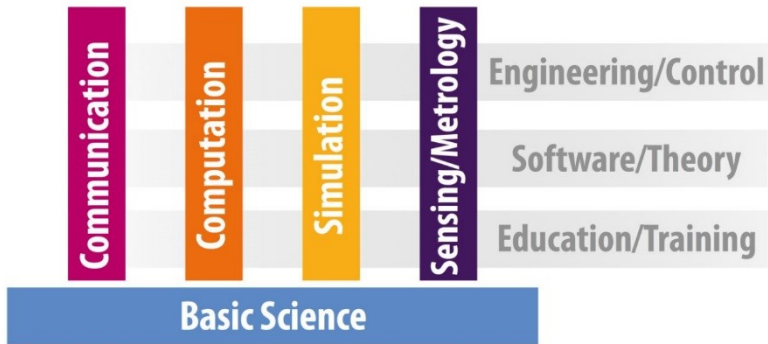


# Testing Quantum Protocols

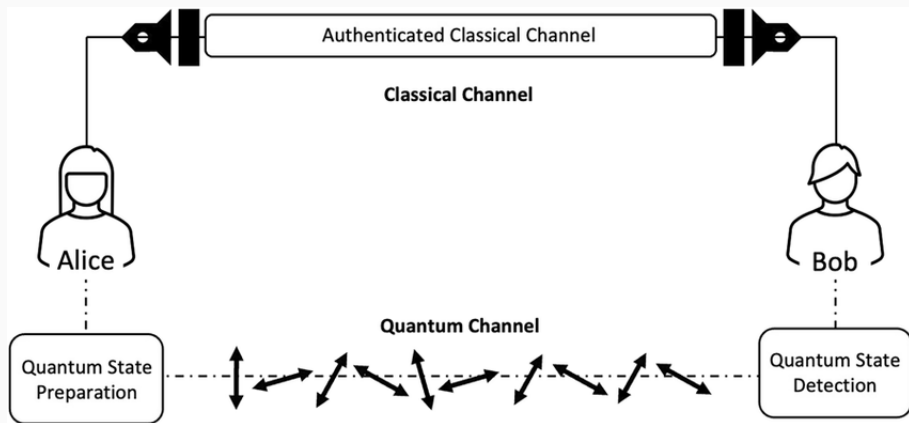
---

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



# Why Quantum Communication

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



# Modeling and Verifying Quantum Distributed Systems

We need:

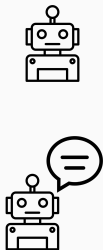
- Description language
- Semantic model
- Technique for checking correctness

We use **Process Algebras** and **Testing Equivalence** – successful for modeling and verifying concurrent systems also with probabilities

# Probabilistic Processes

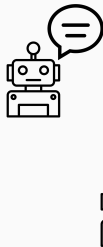
---

# Modelling and Comparing Concurrent Systems



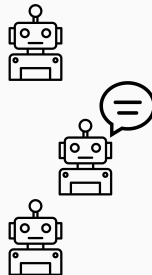
Concurrent  
Processes

+



Communication  
Primitives

+



Nondeterministic  
Choices

# Value Passing CCS

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

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

- $P + Q$  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  $v$  on channel  $c$
- $\mathbf{if} \ v \ \mathbf{then} \ P \ \mathbf{else} \ Q$  behaves as  $P$  if  $v = 0$ , as  $Q$  if  $v \neq 0$ .



# Operational Semantics

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

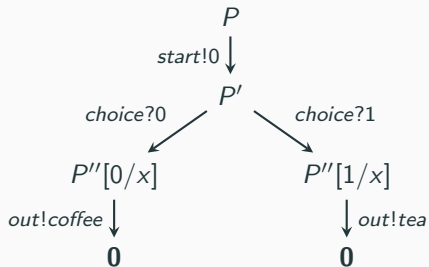
$$\frac{}{c!v.P \xrightarrow{c!v} P} \quad \frac{}{c?x.P \xrightarrow{c?v} P[v/x]}$$

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

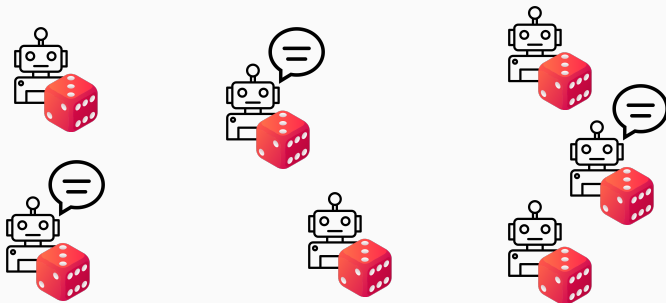
$$\frac{P \xrightarrow{\mu} P'}{P \parallel Q \xrightarrow{\mu} P' \parallel Q} \quad \frac{P \xrightarrow{c!v} P' \quad Q \xrightarrow{c?v} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'} \quad \frac{n = 0 \quad P \xrightarrow{\alpha} P'}{\text{if } n \text{ then } P \text{ else } Q \xrightarrow{\alpha}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

## Example

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



# 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  $[0, 1]$

$$D(x) = \left\{ \Delta : X \rightarrow [0, 1] \mid \sum_{x \in X} \Delta(x) = 1, [\Delta] \text{ is finite} \right\}$$

where  $[\Delta] = \{x \in X \mid \Delta(x) \neq 0\}$

**Point distribution:**

$$\bar{x}(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise} \end{cases} \quad \dots \text{we will often write } x \text{ for } \bar{x}$$

**Convex combination:**

$$(\Delta \oplus_p \Theta)(y) = p(\Delta(y)) + (1 - p)(\Theta(y))$$

# A Probabilistic Version of CCS

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

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

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

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

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

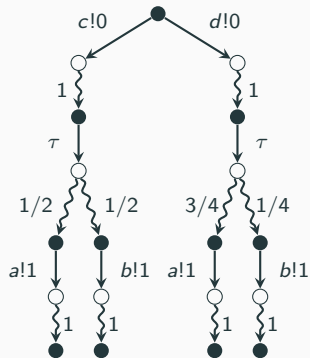
$$\frac{\Delta = \sum_{i \in I} p_i \cdot v_i}{M_{\Delta}(x).P \xrightarrow{\tau} \sum_{i \in I} p_i \cdot P[v_i/x]}$$

## Example

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

+

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



# Testing Equivalence in a Nutshell

How to check if two processes are equivalent?

Consider:

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

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

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



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

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

# Example

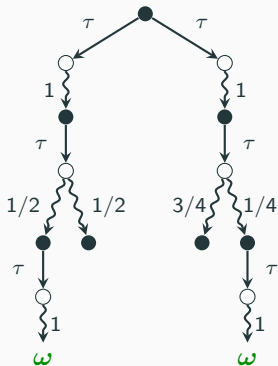
## Process

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

## Test

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

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



# Resolving Non-determinism



## Definition (Resolution through 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



## 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

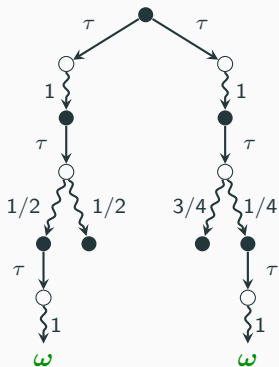
$$c = \langle P_0, T_0 \rangle \xrightarrow{\tau}_R \langle P_1, T_1 \rangle, \dots, \langle P_{n-1}, T_{n-1} \rangle \xrightarrow{\tau}_R \langle P_n, T_n \rangle$$

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

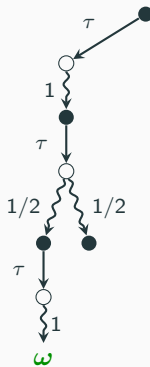
- We say that  $c$  is *maximal* if it is not a proper prefix of any other computation
- The *probability* of  $c$  is  $\text{prob}(c) = \prod_{i=1}^n \Delta_i(P_i, T_i)$

# Example

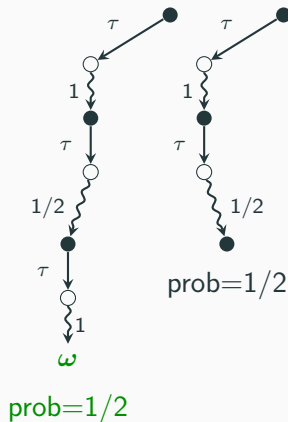
Evolution of  $\langle P, T \rangle$



A resolution



Resolution's traces  
(with probability)



## Definition (Success probability)

Given  $P$ ,  $T$  and  $R$ ,

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

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

## 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

---



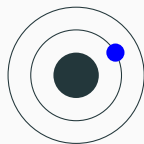
# States of a Quantum System

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

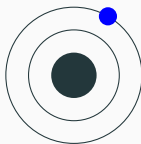
For **bits**: two *classical states* 0 and 1

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

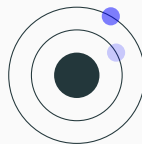
$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{with amplitudes } \alpha, \beta \in \mathbb{C} \text{ such that } |\alpha|^2 + |\beta|^2 = 1$$



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



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



$$\frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} |1\rangle$$

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

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

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

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

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

# Programmers use Unitary Transformations to Change the Qubits State

## Quantum bit flip

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

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

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

$$|0\rangle \xleftrightarrow{X} |1\rangle$$

## Basis mapping $B_{01} \iff B_{\pm}$

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

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

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

$$|0\rangle \xleftrightarrow{H} |+\rangle$$

$$|1\rangle \xleftrightarrow{H} |-\rangle$$

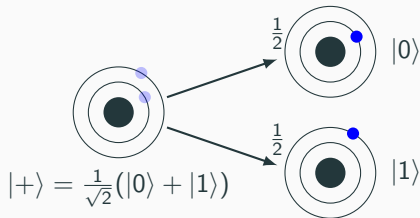
# Projective Measurements

$M_b$  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  $|+\rangle \frac{1}{\sqrt{2}} \oplus |-\rangle$
- measuring  $|+\rangle$  in  $M_{\pm}$  gives  $|+\rangle$
- measuring  $|+\rangle$  in  $M_{01}$  gives  $|0\rangle \frac{1}{\sqrt{2}} \oplus |1\rangle$



**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 *kroncker 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  $\forall |\phi_1\rangle, |\phi_2\rangle. |\psi\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$

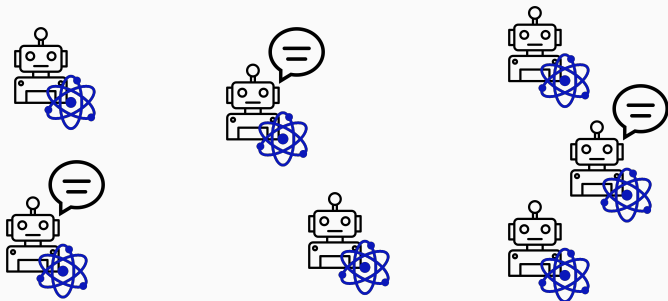
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \implies \begin{aligned} M_{01}(|\Phi^+\rangle) &= |00\rangle_{1/2} \oplus |11\rangle \\ M_{\pm}(|\Phi^+\rangle) &= |++\rangle_{1/2} \oplus |--\rangle \end{aligned}$$



# A Quantum Process Algebra

---

# Modelling and Comparing Quantum Concurrent Systems



Concurrent  
Processes

+

Communication  
Primitives

+

Nondeterministic  
Choices

+

Quantum  
Capable

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

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

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

**N**ondeterministic **P**robabilistic **L**abelled **T**ransition **S**ystem

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

The classical fragment... is quite standard

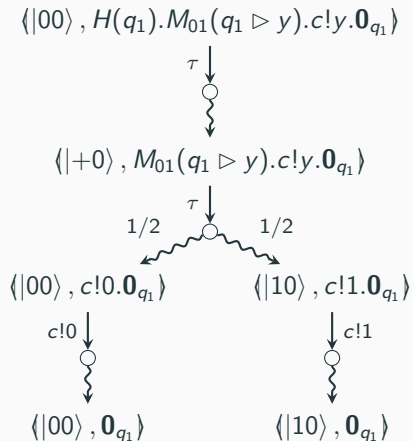
$$\frac{}{\langle |\psi\rangle, \tau.P \rangle \xrightarrow{\tau} \langle |\psi\rangle, P \rangle} \quad \frac{e \Downarrow v}{\langle |\psi\rangle, c!e.P \rangle \xrightarrow{c!v} \langle |\psi\rangle, P \rangle}$$

Together with the quantum operators

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

$$\frac{}{\langle |\psi\rangle, M_{\{b_0, b_1\}}(\tilde{q} \triangleright y).P \rangle \xrightarrow{\tau} \langle |\phi_0\rangle, P[0/y] \rangle_{\rho_0, |\psi\rangle} \oplus \langle |\phi_1\rangle, P[1/y] \rangle}$$

## For Example



## Problem with Cloning Qubits

$$\langle |0\rangle, c!q_1.d!q_1 \parallel c?x.P \parallel d?x.Q \rangle$$



$$\langle |0\rangle, d!q_1 \parallel P[q_1/x] \parallel d?x.Q \rangle$$



$$\langle |0\rangle, \mathbf{0} \parallel P[q_1/x] \parallel Q[q_1/x] \rangle$$

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

$$\frac{\tilde{q} \in \tilde{\Sigma}}{\Sigma \vdash \langle |\psi\rangle, \mathbf{0}_{\tilde{q}} \rangle} \text{DISC} \qquad \frac{e \in \Sigma \quad \Sigma \setminus \{e\} \vdash P}{\Sigma \vdash \langle |\psi\rangle, c!e.P \rangle} \text{QSEND}$$
$$\frac{\Sigma_1 \vdash P \quad \Sigma_2 \vdash Q \quad \Sigma = \Sigma_1 \cup \Sigma_2 \quad \Sigma_1 \cap \Sigma_2 = \emptyset}{\Sigma \vdash \langle |\psi\rangle, P \parallel Q \rangle} \text{PAR}$$

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

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

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

**Non-deterministic Probabilistic Transition System (NPTS)**

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

## 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

**State:**  $|0\rangle$

**Process:**  $QL = Pre \parallel Ann$

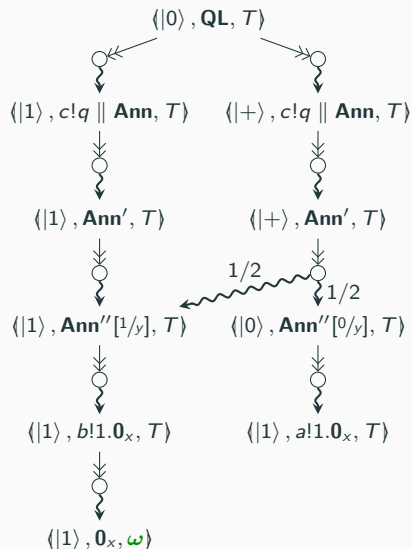
$Pre = (X(q).c!q.0) + (H(q).c!q.0)$

$Ann = c?x.M_{01}(x \triangleright y).if\ y\ then\ a!1.0_x\ else\ b!1.0_x$

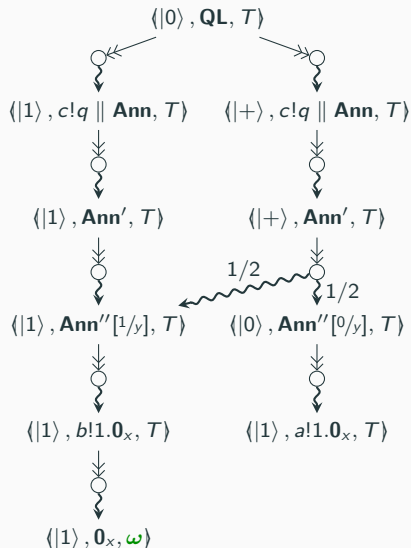
**Test:**  $T = b?x.\omega$

- **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**

$c?x.M_{01}(x \triangleright y). \text{if } y \text{ then } a!1.0_x \text{ else } b!1.0_x$

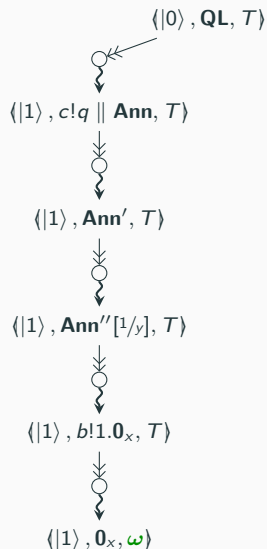
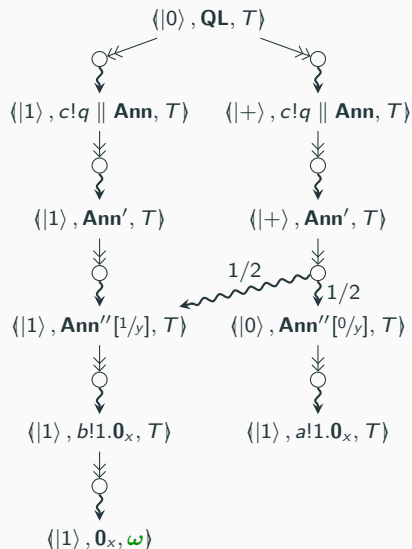
**Ann'**

$M_{01}(x \triangleright y). \text{if } y \text{ then } a!1.0_x \text{ else } b!1.0_x$

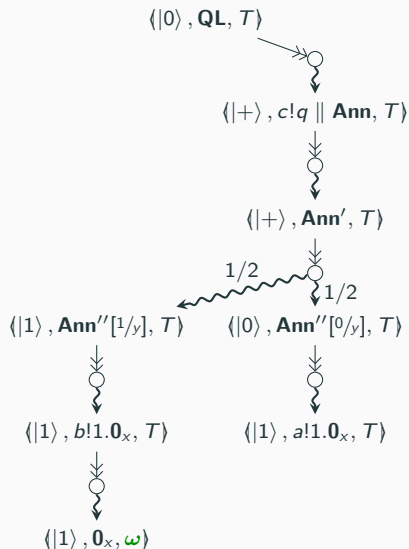
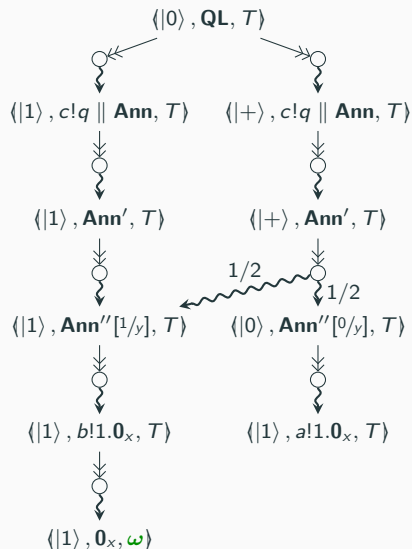
**Ann''**

$\text{if } y \text{ then } a!1.0_x \text{ else } b!1.0_x$

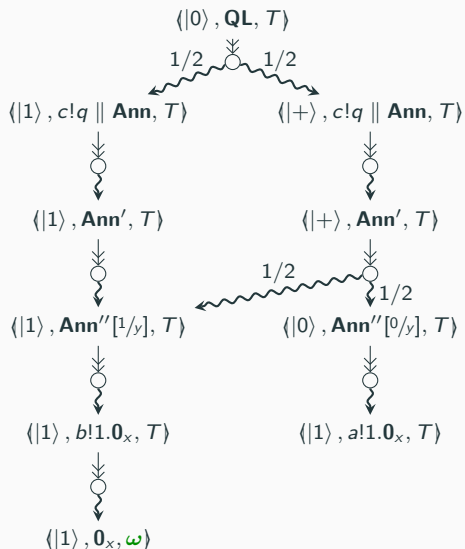
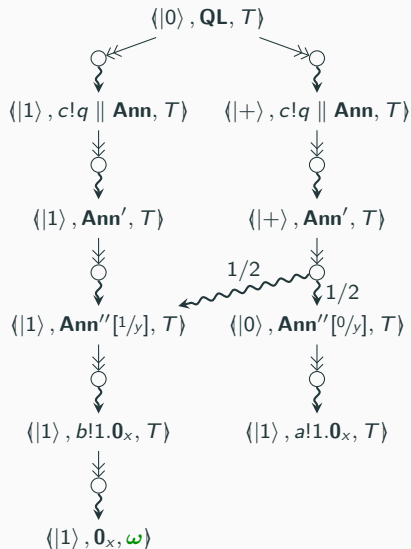
# Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)



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

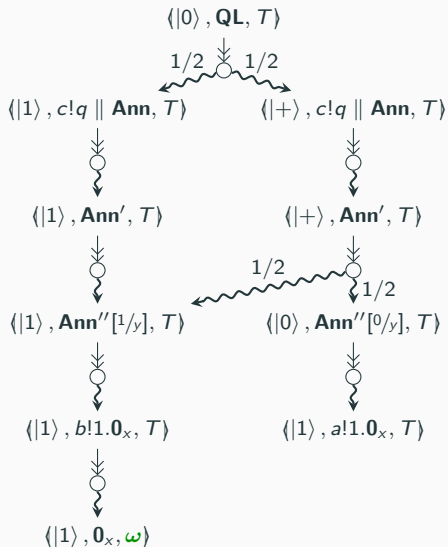


# Example: Quantum Lottery Semantics (NPTS) — and a Resolution (PTS)

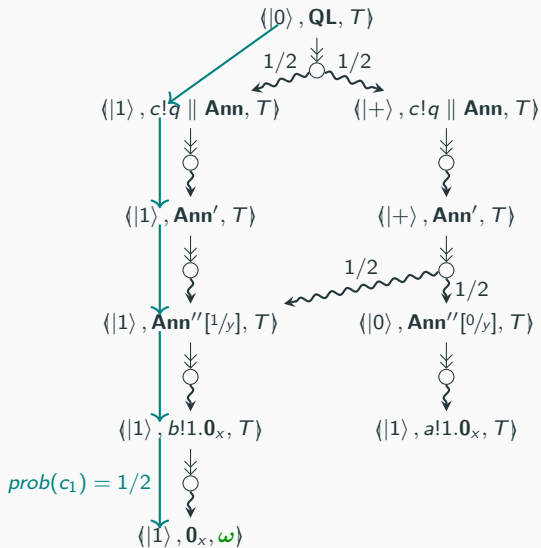




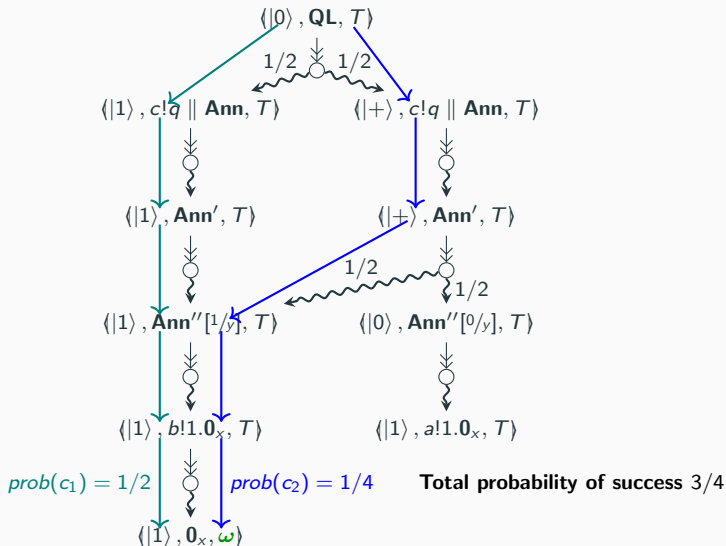
# Example: Quantum Lottery Resolution (PTS) and its Computations



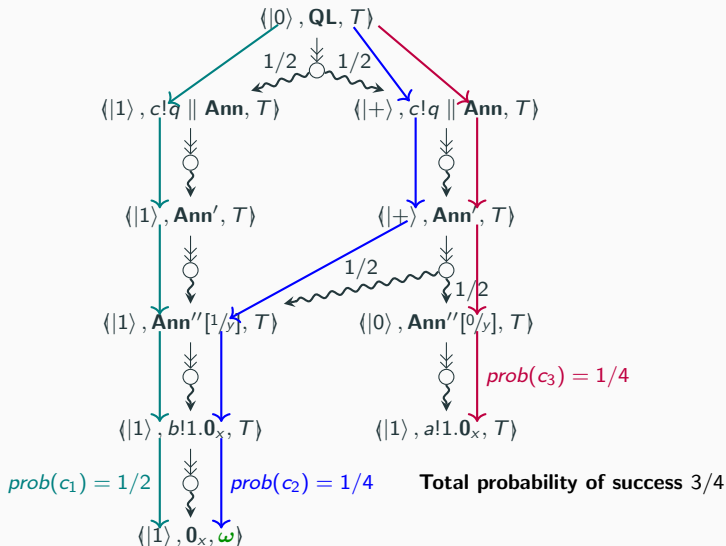
# Example: Quantum Lottery Resolution (PTS) and its Computations



# Example: Quantum Lottery Resolution (PTS) and its Computations



# Example: Quantum Lottery Resolution (PTS) and its Computations



# The Problem of Non-determinism

---

## 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

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

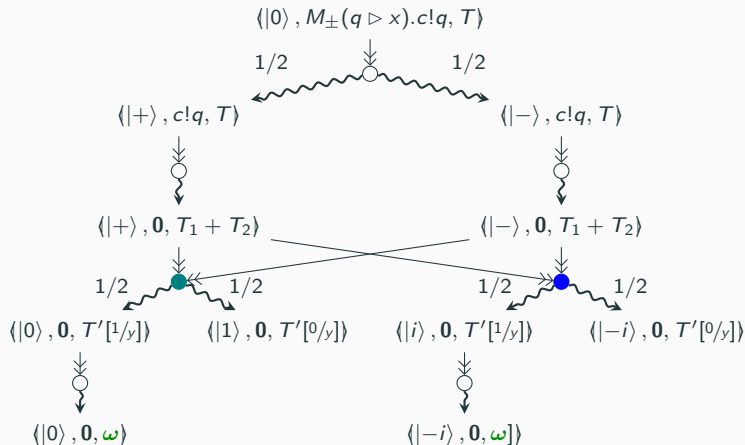
The distinguishing test  $T = c?x.(T_1 + T_2)$  with

$$T_1 = M_{01}(x \triangleright y).\text{if } y \text{ then } \omega \text{ else } 0, \text{ and}$$

$$T_2 = M_{\pm i}(x \triangleright y).\text{if } y \text{ then } \omega \text{ else } 0.$$

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

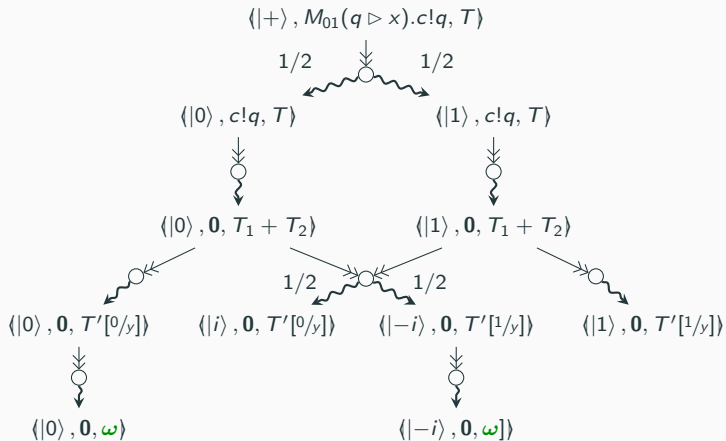
## Testing the Source of $|+\rangle$ and $|-\rangle$



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

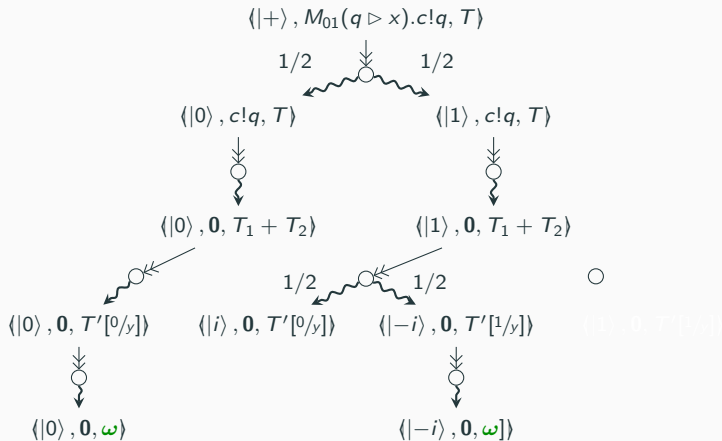


## Testing the Source of $|0\rangle$ and $|1\rangle$



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?

$$C_{01} \not\sim_{T_G} C_{\pm}$$

- 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 through 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

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

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

# Lifting Indistinguishability 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

$$\Delta' = \sum_{i \in I} p_i \cdot \langle |\psi_i\rangle, P \rangle \quad \Theta' = \sum_{j \in J} q_j \cdot \langle |\phi_j\rangle, P \rangle$$

# 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
<b>Bob</b> can cheat and always win!	<b>Alice</b> can cheat and always win!

## Conclusions

---

- **Process algebras** 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: 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**



## 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]

### We plan to investigate

- The relation between our testing equivalence, trace equivalence and bisimilarities
- Decidable and Symbolic approaches
- Constrained non-determinism (preserving our correctness results)
- Logical characterization of these equivalence relations

# Special Collection Call for Papers

Quantum-Centric  
Supercomputing

*International Journal of Networked and  
Distributed Computing*

Dr. Alessandro Berti , Giuseppe Bisicchia,  
Alessandro Poggiali, Gabriele Tedeschi

