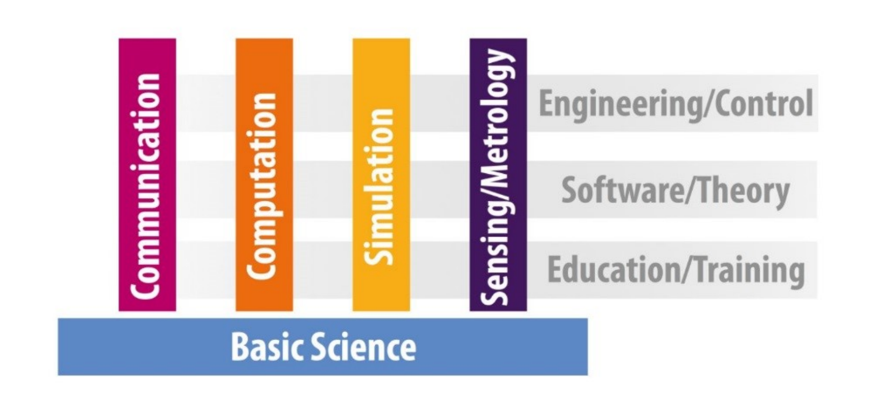
Testing Quantum Protocols

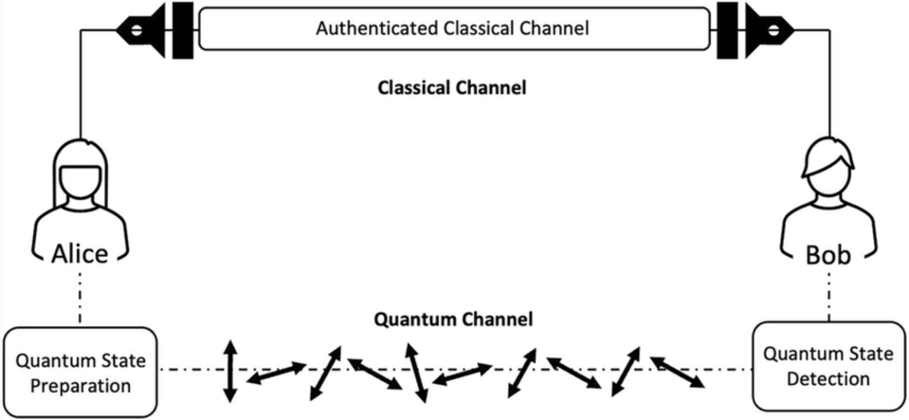
L. Ceragioli F. Gadducci G. Lomurno G. Tedeschi

Quantum Technologies



Why Quantum Communication

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


Authenticated Classical Channel
Classical Channel
Alice
Bob
Quantum Channel
Quantum State Preparation
Quantum State Detection

Modeling and Verifying Quantum Distributed Systems

We need:

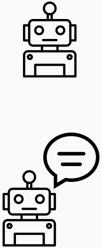
- Description language
- Semantic model
- Technique for checking correctness

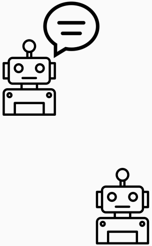
Process algebras have proven successful for modeling and verifying concurrent systems also with probabilities

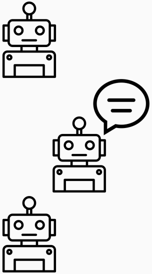
- We use them for modeling quantum concurrent systems
- We compare their behaviour using tests!

Testing Probabilistic Processes

Modelling and Comparing Concurrent Systems







Concurrent Processes + Communication Primitives + Nondeterministic Choices

Value Passing CCS

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

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

- $P + Q$ is the non-deterministic composition of P and Q
- $P \parallel Q$ is the parallel 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 $v = 0$, as Q if $v \neq 0$.

Operational Semantics

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

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

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

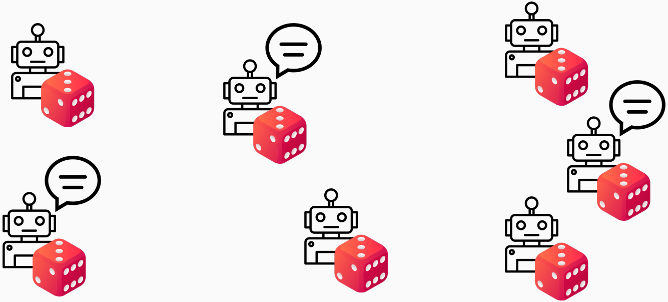
$$\frac{P \xrightarrow{\mu} P'}{P \parallel Q \xrightarrow{\mu} P' \parallel Q} \qquad \frac{P \xrightarrow{c!v} P' \quad Q \xrightarrow{c?v} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'} \qquad \frac{n = 0 \quad P \xrightarrow{\alpha} P'}{\textbf{if } n \textbf{ then } P \textbf{ else } Q \xrightarrow{\alpha}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

Example

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

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

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

Operational Semantics

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

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

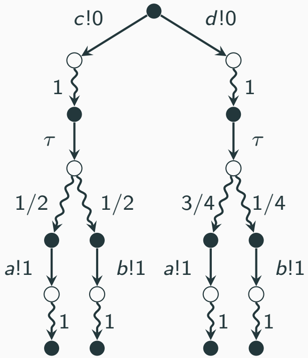
$$\frac{\Delta = \sum_{i \in I} p_i \cdot v_i}{M_\Delta(x).P \xrightarrow{\tau} \sum_{i \in I} p_i \cdot P[{}^{v_i}/_{x}]}$$

Example

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

$$+$$

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



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,

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

- Processes and tests evolve together $\langle P, T\rangle \xrightarrow{\tau} \langle P_1, T_1\rangle \xrightarrow{\tau} \ldots$
- After resolving **both non-determinism and probability**: two possible outcomes
  - $\ldots \xrightarrow{\tau} \langle P_n, \omega\rangle$ — **The test is successful**
  - all other cases — **The test fails**

Test Semantics

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

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

Example

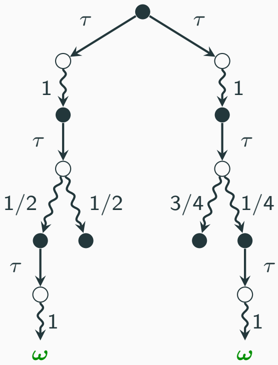
Process

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

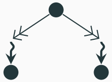
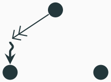
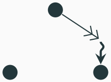
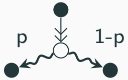
Test

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

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



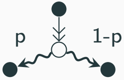
Resolving Non-determinism

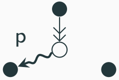
From  to  or  or 

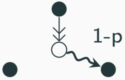
Definition (Resolution though randomized schedulers)
Given an NPTS $(S, \rightarrow)$, a *resolution* R is a PTS $(S, \rightarrow_R)$ such that for every $s \in S$

- 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

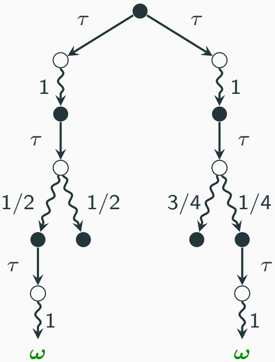
$$c = \langle P_0, T_0 \rangle \xrightarrow{\tau}_R \langle P_1, T_1 \rangle, \cdots, \langle P_{n-1}, T_{n-1} \rangle \xrightarrow{\tau}_R \langle P_n, T_n \rangle$$

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 $\langle P_{i-1}, T_{i-1} \rangle \xrightarrow{\tau}_R \Delta_i$.

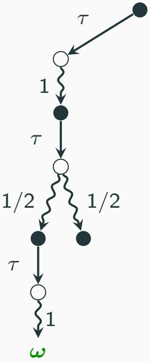
- We say that c is *maximal* if it is not a proper prefix of any other computation
- The *probability* of c is $prob(c) = \prod_{i=1}^{n} \Delta_i(P_i, T_i)$

Example

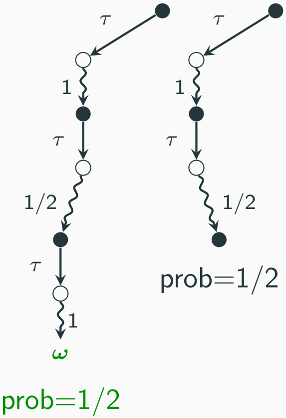
Evolution of $\langle P, T \rangle$



A resolution



Resolution's traces (with probability)



Success Probability

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

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

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 $\langle\!\langle P', \boldsymbol{\omega} \rangle\!\rangle$.

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

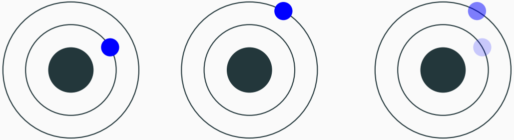
States of a Quantum System

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 $B_{01} \iff B_{\pm}$

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

$$H|0\rangle = |+\rangle$$
$$H|1\rangle = |-\rangle$$
$$H|+\rangle = |0\rangle$$
$$H|-\rangle = |1\rangle$$

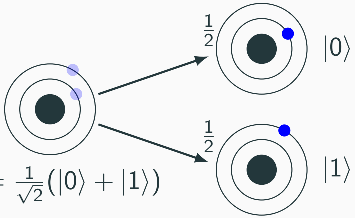
Projective Measurements

M_b is the **measurement** on the basis B_b: it returns a probabilistic result

- a resulting **state** in B_b
- the **classical outcome**

We consider: $M_{01}, M_{\pm}, M_{\pm i}$

- measuring $|0\rangle$ in M_{01} gives $|0\rangle$
- measuring $|0\rangle$ in $M_{\pm}$ gives $|+\rangle \ {}_{1/2}{\oplus}\ |-\rangle$
- measuring $|+\rangle$ in $M_{\pm}$ gives $|+\rangle$
- measuring $|+\rangle$ in M_{01} gives $|0\rangle \ {}_{1/2}{\oplus}\ |1\rangle$



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

Qubits cannot be observed without affecting their state!

A Remark on Measurement

Assume $|\psi\rangle$ is one of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$.

How can you know which one?

- You can try with M_{01}, but maybe $|\psi\rangle$ is in $\{|+\rangle, |-\rangle\}$
- You can try with $M_{\pm}$, but maybe $|\psi\rangle$ is in $\{|0\rangle, |1\rangle\}$

In both cases you may get useless information from the measurement and **destroy** the original state of the qubit

Measurement cannot discriminate with arbitrary precision!

Composite Quantum Systems

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

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

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

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

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!

Entanglement

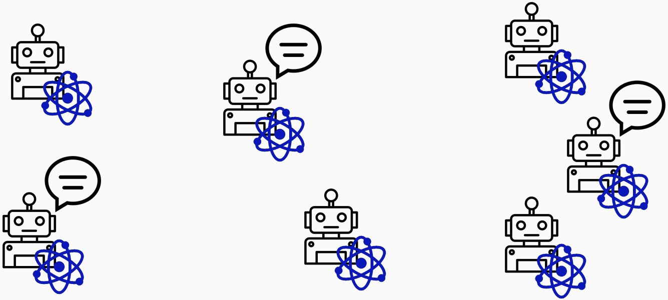
A state that cannot be the product of two smaller states

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

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

where U is a unitary transformation and M_B is a measurement on the basis B

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

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

Together with the quantum operators

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

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

For Example

$$
\begin{tikzcd}[column sep=small]
 & \langle\!\langle \left|00\right\rangle , H(q_1).M_{01}(q_1 \triangleright y).c!y.\mathbf{0}_{q_1} \rangle\!\rangle \arrow[d, "\tau"'] & \\
 & \circ \arrow[d, rightsquigarrow] & \\
 & \langle\!\langle \left|+0\right\rangle , M_{01}(q_1 \triangleright y).c!y.\mathbf{0}_{q_1} \rangle\!\rangle \arrow[d, "\tau"'] & \\
 & \circ \arrow[dl, rightsquigarrow, "1/2"'] \arrow[dr, rightsquigarrow, "1/2"] & \\
\langle\!\langle \left|00\right\rangle , c!0.\mathbf{0}_{q_1} \rangle\!\rangle \arrow[d, "c!0"'] & & \langle\!\langle \left|10\right\rangle , c!1.\mathbf{0}_{q_1} \rangle\!\rangle \arrow[d, "c!1"] \\
\circ \arrow[d, rightsquigarrow] & & \circ \arrow[d, rightsquigarrow] \\
\langle\!\langle \left|00\right\rangle , \mathbf{0}_{q_1} \rangle\!\rangle & & \langle\!\langle \left|10\right\rangle , \mathbf{0}_{q_1} \rangle\!\rangle
\end{tikzcd}
$$

Problem with Cloning Qubits

$$\begin{array}{c}
\langle |0\rangle\,, c!q_1.d!q_1 \parallel c?x.P \parallel d?x.Q \rangle \\
\tau \downarrow \\
\circ \\
\rightsquigarrow \\
\langle |0\rangle\,, d!q_1 \parallel P[{}^{q_1}/_{x}] \parallel d?x.Q \rangle \\
\tau \downarrow \\
\circ \\
\rightsquigarrow \\
\langle |0\rangle\,, \mathbf{0} \parallel P[{}^{q_1}/_{x}] \parallel Q[{}^{q_1}/_{x}] \rangle
\end{array}$$

This process is not physically implementable

- Sends q_1 along both c and d
- Requires copying the qubit state
- Contradicts the no-cloning theorem

Linear Type System for Qubits Names

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

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

- Each qubit is either sent just once 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

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

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

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

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

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

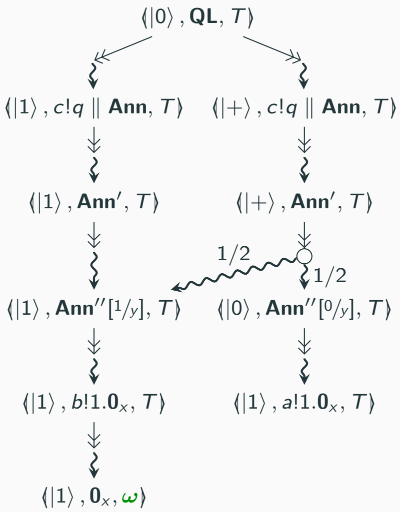
$$sp_{R_2}(\langle\!\langle |\phi\rangle, Q, T \rangle\!\rangle) = sp_{R_1}(\langle\!\langle |\psi\rangle, P, T \rangle\!\rangle)$$

Example: Quantum Lottery

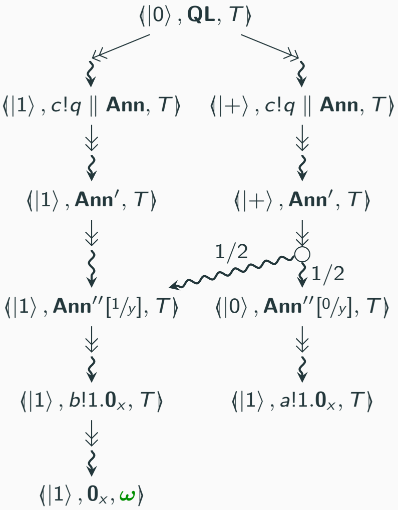
$$
\begin{aligned}
\textbf{State:}\quad & |0\rangle \\
\textbf{Process:}\quad & \mathbf{QL} = \mathit{Pre} \parallel \mathit{Ann} \\
& \quad \mathbf{Pre} = (X(q).c!q.\mathbf{0}) + (H(q).c!q.\mathbf{0}) \\
& \quad \mathbf{Ann} = c?x.M_{01}(x \triangleright y).\mathbf{if}\ y\ \mathbf{then}\ a!1.\mathbf{0}_x\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

- **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)



Ann

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

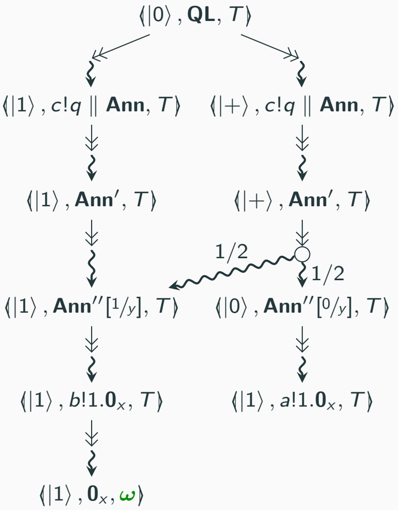
Ann'

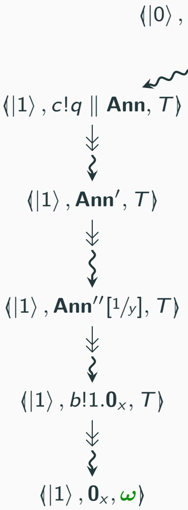
$M_{01}(x \rhd y).\mathbf{if}\ y\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x$

Ann''

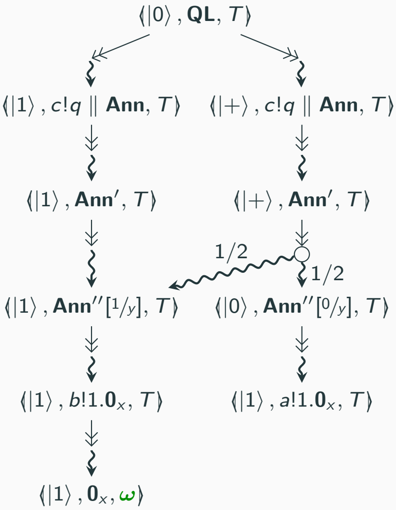
$\mathbf{if}\ y\ \mathbf{then}\ a!1.\mathbf{0}_x\ \mathbf{else}\ b!1.\mathbf{0}_x$

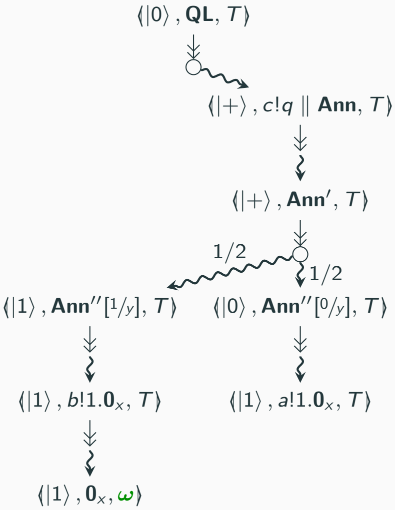
Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)



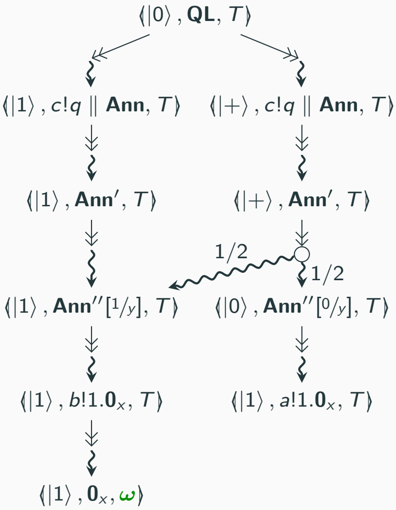


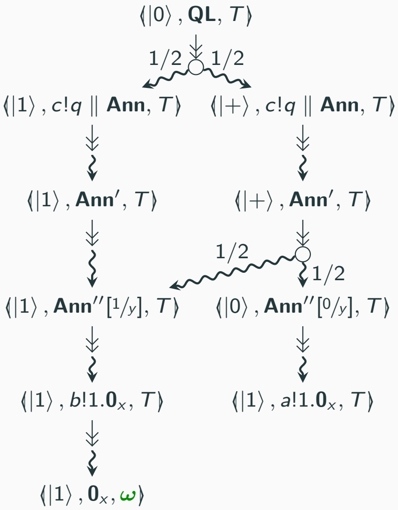
Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)





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

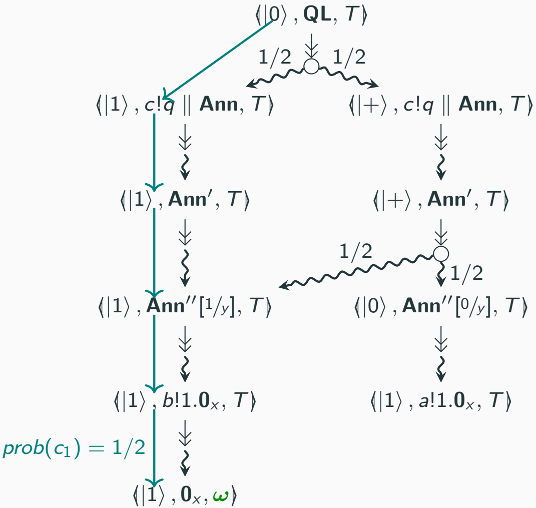




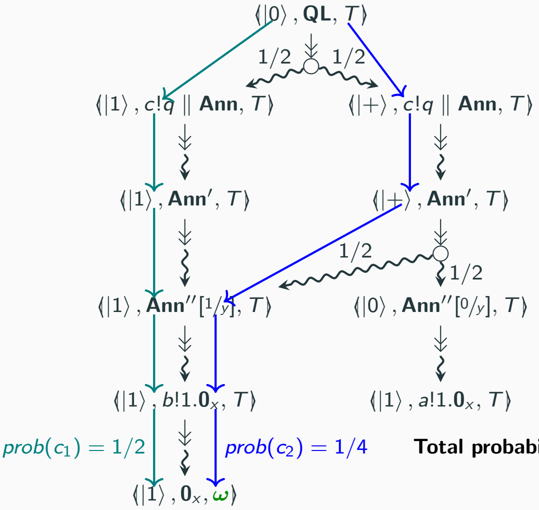
Example: Quantum Lottery Resolution (PTS) and its Computations

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

Example: Quantum Lottery Resolution (PTS) and its Computations

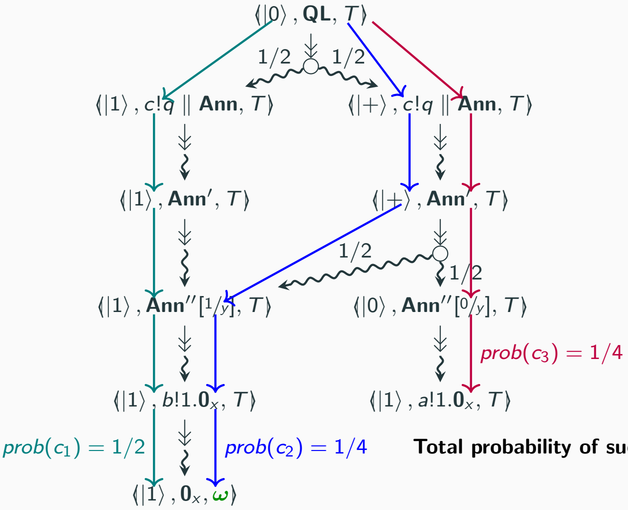


Example: Quantum Lottery Resolution (PTS) and its Computations



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

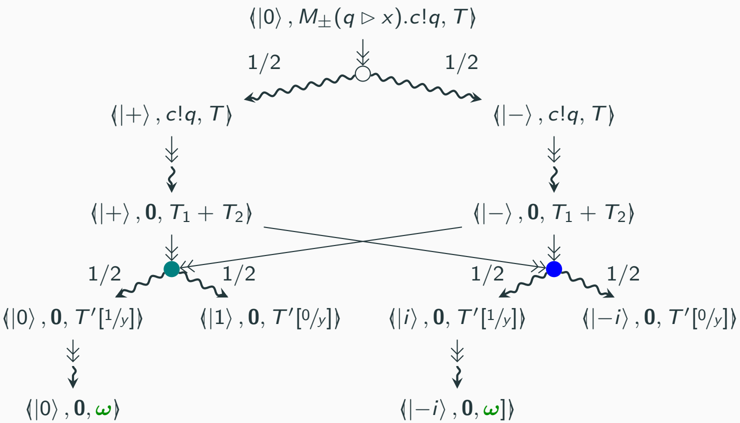
$$C_{01} = \langle\!\langle |+\rangle , M_{01}(q \triangleright x).c!q \rangle\!\rangle \quad \text{and} \quad C_{\pm} = \langle\!\langle |0\rangle , M_{\pm}(q \triangleright x).c!q \rangle\!\rangle$$

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

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

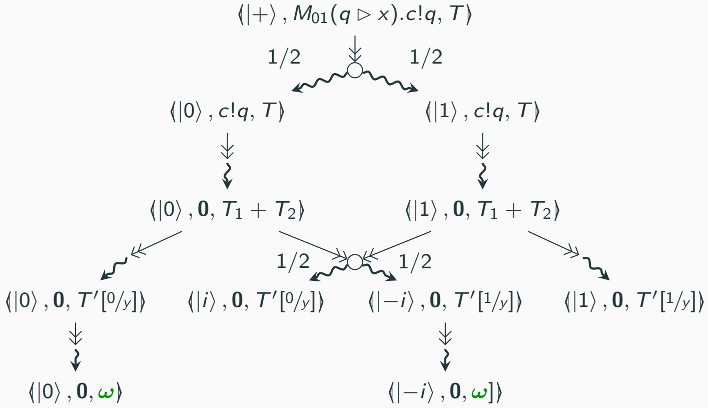
where $M_{\pm i}$ stands for the measurement $\{|i\rangle , |-i\rangle\}$.

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



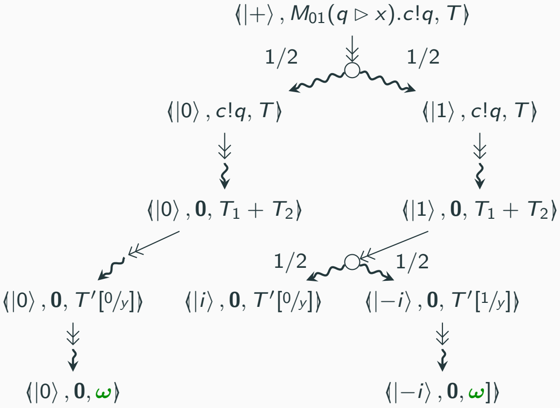
Choosing teal or blue is the same: for any resolution, success probability is $1/2$

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?

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

- 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!

Forbid Non-Determinism in 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 process* P*,* $\Delta' \sim_{\mathbb{T}_D} \Theta'$*, with*

$$\Delta' = \sum\nolimits_{i \in I} p_i \cdot \langle\!\langle |\psi_i\rangle , P \rangle\!\rangle \qquad \Theta' = \sum\nolimits_{j \in J} q_j \cdot \langle\!\langle |\phi_j\rangle , P \rangle\!\rangle$$

Real World Impact with a Simple Example

Quantum Coin Tossing Protocol

- Alice and Bob want to select a **winner at random**
- They do not trust each other and have no trusted third part
- Alice starts the protocol, and Bob replies

Desiderata: if one does not follow the protocol, his success probability must not increase

Analysis Results	
unconstrained non-determinism	**constrained** non-determinism
Bob can cheat and always win!	**Alice** can cheat and always win!

Conclusions

Recap

- Process algebras and transition systems can model concurrent quantum systems
- The standard approach of testing equivalence exceeds the observational limitations prescribed by quantum theory
- Non-determinism is the cause for this problem
- 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]
- Testing equivalence for quantum processes [ISOLA2024]
- 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