deterministic Tests

Definition (Deterministic Tests)
Let $\mathbb{T}_D \subsetneq \mathbb{T}_G$ be the set of deterministic tests, i.e. those that do not contain occurrences of the non-deterministic sum.

- They solve the counterexample presented before

$$C_{01} \not\sim_{\mathbb{T}_G} C_{\pm} \qquad\qquad C_{01} \sim_{\mathbb{T}_D} C_{\pm}$$

- The result can be generalized: deterministic tests do not distinguish distributions of states that behave the same according to quantum theory!

Lifting Indistinguishablity from Quantum Physics to lqCCS

Fact
Two distributions of quantum states $\Delta = \sum_i p_i \bullet |\psi_i\rangle$ and $\Theta = \sum_j q_j \bullet |\phi_j\rangle$ are indistinguishable, written $\Delta \cong \Theta$, if

$$\sum_{i \in I} p_i \cdot |\psi_i\rangle\langle\psi_i| = \sum_{j \in J} q_j \cdot |\phi_j\rangle\langle\phi_j|$$

Theorem
Given two distributions of quantum states $\Delta = \sum_i p_i \bullet |\psi_i\rangle$ and $\Theta = \sum_j q_j \bullet |\phi_j\rangle$ such that $\Delta \cong \Theta$, it holds that for any deterministic test $T \in \mathbb{T}_D$ and resolution R

$$\sum\nolimits_{i \in I} p_i \cdot sp_R(\langle\!\langle |\psi_i\rangle, \mathbf{0}, T \rangle\!\rangle) = \sum\nolimits_{j \in J} q_j \cdot sp_R(\langle\!\langle |\phi_j\rangle, \mathbf{0}, T \rangle\!\rangle)$$

Conclusions

Recap

- Process algebras can model concurrent quantum systems as NPLTSs where probabilities depend on a quantum state
- The standard approach of testing equivalence exceeds the observational limitations prescribed by quantum theory
- Non-determinism is the cause for this mismatch with the expected equivalences
- In a nutshell, it allows you to inspect the state of a qubit without performing a measurement, hence without altering it
- Forbidding non-deterministic tests suffices for recovering the expected indistinguishability

Some Pointers

We worked mainly on bisimilarities

- Saturated bisimilarity: constrained non-determinism in the contexts [POPL2024]
- Scheduled bisimilarity: non-determinism constrained in general [APLAS2024]
- Trace equivalence for quantum processes [WADT2024]
- Alternative, purely quantum model (pLTS $\rightarrow$ qLTS) [CONCUR2024, ACT2024]

Some Future Work

We plan to investigate

- The relation between our testing equivalence, trace equivalence and bisimilarities
- Abstract over the initial quantum state
- Tests with constrained non-determinism (preserving our correctness results)
- Logical characterization of these equivalence relations