**University of Pisa**

DEPARTMENT OF COMPUTER SCIENCE
Master Degree in Computer Science

# Exploring Quantum Process Calculi via barbs and contexts

Thesis supervisor:
**Prof. Fabio Gadducci**

Thesis co-supervisor:
**Dr. Lorenzo Ceragioli**

Candidate:
**Gabriele Tedeschi**

**Academic Year 2021-2022**

## Abstract

With the development of quantum communication protocols, numerous *quantum process calculi* have been proposed, but none as emerged has an accepted standard. Moreover, an established notion of behavioural equivalence is still missing. In this work we present a new asynchronous calculus, *Linear qCCS*, featuring a linear type system and two novel bisimilarity relations. Our language allows to directly compare the semantics of previous proposals, and investigate which notion of behavioural equivalence is most consistent with the quantum mechanical rules. One of the main result is that the usual and well-accepted definition of probabilistic bisimilarity is not appropriate for the quantum setting. Hence we introduce quantum saturated bisimilarity, which adequately formalize the observable properties of quantum systems. Finally, we also explore a foundational approach, presenting a *Minimal Quantum Process Algebra*, in order to investigate, in a minimal framework, the essential characteristics of communicating quantum systems. For this model we define a symbolic semantics, where the probabilistic behaviour of each process is 'parametric' with respect to its input quantum values.

# Contents

# Chapter 1

# Introduction

Quantum computing exploits non-classical phenomena described by quantum mechanics, such as entanglement and superposition, to perform computations, often with considerable speedup with respect to classical computers.

Both theory and practical implementations have attracted considerable research efforts in the last forty years. Different physical systems may be used to represent quantum information, ranging from the state of particles or molecules, e.g. trapped ions [33], to small superconducting circuits [7]. Despite the variety of solutions, realizability of large scale quantum machines is still an open question, since the impact of negative phenomena, such as decoherence, increase exponentially with state size, thus requiring more resources allocated to perform error-correction. However, private enterprises started either selling machines or providing cloud access to them, proving it is actually an emergent technology, with increasing interest among the scientific community.

The theory of quantum computing started with the development of the quantum turing machine model [2], but the most common model in use today is the *quantum circuit model*, based on qubits, quantum gates and measurement operations. A *qubit* is the basic unit of quantum information, a two-state quantum mechanical system. All these models rely on the idea that the state is a set of qubits on which the programmer can apply different transformations. The main models are thus inherently stateful and imperative. Regardless of the physical implementation, two states of the elementary quantum system are denoted as the $|0\rangle$ and $|1\rangle$. The analogy with bits is obvious. A first difference with respect to classical computation is that the state of a qubit can also be a linear combination of $|0\rangle$ and $|1\rangle$, called a *superposition.* In accordance with linear algebra, $|0\rangle$ and $|1\rangle$ form a *basis* of the state space, named the computational basis.

Quantum computing theory is mainly developed along two axis: algorithms and protocols. Even though quantum computers obey the Church-Turing thesis [32], algorithms have been found with more than polynomial speedup over classical counterparts, for example Shor's algorithm for factorization [37] and the HHL algorithm for solving linear systems of equations [16].

Quantum protocols, in particular cryptography-related protocols, have been one of the first applications of quantum theory to computer science. Due to lower physical requirements with respect to algorithms, various protocols have been implemented in real world contexts, also with large-scale commercially available physical implementations. The prototipical case is the BB84 Quantum Key Distribution protocol [36], that has been proven unconditionally secure. As for algorithms, most protocols can be implemented with just classical control and classical communication. However some protocols, such as Quantum Key Distribution [34] and Quantum Leader Election [38], also require *quantum communication* (i.e. sending and receiving qubits).

Correctness proofs are available for some quantum algorithms, but there is no systematic approach for verifying protocols and their application in larger systems. As it is well known, correctness of classical communication protocols is already hard to prove at design stage, with notorious examples of vulnerabilities discovered for protocols previously considered to be secure. This is more-so true for quantum protocols, which must resist both quantum and classical attackers.

Process calculi are a formal model that represents concurrent systems. They are based on 'algebraic' composition of simple processes, and specifically target synchronization and communication. Process calculi have been successful in modeling classical concurrent systems also featuring non-determinism and probability. This formal model provides systematic solutions for analyzing and verifying the correctness of new systems and protocols. We expect the same will hold also in the quantum case, which still turns out to be a challenging setting.

To model quantum protocols, a process calculus needs to handle both classical and quantum communication at once, and must take into account the peculiar rules of quantum computations. Due to the properties of quantum systems, quantum information better fits the imperative stateful paradigm, so the state must of qubits be kept alongside the processes. A result that complicates the definition of quantum communication is the 'No-Cloning Theorem', stating that qubits cannot be copied. For this reason, once a qubit is sent the sender cannot use it anymore. Besides, qubits cannot be directly 'observed', or measured, without losing some information. When measured in a basis, in fact, a qubit in superposition collapses to one of the two basis states in a probabilistic way. Finally, a quantum process calculus must also deal with *entangled qubits*, i.e. qubits that cannot be described separately, one at a time, but must be considered as a whole compound system, even when they are stored in physically distant locations.

Of all the proposed models, none has emerged as a universally accepted standard. Our objective is to address the extension of classical process calculi to the quantum world. For this we will compare the different proposals, with a foundational approach aiming at identifying the best notion of behavioural equivalence. We propose a novel calculus named Linear qCCS, for which we consider different definitions of bisimilarity. Defining an appropriate bisimilarity is in fact the first step towards temporal logics, model checking and all the other tools available for the classical models.

## A lacking standard notion of behavioural equivalence

There is a number of proposals of quantum process calculi in the literature, often with different syntax, semantics and behavioural equivalences, even if they all model the same systems and the same protocols [24, 15, 14, 40, 39]. Of all these, the most established and developed are **QPAlg** [24], **CQP** [15] and **qCCS** [14]. They all differ in a number of minor 'classical' details, that unfortunately make the calculi difficult to compare: some are inspired by $\pi$-calculus, some by CCS; some employ strong bisimilarity while others employ weak or branching bisimilarity; some apply Larsen-Skou probabilistic bisimilarity [25], some apply Segala probabilistic bisimilarity [35].

More importantly, the proposed languages treat quantum information in different ways, leading to different notions of behavioural equivalence. A typical example are the two processes

$$P = c?x.H(x).\mathbf{0} \qquad Q = c?x.X(x).\mathbf{0}$$

(here written in the syntax of qCCS). Both processes receive a qubit on channel $c$ ($c?x$), modify it ($H(x)/X(x)$), and then terminate ($\mathbf{0}$). The two processes apply different transformations, resulting in different quantum states. The discriminating question is, should $P$ and $Q$ be considered bisimilar? That is, do $P$ and $Q$ express the same observable behaviour, and are therefore indistinguishable?

The answer depends on the exact notion of *observable property*, which varies between the proposed calculi. In QPAlg and CQP, a qubit is observable only when it is sent, as it is the case for 'classical' value passing or name passing calculi. In this setting, $P$ and $Q$ are indeed bisimilar, because the qubit they modified is not visible to an external observer. In qCCS instead, after a process has terminated, the qubits it has operated on become observable. When $P$ and $Q$ reach $\mathbf{0}$, they leave the qubit in two different states, and this suffices to refute bisimilarity in qCCS. This discrepancy is due to a sort of 'ambiguity', present in the syntax of all the calculi proposed up to now, on what happens to the qubits after the process termination.

Another crucial notion when defining behavioural equivalence is how to compare qubit values. In a classical process calculus, we can say that $c!0.\mathbf{0}$ is not bisimilar to $c!1.\mathbf{0}$ because they send two different *values* ($c!0/c!1$) before terminating. In a quantum setting it is difficult to talk about the value of a single qubit, because the qubit may be entangled. Take for example the two processes

$$R = Set_{\Phi}(q_1, q_2).c!q_1.c!q_2 \qquad S = Set_{\Psi}(q_1, q_2).c!q_1.c!q_2$$

where $R$ and $S$ set the value of the two qubits ($Set_{\Phi}(q_1, q_2)/Set_{\Psi}(q_1, q_2)$) to different entangled states ($|\Phi\rangle / |\Psi\rangle$), and send them.[1] Quantum theory tells us that entangled states are distinguishable only when taken as a whole, as a compound 2-qubit system. In the presence of entanglement, one cannot describe the state of just qubit $q_1$ without losing some information. For this reason, if the values of qbits are considered only one at the time, we lose some discriminating power allowed by quantum theory.

On the opposite side, quantum theory comes also with negative results about distinguishability of probabilistic mixtures (i.e. distributions) of quantum states. Also in this case, the capability of the observer to discriminate between different entities must be considered carefully, and is addressed or ignored in different calculi.

Summarizing, different calculi deal with quantum features in different ways. In QPAlg the value of a sent qubit ignores entanglement, and so the two processes $R$ and $S$ above are deemed bisimilar. In qCCS, the 'environment', i.e. the state of all visible qubits, is considered when comparing two processes, thus $R$ and $S$ are not bisimilar. In CQP there is a similar notion of environment, but takes into account also the limited discriminating capability of an external observer for probabilistic mixtures of quantum states, naturally arising upon measurements.

## Linear qCCS: a unifying approach

The main objective of this thesis is to introduce **Linear qCCS** (lqCCS), and use it to investigate the different notions of behavioural equivalence of quantum systems. Linear qCCS is designed to resolve the ambiguities and discrepancies of the previous proposals, and to identify the most adequate behavioural equivalence relation.

lqCCS is a (asynchronous) version on qCCS, equipped with a type system that grants linear communication of qubits. Indeed, due to the No-Cloning Theorem, once a qubit is sent on a channel, the sender process cannot use it anymore. In lqCCS each qubit used by a process must be sent *exactly* once. This means that the two processes $P$ and $Q$ of the previous section are not well typed in lqCCS, while $P', Q', P'', Q''$ are.

$$\begin{aligned} P' &= c?x.H(x).c!x & \qquad Q' &= c?x.X(x).c!x \\ P'' &= c?x.H(x).discard(x) & \qquad Q'' &= c?x.X(x).discard(x) \end{aligned}$$

[1] for example, we could take $\Phi = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and $\Psi = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, as it will be explained in the next chapter

The *discard*$(q)$ action is typed the same as a send action $c!q$, but when it comes to bisimilarity, $q$ is not considered a visible qubit.[2]

Thanks to its linear type system, lqCCS forces the designer to make an explicit choice on what happens to the qubits at the end of a computation. By writing processes like $P'$ or $Q'$, the qubits are made visible, thus the two processes are not bisimilar. When writing processes like $P''$ and $Q''$, the qubit is not visible, and the processes are bisimilar. Note that when deciding to use a discard or a send action, we can switch between a behaviour à la QPAlg/CQP (where $P$ is bisimilar to $Q$), and à la qCCS (where they are not).

Having solved the ambiguity on when a qubit should be visible or not, the only relevant detail is how to describe the quantum state. This allows us to compare directly the different bisimilarity relations presented in the literature, and to determine which are the crucial quantum-related details that makes a difference when defining a bisimilarity.

Since there is no unique and accepted notion of 'observable property' of quantum processes, each definition of labeled bisimilarity has to make some assumption on which are the properties to be checked when comparing two processes. Instead we opted for a (probabilistic) *saturated bisimilarity*, which in turn is based on an Unlabeled Transition System, and embodies both bisimilarity and contextual equivalence. Two processes $P$ and $Q$ are saturated bisimilar if they express the same atomic observable properties (called *barbs*), and when put inside the same context they evolve to bisimilar processes. As barbs we take the property of 'being able to send on a specific channel', which is a standard choice for barbs. Notice that in this way we made no a-priori assumption on quantum values representation. In saturated bisimilarity, in fact, it is in charge of the contexts to distinguish different values. For example, $P'$ and $Q'$ seen before are distinguished by a context that receives the modified qubit, measures it and is able to tell the difference.

A technical advantage of such saturated bisimilarity is that, instead of adding requirements to guarantee that the labelled bisimilarity is a congruence, we start from a relation that is a congruence by definition, and explore which are the properties that can be observed by an arbitrary context.

## The unexpected inadequacy of probabilistic bisimilarity

While exploiting lqCCS to compare different approaches of the literature, we discovered an unexpected problem in how behavioural equivalence is usually defined in quantum process calculi.

By using a probabilistic saturated bisimilarity on lqCCS, we succesfully recover the results of qCCS, but not all the one of CQP. The main difference between qCCS and CQP bisimilarity is in the treatment of measurement operators and the resulting probabilistic behaviour.

Consider the two processes

$$P = c?x.M_{01}(x).c!x \qquad Q = c?x.M_{\pm}(x).c!x$$

Both processes receive a qubit, measure it $(M_{01}(x)/M_{\pm}(x))$ and then send the measured qubit. Note that the measurements are of two different basis: the first being the computational basis, the other is the so called *diagonal basis*, composed by $|+\rangle$ and $|-\rangle$, that are both superpositions of $|0\rangle$ and $|1\rangle$. This causes the resulting state of the sent qubits to differ. $P$ measures the qubit in the computational basis, so will send two possible qubits, $|0\rangle$ or $|1\rangle$, each with a certain probability. $Q$ measures in the diagonal basis, so will send two possible qubits, $|+\rangle$ and $|-\rangle$, each with a certain probability. There

[2] For example, in (standard) qCCS *discard*$(q)$ can be implemented with channel restrictions, like $c!q \setminus c$.

is an input for which $P$ will evolve in a symmetric *distribution* of states, i.e. will send a qubit with state $|0\rangle$ with probability 0.5, or a qubit with state $|1\rangle$ with probability 0.5. Similarly, with the same input state, $Q$ will evolve in a symmetric distribution of sending $|+\rangle$ and $|-\rangle$.

The usual notion of probabilistic bisimilarity requires $P$ and $Q$ to behave similarly and with the same probability. In other words, they must evolve with the same probability in bisimilar states. According to this definition, processes $P$ and $Q$ are not bisimilar.

Quantum theory, however, tells that it is not possible to distinguish a source $S_P$ sending half of the time $|0\rangle$ and half of the time $|1\rangle$ from a source $S_Q$ sending half of the time $|+\rangle$ and half of the time $|-\rangle$. This interesting property is due to the inherent limitations of the observer, which, to discriminate the two sources, can only try to perform measurements. For each chosen measurement, the obtained probabilistic distributions coincide. As an example, assume we measure the qubit from $S_P$ in the computational basis, the result will be half of the time $|0\rangle$ and half of the time $|1\rangle$. Similarly, when measuring a qubit coming from $S_Q$, a $|+\rangle$ qubit would decay in $|0\rangle$ or $|1\rangle$, each with half the probability, and the same happens for $|-\rangle$. Hence, the two sources appear the same for an external observer.

In accordance with this peculiar quantum feature, in CQP the processes $P$ and $Q$ are considered bisimilar. This is obtained by defining observable properties directly on distributions, and by considering the limited capability of a quantum observer.

Our goal is to overcome the limitations of probabilistic bisimilarity and to recover the results of CQP with a more standard formalization. Hence we propose a novel notion of *quantum saturated bisimilarity* that represents more correctly the observable properties of probabilistic distribution of quantum states. We model the undistingishability results of quantum theory as an equivalence relation between distributions. Thanks to this equivalence relation, we relax the conditions of probabilistic saturated bisimilarity, allowing to change the 'actual' distribution with an equivalent one to match the behaviour of a bisimilar distribution. We successfully achieved our goal, by showing that quantum bisimilarity agrees with CQP in the critical cases discussed above.

## A minimal quantum process calculus

The usual notion of probabilistic bisimilarity seems not well suited to treat the quantum case, even if quantum systems have some obvious probabilistic features. Given that a well established notion of behavioural equivalence for quantum processes has not emerged yet, we have decided to pursue a foundational approach, investigating the topic on a **Minimal Quantum Process Algebra** (mQPA). Working with a minimal process algebra allows us to omit all the irrelevant classical details, and to target the quantum aspects in isolation. In addition to a minimal set of classical features, mQPA has transformations of quantum states and a novel operator for combining processes, called *projective sum* (intended to model quantum measurements). Similarly to what happens in a probabilistic process algebra, where a probabilistic sum operator produces a distribution of states, the projective sum produces a quantum distribution of states, i.e. a probabilistic distribution that depends on the quantum value to be measured. The state of the qubits is not kept along the process, and is not updated in a small-step fashion as the process evolves. On the contrary, the operational semantics of a mQPA is defined as implicitly parametric on the quantum state. This approach is peculiar, as it resembles none of the current proposals (to the best of our knowledge). A bisimilarity then is defined in a fairly standard way, and is shown to work well with the previous problematic examples.

# Chapter 2

# Background

## 2.1 Quantum Computing

The laws on Quantum Mechanics, as we understand them, are elegantly formalized in a mathematical framework, built upon simple linear algebra. This framework is based on a few *postulates* that describe the nature and evolution of quantum systems. Since quantum computing is just the technique of manipulating quantum systems to perform some computation, it necessarily follows the same postulates. Before presenting each postulate, we recall the necessary basic definition from linear algebra, formulated in the Dirac's 'bra-ket' notation. For further reading, the standard textbook on the subject is [31].

### 2.1.1 State space

A *column vector* in a complex vector space is written $|\psi\rangle$, and it's called a 'ket',

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Its *conjugate transpose* is written $\langle\psi|$, and its called a 'bra'.

$$\langle\psi| = |\psi\rangle^\dagger = (\alpha_1^* \ldots \alpha_n^*)$$

A (finite-dimensional) *Hilbert space*, often denoted as $\mathcal{H}$, is a complex inner product space, i.e. a complex vector space equipped with a binary operator $\langle\,\_\,|\,\_\,\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ called *inner product*, dot product, or simply 'braket'.

$$\langle\psi|\phi\rangle = \begin{pmatrix}\alpha_1^* \ldots \alpha_n^*\end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \sum_i \alpha_i^* \beta_i$$

The inner product satisfies the following properties:

| | |
|---|---|
| Conjugate symmetry | $\langle\psi\|\phi\rangle = \langle\phi\|\psi\rangle^*$ |
| Linearity | $\langle\psi\| (\alpha \|\phi\rangle + \beta \|\varphi\rangle) = \alpha \langle\psi\|\phi\rangle + \beta \langle\psi\|\varphi\rangle$ |
| Positive definiteness | $\langle\psi\|\psi\rangle \geq 0$ |

Notice that $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle$ is the $\mathbf{0}$ vector. Besides, thanks to conjugate symmetry, we have $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle^*$, so $\langle\psi|\psi\rangle$ it's always a real, non-negative number, when $|\psi\rangle \neq \mathbf{0}$.

Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if

$$\langle\psi|\phi\rangle = 0$$

The *norm* of $|\psi\rangle$ is defined as:

$$\| \, |\psi\rangle \, \| = \sqrt{\langle\psi|\psi\rangle}$$

A *unit vector* is a vector $|\psi\rangle$ such that

$$\| \, |\psi\rangle \, \| = 1$$

.

A set of vectors $\{|\psi\rangle_i\}_i$ is an *orthonormal basis* of $\mathcal{H}$ if

- each vector $|\phi\rangle \in \mathcal{H}$ can be expressed as a *linear combination* of the vector in the basis, $|\phi\rangle = \sum_i \alpha_i |\psi\rangle_i$.
- All the vector in the basis are orthogonal
- All the vector in the basis are unit vector

We're now ready to present the postulates of Quantum Mechanics, in the form more convenient for quantum computing.

> **Postulate I**: The state of an isolated physical system is represented, at a fixed time $t$, by a unit vector $|\psi\rangle$, called the *state vector*, belonging to a Hilbert space $\mathcal{H}$, called the *state space.*

When describing the state of a quantum system, we ignore the *global phase factor*[1], i.e.

$$|\psi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} = -\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \lambda\begin{pmatrix}\alpha \\ \beta\end{pmatrix} \text{ for each } \lambda \in \mathbb{C} \text{ such that } |\lambda| = 1$$

The simplest, prototypical example of a quantum physical system is a *qubit*: a qubit is a physical system with associated a two-dimensional Hilbert Space $\mathcal{H}^2$. Such systems comprehend an electron in the ground or excited state, a vertically or horizontally polarized photon, or a spin up or spin down particle.

Taken for example a photon, we could say that the photon is in state $|0\rangle$ when vertically polarized, and in state $|1\rangle$ when is horizontally polarized, where $|0\rangle$ and $|1\rangle$ are the two unit vectors of the Hilbert space defined as

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

The vectors $\{|0\rangle, |1\rangle\}$ form an orthonormal basis of $\mathcal{H}$, called the *computational basis.* Since they form a basis, each vector $|\psi\rangle \in \mathcal{H}^2$ can be expressed as

$$|\psi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

[1] An equivalent formulation, in fact, describes a quantum system as a *ray*, a one-dimensional subspace of $\mathcal{H}$.

So, the state of any qubit can mathematically be described as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, a linear combination of $|0\rangle$ and $|1\rangle$. From the physical point of view, this means that the qubit is in a *quantum superposition* of state $|0\rangle$ and $|1\rangle$, like a photon being diagonally-polarized, or an electron being at the same time in the excited and in the ground state.

Other important vectors in the $\mathcal{H}^2$ state space are $|+\rangle$ and $|-\rangle$,

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \\ |-\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle \end{aligned}$$

that form the so called *diagonal basis*, or Hadamard basis, of $\mathcal{H}^2$. As we will see, $|+\rangle$ and $|-\rangle$ are both an equal superposition of $|0\rangle$ and $|1\rangle$. The difference between $|+\rangle$ and $|-\rangle$ is the *relative phase*, i.e. the phase between the $|0\rangle$ and $|1\rangle$ component. The states $|0\rangle + |1\rangle$, $-\,|0\rangle - |1\rangle$, $i\,|0\rangle + i\,|1\rangle$ are all equal to $|+\rangle$ times a certain global phase, and are considered the same state. The states $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$, $|0\rangle + i\,|1\rangle$, instead, all differ for a relative phase factor, and have a different behaviour when applied to the same computation.

### 2.1.2 Unitary Transformations

For each linear operator $A$ acting on a Hilbert space $\mathcal{H}$, we denote as $A^\dagger$ the *adjoint* of $A$, i.e. the unique linear operator such that

$$\langle\psi|A\phi\rangle = \langle A^\dagger\psi|\phi\rangle$$

A linear operator $A$ acting on a $n$-dimensional Hilbert space $\mathcal{H}^n$ can be represented as a $n \times n$ matrix, and its adjoint is calculated as

$$A^\dagger = (A^*)^T$$

the conjugate transpose of the matrix $A$.

If it holds that $A = A^\dagger$, we say that $A$ is self-adjoint, or *Hermitian.*

A linear operator $U$ is said to be *unitary* when $U^\dagger = U^{-1}$, which implies

$$UU^\dagger = U^\dagger U = I$$

Unitary matrices enjoy many useful properties, first of all that they have a spectral decomposition. Another defining characteristic is that they preserve the inner product, $\langle\psi|\phi\rangle = \langle U\psi|U\phi\rangle$

$$\langle U\psi|U\phi\rangle = \langle\psi|\,U^\dagger U\,|\psi\rangle = \langle\psi|\,I\,|\psi\rangle = \langle\psi|\phi\rangle$$

A corollary of this property is that applying a unitary operator to a unit vector gives a unit vector

$$\langle U\psi|U\psi\rangle = \langle\psi|\psi\rangle = 1$$

The following postulate makes obvious why we are interested in unitary transformations.

> **Postulate II**: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time $t_0$ is related to the state $|\psi'\rangle$ of the system at time $t_1$ by a unitary operator $U$ which depends only on the times $t_0$ and $t_1$.
>
> $$|\psi'\rangle = U\,|\psi\rangle$$

According to what we said before, if a physical system starts in a unit state, it will always remain in a unit state.

In quantum computing, the programmer can manipulate the state of a qubit by applying unitary transformations to it. Some of the most frequent transformations, implemented in every quantum computer, are:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

The first three operators are known as Pauli operators. $X$ is the 'bit-flip operator', the quantum equivalent of the classical not: it transforms $|0\rangle$ in $|1\rangle$ and $|1\rangle$ in $|0\rangle$. In general, the $X$ operators behaves as follows.

$$X|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Notice that the $X$ operator leaves the $|+\rangle$ state unaltered, because it is and it remains in an equal superposition of $|0\rangle$ and $|1\rangle$.

$Z$ is the 'phase-flip operator', it changes the relative phases of the $|0\rangle$ and $|1\rangle$ component. $Z|+\rangle$ becomes $|-\rangle$ and vice versa. When applied to $|0\rangle$ (or $|1\rangle$) the $Z$ operator does nothing,

Finally, the $H$ operator, called the Hadamard operator, or Hadamard gate, is used to *create superpositions*, as it transforms a vector from the computational basis to the diagonal basis:

$$\begin{aligned} H|0\rangle &= |+\rangle \qquad & H|+\rangle &= |0\rangle \\ H|1\rangle &= |-\rangle \qquad & H|-\rangle &= |1\rangle \end{aligned}$$

### 2.1.3 Measurement

The second postulate describes only the evolution of isolated systems. Such systems exchange neither energy nor information with the environment, and all their computations are always reversible (and are in fact formalized with invertible, unitary matrices). To extract classical information from the system, to *measure* the output of a quantum computation, an interaction is needed between the quantum system and the environment. As we will see, this measurement operation is first of all non-invertible, as different state could produce the same outcome when measured, but is also intrinsically probabilistic: a generic state $|\psi\rangle$ could produce different measurement outcomes $m_1, m_2, \ldots$, each with a certain probability that depends on $|\psi\rangle$.

From a physical point of view, if a system is in a superposition of states, measuring it cause the wavefunction to collapse to a base state, in a purely probabilistic way. This means that, even if we compute a state that contains the desired information, this information is often difficult to recover, because directly measuring it can destroy the information and produce a trivial outcome.

> **Postulate III**: Quantum measurements are described by a set $\{M_m\}_m$ of measurement operators, where the index $m$ refers to the measurement outcomes that may occur in the experiment. The set of measurement operators must be *complete*, i.e.:
>
> $$\sum_m M_m^\dagger M_m = I$$

If the state of the quantum system is $|\psi\rangle$ before the measurement, then the probability that the result $m$ occurs is

$$p_m = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and if $m$ is the outcome the state after the measurement will be

$$\frac{1}{\sqrt{p_m}} M_m |\psi\rangle$$

The most common class of quantum measurements is composed of *projective measurements*. Such measurements are described by a set of *orthogonal projectors*, i.e. Hermitian operators such that

$$M_m M_{m'} = \begin{cases} \mathbf{0} & \text{if } m \neq m' \\ M_m & \text{if } m = m' \end{cases}$$

The simplest example of (projective) measurement is simply measuring a state in the computational basis, i.e. projecting it in its $|0\rangle$-$|1\rangle$ component. The measurement in the computational basis, denoted as $M_{01}$ is defined as

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

And its effect of the state $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ is:

$$\frac{1}{\sqrt{p_0}} M_0 |\psi\rangle = \frac{1}{|\alpha|} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_0 |\psi\rangle = |\alpha^2|$$

$$\frac{1}{\sqrt{p_1}} M_1 |\psi\rangle = \frac{1}{|\beta|} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_1 |\psi\rangle = |\beta^2|$$

Notice that, when measuring the $|0\rangle$ state in the computational basis, the outcome will always be $|0\rangle$ with probability $|\alpha|^2 = 1$, in a completely deterministic behaviour. When instead measuring the $|+\rangle$ state we get either $|0\rangle$ or $|1\rangle$, with equal probability $|\alpha|^2 = |\beta|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. The same holds also for the $|-\rangle$ state. As already said, $|+\rangle$ and $|-\rangle$ differ only for the relative phase, and the relative phase has no influence on the outcome of a measurement in the computational basis.

An other projective measurement is the measurement in the Hadamard basis, $M_\pm$, defined as

$$M_+ = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad M_- = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

From the physical point of view, this measurement can be performed composing Hadamard transformations and a measurement in the computational basis: $M_+ = HM_0H$, $M_- = HM_1H$. Just as $M_{01}$ causes a vector to decay in its $|0\rangle$ component or in its $|1\rangle$ component, $M_\pm$ makes a vector decay in its $|+\rangle$ or $|-\rangle$ component. This means that, when measuring $|+\rangle$ in the Hadamard basis, the outcome will always be $|+\rangle$ with probability 1. Notice that a qubit in the state $|0\rangle$ can be considered in an equal superposition of $|+\rangle$ and $|-\rangle$, as $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$. According to this, measuring $|0\rangle$ in the Hadamard gives the outcomes $|+\rangle$ or $|-\rangle$ with half the probability each.

### 2.1.4 Composite quantum systems

In the previous sections we characterized quantum systems and how they evolve, taking the prototypical example of the two-dimensional Hilbert space of a qubit. When dealing with higher-dimensional systems, we can often describe them as *composite system*, made of multiple smaller systems.

If we have for example two photons, each described by a (2-dimensional) Hilbert space $\mathcal{H}$, we can describe the system composed of both photons as the *tensor product* of the 2-dimensional Hilbert spaces.

If $\mathcal{H}_n$ is a $n$-dimensional Hilbert space, and $\mathcal{H}_m$ is a $m$ dimensional Hilbert space, their tensor product $\mathcal{H}_n \otimes \mathcal{H}_m$ is a $nm$ Hilbert space. If $\{\left|\psi_1\right\rangle, \dots \left|\psi_n\right\rangle\}$ is a basis of $\mathcal{H}_n$, and $\{\left|\phi_1\right\rangle, \dots \left|\phi_m\right\rangle\}$ is a base of $\mathcal{H}_m$, then a basis of $\mathcal{H}_n \otimes \mathcal{H}_m$ is

$$\left\{ \left|\psi_i\right\rangle \otimes \left|\phi_j\right\rangle \mid i \in [1, \dots n], j \in [1, \dots m] \right\}$$

where $\left|\psi\right\rangle \otimes \left|\phi\right\rangle$ denotes the Kronecker product. We will often omit the tensor symbol, writing $\left|\psi\right\rangle \left|\phi\right\rangle$ or also $\left|\psi\phi\right\rangle$ instead of $\left|\psi\right\rangle \otimes \left|\phi\right\rangle$. We can now state the last postulate we need:

> **Postulate IV**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

If a single qubit is described by a 2-dimensional space $\mathcal{H}$, we will write $\mathcal{H}^{\otimes n}$ to intend the tensor product $n$ copies of $\mathcal{H}$, of dimension $2^n$. So, a compound system composed of two qubits has a state space $\mathcal{H}^{\otimes 2}$, its canonical basis is

$$\{\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle, \left|11\right\rangle\}$$

and all its vector can be expressed as a linear combination:

$$\left|\psi\right\rangle \in \mathcal{H}^{\otimes 2} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \alpha\left|00\right\rangle + \beta\left|01\right\rangle + \gamma\left|10\right\rangle + \delta\left|11\right\rangle$$

A quantum state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said *separable* when can be expressed as the product of two vectors, one in $\mathcal{H}_1$ and the other in $\mathcal{H}_2$. From the definition of the Kronecker product, all separable states of $\mathcal{H}^{\otimes 2}$ are of the form:

$$\left|\psi\right\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

Some of the defining characteristics of quantum systems derive from the fact that not all states in $\mathcal{H}^{\otimes 2}$ are separable. The existence of such states, called *entangled* states, implies that a composite system cannot always be described as simply the juxtaposition of two smaller states. When a qubit $q_1$ is entangled with an other qubit $q_2$, its evolution depends not only on the transformations applied to $q_1$, but also on the transformations applied on $q_2$, that could be even light-years away. This surprising result does not allow faster then light communication, as we will see in the next section.

The classical example of an entangled state is the so called $\left|\Phi^+\right\rangle$ *Bell state*:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The fourth postulate tells us that the state space of a composite system is simply the tensor product of the state spaces of the smaller systems. The tensor product of Hilbert spaces is still an Hilbert space, the composition of unit vector is still a unit vector, and the composition of unitary transformation is still unitary. For example, the (Kronecker) composition of $H$ and $I$ matrices is defined as a block matrix:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix}$$

And when applied to a two-qubit system, it applies $H$ on the first qubit, and leaves the second one unaltered:

$$(H \otimes I) \left|00\right\rangle = H \left|0\right\rangle \otimes I \left|0\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \left|+\right\rangle \otimes \left|0\right\rangle$$

One of the most common two-qubit unitary that is not just the composition of one-qubit transformations is the CNOT matrix:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

This matrix applies a 'controlled not' operator on the second qubit. That is, it leaves the second qubit unaltered if the first one is $\left|1\right\rangle$, and applies an $X$ transformation on the second qubit if the first one is $\left|1\right\rangle$. Together with linearity, this means that if the first bit is in a superposition of $\left|0\right\rangle$ and $\left|1\right\rangle$, after applying this transformation the whole system will be in a superposition of two states: one where the two bits are left unaffected, one where the second one has been flipped. As an example, we can show how the CNOT transformation is used to create entanglement.

$$\text{CNOT} \left|00\right\rangle = \left|00\right\rangle \qquad \text{CNOT} \left|10\right\rangle = \left|11\right\rangle$$

$$\text{CNOT} \left|+0\right\rangle = \frac{1}{\sqrt{2}} \big(\text{CNOT} \left|00\right\rangle + \text{CNOT} \left|10\right\rangle\big) = \frac{1}{\sqrt{2}} \big(\left|00\right\rangle + \left|11\right\rangle\big) = \left|\Phi^+\right\rangle$$

$$\text{CNOT} \left|-0\right\rangle = \frac{1}{\sqrt{2}} \big(\text{CNOT} \left|00\right\rangle - \text{CNOT} \left|10\right\rangle\big) = \frac{1}{\sqrt{2}} \big(\left|00\right\rangle - \left|11\right\rangle\big) = \left|\Phi^-\right\rangle$$

$$\text{CNOT} \left|+1\right\rangle = \frac{1}{\sqrt{2}} \big(\text{CNOT} \left|01\right\rangle + \text{CNOT} \left|11\right\rangle\big) = \frac{1}{\sqrt{2}} \big(\left|01\right\rangle + \left|10\right\rangle\big) = \left|\Psi^+\right\rangle$$

$$\text{CNOT} \left|-1\right\rangle = \frac{1}{\sqrt{2}} \big(\text{CNOT} \left|01\right\rangle - \text{CNOT} \left|11\right\rangle\big) = \frac{1}{\sqrt{2}} \big(\left|01\right\rangle - \left|10\right\rangle\big) = \left|\Psi^-\right\rangle$$

$\left|\Phi^+\right\rangle, \left|\Phi^-\right\rangle, \left|\Psi^+\right\rangle$ and $\left|\Psi^-\right\rangle$ are four different orthonormal entangled vectors, and form the so called *Bell basis* of $\mathcal{H}^{\otimes 2}$.

Before introducing the density operator formalism, we state one of the defining features of quantum computing: the No-Cloning Theorem, of which a simple proof can be found in [31].

**Theorem 2.1.1.** *There is no unitary operation $U$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that for all states $\left|\psi\right\rangle \in \mathcal{H}_A$ and $\left|\phi\right\rangle \in \mathcal{H}_B$*

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

This theorem tells us that the information codified in a qubit (for example in state $|\psi\rangle$) cannot be duplicated, obtaining two different qubits with the same state $|\psi\rangle$. This has a lot implications, that make quantum computation essentially different from classical computation. If information cannot be copied, it cannot be stored in multiple location, it cannot be broadcast to multiple receivers, and cannot be handled in a 'pass-by-value' functional semantics.

### 2.1.5 Density operator formalism

The formalism presented so far describes quantum system in terms of unit vectors and linear transformations. There is an alternative, more general formulation, the *density operator formalism*, in which states are represented as positive operators, and transformations as linear maps from operators to operators, i.e. superoperators.

The main advantage of this formulation is that it represents also *partial information* about a quantum system. When describing open systems, that are systems which interact with the external environment, it is often impossible to have complete knowledge on the state of our systems. Instead, one could know that the open system is either in state $|\psi\rangle$, with a certain probability $p$, or in state $|\phi\rangle$, with probability $1-p$. In other words, we know that the system is in a *probabilistic mixture of states*, called an *ensemble* of states, or also a *mixed state*.

A typical application of mixed states is in presence of noisy channels. Suppose for example a channel that correctly transmits the sent qubit only with probability 0.9, and with probability 0.1 is causes a 'bit-flip' error, exchanging $|0\rangle$ with $|1\rangle$ and $|1\rangle$ with $|0\rangle$ (that is, the channel applies a $X$ transformation to the qubit with probability 0.1). If Alice sends a qubit with state $|0\rangle$ to Bob, using this noisy channel, Bob receives an ensemble of states, a qubit with a 0.9 probability of being in state $|0\rangle$, and a 0.1 probability of being in state $|1\rangle$.

In general, given an $n$-dimensional Hilbert space $\mathcal{H}$, an *ensemble* of quantum states is a set:

$$\{(|\psi_i\rangle, p_i)\}$$

of quantum states in $\mathcal{H}$, each with a different probability, such that $\forall i\, p_i > 0$ and $\sum_i p_i \leq 1$.

Each ensemble defines a density operator, that is a matrix in $\mathbb{C}^{n\times n}$, i.e. an operator $\mathcal{H} \to \mathcal{H}$. The ensemble $\{(|\psi_i\rangle, p_i)\}$, where $|\psi_i\rangle \in \mathcal{H}$, defines the density operator:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

where $|\psi\rangle\langle\phi|$ denotes the matrix product between the column vector $|\psi\rangle$ and the row vector $\langle\phi|$, known as the *outer product.* Notice that this construction is not injective, as there are different ensembles that correspond to the same density operator. We indicate with $\mathcal{D}(\mathcal{H})$ the set of density operators of $\mathcal{H}$.

Density operators enjoy two useful properties (see [30]):

1. The trace of $\rho$ is the sum of the probabilities of the ensemble $tr(\rho) = \sum_i p_i \leq 1$.

2. $\rho$ is *positive semidefinite*, i.e.

$$\forall |\psi\rangle \in \mathcal{H} \;\; \langle\psi| \rho |\psi\rangle \geq 0$$

Positive semidefinite operators are always diagonalizable with eigenvalues real and positives. So, each positive semidefinite operator with trace $\leq 1$ represents at least one ensemble, with the eigenvectors as states and the corresponding eigenvalues as probabilities.

One of the main application of density operators is to describe the state of a subsystem of a composite quantum system. When dealing with composite system, we write $\rho \otimes \sigma \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, to denote the density matrix given by the Kronecker product of $\rho$ and $\sigma$. Notice that, if $\rho = \sum_{i=1}^{n} p_i \left|\psi_i\middle\rangle\!\middle\langle\psi_i\right|$ and $\sigma = \sum_{j=1}^{m} p_j \left|\phi_j\middle\rangle\!\middle\langle\phi_j\right|$, then

$$\rho \otimes \sigma = \sum_{i=1}^{n} \sum_{j=1}^{m} p_i p_j \left|\psi_i \phi_j\middle\rangle\!\middle\langle\psi_i \phi_j\right|$$

Suppose a composite system, made of two subsystem $A$ and $B$, with state space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Given a generic (not necessarily separable) $\rho^{AB} \in \mathcal{H}$, describing the state of the whole system, the operator $\rho^A$ that describes the subsystem $A$ is obtained as

$$\rho^A = tr_B(\rho^{AB})$$

where the $tr_B$ is called the *partial trace over* $B$, and is defined by

$$tr_B\big( |\psi\rangle\!\langle\psi'| \otimes |\phi\rangle\!\langle\phi'| \big) = |\psi\rangle\!\langle\psi'|\, tr\big( |\phi\rangle\!\langle\phi'| \big)$$

together with linearity. $\rho^A$ is called the *reduced density operator* of system $A$.

When applied to a separable state $\rho^A \otimes \rho^B$, the partial trace $tr_B$ gives exactly $\rho^A$. When applied to an entangled state, instead, it produces a probabilistic mixture of states, because 'forgetting' the information on the state of subsystem $B$ leaves us with only partial information on subsystem $A$. The canonical example is the bell state $\rho = \frac{1}{2} |00\rangle\!\langle 00| + \frac{1}{2} |11\rangle\!\langle 11| \in \mathcal{H}_A \otimes \mathcal{H}_B$:

$$\begin{aligned}
tr_B(\rho) &= \frac{1}{2} tr_B\big( |00\rangle\!\langle 00| \big) + \frac{1}{2} tr_B\big( |11\rangle\!\langle 11| \big) \\
&= \frac{1}{2} tr_B\big( |0\rangle\!\langle 0| \otimes |0\rangle\!\langle 0| \big) + \frac{1}{2} tr_B\big( |1\rangle\!\langle 1| \otimes |1\rangle\!\langle 1| \big) \\
&= \frac{1}{2} |0\rangle\!\langle 0|\, tr\big( |0\rangle\!\langle 0| \big) + \frac{1}{2} |1\rangle\!\langle 1|\, tr\big( |1\rangle\!\langle 1| \big) \\
&= \frac{1}{2}\big( |0\rangle\!\langle 0| + |1\rangle\!\langle 1| \big) = \frac{1}{2} I
\end{aligned}$$

The state $\frac{1}{2}I$ is called the *maximally mixed state*, as it gives us no information on the system. It can be seen as an ensemble of states $|0\rangle$ and $|1\rangle$ both with probability one half, but could also indicate an ensemble of $|+\rangle$ and $|-\rangle$ with the same probability, or even en ensemble of $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, and so on.

According to the density operator formalism, the state of a quantum system is represented as a density operator. This means that a transformation applied to a quantum system can be formalized as a transformation from operators to operators, i.e. a *superoperator*.

For example, the noisy bitflip channel described before, which leaves the input qubit unaltered with 0.9 probability, and applies $X$ to it with 0.1 probability, can be described as the function $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ defined by

$$\mathcal{E}(\rho) = \frac{9}{10} I \rho I + \frac{1}{10} X \rho X^\dagger$$

When applied to a qubit with state $|0\rangle\!\langle 0|$, the output will be

$$\mathcal{E}(|0\rangle\!\langle 0|) = \frac{9}{10} I\, |0\rangle\!\langle 0|\, I + \frac{1}{10} X\, |0\rangle\!\langle 0|\, X^\dagger = \frac{9}{10} |0\rangle\!\langle 0| + \frac{1}{10} |1\rangle\!\langle 1| = \begin{pmatrix} 0.9 & 0 \\ 0 & 0.1 \end{pmatrix}$$

Not all the functions on density matrices are valid superoperators. Before introducing the correct definition, we need an additional notion, namely the tensor product of two functions.

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Given $\mathcal{E} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_A)$ and $\mathcal{F} : \mathcal{D}(\mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_B)$, their tensor product $\mathcal{E} \otimes \mathcal{F} : \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is defined as:

$$(\mathcal{E} \otimes \mathcal{F})(\rho_A \otimes \rho_B) = \mathcal{E}(\rho_A) \otimes \mathcal{F}(\rho_B)$$

together with linearity.

We now define the *superoperators on* $\mathcal{H}$ as all the maps $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ satifying:

- $\mathcal{E}$ is *convex linear*: for any set of probabilities $\{p_i\}_i$,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i)$$

- $\mathcal{E}$ is *completely positive*: for any extra Hilbert space $\mathcal{H}_R$, for any positive $\rho \in \mathcal{H}_R \otimes \mathcal{H}$, $(\mathcal{I}_R \otimes \mathcal{E})(\rho)$ is also positive, where $\mathcal{I}_R$ is the identity operator on $\mathcal{D}(\mathcal{H}_R)$.

- $\mathcal{E}$ is *trace non-increasing*: for any density operator $\rho \in \mathcal{D}(\mathcal{H})$,

$$tr\big(\mathcal{E}(\rho)\big) \leq tr(\rho) \leq 1$$

We call $\mathcal{S}(\mathcal{H})$ the set of all superoperators on $\mathcal{H}$, and $\mathcal{TS}(\mathcal{H}) \subseteq \mathcal{S}(\mathcal{H})$ the set of all *trace-preserving* superoperators, i.e. superoperators such that for any $\rho \in \mathcal{D}(\mathcal{H})$,

$$tr\big(\mathcal{E}(\rho)\big) = tr(\rho)$$

This axiomatic definition of the superoperators on $\mathcal{H}$ specifies they overall properties, but does not give any suggestion on how a superoperator can be constructed. There exists an alternative, equivalent definition, that says that a superoperator is any function $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ that has a *Kraus operator sum decomposition.*

A function $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ is a superoperator on $\mathcal{H}$ if and only if it has a Kraus decomposition, i.e. a finite set of operators $\{E_i\}_i$, with $1 \leq i \leq dim(\mathcal{H})$ such that

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

$$\sum_i E_i^\dagger E_i \sqsubseteq I_\mathcal{H}$$

Where $A \sqsubseteq B$ means that $B - A$ is a positive semidefinite matrix, and $I_\mathcal{H}$ is the identity linear operator on $\mathcal{H}$.

Although there are possibly multiple Kraus decompositions for any superoperator $\mathcal{E} \in \mathcal{S}(\mathcal{H})$, they are related by a unitary transformation. Formally, for any two set of decompositions $\{C_i\}_i$ and $\{B_j\}_j$, there is a unitary matrix $U = \{u_{ij}\}_{ij}$ such that $C_i = \sum_j u_{ij} B_j$.

Given $\mathcal{E} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_A)$ and $\mathcal{F} : \mathcal{D}(\mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_B)$, respectively expressed in Kraus form as $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ and $\mathcal{F}(\rho) = \sum_j F_j \rho E_j^\dagger$, the tensor product $\mathcal{E} \otimes \mathcal{F}$ can be expressed in Kraus form as

$$(\mathcal{E} \otimes \mathcal{F})(\rho) = \sum_i \sum_j (E_i \otimes F_j)\, \rho\, (E_i \otimes F_j)^\dagger$$

Using density matrices and superoperators, it is possible to restate all the quantum postulate seen in the previous sections. A physical system is represented by a density matrix $\rho \in \mathcal{D}(\mathcal{H})$ with trace 1. A composite physical system is described by a density matrix $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$. The second and the third postulate can be merged together: the evolution of an open quantum system can always be described by a superoperator. That is, the state $\rho$ of the system at time $t_0$ is related to the state $\rho'$ of the system at time $t_2$ by a superoperator $\mathcal{E}$

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

Superoperators can in fact describe both unitary transformations and measurements, as well as more general transformations. Given unitary operator $U$ on $\mathcal{H}$, we can define the (trace preserving) superoperator $\mathcal{E}_U \in \mathcal{S}(\mathcal{H})$ as:

$$\mathcal{E}_U(\rho) = U\rho U^\dagger$$

Given a measurement $\{M_m\}_m$, we can define the (trace non-increasing) superoperator $\mathcal{E}_m \in \mathcal{S}(\mathcal{H})$ as

$$\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$$

Notice that $\mathcal{E}_m(\rho)$ is equal to $p_m\rho_m$, where $p_m$ is the probability of the outcome $m$ when measuring the state $\rho$, and $\rho_m$ is the (normalized) state after outcome $m$ has occurred.

Another class of useful superoperators are noisy channels or noisy gates, i.e. transformations that perform the desired operation only with a high probability. We have already seen the noisy bitflip channel:

$$\mathcal{E}(\rho) = (p)I\rho I + (1-p)X\rho X^\dagger$$

with Kraus decomposition $\{\sqrt{p}I, \sqrt{1-p}X\}$.

Finally, there are also ‘constant’ superoperators, which completely destroy the information of a quantum system, and return always the same state. For example, we will often use a *Set* operator like

$$Set_0(\rho) = |0\rangle\langle 0|\, \rho\, |0\rangle\langle 0| + |0\rangle\langle 1|\, \rho\, |1\rangle\langle 0|$$

that always returns $|0\rangle\langle 0|$ for any possible input.

## 2.2 Process Calculus

We review here some results on process calculi and bisimilarity, that will be used in the following. Given the probabilistic nature of quantum mechanics, we include probabilistic systems in our discussion.

### 2.2.1 Process Calculi and LTS

Process Calculus, also known as Process Algebra, is an algebraic approach to model concurrent computations, focusing on the communication between different agents. Each agent is formalized as a *process*, a syntactic element that describes its capabilities. Processes can be composed in different ways, and so form an *algebra of processes*, with various operators for parallel composition, sequential compositions, probabilistic and non-deterministic sum, and so on.

All the foundational and most successful process calculi [26, 3, 20, 28], have a number of key features in common:

- **Nil Process**: Each calculus has a *constant process*, usually denoted as *nil* or **0**, that is in a terminal state, i.e. it cannot perform any action.

- **Visible Actions**: Each calculus has *action prefixes*, usually denoted as $\alpha, \overline{\alpha}, \beta, \overline{\beta}, \ldots$ If $P$ is a process, $\alpha.P$ is a process that performs an action $\alpha$, and then behaves as $P$. The two actions $\alpha$ and $\overline{\alpha}$ are called *coactions*, and denotes two dual views of the same communication event. If $\alpha$ is the action of sending a message through a channel, $\overline{\alpha}$ is the dual action of receiving that message.
- **Internal Actions** Each calculus defines also a $\tau$ action, called *internal action* or silent action. Process calculi are designed to model the interaction between system, and abstract away from the low level details. A process $\tau.P$ can then performs a silent action, indicating internal operations, not known to an external observer, outside the scope of the system being modeled.
- **Non-determinism**: Each calculus has a *non-deterministic sum* of processes, denoted as $P + Q$. Such a process can non-deterministically 'choose' to behave like $P$ or like $Q$.
- **Parallel Execution**: Each calculus has *parallel composition* of processes, denoted as $P \parallel Q$. Such a process represents the concurrent execution of both $P$ and $Q$, and can perform all the actions of $P$ as well as all the actions of $Q$, in a interleaving manner. Differently from the nondeterministic sum, after $P \parallel Q$ performs an action of $P$, it can still perform the actions of $Q$.
- **Synchronization**: Each calculus has inter-process communication. Two parallel processes can *synchronize*, performing at the same time an action and a coaction. A parallel process $\alpha.P \parallel \overline{\alpha}.Q$ can evolve in $P \parallel Q$, as the two processes had performed a synchronous communication. Such synchronization transition results in an invisible action, as synchronization can be understood as a internal action of the (composite) process $\alpha.P \parallel \overline{\alpha}.Q$

To give a running example of a calculus with these features, we will define syntax and semantics of *value-passing CCS* [17].

$$P ::= \mathbf{0} \mid c!v.P \mid c?x.P \mid \tau.P \mid P + P \mid P \parallel P$$

In value passing CCS, $c!v$ is the action of sending a value $v$ through a channel $c$, and its coaction is $c?v$, of receiving a value from channel $c$. In the process $c?x.P$, we say that $x$ is a bound variable, otherwise it is free.

Usually, the semantics of a process calculus is given in a SOS-fashion, as a *Labeled Transition System.* Given a process $P$, its LTS can be understood as a rooted directed graph, where the nodes are processes, i.e. states of the computation, and the outgoing edges are the actions that a process can perform.

Formally, a Labeled Transition System is a triple $\langle S, Act, \rightarrow \rangle$ where

- $S$ is a set of states
- $Act$ is a set of transition labels
- $\rightarrow \subseteq S \times Act_\tau \times S$ is the transition relation, with $Act_\tau = Act \cup \{\tau\}$

An element $(s, \alpha, t) \in \rightarrow$ is called a *transition*, and is often written as $s \xrightarrow{\alpha} t$. We denote with $\Rightarrow$ the reflexive and transitive closure of $\xrightarrow{\tau}$, and use $s \overset{\alpha}{\Longrightarrow} t$ as an abbreviation for $s \Rightarrow s' \xrightarrow{\alpha} t' \Rightarrow t$ for some $s', t' \in S$. When dealing with process calculi, the set $S$ of states is the set of all processes, and a transition $P \xrightarrow{\alpha} P'$ means that the process $P$ performs an action $\alpha$ and evolves in $P'$.

The LTS of a process in value passing CCS is given by the following set of inference rules:

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

$$\frac{P \xrightarrow{\alpha} P'}{P + Q \xrightarrow{\alpha} P'} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P + Q \xrightarrow{\alpha} Q'}$$

$$\frac{P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P \parallel Q \xrightarrow{\alpha} P \parallel Q'}$$

$$\frac{P \xrightarrow{c!v} P' \quad Q \xrightarrow{c?v} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'} \qquad \frac{P \xrightarrow{c?v} P' \quad Q \xrightarrow{c!v} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}$$

### 2.2.2 Bisimulation

One of the most important notion in the theory of process calculi is behaviourally equivalence, i.e. recognizing when two processes express exactly the same behaviour. Different ways to compare the behaviour of two processes yields different definitions of equivalence. Since from the birth of process calculi, one of the most common definition of behavioural equivalence has been the *bisimilarity* relation. Two processes are bisimilar if each one can 'simulate', i.e. replicate, the behaviour of the other.

The simplest notion of bisimilarity is *strong bisimilarity*, where two bisimilar processes must perform exactly the same actions, both visible and silent. If we ignore the silent actions, we get instead *weak bisimilarity*, as it will be explained formally explained in the next paragraph.

Let $\langle S, Act, \rightarrow\rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *strong bisimulation* if and only if, whenever $s\mathcal{R}t$, then

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \xrightarrow{\alpha} t' \text{ for some } t' \text{ such that } s'\mathcal{R}t'$$

Two states $s, t \in S$ are said to be *strongly bisimilar*, written $s \sim t$, if a strong bisimulation $\mathcal{R}$ exists such that $s\mathcal{R}t$. This means that bisimilarity is the the union of all the bisimulation relations, and so the largest bisimulation. Strong bisimulation is an equivalence relation, i.e. is reflexive, symmetrical and transitive, and it is also a *congruence*, meaning that, if $P$ and $Q$ are bisimilar, so must be $P \parallel R$ and $Q \parallel R$, and $P + R$ and $Q + R$, and so on.

A weaker notion of behavioural equivalence is *weak bisimilarity*, which requires that two bisimilar processes exhibit the same visible actions, but allows each internal action to be matched by zero or more internal actions. Let $\langle S, Act, \rightarrow\rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *weak bisimulation* if and only if, whenever $s\mathcal{R}t$,

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \overset{\alpha}{\Longrightarrow} t' \text{ for some } t' \text{ such that } s'\mathcal{R}t'$$

$$\text{if } s \xrightarrow{\tau} s' \text{ then } t \Rightarrow t' \text{ for some } t' \text{ such that } s'\mathcal{R}t'$$

Two states $s, t \in S$ are said to be *weakly bisimilar*, written $s \approx t$, if a weak bisimulation $\mathcal{R}$ exists such that $s\mathcal{R}t$. Weak bisimilarity is not a congruence, as $P = \alpha.\mathbf{0}$ and $Q = \tau.\alpha.\mathbf{0}$ are bisimilar, but $P + \beta.\mathbf{0}$ and $Q + \beta.\mathbf{0}$ are not.

Halfway between strong and weak bisimilarity there is the notion of *branching bisimilarity*, that is coarser than strong bisimilarity, as its internal actions are not directly observed, but is finer than weak bisimilarity, as it matches the braching structure more accurately. Let $\langle S, Act, \rightarrow\rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *branching bisimulation* if and only if, whenever $s\mathcal{R}t$,

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \Rightarrow t' \xrightarrow{\alpha} t'' \text{ for some } t', t'' \text{ such that } s\mathcal{R}t' \text{ and } s'\mathcal{R}t''$$

Two states $s, t \in S$ are said to be *branching bisimilar*, written $s \simeq t$, if a branching bisimulation $\mathcal{R}$ exists such that $s\mathcal{R}t$.

The two processes

$$P = \alpha.\mathbf{0} + \tau.\beta.\mathbf{0} \qquad Q = \alpha.\mathbf{0} + \beta.\mathbf{0} + \tau.\beta.\mathbf{0}$$

are weakly bisimilar, because obviously if $P$ performs an action $Q$ can replicate it, and in $Q$ performs its additional $\beta$ action, $P$ can replicate it as $\tau.\beta$. These two processes are instead not branching bisimilar, because if $Q$ performs its $\beta$ action, $P$ cannot replicate it, as after a $\tau$ transition it evolves in $\beta.\mathbf{0}$, which is not bisimilar to $Q$.

### 2.2.3 Probabilistic LTS

The usual concepts of process calculus has been successfully extended to model probabilistic systems. We will present in this section the most common definitions of probabilistic LTS and probabilistic bisimulation, following the comprehensive analysis of [18, 9].

**Probabilistic Lifting**

First of all, we give some preliminary mathematical definitions about probabilistic distributions, and about the very general concept of *lifting* a relation between objects to a relation between distributions of objects.

Given a set $S$, a (discrete) *probability distribution on* $S$ is a mapping $\Delta : S \to [0, 1]$ such that $\sum_{s \in S} \Delta(s) = 1$. We indicate with $\mathfrak{D}(S)$ the set of all probability distribution on $S$. The *support* of $\Delta \in \mathfrak{D}(S)$ is defined as $\lceil \Delta \rceil = \{s \in S \mid \Delta(s) > 0\}$.

We use $\overline{s}$ to denote the *point distribution* on $s$ (also known as Dirac distribution, in the continuous case):

$$\overline{s}(t) = \begin{cases} 1 \text{ if } t = s \\ 0 \text{ if } t \neq s \end{cases}$$

Given a set $\{p_i\}$ of probabilities (i.e. $\sum_i p_i = 1$ and $p_i > 0$ for each $i$), we define the *convex combination* of distributions $(\sum_i p_i \Delta_i)$ as the only distribution such that

$$\left( \sum_i p_i \Delta_i \right)(s) = \sum_i p_i \Delta_i(s)$$

We often abbreviate $p\Delta + (1 - p)\Theta$ as $\Delta \;{}_p\!\oplus\; \Theta$.

For any set $D \subseteq \mathfrak{D}(S)$ of distributions, we denote with $CC(D)$ the *convex closure* of $D$, i.e. the least subset of $\mathfrak{D}(S)$ that contains $D$ and is closed un the operations $- \;{}_p\!\oplus\; -$ for any $p$ with $0 \leq p \leq 1$.

In order to extend the notions from to ‘classical’ process algebraic approach to a probabilistic setting, it is useful to define a *probabilistic lifting*, based on the concept of linearity.

A relation $\mathcal{R} \subseteq \mathfrak{D}(S) \times \mathfrak{D}(S)$ between distributions is said to be *linear* if $\Delta_1 \mathcal{R} \Theta_1$ and $\Delta_2 \mathcal{R} \Theta_2$ implies $(\Delta_1 \;{}_p\!\oplus\; \Delta_2)\mathcal{R}(\Theta_1 \;{}_p\!\oplus\; \Theta_2)$ of any $0 \leq p \leq 1$.

Given a relation $\mathcal{R} \subseteq S \times S$, we define its *lifting* $\mathring{\mathcal{R}} \subseteq \mathfrak{D}(S) \times \mathfrak{D}(S)$ as the smaller linear relation such that $s\mathcal{R}t$ implies $\overline{s}\mathring{\mathcal{R}}\overline{t}$.

With abuse of notation, we denote with the same symbol also the lifting of relations $\mathcal{R} \subseteq S \times \mathfrak{D}(S)$. Given a relation $\mathcal{R} \subseteq S \times \mathfrak{D}(S)$, we define its *lifting* $\mathring{\mathcal{R}} \subseteq \mathfrak{D}(S) \times \mathfrak{D}(S)$ as the smallest linear relation such that $s\mathcal{R}\Delta$ implies $\overline{s}\mathring{\mathcal{R}}\Delta$.

These lifted relations enjoy two useful properties. Interestingly, both this property are equivalent to the given definition, and are indeed used as the definition in various works on probabilistic bisimulation.

- Given $\mathcal{R} \subseteq S \times S$, $\Delta \overset{\circ}{\mathcal{R}} \Theta$ if and only if $\Delta$ and $\Theta$ can be decomposed as follows:
  1. $\Delta = \sum_{i \in I} p_i \overline{s_i}$, where $I$ is a finite index set and $\sum_{i \in I} p_i = 1$
  2. For each $i \in I$ there is a state $t_i$ such that $s_i \mathcal{R} t_i$
  3. $\Theta = \sum_{i \in I} p_i \overline{t_i}$
- Given an equivalence relation $\mathcal{R} \subseteq S \times S$, then $\Delta \overset{\circ}{\mathcal{R}} \Theta$ if and only if, for all equivalence classes $C \in S/R$
$$\sum_{s \in C} \Delta(s) = \sum_{s \in C} \Theta(s)$$

**Probabilistic Labelled Transition Systems**

We are now ready to introduce the main features of probabilistic process calculi. In addition to the usual operators of action prefixes, parallel composition and nondeterministic sum, such calculi often include a *probabilistic choice* operator, like $P\ {}_p\!\oplus Q$, where $p$ is any probability $0 \leq p \leq 1$. A process $P\ {}_p\!\oplus Q$ makes a probabilistic choice between $P$ and $Q$, that is, it evolves in a *distribution of processes.*

Formally, we define the operational semantic of a probabilistic process calculus as a *pLTS.*

A *Probabilistic Labelled Transition System* (pLTS) is a triple $\langle S, Act, \rightarrow \rangle$ where

- $S$ is a set of states
- $Act$ is a set of transition labels
- $\rightarrow \subseteq S \times Act_\tau \times \mathcal{D}(S)$ is the transition relation, with $Act_\tau = Act \cup \{\tau\}$

For example, we could write

$$\alpha.(P\ {}_{\frac{2}{3}}\!\oplus Q) \xrightarrow{\alpha} \overline{P}\ {}_{\frac{2}{3}}\!\oplus \overline{Q}$$

where $P\ {}_{\frac{2}{3}}\!\oplus Q$ is a single state, a syntactic element, and $\overline{P}\ {}_{\frac{2}{3}}\!\oplus \overline{Q}$ is a distribution of states, that assigns to state $P$ the probability $\frac{2}{3}$, and to state $Q$ the probability $\frac{1}{3}$

On this definition of pLTS, there are actually two separate notion of (strong) probabilistic bisimilarity, that differ for how they relate probabilities and non-determinism.

The first goes under the name of *Larsen-Skou bisimulation.* Let $\langle S, Act, \rightarrow \rangle$ be a pLTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *Larsen-Skou bisimultion* if and only if, whenever $s \mathcal{R} t$, then

$$\text{if } s \xrightarrow{\alpha} \Delta \text{ then } t \xrightarrow{\alpha} \Theta \text{ for some } \Theta \text{ such that } \Delta \overset{\circ}{\mathcal{R}} \Theta$$

The usual definition of Larsen-Skou bisimulation does not use the lifting operation, and requires that $\Theta$ assigns the same probability as $\Delta$ to each equivalence class of $S/R$, which is an equivalent formulation, according to the property of lifting seen in the previous section. Two states $s, t \in S$ are said to be *Larsen-Skou bisimilar*, written $s \sim_{LS} t$, if a Larsen-Skou bisimulation $\mathcal{R}$ exists such that $s \mathcal{R} t$.

The second, strictly coarser notion of probabilistic bisimilarity is *Segala bisimilarity*, which consider also the probabilistic behaviour that could happen in presence of an *adversary.* When there is a non-deterministic choice, like in $\alpha.P + \alpha.Q$, it is common to assume the existance of an external agent, an adversary, that resolves such nondeterministic choices in an arbitrary way. In the example made before, one could suppose an adversary that always chooses the left transition, or one that always chooses the right transition. Segala bisimilarity consider the cases when the adversary can randomize, and for example choose the left transition with probability $p$ and the right transition with probability $1 - p$.

To define Segala bisimilarity, is necessary to introduce *combined transitions*, i.e. a transition relation $\longrightarrow_{cc} \subseteq S \times Act_t \times \mathfrak{D}(S)$ such that

$$s \xrightarrow{\alpha} \Delta \text{ if and only if } \Delta \in CC(\big\{\Theta \mid s \xrightarrow{\alpha} \Theta\big\})$$

that is, $\Delta$ is reachable from $s$, or is a convex combination of distributions reachable from $s$. Hence, for example, $\alpha.P + \alpha - Q$ can evolve in $P_{\frac{1}{2}Q}\oplus$. Let $\langle S, Act, \rightarrow\rangle$ be a pLTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *Segala bisimultion* if and only if, whenever $s\mathcal{R}t$, then

$$\text{if } s \xrightarrow{\alpha} \Delta \text{ then } t \xrightarrow{\alpha}_{cc} \Theta \text{ for some } \Theta \text{ such that } \Delta\mathring{\mathcal{R}}\Theta$$

Two states $s, t \in S$ are said to be *Segala bisimilar*, written $s \sim_S t$, if a Segala bisimulation $\mathcal{R}$ exists such that $s\mathcal{R}t$.

### From pLTS to LTS

The given definition of pLTS can be seen as a disconnected, bipartite graph, where each node is either an element of $S$, i.e. a process, or an element of $\mathfrak{D}(S)$, i.e. a distribution of processes, and all the edges go from $S$ to $\mathfrak{D}(S)$. This is not a problem to define probabilistic bisimilarity, but there are other settings where a connected LTS is preferred, for example when defining weak bisimilarity, temporal logics or model checking algorithms.

To 'complete' a pLTS it is necessary to define how a distribution 'evolves', which are its outgoing transitions. There are two alternative approaches, that we could call 'probabilistic branching' and 'distribution transformer'.

The first, arguably more standard approach is *probabilistic branching*, that proposes a derivation rule like

$$\sum_i p_i\overline{s_i} \quad \overset{p_i}{\rightsquigarrow} \quad s_i$$

Where a distribution of processes 'picks' just one process, evolving with a *probabilistic transition.* This approach, used also in probabilistic model checking [22], gives a probability to the single transition, and so allows to define a probabilistic measure for a whole path of computation.

With such a rule, a pLTS $\langle S, Act, \rightarrow\rangle$ can be 'completed' to a bipartite LTS, where the states are either processes or distribution of processes, the $\rightarrow$ transition goes from states to distribution, with labels in $Act_\tau$, and the $\rightsquigarrow$ transition goes from distributions to states, with labels in $[0, 1]$.

The second, most recent approach, is known as the *distribution transformer* semantics, also called belief-state transformer semantics or labeled Markov process semantics [11, 21, 19]. It specifies that a distribution of processes must evolve in a distribution of processes, with a derivation rule like

$$\frac{p_i \xrightarrow{\alpha} \Delta_i \qquad \text{for each } i}{\sum_i p_i\overline{s_i} \xrightarrow{\alpha} \sum_i p_i\Delta_i}$$

So, for a distribution to evolve, it is necessary that all the precesses in its support can perform the same action $\alpha$. A distribution like $\alpha.P\,{}_{\frac{1}{2}}\!\oplus \beta.Q$, for example, has no outgoing transition.

Notice that the addition of this rule is equivalent to lifting the transition relation $\rightarrow \subseteq S \times Act \times \mathfrak{D}(S)$ to a relation $\overset{\circ}{\rightarrow} \subseteq \mathfrak{D}(S) \times Act \times \mathfrak{D}(S)$. Since each state $s \in S$ can be also seen as a distribution $\overline{s} \in \mathfrak{D}(S)$, this lifting relation de facto defines a 'complete' LTS of distributions $\langle \mathfrak{D}(S), Act, \overset{\circ}{\rightarrow} \rangle$. Observe that $\rightarrow_{cc} \subset \overset{\circ}{\rightarrow}$, and in fact this distribution transformation semantic is more often than not associated to a Segala bisimilarity.

### 2.2.4 Reduction systems

In the early works on process calculus, bisimilarity in its various forms was adopted as the mainstream notion of behavioural equivalence. Starting from [29], a different notion of equivalence was considered, conceptually simpler and more general, under the name of **barbed congruence**. According to this notion, two processes are equivalent if they cannot be distinguished by an external observer. That is, two processes $P$ and $Q$ are equivalent if, under any context $B[-]$, $B[P]$ and $B[Q]$ express the same observable behaviour, based on a general concept of 'observable', called *barb*.

We will first introduce the *reduction semantic* for process calculi, and then show how it can be used to define barbed equivalence.

A reduction semantic for a process calculus [27, 4], is an alternative way to define the dynamics of a process, using a *Reduction system* instead of a Labelled Transition System.

A *Reduction System* (RS), or unlabelled transition system, is a couple $\langle S, \rightarrow \rangle$ where

- $S$ is a set of states
- $\rightarrow \subseteq S \times S$ is the transition relation.

In a reduction system, like lambda calculus and other term-rewriting formalism, a reduction is possible only when the two subterms that interacts are syntactically contiguous, i.e. they form a redex.

It is possible to define a reduction system for a process calculus like value-passing CCS, for example identifying the redexes:

$$\tau.P \rightarrow P \qquad c!v.P \parallel c?x.Q \rightarrow P \parallel Q[v/x]$$

together with the usual rules

$$\frac{P \rightarrow P'}{P \parallel Q \rightarrow P' \parallel Q} \qquad \frac{P \rightarrow P'}{P + Q \rightarrow P'}$$

In process calculi, thanks to the labelled semantic, subprocesses are allowed to interact also when they are syntactically 'distant', like $c!v.\mathbf{0} \parallel d?x.\mathbf{0} \parallel c?x.P$. So in order to define a reduction system as the one above, it is necessary to introduce a way to ignore the syntactic arrangement and 'reorder' the subprocess as needed. This is achieved considering the reduction system modulo a *structural congruence relation.* In the case of value-passing CCS, this relaction could be the smallest equivalence relation that is closed for $\alpha$-conversion and satisfies

$$\begin{array}{ccc} P \parallel \mathbf{0} \equiv P & P \parallel Q \equiv Q \parallel P & P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R \\ P + \mathbf{0} \equiv P & P + Q \equiv Q + P & P + (Q + R) \equiv (P + Q) + R \end{array}$$

Notice that the reduction system presented above, together with the structural congruence relation, determines exactly the $\xrightarrow{\tau}$ transition of the LTS semantics presented in the previous section. Reduction systems are in fact often used to describe the dynamics of calculi with no interaction with an 'outside environment', so with no input nor output transitions, only inter-process communication.

Obiously, a bisimularity relation defined on a reduction system is a very coarse relation, that simply consider the number of computational steps a process can make. To recover the notion of strong LTS-bisimilarity in the reduction semantics setting, it is necessary to recover some of the 'observational power' of labelled bisimulations, through the concept of *barbs.*

We call *barb* a predicate on states, often used to capture a certain notion of 'observable property'. Given a barb $b$, we write $s \downarrow_b$ to say that $s$ statisfies the predicate $b$, i.e. expresses that property. For value-passing CCS, a suitable observable property is '$P$ is capable to send something on channel $c$'. That is, we define the barb $c$ as the predicate

$$\{P \mid \exists v, P' \; P \xrightarrow{c!v} P'\}$$

It is important to remark that in this case we defined, for simplicity, a barb as a property based on a preexisting labelled semantic. In all the most recent calculus the semantic of a process can be formulated directly as a reduction system, and the barbs are usually syntactic in nature.

Given a set of barbs, i.e. a set of observable properties, it is possible to define a *strong barbed bisimulation.* Let $\langle S, \rightarrow\rangle$ be a RS, and $B$ a set of barbs. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *barbed bisimulation* if and only if, whenever $s\mathcal{R}t$, then

- If $s \downarrow_b$ for some barb $b \in B$, then $t \downarrow_b$
- If $s \rightarrow s'$ then $t \rightarrow t'$ for some $t'$ such that $s'\mathcal{R}t'$

Two states $s, t \in S$ are said to be *barbed bisimilar*, written $s \sim_b t$, if a barbed bisimulation $\mathcal{R}$ exists such that $s\mathcal{R}t$.

Barbed bisimilarity is often not useful per se, as for example $c!0.a!0.\mathbf{0} \sim_b c!0.b!0.\mathbf{0}$, since they both express the barb $\downarrow_c$, and have no outgoing transition. Barbed bisimulation is commonly used as the discriminating property of a contextual equivalence, called *barbed equivalence.*

A context is a 'process with a hole', for example $B[-] = [-] \parallel R$ or $B[-] = [-] + R$, where $R$ is any process. Given a context $B[-]$, we define as $B[P]$ as the process obtained 'filling' the hole with $P$, i.e. substituting $P$ in place of $[-]$.

Given a set of contexts, two processes $P$ and $Q$ are said to be *barbed equivalent*, or barbed congruent, written $P \simeq_b Q$, if for any context $C[]$, it holds that $C[P] \sim_b C[Q]$. With the previously defined barb $\downarrow_c$, and choosing just parallel context of the form $[] \parallel R$, it is possible to prove that

$$P \simeq_b Q \text{ if and only if } P \sim Q$$

that is, barbed equivalence is exactly the same as labelled bisimilarity. Similar results can be obtained also for weak bisimilarity, with an appropriate notion of weak barb.

To sum up, a reduction semantic allows to define a barbed equivalence relation, that:

- Has the same power of labelled bisimilarity, but is defined in terms of a simpler transition system, inspired by term rewriting system;
- is 'parametric' with respect to different barbs and different contexts, allowing for different observational power for the same calculus;
- is based on the very general concept of contextual equivalence, and it is used as the prototype of 'natural, standard behavioural equivalence' for a lot of new calculi;
- is more difficult to prove, as it involves a universal quantification on all possible contexts, whereas usually proving bisimilarity requires only to provide a bisimulation.

# Chapter 3

# Comparison of Quantum Process Calculi

There is a number of proposals of quantum process calculi in the literature, often with different syntax, semantics and behavioural equivalences, even if they all model the same systems and the same protocols. There are three main lines of research that developed in recent years. The first, started with QPAlg and then developed with CQP, is inspired by the $\pi$-calculus. The second approach, developed simultaneously but independently, is centered around qCCS, that is a quantum extension of value-passing CCS. This thesis will focus on analyzing similarities and differences of these three calculi, QPAlg, CQP and qCCS. The third proposal, qACP, is less directly related and comparable with the first two, in the same way as its classical counterpart ACP is designed in a different fashion with respect to CCS/$\pi$-calculus. We postopone its comparison to future work.

## 3.1 LTS and quantum states

### 3.1.1 QPAlg

In classical process calculi, the operational semantics is given in terms of transitions $P \xrightarrow{\alpha} P'$ between processes. In [24], the authors describe how to 'quantumize' a simple classical process caulculus, adding quantum variables and quantum actions to it. To do so, processes manipulating and communicating quantum data are always coupled with a state vector, describing the current value of the quantum variables. The operational semantic of QPAlg describes in fact an LTS composed of *configurations*, i.e. states of the form [1]

$$\langle q_0, \ldots, q_n = \rho, P \rangle$$

in which $P$ is a process containing $q_0 \ldots q_n$ as free quantum variables, and $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$ describes the state of the qubits manipulated by $P$. The same approach is used in (almost) all the other calculi proposed so far, and has become somewhat standard. We will often write $\widetilde{q}$ to denote the $n$-tuple $q_1 \ldots q_n$.

This idea captures the imperative, stateful nature of quantum computation, in which a sequence of transformations are applied to the quantum variables (the qubits), treated as a mutable data structure. In QPAlg, processes can be contructed with the usual actions of vaule-passing calculi, $c?x$, $c!v$, but also with *quantum actions*, like $X, Z, H, M_{01}$,

[1] The actual configurations described in QPAlg are more complex than this, containing also a stack to manage variable declaration. We will omit these non-quantum constructs to simplify the presentation and the comparisons.

that correspond to applying unitaries or measurement to the underlying quantum state:

$$\langle q = \rho, H[q].P\rangle \xrightarrow{\tau} \langle q = H\rho H^\dagger, P\rangle$$

Separating the syntactic, control part of the configuration (the process $P$) from the underlying quantum data (the statevector $|\psi\rangle$) allows also for a 'pass-by-reference' way of communication, opposed to the 'pass-by-value' of classical value passing process algebras. The usual rule for reception, in fact, would be

$$c?x.P \xrightarrow{c?v} P[v/x] \qquad \text{for any value } v$$

In this way, if $Q$ contains two occurrences of $x$, each of them gets instantiated with a different, independent copy of the value $v$. But if the value $v$ was a quantum state $\rho$, this would require duplicating the quantum information, which is impossible due to the No-cloning theorem (Theorem 2.1.1). The solution proposed in various quantum calculi is substituting just the name of the variable, duplicating only the 'pointers' to the same value.

$$\langle \widetilde{q} = \rho, c?x.P\rangle \xrightarrow{c?q} \langle \widetilde{q} = \rho, P[q/x]\rangle \qquad \text{for any } q \in \widetilde{q}$$

Notice that this idea requires the peculiar assumption that the *value* recived from the external environment is already represented in the configuration. In QPAlg and in other early works [14] there was a different rule, where the state vector is extended with a new value received from the environment. This approach was abandoned in more recent calculi, because extending the state vector when a qubit is received (or shrinking it when a qubit is sent) works poorly when exchanging entangled qubits. Suppose that a process $P$ receives just one qubit of a Bell pair, i.e. a qubit that is entangled with something on which $P$ has no control. The only way to represent the new qubit in the configuration is with its reduced density operator $\frac{1}{2}I$. But what happens if the process then receives also the second qubit of the Bell pair? It is now impossible to reconstruct the original Bell pair.

Besides, the assumption that the qubit to be received is already represented in the configuration is indeed correct when there is a synchronization between two processes. In that situation, it would be inaccurate to extend the configuration with a new density operator. The systems that allocate a new qubit when receiving end up with de facto two different behaviors, one for communication between processes and one for communication with an unknown environment. This difference is reasonable, but is in contrast with the compositional design of process algebras, and has been abandoned in later systems.

Another key feature present in QPAlg and in all other calculi is the coexistence of *nondeterminism*, arising from sums and parallel composition, and probabilistic behaviour, arising from the probabilistic nature of quantum measurements. When the process P, with state $\rho$ performs a measurement, there is a distribution of possible configurations in which it could evolve. So in all quantum process calculi, the semantics of a process can be defined by a pLTS $\langle Conf, Act, \to\rangle$, where $Conf$ is the set of all possible configurations, and $\to$ goes from $Conf$ to $\mathfrak{D}(Conf)$

$$\langle q = |+\rangle\langle+| \, , M_{01}[q].P\rangle \xrightarrow{\tau} \langle q = |0\rangle\langle 0| \, , P'\rangle \;{}_{1/2}{\oplus}\; \langle q = |1\rangle\langle 1| \, , P''\rangle$$

QPAlg follows the 'probabilistic-transition' approach, so the distributions state branches probabilistically in one of the possible outcomes.

The last relevant detail of the rules of QPAlg, shared also by the other calculi, is the treatment of parallel composition. Due to entangled states, the parallel operator is not entirely compositional. That is, the behaviour of $P \parallel Q$ cannot be described simply as the interleaving of $P$ and $Q$.

Only if two processes $P$ and $Q$ act on separable qubits, in fact, it would possible to treat them independently

$$\frac{\langle \widetilde{p} = \rho, P\rangle \xrightarrow{\alpha} \langle \widetilde{p} = \rho', P'\rangle}{\langle \widetilde{p}, \widetilde{q} = \rho \otimes \sigma, P \parallel Q\rangle \xrightarrow{\alpha} \langle \widetilde{p}, \widetilde{q} = \rho' \otimes \sigma, P' \parallel Q\rangle}$$

But when $p, q$ are entangled, the quantum actions of $P$ cannot always be considered 'local' to the process, as they effect also the value of $q$ (despite being labelled as internal transitions). So in QPAlg a more general rule is used:

$$\frac{\langle \widetilde{p}, \widetilde{q} = \nu, P\rangle \xrightarrow{\alpha} \langle \widetilde{p}, \widetilde{q} = \nu', P'\rangle}{\langle \widetilde{p}, \widetilde{q} = \nu, P \parallel Q\rangle \xrightarrow{\alpha} \langle \widetilde{p}, \widetilde{q} = \nu', P' \parallel Q\rangle}$$

where the quantum actions of $P$ must be intended as transformations on the whole Hilbert space $\mathcal{H}_p \otimes \mathcal{H}_q$.

### 3.1.2 CQP

In [15], the authors presented their calculus Communicating Quantum Process. The main contribution of their work is the introduction of affine type system, used to restrict the set of possible processes of the algebra to the 'admissible' ones. Under the assumption that Alice, Bob and Charlie are in three different physical locations, in fact, the process

$$Alice = b!q.c!q.P$$

should not be well typed, because Bob could read from the $b$ channel, Charlie from the $c$ channel, and quantum information would be duplicated .

Variables and expressions in CQP can have types **Int**, **Qbit** and **Unit**, and channels have the corresponding types $\hat{}$**Int**, $\hat{}$**Qbit**, $\hat{}$**Unit**. The typing judgements in CQP have the form

$$\Gamma \vdash P$$

meaning that $P$ is well typed under the context $\Gamma$. $\Gamma$ contains both classical variables and quantum variables: the former are treated as usual, the latter are subject to affine typing rules. Affine rules guarantee that each quantum variable will be sent at most once, and cannot be used after it is sent.

From the practical point of view, this means that,

- if $c!q.P$ is well typed, where $q$ is a quantum variable, then $P$ cannot contain any other occurrences of $q$.
- if $P \parallel Q$ is well typed, then $P$ and $Q$ cannot have occurrences of the same free quantum variables. The authors call this property *unique ownership of qubits.*

Notice that the typing rules are not *linear*, as that weakening holds both for classical and quantum variables. This means that the quantum variables must be sent at most once, not exactly once. So a process like

$$P = c?q.H[q].\mathbf{0}$$

is well typed, and the qubit denoted by $q$ becomes inaccessible for all other processes.

An important remark is that the typing rules are intended to model processes in different physical location, where sending a qubit means physically moving the quantum system. In other settings this type system could be not necessary. For example different processes in a quantum computer, manipulating the same set of quantum registers, situations like

$$H[q].P \parallel Y[q].Q$$

are reasonable, and their behaviour would be described as usual as a race condition between the to processes acting on the same shared data.

All the characteristics of QPAlg, in terms of configurations, probabilistic branching and parallel composition are also present in CQP. Differently from QPAlg, CQP describes *closed quantum systems*, without an unknown environment. That is, there are no transitions $\xrightarrow{c?x}$ or $\xrightarrow{c!v}$, all the communication happens as synchronization between processes. According to this, CQP semantics is described as a reduction system, where the transitions corresponds either to internal actions or infra-process communication.

Without interaction with an external environment, all the information is completely represented in the initial configuration, and then there is no need to use mixed quantum states. The state of the quantum variables is thus described as a state vector.

CQP is based on the typed pi calculus, with constructs to create new (typed) channel names, new classical variables and new quantum variables. When a declaring new qubit, the state vector is extended with the default value $|0\rangle$

$$\langle q_1, \dots q_n = |\psi\rangle, \texttt{qbit}\ x.P\rangle \to \langle x, q_1, \dots q_n = |0\rangle \otimes |\psi\rangle, P\rangle$$

Thanks to its type system, CQP supports integers and arithmetic expressions, and also *quantum expressions* like $q_1 \dots q_n {*}= U$ and $M[q_1 \dots q_n]$. These expressions take the place of quantum action prefixes of QPAlg, changing the underlying quantum state and causing probabilistic branching.

In [8], the author introduces a labelled semantics to CQP, so to define a bisimilarity relation on CQP processes. On top of internal actions and synchronization, the possible actions of a process are as usual reception and sending, in the form $c?x$ and $c!v$. A process $\langle q_1 \dots q_n = |\psi\rangle, c?x.P\rangle$ can evolve receiving a qubit $q_i$ from the environment, but its names and values must already be present in the configuration. Reception and sending in CQP do not modify the quantum state, simply move the quantum names around. As already said, this can be seen as physically moving qubits between different location, but also as concurrent processes exchanging lock on some shared variable, to guarantee mutual exclusion.

As for the previous work, all the information is contained in the initial configuration and is never lost, so quantum variables state is expressed as a state vector, instead of as a density matrix.

In order to define a bisimilarity relation that is also a congruence, in [8] a different semantics is proposed, featuring so called *mixed configurations*. These mixed configurations can be considered as probabilistic distributions of configurations, but must be treated as a single state. In other words this semantics mixes the 'probabilistic transition' and 'probabilistic state' approches of Section 2.2.3: after a measurement, a configuration evolves in a mixed configuration (that is, a distribution of configurations), and this mixed configuration does not perform a probabilistic transition, so does not decays in a single configuration.

Mixed configurations represent partial knowledge of the classical variables in a configuration, just like mixed states represent partial knowledge of quantum state. So, after a measurement, a configuration must evolve in a mixed configuration, because to an external observer, the outcome of the measurement is unknown. Only when the mixed configuration performs an output transition, where it communicates the output of the measurement, a mixed configuration can branch probabilistically in one of its possible configurations. As we will see, this difference is crucial, because it changes the observable properties of the defined system: in the previous semantics, after a measurement there would be always a probabilistic branching, i.e. the outcome probabilities are immediately observable; in the mixed configuration semantics, after a measurement there are no probabilities to observe (as that outcome is still local to the process), and the probabilities appear only when and if the outcome is comunicated.

### 3.1.3 qCCS

In [14], the authors present qCCS, applying the ideas of in QPAlg and CQP to a simpler CCS-inspired calculus, without new name declaration and without expressions. A qCCS process is defined assuming a fixed set con classical channels, of quantum channels, and of quantum names. qCCS enforces the same conditions of 'unique ownership of qubits' of CQP, but without the use of a type system. The terms in qCCS are in fact inductively constructed in a way that preserves this property, for example specifying that $c!q.P$ is a process only if $q$ is not a free quantum variable in $P$.

In the first work on qCCS two different rules for quantum input where presented, one adding a qubit to the configuration, the other assuming that the qubit is already present in the configuration. As already said, only the second rule was used in subsequent works.

All the characteristics of QPAlg and CQP, in terms of configurations, parallel composition and communication are also present in CQP. The main difference between qCCS and the previous calculi is its 'distribution transfomer' approach to treat probabilities and nondeterminism, discussed below. Another distinctive characteristics is that qCCS features recursive processes, which are absent in QPAlg and CQP. For the sake of comparison, we will ignore recursive processes in the rest of this chapter.

Like in QPAlg, a process can be constructed with *quantum actions*, that in qCC are unitaries, superoperators and measurements. A measurement introduces a new classical variable to represent the outcome, and evolves in a distribution of configurations

$$\langle q = |+\rangle\langle+| \, , M_{01}[q \triangleright x].P\rangle \xrightarrow{\tau} \langle q = |0\rangle\langle 0| \, , P[0/x]\rangle \;{}_{1/2}{\oplus}\; \langle q = |0\rangle\langle 0| \, , P[1/x]\rangle$$

In [14], a distribution of configurations cannot evolve in any manner, but in [13, 10], the transition relations $\longrightarrow \subseteq Conf \times Act_\tau \times \mathfrak{D}(Conf)$ is lifted to a relation between distributions $\longrightarrow \subseteq \mathfrak{D}(Conf) \times Act_\tau \times \mathfrak{D}(Conf)$, i.e. following the 'distribution transformer' approach described in Section 2.2.3.

Among the various semantics developed for qCCS, in order to find a bisimilarity equation that was also a congruence, in [40] the authors proposed a simplified fragment of qCCS, without measurements and classical data. The semantic is purely non-deterministic, without probabilistic behaviour, and the superoperators applied are treated as *observable actions*, as possible labels of the transition relation. This calculus is an alternative approach to the other calculi in literature, relying on different assumptions, and we will not discuss in more detail in this chapter.

## 3.2 Bisimulation

We now focus on the various bisimilarity notion for quantum processes presented in the literature. All of these bisimilarities employ the probabilistic lifting seen in section 2.2.3, some defining a Larsen-Skou bisimilarity, some others a Segala bisimilarity. What really tells apart the different notions are their quantum related details, reguarding which are the observable properties of quantum values, and when these values are considered visible.

### 3.2.1 QPAlg/CQP

In [23], the authors propose a notion of bisimilarity for QPAlg, that was adapted in [8] for the labelled semantic of CQP. This bisimilarity is based on a probabilistic branching bisimilarity, and deals with quantum communication equating the reduced density matrices of sent qubits. In other words, when a process $P$ performs an output transition $c!v$, for a classical value $v$, a bisimilar process $Q$ should perform an output transition on the same channel with the same value. When a process $P$ performs an output transition $c!x$, for a *quantum name* $x$, $Q$ is not required to output the same *name* $x$, it must instead send a qubit with the same *state* of $x$. The chosen way to define the state of qubit $q$ in the configuration with (global) state $q, q_1 \dots q_n = \rho$ is the reduced density matrix of $q$, i.e. $tr_{q_1 \dots q_n}(\rho)$.

In QPAlg, as in all the other quantum calculi, the bisimilarity is given as a relation between configurations, and then lifted to a relation between processes. Two processes $P$ and $Q$ are considered bisimilar, written $P \sim Q$, when $\langle \widetilde{q} = \rho, P\rangle$ is bisimilar to $\langle \widetilde{q} = \rho, Q\rangle$ for any $\rho$.

This bisimilarity considers the state of a qubit an observable only when it is sent to the external environment. This means that the processes

$$P = X[q].\mathbf{0} \qquad Q = Z[q].\mathbf{0}$$

are indeed bisimilar, as the qubit $q$ ends up with a different quantum state, but the difference is never observed, because the qubit is never sent.

This bisimilarity is not a congruence with respect to summation and parallel composition. The former is expected with weak or branching bisimilarity, and is due to the usual not quantum-related problem

$$\begin{gathered} c!v.\mathbf{0} \sim \tau.c!v.\mathbf{0} \\ c!v.\mathbf{0} + d!v \not\sim \tau.c!v.\mathbf{0} + d!v \end{gathered}$$

The problem with parallel composition is instead purely quantum-related, as it is caused by the side effect of measurements and entanglement. Consider the following example:

*Example* 3.2.1. The two processes $P$ and $Q$ are bisimilar, but $P \parallel c!q_2$ is not bisimilar to $Q \parallel c!q2$:

$$\begin{array}{ccc} P = M_{01}[q_1].\mathbf{0} & \sim & Q = M_{\pm}[q_1].\mathbf{0} \\ P \parallel c!q_2 = M_{01}[q_1].\mathbf{0} \parallel c!q_2 & \not\sim & Q \parallel c!q_2 = M_{\pm}[q_1].\mathbf{0} \parallel c!q_2 \end{array}$$

$P$ and $Q$ are clearly bisimilar, as they do not perform any visible action. But when $P \parallel c!q_2$ operates on an entangled state, like the Bell state $\Phi^+ = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$, the measurement that happens on $q_1$ has effect on $q_2$, and $q_2$ will decay in state $|0\rangle$ or $|1\rangle$. The same happens when $Q \parallel c!q_2$ operates on the same Bell state, and $q_2$ will decay in state $|+\rangle$ or $|-\rangle$. When $q_2$ is sent, this difference becomes observable, and the two processes are not bisimilar.

### 3.2.2 qCCS

The bisimilarity relations proposed for qCCS differ from the one for QPAlg in a number of 'classical' details, not related to the quantum properties. First of all, for qCCS strong and weak bisimilarity are defined, not branching bisimilarity. QPAlg addresses probabilistic behaviour with a Larsen-Skou bisimulation, qCCS with a Segala bisimulation.

Besides these 'non-quantum' differences in the treatment of silent transitions and probabilities, one key difference telling the two relations apart is the notion of 'observable' quantum state. While in QPAlg the state of a qubit could be observed only when it is sent, in qCCS the state of a qubit can be observed as soon as the computation has 'ended', i.e. when there are no more transformations to be applied to that qubit.

In [14], two configurations $\langle \widetilde{q} = \rho, P\rangle$ and $\langle \widetilde{q} = \sigma, Q\rangle$ being bisimilar requires that if $\langle \widetilde{q} = \rho, P\rangle \not\to$, then $\langle \widetilde{q} = \sigma, Q\rangle \not\to$ and $\rho$ is equal to $\sigma$, up to a permutation of the quantum names in $\widetilde{q}$.

An equivalent condition was present in [40], where the quantum actions $U[q]$, $M[q]$ and $\mathcal{E}[q]$ were considered observable actions, and used as labels of the LTS. Since two bisimilar processes perform the same observable action, when starting from the same quantum state $\rho$ they will necessarily end up in the same quantum state $\rho'$.

The condition presented in [14] was too strict, and did not work well with non-terminating recursive processes. So in [13] a more general version has been proposed, requiring the equality not of the whole quantum state, but only of the qubits that will not be further modified. For example, in a configuration $\langle q_1, q_2 = \rho, H[q_2].\mathbf{0}\rangle$, the bit $q_1$ should be regarded as observable, as it does not appear as a free quantum variable in $H[q_2].\mathbf{0}$. The bit $q_2$, instead, should not be considered when checking for bisimilarity, as it is not in its final state.

More formally, [13] defines the notion of *environment* of a configuration, namely the reduced density operator of the values of the qubits not used by the process.

$$env(\langle \widetilde{q} = \rho, P\rangle) = tr_{qv(P)}(\rho)$$

The bisimilarity of $\langle \widetilde{q} = \rho, P\rangle$ and $\langle \widetilde{q} = \sigma, Q\rangle$ then requires that $env(\langle \widetilde{q} = \rho, P\rangle) = env(\langle \widetilde{q} = \sigma, P\rangle)$. Thanks to this condition, the bisimilarity proposed in [13] is a congruence, as it is preserved by parallel composition (contrary to QPAlg).

Consider the example seen before

$$P = M_{01}[q_1].\mathbf{0} \qquad Q = M_{\pm}[q_1].\mathbf{0}$$

$P$ and $Q$ are not bisimilar for [14, 13, 10] , as they end in different quantum states. $\langle q = |0\rangle\langle 0| \, , P\rangle$ will evolve in a (point) distiribution $\overline{\langle q = |0\rangle\langle 0| \, , \mathbf{0}\rangle}$, while $\langle q = |0\rangle\langle 0| \, , Q\rangle$ will evolve in a distribution $\langle q = |+\rangle\langle +| \, , \mathbf{0}\rangle \; {}_{\frac{1}{2}}\!\oplus \; \langle q = |+\rangle\langle +| \, , \mathbf{0}\rangle$. Since the state of $q$ is observable, the two distributions are not bisimilar in the sense of probabilistic bisimulation, as they are composed by not-bisimilar states.

In [10], a new, definitive notion of bisimilarity for qCCS is defined, in the form of an open bisimilarity. This bisimilarity is similar to the previous one [13], but it is *closed with respect to superoperator application.* That is, two configurations $\mathcal{C}$ and $\mathcal{C}'$ being bisimilar requires that also $\mathcal{E}(\mathcal{C})$ and $\mathcal{E}(\mathcal{C}')$ are bisimilar, for any trace-preserving superoperator $\mathcal{E}$ that acts on the qubits not used by $\mathcal{C}$ and $\mathcal{C}'$. The intuition behind this condition is that, if two configurations are bisimilar, they must still be bisimilar also when the external environment performs any kind of transformation on the unused qubits of the system. As this bisimilarity incorporates and extends all the ideas of [13, 40, 13] we will use this open bisimilarity as a touchstone for the novel behavioural equavelences defined in the next chapter.

In [12] the authors propose a symbolic semantic for qCCS, that abstracts away from the actual quantum state in the initial configuration. Instead of probabilistic distribution, the concept of *superoperator-valued distribution* is used, i.e. functions that associate each process with a trace non-increasing superoperator. In this context, a superoperator valued distribution represents both the probability that a process is reached, and also the accumulated transformations that were applied to the quantum state to reach that process. The associated symbolic bisimilarity is proven to be equivalent to open bisimilarity of [10], but has the advantage of considering smaller transition systems, and so it is better suited for model checking.

### 3.2.3 Mixed Configuration CQP

In [8], the author provides a labelled semantics and a bisimilarity notion for CQP, which is not a congruence with respect to parallel composition, as seen in section 3.2.1. In [8], the author defines the mixed configuration semantic for CQP, and on that system describes a bisimilarity that is also a congruence. This bisimilarity, similar to the one in QPAlg, is a probabilistic branching bisimilarity, that observes the quantum values only when they are sent. Differently from the previous proposal, it also requires the equality of the 'environment' of a configuration, like in qCCS.

Recall that in this semantics a configuration that performs a quantum measurement evolves in a 'mixed configuration', i.e. a sort of probabilistic distribution of configurations, in which the probabilities are not immediately observable.

Both mixed configurations and distributions of configurations describe all the various outcomes with their relative probabilities. The difference is that a distribution exhibits immediately this probabilistic behaviour, choosing only one of the possible configurations with a probabilistic transition. A mixed configuration, instead, can perform all the usual labeled actions, remaining a mixed configuration, without picking a single outcome and dropping the others.

Reguarding bisimilairity, the consequence is that the configuration $\mathcal{C}$, bisimilar to the configuration $\mathcal{C}'$, must exhibit the same probabilistic moves of $\mathcal{C}'$ only when the outcome is sent, and not immediately after the measurement.

Also the environment of $\mathcal{C}$ must be equal to the environment of $\mathcal{C}'$ only when $\mathcal{C}$ and $\mathcal{C}'$ perform an output transition. Note that, since mixed configurations must be treated as a single state, the notion of environment must be extended accordingly. If $\langle \widetilde{q} = \rho, P \rangle \;{}_p\!\oplus \langle \widetilde{q} = \sigma, Q \rangle$ is a mixed configuration, the environment is defined as:

$$env(\langle \widetilde{q} = \rho, P \rangle \;{}_p\!\oplus \langle \widetilde{q} = \sigma, Q \rangle) = p * env(\langle \widetilde{q} = \rho, P \rangle) + (1-p) * env(\langle \widetilde{q} = \sigma, Q \rangle)$$

and the environment of a configuration is defined as the reduced density operator of the qubits not owned by the process.

This bisimulation is coarser than the one in qCCS, and arguably captures more appropriately the expected beheavioural equivalence of quantum processes. For this bisimulation, for example, it holds that

$$\begin{array}{ccc} P = M_{01}[q_1].\mathbf{0} & \sim & Q = M_{\pm}[q_1].\mathbf{0} \\ P \parallel c!q_2 = M_{01}[q_1].\mathbf{0} \parallel c!q_2 & \sim & Q \parallel c!q_2 = M_{\pm}[q_1].\mathbf{0} \parallel c!q_2 \end{array}$$

In fact, since the qubit $q_1$ is lost, an external observer can rely only on $q_2$ to distinguish $P$ and $Q$, which is not possible because of quantum properties of mixed states.

As a drawback, this result is obtained through a considerably not-standard approach, diverging from the usual rules of probabilistic calculi. Recovering this result in the usual framework of pLTS remains an interesting open problem, that we target in the following part of the thesis.

# Chapter 4

# Linear qCCS

We present a new quantum process calculus, designed to resolve the ambiguities and differences present in the other proposals. This allows to investigate more deeply the different notions of behavioural equivalence of quantum systems. This novel calculus goes under the name of Linear qCCS (lqCCS), as it is an asynchronous version of qCCS, but employs a linear type system, similar to the affine type system for CQP.

After introducing lqCCS and its type system, we overview some desired properties of behavioural equivalence, in the light of which we investigates two alternative notions of bisimilarity. More in detail, we see how the type system disambiguates between two alternative notions of observability of quantum states. We show that some distinctive features of different approaches coincides when such ambiguity is removed. We define then a standard probabilistic bisimulation a là Larsen-Skou, in the spirit of [10], and we give some properties that help proving it.

Then we show some limitations of the fully-probabilistic approach, proving it is too fine-graned for the quantum case. Thus, we derive an updated versione of bisimilarity that solves this issue while maintaining the previous properties. Finally, we compare our proposal with related works.

## 4.1 The Language

Linear qCCS is equipped with all the common features of 'classical' process calculi, like action prefixes, nondeterministic choice, parallel composition and classical communication. It includes also the most general 'quantum' components, like quantum communication, measurements and superoperator application (that subsumes unitary transformations).

Linear qCCS is an *asynchronous* calculus [6], meaning that the output actions $c!v$ are *non-blocking*, the process cannot wait for the 'reception' of the sent value, i.e. the dual input coaction. In an asynchronous calculus, a term like $c!v.P$ is not a valid process, as there cannot be any continuation after an output action. A synchronous process like $c!v_1.c!v_2.P$ is usually rewritten in an asynchronous calculus as $c!v_1 \parallel c!v_2 \parallel P$. A key consequence of asynchrony is that the process has no control on the order in which $v_1$ and $v_2$ will be received.

We adopted a state-of-the-art asynchronous system as it simplifies the syntax, works well with linearity, and reduces the conditions to be checked to ensure single ownership of qubits.

### 4.1.1 Syntax

The syntax of lqCCS is designed to be consistent with qCCS, with a few exceptions: we divide the syntactic terms in parallel processes $P$ and sequential processes $K$, we provide a simple syntax for expressions, we consider only output actions without a continuation, and we replace the guard with a **If Then Else** operator.

A lqCCS *pre*-term is generated by the syntax:

$$\begin{aligned} P &::= K \mid c!e \mid P \parallel P \mid P\{f\} \mid P \setminus c \\ K &::= nil \mid \tau.P \mid \mathcal{E}(\widetilde{x}).P \mid M(\widetilde{x} \triangleright y).P \mid c?x.P \mid \\ &\qquad K + K \mid \textbf{if } e \textbf{ then } P \textbf{ else } P \\ e &::= x \mid b \mid n \mid \neg e \mid e \vee e \mid e \leq e \end{aligned}$$

where $b \in \mathbb{B}$, $n \in \mathbb{N}$, $x, y \in$ Var, $c \in$ Chan, with Var a denumerable set of variable names, and Chan a set of channel names. We use $\widetilde{x}$ to indicate a tuple of variables $x_1, \dots x_n$.

Each superoperator symbol $\mathcal{E}$ has a given arity $n$, and denotes a particular trace preserving superoperator on $\mathcal{H}^{\otimes n}$, where $\mathcal{H}$ is the two-dimensional Hilbert space of a qubit. We will often use symbols like $\mathcal{E}_U$ to denote the superoperator $\mathcal{E}(\rho) = U\rho U^{\dagger}$, but also symbols like $Set_0$, $Set_+$, $Set_{\Phi^+}$ to denote the corresponding superoperators. We write $\mathcal{E} : Op(n)$ to indicate that $\mathcal{E}$ is a suoperoperator symbol with arity $n$.

Each measurement symbol $M$ has a given arity $n$, and denotes a measurement $\{ M_0, \dots, M_{k-1} \}$ with $k$ different outcomes, where for each $0 \leq m \leq k-1$, $M_m$ is a linear operator on $\mathcal{H}^{\otimes n}$ and $\mathcal{H}$ is the two-dimensional Hilbert space of a qubit. We will use the symbol $M_{01}$ to denote the one-qubit measurement on the computational base $\{ M_0 = | 0\rangle\langle 0 | , M_1 = | 1\rangle\langle 1 | \}$, and the symbol $M_{\pm}$ to denote the one-qubit measurement on the diagonal base $\{ M_0 = | +\rangle\langle + | , M_1 = | -\rangle\langle - | \}$. We write $M : Meas(n)$ to indicate that $M$ is a measurement symbol with arity $n$.

We say that the channel name $c$ is *bound* in $P \setminus c$, and it is *free* when it is not bound by any restriction operator. We denote with $fc(P)$ the set of free channels of $P$.

We use $discard(e)$, as syntactic sugar for $c!e \setminus c$, and $discard(\widetilde{e})$, or also $disc(\widetilde{e})$, as syntactic sugar for $discard(e_1) \parallel \dots \parallel discard(e_n)$.

The expressions contain simple operators $\neg$, $\vee$, $\leq$, and can be trivially extended with $\wedge, \Rightarrow, \geq, =$ and so on.

lqCCS features a boolean match operator, **if** $e$ **then** $P_1$ **else** $P_2$, roughly equivalent to $[e]P_1 + [\neg e]P_2$ of qCCS. The advantage of the former is that it always evolves in exactly one branch. On the countrary, guarded sums may be neither mutually exclusive nor exaustive, like in $c?x.[x > 0].P + [x < 0].Q$. As we will see, the **if then else** construct is helpful when constructing linear processes.

We decided to keep the presentation as simple as possible, hence to omit recursively defined processes. This simplifies our type system and the comparison with other calculi.

### 4.1.2 Type System

CQP type system, as well as the equivalent syntactic rules for qCCS, treats quantum name communication in an affine way: each quantum variable can be sent at most once. This allows processes like

$$P = H[q].\mathbf{0} \qquad Q = X[q].\mathbf{0}$$

This syntax has created a crucial ambiguity in the literature, with consequences on the different notion of bisimilarity defined in QPAlg/CQP and qCCS. In QPAlg and CQP, the qubit $q$, owned by the processes $P$ and $Q$ above is *not* visible for an outside observer, as it is never sent. In qCCS, the qubit $q$ *is* indeed visible for an external observer, as explained in Section 3.2. In QPAlg/CQP $P$ and $Q$ are bisimilar, while in qCCS they are not.

To resolve this ambiguity, we introduce a *linear* type system, where each quantum variable must be sent exactly once. A linear type system rejects the two processes above, while for example accepts the following

$$P' = H[q].c!q \qquad Q' = X[q].c!q$$

that are bisimilar neither in QPAlg/CQP nor in qCCP.

Notice that in lqCCS is also possible to write processes like

$$P'' = H[q].discard(q) \qquad Q'' = X[q].discard$$

$P''$ and $Q''$ follow an approach a là QPAlg, where the qubit $q$ is not visible, and are in fact bisimilar.

The typing judgment are of the form $\Gamma \vdash e : T$ for classical expressions, $\Sigma \vdash e$ for quantum expressions, and $\Gamma; \Sigma \vdash P$ for processes.

- $\Gamma$ is a typing context, namely a set of typing assumptions $x : T$, both for classical variables and for classical and quantum channels. The possible types for a variables and expressions are $\{ \mathbb{N}, \mathbb{B} \}$, while the possible types for channels are $\{ \hat{\mathcal{Q}}, \hat{\mathbb{N}}, \hat{\mathbb{B}} \}$. $\Gamma$ follows the usual structural typing rules, and we write $\Gamma, x : T$ to denote the union of the sets $\Gamma$ and $\{ x : T \}$. We also use the notation

$$\Gamma - x = \begin{cases} \Gamma \setminus \{x : T\} & \text{if } x : T \in \Gamma \text{ for some } T \\ \Gamma & \text{otherwise} \end{cases}$$

- $\Sigma$ is a set of quantum variables, that are subject to linear typing rules. We write $\Sigma, x$ to denote the union of the *disjoint* sets $\Sigma$ and $\{ x \}$.

We report in Figure 4.1 the typing rules for Linear qCCS.

Thanks to the asynchronous syntax, a single typing rule Par is sufficient to guarantee single ownership of qubits (instead of the two different rules for $P \parallel Q$ and $c!v.P$ needed in CQP). Besides, weakening does not hold, and all sequential processes that use some quantum variables must end with the terminal process $c!q$, and only the processes that do not own any quantum variable end with $\mathbf{0}$.

Notice that in a well typed process $P + Q$, it must be $\Gamma; \Sigma \vdash P$ and $\Gamma'; \Sigma \vdash Q$ for the same $\Sigma$, i.e. $P$ and $Q$ must send (or discard) the same quantum variables. The same holds also for **if** $e$ **then** $P$ **else** $Q$, as common in statically typed programming languages. The **if then else** construct, where in any case one of the two branches is chosen, has been introduced specifically to write conditional processes in a linear setting. Note that using the simpler 'sum of guards' construct $[e_1].P + [e_2].P$ of qCCS, both $e_1$ and $e_2$ may evaluate to $ff$, hence a safe type system must require that $P$ and $Q$ do not use any quantum variable, i.e. $\Gamma; \emptyset \vdash [e_1].P$ and $\Gamma'; \emptyset \vdash [e_2].Q$, which is prohibitive.

The purpose of our linear type system is to force the user to explicitly choose if the qubits used by a process $P$ should be considered observable or not when $P$ ends its computation. Consider as an example a process that just applies an Hadamard gate to a qubit $q$: since $H[q].\mathbf{0}$ is not well typed, one must choose between

$$P = H[q].c!q \quad \text{and} \quad P' = H[q].discard(q)$$

(recall that $discard(q)$ is syntactic sugar for $c!q \setminus c$)

In the first case the qubit $q$ is observable, and the same happens also for QPAlg/CQP and qCCS. In the second case, $P'$ ends up in a deadlock process $c!q \setminus c$, where the qubit

Figure 4.1: Type system for Linear qCCS

$$\frac{b \in \mathbb{B}}{\vdash b : \mathbb{B}}\ \textsc{CBool} \qquad \frac{n \in \mathbb{N}}{\vdash n : \mathbb{N}}\ \textsc{CNat} \qquad \frac{}{\{\,x\,\} \vdash x}\ \textsc{QVar} \qquad \frac{}{x : T \vdash x : T}\ \textsc{CVar}$$

$$\frac{\Gamma_1 \vdash e_1 : \mathbb{B} \quad \Gamma_2 \vdash e_2 : \mathbb{B}}{\Gamma_1 \cup \Gamma_2 \vdash e_1 \vee e_2 : \mathbb{B}}\ \textsc{BoolOr} \qquad \frac{\Gamma \vdash e : \mathbb{B}}{\Gamma \vdash \neg e : \mathbb{B}}\ \textsc{BoolNeg} \qquad \frac{\Gamma_1 \vdash e_1 : \mathbb{N} \quad \Gamma_2 \vdash e_2 : \mathbb{N}}{\Gamma_1 \cup \Gamma_2 \vdash e_1 \leq e_2 : \mathbb{B}}\ \textsc{NatLEq}$$

$$\frac{\Gamma; \Sigma \vdash P \quad x \text{ fresh}}{\Gamma, x : T; \Sigma \vdash P}\ \textsc{CWeak}$$

$$\frac{}{\emptyset; \emptyset \vdash nil}\ \textsc{Nil} \qquad \frac{\Gamma; \Sigma \vdash P}{\Gamma; \Sigma \vdash \tau.P}\ \textsc{Tau} \qquad \frac{\Gamma \vdash e : \mathbb{B} \quad \Gamma_1; \Sigma \vdash P_1 \quad \Gamma_2; \Sigma \vdash P_2}{\Gamma \cup \Gamma_1 \cup \Gamma_2; \Sigma \vdash \textbf{if } e \textbf{ then } P_1 \textbf{ else } P_2}\ \text{ITE}$$

$$\frac{\mathcal{E} : Op(n) \quad |\widetilde{x}| = n \quad \forall i, j.\, x_i \neq x_j \quad \Sigma \vdash \widetilde{x} \quad \Gamma; \Sigma \vdash P}{\Gamma; \Sigma \vdash \mathcal{E}(\widetilde{x}).P}\ \textsc{QOp}$$

$$\frac{M : Meas(n) \quad |\widetilde{x}| = n \quad \forall i, j.\, x_i \neq x_j \quad \Sigma \vdash \widetilde{x} \quad \Gamma, y : \mathbb{N}; \Sigma \vdash P}{\Gamma; \Sigma \vdash M(\widetilde{x} \rhd y).P}\ \textsc{QMeas}$$

$$\frac{\Gamma, x : T; \Sigma \vdash P}{\Gamma, c : \hat{T}; \Sigma \vdash c?x.P}\ \textsc{CRecv} \qquad \frac{\Gamma; \Sigma, x \vdash P}{\Gamma, c : \hat{\mathcal{Q}}; \Sigma \vdash c?x.P}\ \textsc{QRecv}$$

$$\frac{\Gamma \vdash e : T}{\Gamma, c : \hat{T}; \emptyset \vdash c!e}\ \textsc{CSend} \qquad \frac{}{c : \hat{\mathcal{Q}}; \{\,e\,\} \vdash c!e}\ \textsc{QSend}$$

$$\frac{\Gamma_1; \Sigma \vdash P_1 \quad \Gamma_2; \Sigma \vdash P_2}{\Gamma_1 \cup \Gamma_2; \Sigma \vdash P_1 + P_2}\ \textsc{Sum} \qquad \frac{\Sigma_1 \cap \Sigma_2 = \emptyset \quad \Gamma_1; \Sigma_1 \vdash P_1 \quad \Gamma_2 q; \Sigma_2 \vdash P_2}{\Gamma_1 \cup \Gamma_2; \Sigma_1 \cup \Sigma_2 \vdash P_1 \parallel P_2}\ \textsc{Par}$$

$$\frac{f(\Gamma); \Sigma \vdash f(P)}{\Gamma; \Sigma \vdash P\{f\}}\ \textsc{Rename} \qquad \frac{\Gamma; \Sigma \vdash P}{\Gamma - c; \Sigma \vdash P \setminus c}\ \textsc{Restrict}$$

$q$ is never sent, and it is not observable the same happens also for both QPAlg/CQP and qCCS (technically because it remains part of the free quantum variables of $P'$).

In other words, writing processes like $P$, which always send their qubits, we obtain the observable properties assumed in qCCS, where the quantum state is visible. Writing processes like $P'$, which always discard their qubits, we obtain the observable properties of QPAlg/CQP, where the state is invisible. Linear qCCS allows to mix the two notions, specifying which qubits should be visible for an external observer and which should not.

Finally, observe that the construct $discard(q) = c!q \setminus c$ is implementable also in standard qCCS, **if** $e$ **then** $P$ **else** $Q$ is equivalent to $[e].P + [\neg e].Q$, and so the well-typed terms of lqCCS are a subset of the valid terms of qCCS, inteded to capture only the asynchronous, unambiguous linear processes.

### 4.1.3 Contexts

After introducing the syntax and type system of lqCCS, we can now define contexts, which will be useful in Section 4.3. A context is usually defined as a 'process with a hole', but in our case we need to restrict ourselves to contexts that respect the linear typing rules. So we introduce *typed contexts*, i.e. contexts that 'accept' only processes typed by a specific $\Gamma; \Sigma$, and are admitted by the linear type system.

**Definition 4.1.1.** *A typed context $B[-]_{\Gamma;\Sigma}$ is generated by the grammar:*

$$B[-]_{\Gamma;\Sigma} ::= \ [-]_{\Gamma;\Sigma} \mid [-]_{\Gamma;\Sigma} \parallel P$$

*and for some $\Gamma'$ and $\Sigma'$, $\Gamma'; \Sigma' \vdash B[-]_{\Gamma;\Sigma}$ according to the typing rules:*

$$\frac{}{\Gamma; \Sigma \vdash [-]_{\Gamma;\Sigma}}\ \textsc{Hole} \qquad \frac{\Gamma_1; \Sigma_1 \vdash [-]_{\Gamma;\Sigma} \quad \Gamma_2; \Sigma_2 \vdash P \quad \Sigma_1 \cap \Sigma_2 = \emptyset}{\Gamma_1 \cup \Gamma_2; \Sigma_1 \cup \Sigma_2 \vdash [-]_{\Gamma;\Sigma} \parallel P}\ \textsc{ParHole}$$

Given a typed context $B[-]_{\Gamma;\Sigma}$ and a process $P$, the process $B[P]$, obtained 'filling' the hole in $B$ with $P$, is well defined only if $\Gamma; \Sigma \vdash P$.

**Theorem 4.1.1.** *Suppose a context $B[-]_{\Gamma;\Sigma}$ such that $\Gamma'; \Sigma' \vdash B[-]_{\Gamma;\Sigma}$. For any process $P$ such that $\Gamma; \Sigma \vdash P$, it holds that $\Gamma'; \Sigma' \vdash B[P]$.*

*Proof.* The proof is trivial, proceeding by induction on the rules Hole and ParHole. □

Notice that according to the given syntax, a context can be either the degenerate empty context $[-]_{\Gamma;\Sigma}$, or the parallel context $[-]_{\Gamma;\Sigma} \parallel P$ for some $P$. When used to define saturated bisimilarity (Section 4.3), these are the only *discriminating* contexts, as in [5].

## 4.2 Semantics

We present a reduction semantics for lqCCS, consistent with the labeled semantics for qCCS presented in [13, 10]. A reduction semantics does not make any assumption on the observable properties of the system (like the labels of a transition), and so is better suited to explore and compare different notions of behavioural equivalence.

Besides, as explained in Chapter 3, in a labelled transition system a quantum input transition like $\xrightarrow{c?q}$ requires the value of qubit $q$ to be already present in the state. This is an atypical assumption, as a labeled transition usually models the communication with an unknown external environment, but in this case requires at least some partial knowledge of the environment. In a reduction system there are no such labelled transitions, so a process communicates only with other processes, on which we have total information.

Our semantics defines a probabilistic reduction system $(S, \rightarrow)$, where

- $S$ is a set of *configurations*, of the form $\langle \rho, P \rangle$ (like in qCCS).
- $\rightarrow \subseteq S \times \mathfrak{D}(S)$ is the probabilistic transition relation, corresponding to the $\xrightarrow{\tau}$ transition in qCCS [13, 10].

We assume a fixed set $QN = q_1, q_2, \dots q_n$ of quantum names, where each name $q_i$ refers to a unique qubit with state space $\mathcal{H}_i$. We denote as $\mathcal{H}_{QN}$ the $2^n$-dimensional Hilbert space $\bigotimes_{i=1}^n \mathcal{H}_i$, and so any state $\rho \in \mathcal{D}(\mathcal{H}_{QN})$ associates each name with a value.

We also assume a fixed typing contest $\Gamma_c = \{ c_i : \widehat{T}_i \}_i$, containing typing assumptions for a finite set of classical and quantum channels.

**Definition 4.2.1.** *Let $P$ be a process and $\rho \in \mathcal{D}(\mathcal{H}_{QN})$ an arbitrary density operator. We say that a configuration $\langle \rho, P \rangle$ is well typed, given a set of quantum names $QN$ and a set of typed channels $\Gamma_c$, if $\Gamma_c; \Sigma \vdash P$ for some $\Sigma \subseteq QN$.*

Notice that the context $\Gamma_c$ contains assignments only for channels, not for classical variables. This means that in well typed configurations, $P$ does not contain any free classical variable, and all the free quantum variables are references to qubits in the configuration.

From now on, we will consider only well typed configurations.

### 4.2.1 Reduction System

In order to define the reduction transition, we first need to introduce a semantics for expressions and a structural congruence relation on processes, like in [15].

We consider as a *value* any expression $n \in \mathbb{N}$, $b \in \mathbb{B}$, $x \in \text{Var}$, and use $v$ as a metavariable for them.

In Figure 4.2, we define a big step semantics for classical and quantum expression in the usual way. We write $e \Downarrow v$ to indicate that the expression $e$ evaluates to value $v$. Recall that the only quantum expressions admitted by the type system are quantum variables.

$$\frac{}{x \Downarrow x}\ \textsc{Var} \qquad \frac{}{n \Downarrow n}\ \textsc{Nat} \qquad \frac{}{b \Downarrow b}\ \textsc{Bool}$$

$$\frac{e_1 \Downarrow b_1 \quad e_2 \Downarrow b_2 \quad b = b_1 \vee b_2}{(e_1 \vee e_2) \Downarrow b}\ \textsc{Or} \qquad \frac{e \Downarrow b_1 \quad b = \neg b_1}{\neg e \Downarrow b}\ \textsc{Neg}$$

$$\frac{e_1 \Downarrow n_1 \quad e_2 \Downarrow n_2 \quad b = n_1 \leq n_2}{(e_1 \leq e_2) \Downarrow b}\ \textsc{Leq}$$

Figure 4.2: Big step semantic for Linear qCCS expressions

We define as the *structural congruence relation* $\equiv$ the smallest equivalence relation that satisfies the axioms in Figure 4.3. We employed the usual axioms of [27] for parallel composition, summation and restriction. We also add axioms to evaluate classical expressions and to resolve **If Then Else** occurrences.

$$\frac{}{P \parallel nil \equiv P}\ \textsc{ParNil} \qquad \frac{}{P \parallel Q \equiv Q \parallel P}\ \textsc{ParComm} \qquad \frac{}{P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R}\ \textsc{ParAssoc}$$

$$\frac{}{M + nil \equiv M}\ \textsc{SumNil} \qquad \frac{}{M + N \equiv N + M}\ \textsc{SumComm} \qquad \frac{}{M + (N + O) \equiv (M + N) + O}\ \textsc{SumAssoc}$$

$$\frac{}{P \setminus c \setminus d \equiv P \setminus d \setminus c}\ \textsc{RestrOrd} \qquad \frac{}{nil \setminus c \equiv nil}\ \textsc{RestrNil} \qquad \frac{c \notin fc(P)}{(P \parallel Q) \setminus c \equiv P \parallel (Q \setminus c)}\ \textsc{RestrPar}$$

$$\frac{}{\textbf{If } tt \textbf{ Then } P \textbf{ Else } Q \equiv P}\ \textsc{TrueGuard} \qquad \frac{}{\textbf{If } ff \textbf{ Then } P \textbf{ Else } Q \equiv Q}\ \textsc{FalseGuard}$$

$$\frac{e \Downarrow v}{P \equiv P[{}^{v}/_{e}]}\ \textsc{ValExpr}$$

Figure 4.3: Structural congruence for Linear qCCS

We can now define the transition relation $\rightarrow$, presented in Figure 4.4. As usual, we write $\langle \rho, P \rangle \rightarrow \Delta$ to intend $(\langle \rho, P \rangle, \Delta) \in \rightarrow$. To lighten the notation, we will also write $\langle \rho, P \rangle \rightarrow \langle \rho', P' \rangle$ instead of $\langle \rho, P \rangle \rightarrow \overline{\langle \rho', P' \rangle}$.

This transition relation cannot be composed with itself, since it is a relation from configurations to distributions. As in [13], we can *lift* the relation $\to$ into $\overset{\circ}{\to}$, that is a relation from distributions to distributions, as described in Section 2.2.3. This is useful to talk about reachability and temporal logics, but will not be used in the definitions of strong bisimulations in the next sections.

$$\frac{}{\langle \rho, \tau.P\rangle \longrightarrow \langle \rho, P\rangle}\ \textsc{SemTau}$$

$$\frac{\langle \rho, f(P)\rangle \longrightarrow \langle \rho', f(P')\rangle}{\langle \rho, P\{f\}\rangle \longrightarrow \langle \rho', P'\{f\}\rangle}\ \textsc{SemRename} \qquad \frac{\langle \rho, P\rangle \longrightarrow \langle \rho', P'\rangle}{\langle \rho, P \setminus L\rangle \longrightarrow \langle \rho, P' \setminus L\rangle}\ \textsc{SemRestrict}$$

$$\frac{}{\langle \rho, \mathcal{E}(\widetilde{x}).P\rangle \longrightarrow \langle \mathcal{E}_{\widetilde{x}}(\rho), P\rangle}\ \textsc{SemQOp}$$

$$\frac{\rho_m = M_m \rho M_m^\dagger \quad p_m = tr(\rho_m)}{\langle \rho, M(\widetilde{x} \triangleright y).P\rangle \longrightarrow \sum_{m=0}^{2^{|\widetilde{x}|}} p_m(\rho) \left\langle \frac{1}{p_m}\rho_m, P[{}^{m}/_{y}]\right\rangle}\ \textsc{SemQMeas}$$

$$\frac{\langle \rho, P\rangle \longrightarrow \langle \rho', P'\rangle}{\langle \rho, P \parallel R\rangle \longrightarrow \langle \rho', P' \parallel R\rangle}\ \textsc{SemPar} \qquad \frac{\langle \rho, P\rangle \longrightarrow \langle \rho', P'\rangle}{\langle \rho, P + R\rangle \longrightarrow \langle \rho', P'\rangle}\ \textsc{SemSum}$$

$$\frac{}{\langle \rho, c!v \parallel c?x.P\rangle \longrightarrow \langle \rho, P[{}^{v}/_{x}]\rangle}\ \textsc{SemReduce}$$

$$\frac{P \equiv Q \quad \langle \rho, Q\rangle \to \langle \rho', Q'\rangle \quad Q' \equiv P'}{\langle \rho, P\rangle \longrightarrow \langle \rho', P'\rangle}\ \textsc{SemCongr}$$

Figure 4.4: Reduction system for Linear qCCS

*Example* 4.2.1. We can formalize in lqCCS the famous *quantum teleportation* algorithm:

$$\begin{aligned}
\mathbf{A} &::= \mathrm{in}_a?x.\mathrm{CNOT}(q_0, x).\mathrm{H}(q_0).M(q_0, x \triangleright n).(\mathrm{m}_a b!n \parallel \mathit{discard}(q_0, x)) \\
\mathbf{B} &::= \mathrm{in}_b?x.\mathrm{m}_{ab}?n. \\
&\quad \mathbf{if}\ n = 0\ \mathbf{then}\ I(x).\mathrm{out}_b!x \\
&\quad\ \ \mathbf{else\ if}\ n = 1\ \mathbf{then}\ X(x).\mathrm{out}_b!x \\
&\quad\ \ \mathbf{else\ if}\ n = 2\ \mathbf{then}\ Z(x).\mathrm{out}_b!x \\
&\quad\ \ \mathbf{else}\ Y(x).\mathrm{out}_b!x \\
\mathbf{S} &::= \mathit{Set}_{\Phi^+}(q_1, q_2).(\mathrm{in}_a!q_1 \parallel \mathrm{in}_b!q_2) \\
\mathbf{Tel} &::= (A \parallel B \parallel S) \setminus \{\, \mathrm{in}_a, \mathrm{in}_b, \mathrm{m}_{ab} \,\}
\end{aligned}$$

Which is well typed under the context $\Gamma = \{\, \mathrm{out}_b : \hat{\mathcal{Q}} \,\}$, $\Sigma = \{\, q_0, q_1, q_2 \,\}$.

### 4.2.2 Type system properties

We now prove that reductions preserve typing. This is critical for the further developments of this thesis and is a standard property. Note that the absence of a weakening rule for quantum variables requires a different approach w.r.t. the case of CQP [15].

We need some auxiliary results, starting from typing preservation for expression evaluation and structural congruence.

**Theorem 4.2.1** (Evaluation Preserves Typing)**.** *If* $\Gamma \vdash e$ *and* $e \Downarrow v$*, then* $\Gamma \vdash v$*.*

*Proof.* Follows by induction on the evaluation rules. □

**Theorem 4.2.2** (Structural Congruence Preserves Typing). *If* $\Gamma;\Sigma \vdash P$ *and* $P \equiv Q$, *then* $\Gamma;\Sigma \vdash Q$.

*Proof.* By induction on the derivation of $P \equiv Q$. All rules follow trivially with the possible need of additional CWEAK applications in the derivation of $\Gamma;\Sigma \vdash Q$ as the subcomponents of the if-then-else, non-deterministic sum and parallel operator may be typed by a context $\Gamma' \subseteq \Gamma$. □

Others technical results we need are substitution lemmas for expressions, classical and quantum substitutions.

**Lemma 4.2.1** (Expression Substitution). *Let* $\Gamma, x : T' \vdash e : T$ *and let* $\Gamma \vdash v : T'$, *then* $\Gamma \vdash e[{}^{v}\!/\!_{x}]$.

*Proof.* Trivially by structural induction on the derivation of $\Gamma, x : T' \vdash e$. □

**Theorem 4.2.3** (Classical Substitution). *Let* $\Gamma, x : T;\Sigma \vdash P$ *and let* $\Gamma \vdash v : T$, *then* $\Gamma;\Sigma \vdash P[{}^{v}\!/\!_{x}]$.

*Proof.* By structural induction on the derivation of $\Gamma, x : T;\Sigma \vdash P$. □

**Theorem 4.2.4** (Quantum Substitution). *Let* $\Gamma;\Sigma, x \vdash P$ *and let* $v \notin \Sigma$, *then* $\Gamma;\Sigma, v \vdash P[{}^{v}\!/\!_{x}]$.

*Proof.* By structural induction on the derivation of $\Gamma;\Sigma, x \vdash P$. Let us analyze the interesting cases: For the QOP rule it must be that $P = \mathcal{E}(\widetilde{x}).Q$ for some process $Q$. By induction hypothesis it holds that $\Gamma;\Sigma, v \vdash Q$, but $v \notin \widetilde{x}$ by the hypothesis $v \notin \Sigma$, thus we can apply the QOP rule. The same line of reasoning is valid for the QMEAS rule. The QSEND rule is also guaranteed by the $v \notin \Sigma$ requirement. Finally, the derivation of PAR imposes that only one of the components, w.l.o.g. $P_i$, contains the variable $x$ in its quantum environment $\Sigma_i$. Thus by induction we obtain $\Gamma_i;\Sigma_i[{}^{v}\!/\!_{x}] \vdash P_i$. While, for the other components there is no change since they do not contain the variable $x$. However, since $v \notin \Sigma$, we can conclude that all smaller environments are still pairwise distinct, thus we can apply the PAR rule again. □

We now prove the desired result, namely that reductions preserve typing.

**Theorem 4.2.5** (Typing Preservation). *If* $\Gamma;\Sigma \vdash P$ *and* $\langle \rho, P\rangle \longrightarrow \sum_{i\in I} p_i \langle \rho_i, P_i\rangle$ *then* $\forall i \in I.\, \Gamma;\Sigma \vdash P_i$.

*Proof.* By structural induction on the transition relation $\longrightarrow$. Let us analyze the interesting cases: if the last step in the derivation is a SEMQMEAS rule, then $P = M(\widetilde{x} \triangleright y).Q$ for some process $Q$, where $Q$ is typed with $\Gamma, m : \mathbb{N};\Sigma \vdash Q$. Each component of the box sum is of the form $Q[{}^{m}\!/\!_{y}]$ with $m \in \mathbb{N}$, thus by the classical substitution theorem it holds that $\Gamma;\Sigma \vdash Q[{}^{m}\!/\!_{y}]$. If the last step is a SEMPAR rule, then $P = Q \parallel R$ for some processes $Q$ and $R$, where $\Gamma_1;\Sigma_1 \vdash Q$ and $\Gamma_2;\Sigma_2 \vdash R$ with $\Gamma = \Gamma_1 \cup \Gamma_2$, $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\Sigma_1 \cap \Sigma_2 = \emptyset$. By induction $\Gamma_1;\Sigma_1 \vdash Q'$, however since the conditions on the $\Sigma$ are still true, it also holds that $\Gamma;\Sigma \vdash Q' \parallel R$, by applying CWEAK if $\Gamma_1 \subset \Gamma$. The argument is similar for the SEMSUM rule. If the last step is a SEMREDUCE rule, then $P = c!e \parallel c?x.Q$ for some process $Q$. If $c : \hat{T}$ where $T = \mathbb{N}$ or $T = \mathbb{B}$, then the theorem holds trivially by the classical substitution theorem. If $c : \hat{\mathcal{Q}}$ then it must be that $c : \hat{\mathcal{Q}};\{\, e \,\} \vdash c!e$ and $\Gamma', c : \hat{\mathcal{Q}};\Sigma' \vdash c?x.Q$ thus $\Gamma';\Sigma', x \vdash Q$, with $e \notin \Sigma'$ and $x \notin \Sigma'$ respectively by the PAR and QRECV rules. By the quantum substitution theorem, $\Gamma';\Sigma', e \vdash Q[{}^{e}\!/\!_{x}]$, but since $\Sigma', e = \Sigma$ and by application of the CWEAK it holds that $\Gamma;\Sigma \vdash Q[{}^{e}\!/\!_{x}]$. □

## 4.3 Behavioural Equivalence

We have seen that a number of different behavioural equivalences have been proposed in the literature. We have also seen that this is partially due to an ambiguity related to implicitly discarded qbits; a problem that is solved by lqCCS. Noticeably, others differences of observable properties are more involved and inherently quantum related. As in classical process algebra, it is always possible to observe if a process $P$ can perform a classical input or output action, which is the foundation of both *labeled* and *barbed* bisimilarity. The discrepancies in state-of-the-art proposals are mainly about the observable properties of quantum states. In QPAlg, the quantum state is observed only when sent, while in qCCS, the whole 'environment' is visible, i.e. all the qubits that are not used by $P$ anymore. In (mixed configuration) CQP there is again a similar notion of 'environment', but what is observable is the environment of the whole distribution, not the environment of the single configurations.

The main purpose of this section is to investigate which are the most natural notions of behavioural equivalence, and how some apparently minor details lead to completely diverse equivalence relations. Being interested in the purely quantum aspect of behavioural equivalence, we will only consider 'strong' relations, like strong bisimilarity and strong barbed congruence. Strong relations in fact are usually the first, simpler step to develop a beheavioural equivalence notion, and after establishing the most appropriate notion of observable property of quantum states, we plan to extend it to the weak case.

We will first define a *probabilistic saturated bisimilarity* [5] for Linear qCCS. Saturated bisimilarity is a solid and general notion of observable equivalence, aiming to capture when two processes can or cannot be distinguished by an external observer, i.e. by an arbitraty context. We will describe some examples of such a bisimilarity, together with a useful property that helps when proving the bisimilarity of two processes.

Then we will analyze some peculiarities of these probabilistic equivalence notions, extending the ideas already discussed in [8]. In particular, the bisimilarities defined for QPAlg and qCCS and lqCCS, seem to grant the external observer a greater discerning power then what is prescribed by quantum mechanics. That is, the resulting behavioural equivalence is too much fine-grained. We identify the well established notion of Larsen-Skou bisimulation (as described in 2.2.3) as the cause of these undesired behaviours, and propose a novel notion of *quantum saturated bisimilarity* that better fits the observable properties of distribution of quantum configurations. We believe that this bisimilarity complies with the ideas presented by [8] for mixed configuration CQP, albeit here presented on an essentially different transition system.

Finally we will rephrase some of the examples in the previous chapter in lqCCS, comparing our bisimilarity with the other behavioural equivalences presented in the literature. We will show that our notion of probabilistic saturated bisimilarity for lqCCS is consistent with the open bisimilarity [10] for qCCS, while quantum saturated bisimilarity is strictly larger.

### 4.3.1 Probabilistic Saturated Bisimilarity

Saturated bisimilarity [5] grants the external observer, when comparing two configurations $\mathcal{C}$ and $\mathcal{C}'$, the power to put $\mathcal{C}$ and $\mathcal{C}'$ inside any context at each step of the computations. Recall that in barbed congruence (as defined in section 2.2.4), the observer can compare $\mathcal{C}$ and $\mathcal{C}'$ using just one arbitrary context at the start of the computation, not any context at each step like in saturated bisimilarity.

We use (probabilistic) saturated bisimilarity as it is an established, general behavioural equivalence, useful to investigate reduction systems where there is no affirmed notion of observable property. Besides, as we will see, saturated bisimilarity is able to capture some properties used in [10] to define open bisimilarity.

We define 'the capability of performing an output on a channel' as the only barbs, i.e. the atomic observable properties. We do not assume input actions to be observable, following the standard for asynchronous calculi [1]. Since the external observer is asynchronous, it cannot observe the process $P$ to discover if a $c?x$ transition is available: the context can only perform $c!v$ as a terminal action, hence it cannot discover if the message is ever received.

**Definition 4.3.1** (Barb)**.** *A* barb *is a predicate $\downarrow_c$ over well typed processes, defined as follows: $P \downarrow_c$ if and only if $P \equiv c!e \parallel R$ for some expression $e$, and process $R$.*

If $\mathcal{C} = \langle \rho, P \rangle$ is a configuration, we will often write $C \downarrow_c$ instead of $P \downarrow_c$, and $B[\mathcal{C}]$ instead of $\langle \rho, B[P] \rangle$.

**Definition 4.3.2** (Probabilistic Saturated Bisimilarity)**.** *A symmetric relation $\mathcal{R} \subseteq \mathcal{C} \times \mathcal{C}$ is* probabilistic saturated (barbed) bisimulation *if $\langle \rho, P \rangle \ \mathcal{R} \ \langle \sigma, Q \rangle$ implies that $P$ and $Q$ are well-typed under the same typing context $\Gamma; \Sigma$, and for any context $B[\_]_{\Gamma,\Sigma}$*

- *If $P \downarrow_c$ then $Q \downarrow_c$*
- *If $\langle \rho, B[P] \rangle \rightarrow \Delta$, there exists $\Theta$ such that $\langle \sigma, B[Q] \rangle \rightarrow \Theta$ and $\Delta \ \overset{\circ}{\mathcal{R}} \ \Theta$*

*Let* probabilistic saturated bisimilarity $\sim_{PS}$ *be the union of all saturated probabilistic barbed bisimulations.*
*We say that two processes $P$ and $Q$ are* bisimilar*, written $P \sim_{PS} Q$, if for any $\rho \in \mathcal{D}(\mathcal{H}_{QN})$ it holds $\langle \rho, P \rangle \sim_{PS} \langle \rho, Q \rangle$.*

Note that it is not necessary to use a barb $\downarrow_{c!v}$, so to consider also which is the value that is communicated. A context, in fact, is capable to discern $c!v.P$ from $c!v'.P$ thanks to the **if-then-else** construct for classical values, or to the measure operator for quantum values. This is an innovation with respect to QPAlg, wehere the observables of $\langle \rho, c!q.P \rangle$ were both the channel and the value (i.e. the reduced density operator) of $q$.

Note also that $B[-]$ has barb $\downarrow_c$ if and only if either $B[-]$ has or it $P$ has it. Hence it is not required to use contexts when comparing the barbs of two configurations for checking saturated bisimilarity.

*Example* 4.3.1*.* We can now prove that the teleportation algorithm presented in the last Section adheres to the intended specification .

The specification expressing the expected behaviour of teleportation is as follows:

$$\textbf{TelSpec} ::= \tau^8.\mathrm{SWAP}(q_0, q_2).(\mathrm{out}_b!q_2 \parallel \mathit{discard}(q_0, q_1))$$

where $\tau^8$ denotes 8 repetitions of $\tau$. These are needed since we relies on strong bisimilarity.

Note that the exchanged qbit is sent on an output channel, because the correctness of the algorithm depends on its value. Note also that the value of the others qbit is not visible, as they are discarded. This because any implementation that succeeds in sending the target qubit is satifactory, regardless of what happens to the other qubits.

The implementation presented in the last section was:

$$\begin{aligned}
\mathbf{A} &::= \mathrm{in}_a?x.\mathrm{CNOT}(q_0,x).\mathrm{H}(q_0).M(q_0,x \rhd n).(\mathrm{m}_a b!n \parallel \mathit{discard}(q_0,x) \\
\mathbf{B} &::= \mathrm{in}_b?x.\mathrm{m}_{ab}?n. \\
&\quad \textbf{if } n = 0 \textbf{ then } I(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else if } n = 1 \textbf{ then } X(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else if } n = 2 \textbf{ then } Z(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else } Y(x).\mathrm{out}_b!x \\
\mathbf{S} &::= \mathit{Set}_{\Phi^+}(q_1,q_2).(\mathrm{in}_a!q_1 \parallel \mathrm{in}_b!q_2) \\
\mathbf{Tel} &::= (A \parallel B \parallel S) \setminus \{\, \mathrm{in}_a, \mathrm{in}_b, \mathrm{m}_{ab} \,\}
\end{aligned}$$

We can prove that **TelSpec** $\sim_{PS}$ **Tel**. Notice in fact that the channels $\mathrm{in}_a, \mathrm{in}_b, \mathrm{m}_{ab}$ in **Tel** are limited, so the only visible communications happen on the $\mathrm{out}_b$ channel. After all the transformations and measurements, **Tel** will leave the $q_2$ qubit exactly as **TelSpec**, and the other qubits are not visible.

Consider now the first definition of teleportation reported in [13]. This corresponds to an alternative specification of quantum teleportation, where all the final qubits are sent on channels. As a consequence, to match the specification, the implementation must behave the same also in the qbits that are not 'teleported'. We will see that the following implementation, similar to the previous one but where no qubit is discarded, does not match the given specification.

*Example* 4.3.2.

$$\begin{aligned}
\mathbf{A'} &::= \mathrm{in}_a?x.\mathrm{CNOT}(q_0,x).\mathrm{H}(q_0).M(q_0,x \rhd n).(\mathrm{m}_a b!n \parallel \mathrm{out}_a(q_0,x) \\
\mathbf{B} &::= \mathrm{in}_b?x.\mathrm{m}_{ab}?n. \\
&\quad \textbf{if } n = 0 \textbf{ then } I(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else if } n = 1 \textbf{ then } X(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else if } n = 2 \textbf{ then } Z(x).\mathrm{out}_b!x \\
&\quad\ \textbf{else } Y(x).\mathrm{out}_b!x \\
\mathbf{S} &::= \mathit{Set}_{\Phi^+}(q_1,q_2).(\mathrm{in}_a!q_1 \parallel \mathrm{in}_b!q_2) \\
\mathbf{Tel'} &::= (A \parallel B \parallel S) \setminus \{\, \mathrm{in}_a, \mathrm{in}_b, \mathrm{m}_{ab} \,\} \\
\mathbf{TelSpec'} &::= \tau^8.\mathrm{SWAP}(q_0,q_2).(\mathrm{out}_b!q_2 \parallel \mathrm{out}_a(q_0,q_1))
\end{aligned}$$

We have that **Tel** $\not\sim_{PS}$ **TelSpec**. Consider indeed a context:

$$B[-] = \mathit{out}_a?x.M[x \rhd y].\textbf{if } y = 1 \textbf{ then } c!y \textbf{ else } \mathit{nil}.$$

the configurations $\langle |\psi 00\rangle\langle\psi 00|\,, B[\mathbf{Tel'}]\rangle$ and $\langle |\psi 00\rangle\langle\psi 00|\,, B[\mathbf{TelSpec'}]\rangle$

We show now some useful properties that helps in deciding bisimilarity. The first result is that $\sim_{PS}$ *is closed with respect to addition of discarded qbits*. Roughly, this means that if $\langle\rho, P\rangle$ and $\langle\sigma, Q\rangle$ are bisimilar, we can add a qbit $q$ and its discard $\mathit{disc}(q)$ to them, as in $\langle\rho \otimes |\psi\rangle\langle\psi|\,, P \parallel \mathit{disc}(q)\rangle$ and $\langle\sigma \otimes |\psi\rangle\langle\psi|\,, Q \parallel \mathit{disc}(q)\rangle$, obtaining bisimilar configurations. More in details, this holds also for non separable states, as shown later.

We first need some technical lemmas.

**Lemma 4.3.1.** *Let $\sigma \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$, with $\widetilde{p} = p_0 \dots p_{n-1}$ and $\widetilde{q} = q_0 \dots q_{m-1}$. Then, for any trace non-increasing superoperator $\mathcal{E}_{\widetilde{p}} \in \mathcal{S}(\mathcal{H}_{\widetilde{p}})$*

$$tr_{\widetilde{q}}((\mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}})(\sigma)) = \mathcal{E}_{\widetilde{p}}(tr_{\widetilde{q}}(\sigma))$$

*Proof.* We know that $\sigma$ is a probabilistic mixture of pure states, $\sigma = \sum_l p_l \left|\psi_l\right\rangle\!\left\langle\psi_l\right|$, and each pure state is a linear combination of separable states

$$\sigma = \sum_l p_l \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right|$$

and we know that $\mathcal{E}_{\widetilde{p}}$ has a Kraus decomposition

$$\mathcal{E}_{\widetilde{p}}(\rho) = \sum_k A_k \rho A_k^\dagger$$

Then we can write

$$\begin{aligned}
tr_{\widetilde{q}}((\mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}})(\sigma)) &= \mathcal{E}_{\widetilde{p}}(tr_{\widetilde{q}}(\sigma)) \\
tr_{\widetilde{q}}((\mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}}) \left( \sum_l p_l \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right| \right)) &= \mathcal{E}_{\widetilde{p}}(tr_{\widetilde{q}} \left( \sum_l p_l \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right| \right)) \\
\sum_l p_l tr_{\widetilde{q}}((\mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}}) \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right| \right)) &= \sum_l p_l \mathcal{E}_{\widetilde{p}}(tr_{\widetilde{q}} \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right| \right)) \\
tr_{\widetilde{q}}(\sum_k (A_k \otimes I_{\widetilde{q}}) \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|pq\right\rangle\!\left\langle pq\right| \right) (A_k \otimes I_{\widetilde{q}})^\dagger) &= \sum_k A_k \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} tr_{\widetilde{q}}(\left|pq\right\rangle\!\left\langle pq\right|) \right) A_k^\dagger \\
tr_{\widetilde{q}}(\sum_k \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} (A_k \otimes I_{\widetilde{q}}) \left|pq\right\rangle\!\left\langle pq\right| (A_k \otimes I_{\widetilde{q}})^\dagger \right)) &= \sum_k A_k \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} tr_{\widetilde{q}}(\left|pq\right\rangle\!\left\langle pq\right|) \right) A_k^\dagger \\
tr_{\widetilde{q}}(\sum_k \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} (A_k \left|p\right\rangle) \left|q\right\rangle (\left\langle p\right| A_k^\dagger) \left\langle q\right| \right)) &= \sum_k A_k \left( \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \left|p\right\rangle\!\left\langle p\right| \left\langle q|q\right\rangle \right) A_k^\dagger \\
\sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \sum_k tr_{\widetilde{q}}((A_k \left|p\right\rangle) \left|q\right\rangle (\left\langle p\right| A_k^\dagger) \left\langle q\right|) &= \sum_k \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \sum_k A_k \left|p\right\rangle\!\left\langle p\right| A_k^\dagger \\
\sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \sum_k (A_k \left|p\right\rangle\!\left\langle p\right| A_k^\dagger) &= \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \mathcal{E}_{\widetilde{p}}(\left|p\right\rangle\!\left\langle p\right|) \\
\sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \mathcal{E}_{\widetilde{p}}(\left|p\right\rangle\!\left\langle p\right|) &= \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^m-1} \lambda_{pq} \mathcal{E}_{\widetilde{p}}(\left|p\right\rangle\!\left\langle p\right|)
\end{aligned}$$

Where we made use of the fact that both $tr_{\widetilde{q}}$ and matrix multiplication are closed for linearity. □

**Lemma 4.3.2.** *Let $\sigma \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$, with $\widetilde{p} = p_0 \dots p_{n-1}$ and $\widetilde{q} = q_0 \dots q_{m-1}$. Then, for any trace non-increasing superoperator $\mathcal{E}_{\widetilde{q}} \in \mathcal{S}(\mathcal{H}_{\widetilde{q}})$*

$$tr_{\widetilde{q}}((\mathcal{I}_{\widetilde{p}} \otimes \mathcal{E}_{\widetilde{q}})(\sigma)) = tr_{\widetilde{q}}(\sigma)$$

The proof of this lemma is extremely similar to the one before, and thus omitted.

Now we prove that the behaviour of a configuration $\langle \rho, P \rangle$ is identical to the behaviour of a 'bigger' configuration with additional qubits, if these additional qubits are discarded, and so cannot be modified nor measured.

**Lemma 4.3.3.** *Let $\sigma \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$, and $\rho = tr_{\widetilde{q}}(\sigma) \in \mathcal{H}_{\widetilde{p}}$. Then, for any process*

$$\langle \rho, P \rangle \rightarrow \sum_i p_i \langle \rho_i, P_i \rangle \qquad \Leftrightarrow \qquad \langle \sigma, P \parallel disc(\widetilde{q}) \rangle \rightarrow \sum p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q}) \rangle$$

*and* $\forall i\ \rho_i = tr_{\widetilde{q}}(\sigma_i)$

*Proof.* We proceed by induction on $\rightarrow$. For the simple base cases SemTau and SemReduce, where the quantum state remains unchanged, we have

$$\langle \rho, \tau.P \rangle \rightarrow \langle \rho, P \rangle \Leftrightarrow \langle \sigma, \tau.P \parallel disc(\widetilde{q}) \rangle \rightarrow \langle \sigma, P \parallel disc(\widetilde{q}) \rangle$$
$$\langle \rho, c?x.P \parallel c!v \rangle \rightarrow \langle \rho, P[v/x] \rangle \Leftrightarrow \langle \sigma, c?x.P \parallel c!v \parallel disc(\widetilde{q}) \rangle \rightarrow \langle \sigma, P[v/x] \parallel disc(\widetilde{q}) \rangle$$

and in both cases $\rho' = \rho = tr_{\widetilde{q}}(\sigma)$.

For the base case SemQOp we have

$$\langle \rho, \mathcal{E}(\widetilde{p}).P \rangle \rightarrow \langle \mathcal{E}_{\widetilde{p}}(\rho), P \rangle \qquad \Leftrightarrow \qquad \langle \sigma, \mathcal{E}(\widetilde{p}).P \parallel disc(\widetilde{q}) \rangle \rightarrow \langle \mathcal{E}_{\widetilde{p}}(\sigma), P \parallel disc(\widetilde{q}) \rangle$$

where $\rho' = \mathcal{E}_{\widetilde{p}}(\rho) = \mathcal{E}_{\widetilde{p}}(tr_{\widetilde{q}}(\sigma))$ and $\sigma' = \mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}}(\sigma)$, and so we have $\rho' = tr_{\widetilde{q}}(\sigma') = tr_{\widetilde{q}}(\mathcal{E}_{\widetilde{p}} \otimes \mathcal{I}_{\widetilde{q}}(\sigma))$ thanks to lemma 4.3.1.

The base case SemQMeasure is similar, we have

$$\langle \rho, M[\widetilde{p} \rhd x].P \rangle \rightarrow \sum p_m \langle p_m^{-1} \mathcal{E}_m(\rho), P \rangle$$
$$\Leftrightarrow$$
$$\langle \sigma, M[\widetilde{p} \rhd x].P \parallel disc(\widetilde{q}) \rangle \rightarrow \sum p'_m \langle p_m^{-1} \mathcal{E}_m(\sigma), P \parallel disc(\widetilde{q}) \rangle$$

where thanks to lemma 4.3.1, we have $p_m = tr(\mathcal{E}_m(\rho)) = tr(\mathcal{E}_m(tr_{\widetilde{q}}(\sigma))) = tr(tr_{\widetilde{q}}(\mathcal{E}_m \otimes \mathcal{I}_{\widetilde{q}}(\sigma)))$ and $\forall i\ \rho_i = tr_{\widetilde{q}}(\sigma_i)$, as in the previous case.

The inductive cases are all trivial, as none of them modifies the quantum values $\rho$ and $\sigma$. □

**Theorem 4.3.1** ($\sim_{PS}$ is closed with respect to additional discarded qubits)**.** *If* $\langle tr_{\widetilde{q}}(\sigma), P \rangle \sim \langle tr_{\widetilde{q}}(\nu), Q \rangle$ *then* $\langle \sigma, P \parallel disc(\widetilde{q}) \rangle \sim \langle \nu, Q \parallel disc(\widetilde{q}) \rangle$.

*Proof.* Let $\sigma, \nu \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$. We show that if $\mathcal{R}$ is a bisimulation, then $\mathcal{R}_{tr_{\widetilde{q}}}$ is a bisimulation, where $\mathcal{R}_{tr_{\widetilde{q}}}$ is defined as

$$\mathcal{R}_{tr_{\widetilde{q}}} = \{ \Big( \langle \sigma, P \parallel disc(\widetilde{q}) \rangle, \langle \nu, Q \parallel disc(\widetilde{q}) \rangle \Big) \quad | \quad \langle tr_{\widetilde{q}}(\sigma), P \rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q \rangle \}$$

From this, it easily follows that $\sim_{PS}$ is closed for additional discarded qubits, because if $\langle tr_{\widetilde{q}}(\sigma), P \rangle \sim \langle tr_{\widetilde{q}}(\nu), Q \rangle$, then there exist a bisimulation $\mathcal{R}$ such that $\langle tr_{\widetilde{q}}(\sigma), P \rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q \rangle$, and so there exists a bisimulation $\mathcal{R}_{tr_{\widetilde{q}}} \subseteq \sim_{PS}$ such that $\langle \sigma, P \parallel disc(\widetilde{q}) \rangle \mathcal{R}_{tr_{\widetilde{q}}} \langle \nu, Q \parallel disc(\widetilde{q}) \rangle$.

To show that $\mathcal{R}_{tr_{\widetilde{q}}}$ is a bisimulation, we need first of all to show that is symmetric, which is when $\mathcal{R}$ is symmetric. The we suppose that $\langle \sigma, P \parallel disc(\widetilde{q}) \rangle \mathcal{R}_{tr_{\widetilde{q}}} \langle \nu, Q \parallel disc(\widetilde{q}) \rangle$ and have to show that

- For any barb $b$, if $\langle \sigma, P \parallel disc(\widetilde{q}) \rangle \downarrow_b$ then $\langle \nu, Q \parallel disc(\widetilde{q}) \rangle \downarrow_b$. We have that $\langle \sigma, P \parallel disc(\widetilde{q}) \rangle \downarrow_b \Leftrightarrow \langle tr_{\widetilde{q}}(\sigma), P \rangle \downarrow b$, $\langle \nu, Q \parallel disc(\widetilde{q}) \rangle \downarrow_b \Leftrightarrow \langle tr_{\widetilde{q}}(\nu), Q \rangle \downarrow b$, and $\langle tr_{\widetilde{q}}(\sigma), P \rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q \rangle$, so they all express the same barbs.

- For any process $R$, if $\langle \sigma, P \parallel R \parallel disc(\widetilde{q}) \rangle \rightarrow \Delta$, then $\langle \nu, Q \parallel R \parallel disc(\widetilde{q}) \rangle \rightarrow \Theta$, and $\Delta \ \overset{\circ}{\mathcal{R}}_{tr_{\widetilde{q}}} \ \Theta$. Notice that $disc(\widetilde{q})$ cannot evolve, and so we start from the hypothesis $\langle \sigma, P \parallel R \parallel disc(\widetilde{q}) \rangle \rightarrow \sum p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q}) \rangle$. Then, from lemma 4.3.3, we know that $\langle tr_{\widetilde{q}}(\sigma), P \parallel R \rangle \rightarrow \sum p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i \rangle$. But since $\langle tr_{\widetilde{q}}(\sigma), P \rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q \rangle$, and $\mathcal{R}$ is a saturated bisimulation, it must be that $\langle tr_{\widetilde{q}}(\nu), Q \parallel R \rangle \rightarrow \sum p_i \langle \xi_i, Q_i \rangle$ with $\langle tr_{\widetilde{q}}(\sigma_i), P_i \rangle \mathcal{R} \langle \xi_i, Q_i \rangle$ for each $i$. But using the same lemma 4.3.3 in the other direction, we get $\langle \nu, Q \parallel R \parallel disc(\widetilde{q}) \rangle \rightarrow \sum p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q}) \rangle$ with $\xi_i =$

$tr_{\widetilde{q}}(\nu_i)$. In conclusion, for each transition $\langle \sigma, P \parallel R \parallel disc(\widetilde{q})\rangle \rightarrow \sum p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle$ exists a transition $\langle \nu, Q \parallel R \parallel disc(\widetilde{q})\rangle \rightarrow \sum p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q})\rangle$ such that $\forall i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu_i), Q_i\rangle$, and so from the definition of $\mathcal{R}_{tr_{\widetilde{q}}}$ together with probabilistic lifting we get $\sum p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle \overset{\circ}{\mathcal{R}}_{tr_{\widetilde{q}}} \sum p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q})\rangle$.

□

Theorem 4.3.1 is useful when proving bisimilarity of processes that use discard.

*Example* 4.3.3. Thanks to Theorem 4.3.1 we can prove that $P = H[q].discard(q)$ and $Q = X[q].discard(q)$ are bisimilar.

Given that $\emptyset, q \vdash P$ and $\emptyset, q \vdash Q$, we show that

$$\mathcal{R} = \left\{ \langle \sigma, B[P]\rangle, \langle \sigma, B[Q]\rangle \mid \sigma \in \mathcal{D}(\mathcal{H}_{QN}), B[-]_{\emptyset;\{q\}} \text{ typed context} \right\}^S \cup \sim_{PS}$$

is a probabilistic saturated bisimulation, where $\mathcal{R}^S$ denotes the symmetric closure of a relation $\mathcal{R}$. From this follows trivially that $\langle \sigma, P\rangle \sim_{PS} \langle \sigma, Q\rangle$ for any $\sigma$, and so $P$ and $Q$ are bisimilar processes.

$\mathcal{R}$ is a *saturated* relation, meaning that if $\mathcal{C}\mathcal{R}\mathcal{C}'$, then $B[\mathcal{C}]\mathcal{R}B[\mathcal{C}']$ for any $B$. So, to prove that $\mathcal{R}$ is a probabilistic saturated bisimulation, we just need to show that $\mathcal{R}$ is a probabilistic bisimulation.

Suppose that $\langle \sigma, R \parallel P\rangle \mathcal{R} \langle \sigma, R \parallel Q\rangle$, and that $\langle \sigma, R \parallel P\rangle \rightarrow \sum_i p_i \mathcal{C}_i$.

- $\langle \sigma, P \parallel disc(\widetilde{q})\rangle \sim \langle \nu, Q \parallel disc(\widetilde{q})\rangle$.

- If the reductions happens in $R$, it must be of the form $\langle \sigma, R \parallel P\rangle \rightarrow \sum_i p_i \langle \sigma_i, R' \parallel P\rangle$, but then there exists a transition $\langle \sigma, R \parallel Q\rangle \rightarrow \sum_i p_i \langle \sigma_i, R_i \parallel Q\rangle$, and for each $i$, $\langle \sigma_i, R_i \parallel P\rangle \mathcal{R} \langle \sigma_i, R_i \parallel Q\rangle$ by definition of $\mathcal{R}$.

- If the reductions happens in $P$, it must be $\langle \sigma, R \parallel H[q].disc(q)\rangle \rightarrow \langle \mathcal{E}_{H,q}(\sigma), R \parallel disc(q)\rangle$, but then $\langle \sigma, R \parallel X[q].disc(q)\rangle \rightarrow \langle \mathcal{E}_{X,q}(\sigma), R \parallel disc(q)\rangle$, where $\mathcal{E}_{H,q}$ is the superoperator that applies the H transformation only on qubit $q$, and $\mathcal{E}_{Z,q}$ is the superoperator that applies the Z transformation only on qubit $q$. Since $tr_q(\mathcal{E}_{H,q}(\sigma)) = tr_q(\mathcal{E}_{Z,q}(\sigma)) = tr_q(\sigma)$ for lemma 4.3.2, we have that $\langle \mathcal{E}_{H,q}(\sigma), R \parallel disc(q)\rangle \sim_{PS} \langle \mathcal{E}_{X,q}(\sigma), R \parallel disc(q)\rangle$ for theorem 4.3.1, and so

  $$\langle \mathcal{E}_{H,q}(\sigma), R \parallel disc(q)\rangle \mathcal{R} \langle \mathcal{E}_{X,q}(\sigma), R \parallel disc(q)\rangle$$

  by definition of $\mathcal{R}$.

### 4.3.2 Exploring quantum behavioural equivalence

We now investigate some expected properties of a bisimulation for quantum processes, and show that they are not met by the standard probabilistic bisimulation. We will see that these problems are related to the use of density operators to represent mixed states, with interesting consequences on non-determinism.

**The problem of mixed states**

We show that the usual way of defining behavioural equivalence through probabilistic lifting (Section 2.2.3) does not work in the quantum case. This happens because probabilistic mixtures of quantum states are represented in two alternative ways, i.e., using density operators and using distributions of configurations. Two different representations of the same mixture should be equivalent, but this is not always the case in the proposed bisimilarity (and in literature).

*Example* 4.3.4. Consider the following configurations and distributions.

$$\begin{aligned}
\mathcal{C} &= \langle |0\rangle\langle 0| \,, Set_{|+\rangle\langle +|}(q).M_{0,1}(q \triangleright x).(c!0 \parallel discard(q))\rangle \\
\mathcal{C}' &= \langle |0\rangle\langle 0| \,, Set_{\frac{1}{2}I}(q).\tau.(c!0 \parallel discard(q))\rangle \\
\Delta &= \overline{\langle |0\rangle\langle 0| \,, c!0 \parallel discard(q)\rangle} \;{}_{1/2}\!\oplus\; \overline{\langle |1\rangle\langle 1| \,, c!0 \parallel discard(q)\rangle} \\
\Delta' &= \overline{\langle 1/2I, c!0 \parallel discard(q)\rangle}
\end{aligned}$$

It is trivial that $\mathcal{C} \sim_{PS} \mathcal{C}'$ iff $\Delta \overset{\circ}{\sim}_{PS} \Delta'$. It seems obvious that the former should hold. Indeed the behaviour of $\langle \rho, c!0 \parallel discard(q)\rangle$ does not depend on $\rho$. Unfortunately, this is not the case for $\overset{\circ}{\sim}_{PS}$ .

Indeed, $\mathcal{C}$ and $\mathcal{C}'$ of the previous example are not bisimilar in qCCS according to [13, 10].

A related problem is that a single density operator may represent different probabilistic ensembles (i.e. distribution), that are indistinguishable according to quantum theory. In (l)qCCS, however, these distributions of configurations can be distinguished in $\sim_{PS}$ by some context.

*Example* 4.3.5. Consider the following distributions.

$$\begin{aligned}
\Delta &= \overline{\langle |0\rangle\langle 0| \,, c!q\rangle} \;{}_{1/2}\!\oplus\; \overline{\langle |1\rangle\langle 1| \,, c!q\rangle} \\
\Delta' &= \overline{\langle |+\rangle\langle +| \,, c!q\rangle} \;{}_{1/2}\!\oplus\; \overline{\langle |-\rangle\langle -| \,, c!q\rangle}
\end{aligned}$$

The two distributions only send a qbit on the channel $c$, and the qbit may be in state $|0\rangle$ or $|1\rangle$ for $\Delta$ ($|+\rangle$ or $|-\rangle$ for $\Delta'$) with equal probability. It seems reasonable that $\Delta$ and $\Delta'$ cannot be distinguished by an external observer receiving the qbit. This because the received qbit is in the probabilistic mixture $\{(|0\rangle, 1/2), (|1\rangle, 1/2)\}$ for $\Delta$ and $\{(|+\rangle, 1/2), (|-\rangle, 1/2)\}$ respectively for $\Delta'$, but the two mixtures are both represented by the same density operator $1/2I = 1/2\,|0\rangle\langle 0| + 1/2\,|1\rangle\langle 1| = 1/2\,|+\rangle\langle +| + 1/2\,|-\rangle\langle -|$. Unfortunately, this is not the case for $\overset{\circ}{\sim}_{PS}$, because the two distributions are composed by configurations that are not 'point-wise' bisimilar.

Once more, [13, 10] distinguish the two distributions, hence, e.g., the two processes $Set_{\frac{1}{2}I}(q).M_{0,1}[q \triangleright x].c!q$ and $Set_{\frac{1}{2}I}(q).M_{+,-}[q \triangleright x].c!q$ are not considered bisimilar.

**The problem of non-determinism**

We present here a strange behaviour that common process algebras express when mixing quantum states with non-deterministic choices. Assume a distribution obtained by tracing out one qubit of a Bell pair $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. This can be obtained, e.g., with the following configuration $\langle |\Phi^+\rangle, discard(q_0) \parallel \ldots\rangle$. The qbit is in a probabilistic ensemble of pure states, represented with the density opertator $1/2I$, which stands for both $\{(|0\rangle, 1/2), (|1\rangle, 1/2)\}$ and $\{(|+\rangle, 1/2), (|-\rangle, 1/2)\}$. The two ensembles are indeed indistinguishable from the quantum point of view. However, the two express a different behaviour according to a trivial semantics that just applies probabilistic reasoning to quantum processes, as shown in the following.

*Example* 4.3.6. Let the processes $P$ and $Q$ and distributions $\Delta$, $\Theta$ be

$$\begin{aligned}
P &= M_{0,1}[q \triangleright x].\textbf{if } x = 0 \textbf{ then } z!0 \textbf{ else } u!0 \\
Q &= M_{+,-}[q \triangleright x].\textbf{if } x = 0 \textbf{ then } p!0 \textbf{ else } m!0 \\
\Delta &= \langle |0\rangle\langle 0| \,, P + Q\rangle \;{}_{1/2}\!\oplus\; \langle |1\rangle\langle 1| \,, P + Q\rangle \\
\Theta &= \langle |+\rangle\langle +| \,, P + Q\rangle \;{}_{1/2}\!\oplus\; \langle |-\rangle\langle -| \,, P + Q\rangle
\end{aligned}$$

There is a way of performing the non deterministic choice such that $\Delta \rightarrow \langle |0\rangle\!\langle 0|\,, z!0\rangle$ with probability 1/2, $\Delta \rightarrow \langle |+\rangle\!\langle +|\,, p!0\rangle$ and $\Delta \rightarrow \langle |-\rangle\!\langle -|\,, m!0\rangle$ both with probability 1/4. The apparent contradiction is that $\Theta$ cannot replicate this behaviour.

Apparently, the previous example seems to contradict the common understanding of indistinguishability of quantum states. To recover it, either this behaviour must be expressed by both $\Delta$ and $\Theta$, or by none of them, resulting in two different notions of non deterministic choice. Actually, something strange happens in the example, namely, the non deterministic choice is performed in the two probabilistic branches, possibly in different ways.

### 4.3.3 Quantum Saturated Bisimilarity

We target the previousy highlighted problems by updating the proposed bisimilarity. The main idea is that density matrices represents equivalence classes of probabilistic mixtures of quantum states that are indistinguishable, and that this equivalence must be lifted from distribution of quantum states to distributions of lqCCS configurations.

The implicit equivalence relation implied by density operators is $\{(|\phi_i\rangle\,, p_i)\}_i \cong \{(|\phi_j\rangle\,, p_j)\}$ if and only if $\sum_i p_i\,|\phi_i\rangle\!\langle\phi_i| = \sum_j p_j\,|\phi_j\rangle\!\langle\phi_j|$. The physical justification of this equivalence is that different mixtures resulting in the same density operator cannot be distinguished since they behave the same. Note that this applies both to pure quantum states, where $|0\rangle$ and $-|0\rangle$ are equivalent, and mixed states, where $|0\rangle\ {}_{\frac{1}{2}}\!\oplus |1\rangle$ is the same as $|+\rangle\ {}_{\frac{1}{2}}\!\oplus |-\rangle$.

The same equivalence relation is trivially extended to configurations, where the use of density operators for the quantum state allows a common representation of different configurations with equivalent mixtures of quantum states. We extend here this equivalence relation to distributions of configurations. Intuitively, we give rules for exchanging the probabilistic combination ${}_p\!\oplus$ in the state of some configurations for probabilistic combination of configurations, and vice-versa.

**Definition 4.3.3.** *The* quantum equivalence *on distributions is the smallest symmetric relation* $\equiv \subseteq \mathfrak{D}(S) \times \mathfrak{D}(S)$ *generated by the rules:*

$$(\overline{\langle \rho, P\rangle}\ {}_p\!\oplus\ \overline{\langle \sigma, P\rangle}) \equiv \overline{\langle p\rho + (1-p)\sigma, P\rangle}$$

$$\frac{\Delta_1 \equiv \Theta_1 \quad \Delta_2 \equiv \Theta_2}{\Delta_1\ {}_p\!\oplus \Delta_2 \equiv \Theta_1\ {}_\Theta\!\oplus\ 2}$$

**Theorem 4.3.2.** $\equiv$ *is an equivalence relation, since it is reflexive, symmetric and transitive.*

*Proof.* Trivial by induction on the rules of $\equiv$. □

We can now present Quantum Saturated Bisimilarity, that is a relaxation of probabilistic saturated bisimilarity.

**Definition 4.3.4** (Quantum Saturated Bisimilarity)**.** *A symmetric relation* $\mathcal{R} \subseteq \mathcal{C} \times \mathcal{C}$ *is* quantum saturated (barbed) bisimulation *if* $\langle \rho, P\rangle\ \mathcal{R}\ \langle \sigma, Q\rangle$ *implies that* $P$ *and* $Q$ *are well-typed under the same typing context* $\Gamma; \Sigma$*, and for any context* $B[\_]_{\Gamma,\Sigma}$

- *If* $P \downarrow_c$ *then* $Q \downarrow_c$
- *If* $\langle \rho, B[P]\rangle \rightarrow \Delta$*, there exist* $\Delta', \Theta, \Theta'$ *such that* $\langle \sigma, B[Q]\rangle \rightarrow \Theta$ *and*

$$\Delta \equiv \Delta'\ \ \mathring{\mathcal{R}}\ \ \Theta' \equiv \Theta$$

*Let* quantum saturated bisimilarity $\sim_{QS}$ *be the union of all saturated probabilistic barbed bisimulation.*
*We say that two processes $P$ and $Q$ are* bisimilar*, written $P \sim_{QS} Q$, if for any $\rho \in \mathcal{D}(\mathcal{H}_{QN})$ it holds $\langle \rho, P\rangle \sim_{QS} \langle \rho, Q\rangle$.*

In other words, when $\mathcal{C} \to \Delta$, a bisimilar configuration $\mathcal{C}'$ must perform a transition $\mathcal{C}' \to \Theta$, but differently from $\sim_{PS}$, $\Delta$ and $\Theta$ are not required to be themselves Larsen-Skou bisimilar, but two distributions in their equivalence classes must be Larsen-Skou bisimilar.

**Theorem 4.3.3.** *Quantum saturated bisimilarity is strictly coarser then probabilistic saturated bisimilarity.*

*Proof.* To prove that $\sim_{PS} \subseteq \sim_{QS}$ is sufficient to observe that all probabilistic saturated bisimulations are also quantum probabilistic bisimulations, since $\equiv$ is reflexive. To prove that $\sim_{PS}$ is strictly finer, we need to show two processes that are not probabilistic bisimilar but are quantum bisimilar, like

$$P = M_{01}[q \rhd x].disc(q) \qquad Q = M_{\pm}[q \rhd x].disc(q)$$

The formal proof that these two processes are quantum bisimilar is postponed to the end of the section. □

To ease the bisimilarity proofs, we now prove that, like probabilistic bisimilarity, also quantum bisimilarity is closed for additional discarded qubits:

$$\langle tr_{\widetilde{q}}(\sigma), P\rangle \sim_{QS} \langle tr_{\widetilde{q}}(\nu), Q\rangle \Rightarrow \langle \sigma, P \parallel disc(\widetilde{q})\rangle \sim_{QS} \langle \nu, Q \parallel disc(\widetilde{q})\rangle$$

For the probabilistic case, we proved that

$$\langle tr_{\widetilde{q}}(\sigma), P\rangle \sim_{PS} \langle tr_{\widetilde{q}}(\nu), Q\rangle \Rightarrow \langle \sigma, P \parallel disc(\widetilde{q})\rangle \sim_{PS} \langle \nu, Q \parallel disc(\widetilde{q})\rangle$$

so now we have a weaker hypothesis, since $\sim_{QS}$ is coarser then $\sim_{PS}$.

Note that we can use Lemmas 4.3.1, 4.3.2 and 4.3.3 as they do not depend on the bisimulation in hand. To deal with the weaker hypothesis, we need only one further lemma, saying that additional discarded qubits preserve the equivalence relation.

**Lemma 4.3.4.** *Let $\sum_i p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle$ be a distribution of configuration, with $\sigma_i \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$ for each $i$. If*

$$\sum_i p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle \equiv \sum_j p_j \langle \rho_j, P_j\rangle$$

*then*

$$\sum_i p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle \equiv \sum_j p_j \langle \sigma_j, P_j \parallel disc(\widetilde{q})\rangle$$

*and $\rho_j = tr_{\widetilde{q}}(\sigma_j)$ for each $j$.*

*Proof.* We proceed by induction on the rules of $\equiv$. For the base case, suppose

$$\langle tr_{\widetilde{q}}(\sigma), P\rangle \;_p\!\oplus \langle tr_{\widetilde{q}}(\sigma'), P\rangle \equiv \langle (p)tr_{\widetilde{q}}(\sigma) + (1-p)tr_{\widetilde{q}}(\sigma'), P\rangle$$

We also have, by definition,

$$\langle \sigma, P \parallel disc(\widetilde{q})\rangle \;_p\!\oplus \langle \sigma', P \parallel disc(\widetilde{q})\rangle \equiv \langle (p)\sigma + (1-p)\sigma', P \parallel disc(\widetilde{q})\rangle$$

Notice that, due to linearity of partial trace, $(p)tr_{\widetilde{q}}(\sigma) + (1-p)tr_{\widetilde{q}}(\sigma') = tr_{\widetilde{q}}((p)\sigma + (1-p)\sigma')$, and so we have proven the final condition of the base case. The inductive case is trivial, as it simply combines two distributions, without changing the density matrix of configurations □

We can now prove the desired theorem on additional discarded qubits, now in the quantum case.

**Theorem 4.3.4** ($\sim_{QS}$ is closed for additional discarded qubits)**.** *If* $\langle tr_{\widetilde{q}}(\sigma), P\rangle \sim_{QS} \langle tr_{\widetilde{q}}(\nu), Q\rangle$ *then* $\langle \sigma, P \parallel disc(\widetilde{q})\rangle \sim_{QS} \langle \nu, Q \parallel disc(\widetilde{q})\rangle$.

*Proof.* Let $\sigma, \nu \in \mathcal{D}(\mathcal{H}_{\widetilde{p}} \otimes \mathcal{H}_{\widetilde{q}})$. As for theorem 4.3.1, we need to prove that if $\mathcal{R}$ is a quantum saturated bisimulation, then $\mathcal{R}_{tr_{\widetilde{q}}}$ is a quantum saturated bisimulation, where $\mathcal{R}_{tr_{\widetilde{q}}}$ is defined as

$$\mathcal{R}_{tr_{\widetilde{q}}} = \{ \Big(\langle \sigma, P \parallel disc(\widetilde{q})\rangle, \langle \nu, Q \parallel disc(\widetilde{q})\rangle\Big) \quad | \quad \langle tr_{\widetilde{q}}(\sigma), P\rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q\rangle \}$$

The proof is similar to the probabilistic bisimulation case, so we will omit some steps. For any process $R$ we suppose $\langle \sigma, P \parallel R \parallel disc(\widetilde{q})\rangle \to \sum p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle$. Then, from lemma 4.3.3, we know that $\langle tr_{\widetilde{q}}(\sigma), P \parallel R\rangle \to \sum p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle$. But since $\langle tr_{\widetilde{q}}(\sigma), P\rangle \mathcal{R} \langle tr_{\widetilde{q}}(\nu), Q\rangle$, and $\mathcal{R}$ is a quantum saturated bisimulation, it must be that

$$\begin{array}{lcc}
\langle tr_{\widetilde{q}}(\sigma), P \parallel R\rangle \to \sum\limits_i p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle & \equiv & \sum\limits_j p_j \langle \rho_j, P_j\rangle \\
 & & \overset{\circ}{\mathcal{R}} \\
\langle tr_{\widetilde{q}}(\nu), Q \parallel R\rangle \to \quad \sum\limits_i p_i \langle \xi_i, Q_i\rangle & \equiv & \sum\limits_j p_j \langle \xi'_j, Q_j\rangle
\end{array}$$

Then, we can apply our lemmas to each part of the above diagram:

- From $\sum_i p_i \langle tr_{\widetilde{q}}(\sigma_i), P_i\rangle \equiv \sum_j p_j \langle \rho_j, P_j\rangle$ follows, for lemma 4.3.4, $\sum_i p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle \equiv \sum_j p_j \langle \sigma_j, P_j \parallel disc(\widetilde{q})\rangle$, with $\rho_j = tr_{\widetilde{q}}(\sigma_j)$
- From $\langle tr_{\widetilde{q}}(\nu), Q \parallel R\rangle \to \quad \sum_i p_i \langle \xi_i, Q_i\rangle$ follows, for lemma 4.3.3, $\langle \nu, Q \parallel R \parallel disc(\widetilde{q})\rangle \to \sum_i p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q})\rangle$, with $\xi_i = tr_{\widetilde{q}}(\nu_i)$
- From $\sum_i p_i \langle \xi_i, Q_i\rangle \equiv \sum_j p_j \langle \xi'_j, Q_j\rangle$ follows, for lemma 4.3.4, $\sum_i p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q})\rangle \equiv \sum_j p_j \langle \nu_j, Q_j \parallel disc(\widetilde{q})\rangle$, with $\xi'_j = tr_{\widetilde{q}}(\nu_j)$.

In conclusion, together with the definition of $\mathcal{R}_{tr_{\widetilde{q}}}$, we get

$$\begin{array}{lcc}
\langle \sigma, P \parallel R \parallel disc(\widetilde{q})\rangle \to \sum\limits_i p_i \langle \sigma_i, P_i \parallel disc(\widetilde{q})\rangle & \equiv & \sum\limits_j p_j \langle \sigma_j, P_j \parallel disc(\widetilde{q})\rangle \\
 & & \overset{\circ}{\mathcal{R}}_{tr_{\widetilde{q}}} \\
\langle \nu, Q \parallel R \parallel disc(\widetilde{q})\rangle \to \quad \sum\limits_i p_i \langle \nu_i, Q_i \parallel disc(\widetilde{q})\rangle & \equiv & \sum\limits_j p_j \langle \nu_j, Q_j \parallel disc(\widetilde{q})\rangle
\end{array}$$

And so $\langle \sigma, P \parallel R \parallel disc(\widetilde{q})\rangle \mathcal{R}_{tr_{\widetilde{q}}} \langle \nu, Q \parallel R \parallel disc(\widetilde{q})\rangle$. □

As an example, considere the following formula, that from [8] we expect to hold.

*Example* 4.3.7. We expect that

$$P = M_{01}[q_0 \rhd x].disc(q_0) \sim_{QS} Q = M_{\pm}[q_0 \rhd x].disc(q_0)$$

To prove this result, we need the above Theorem 4.3.4
Given that $\emptyset, q_0 \vdash P$ and $\emptyset, q_0 \vdash Q$, we show that

$$\mathcal{R} = \big\{\langle \sigma, B[P]\rangle, \langle \sigma, B[Q]\rangle \mid \sigma \in \mathcal{D}(\mathcal{H}_{QN}), B[-]_{\emptyset;\{\,q\,\}} \text{ typed context}\big\}^{S} \cup \sim_{PS}$$

is a quantum saturated bisimulation, where $\mathcal{R}^S$ denotes the symmetric closure of a relation $\mathcal{R}$. This is sufficient to prove our statement as it trivially follows that $\langle \sigma, P\rangle \sim_{QS} \langle \sigma, Q\rangle$ for any $\sigma$, and so $P$ and $Q$ are bisimilar processes.

$\mathcal{R}$ is a *saturated* relation, meaning that if $\mathcal{C}\mathcal{R}\mathcal{C}'$, then $B[\mathcal{C}]\mathcal{R}B[\mathcal{C}']$ for any $B$. So, to prove that $\mathcal{R}$ is a quantum saturated bisimulation, we just need to show that $\mathcal{R}$ is a quantum bisimulation.

Suppose that $\langle \sigma, R \parallel P\rangle \mathcal{R} \langle \sigma, R \parallel Q\rangle$, and that $\langle \sigma, R \parallel P\rangle \to \sum_i p_i \mathcal{C}_i$.

- If the reductions happens in $R$, it must be of the form $\langle \sigma, R \parallel P\rangle \to \sum_i p_i \langle \sigma_i, R_i \parallel P\rangle$, but then there exists a transition $\langle \sigma, R \parallel Q\rangle \to \sum_i p_i \langle \sigma_i, R_i \parallel Q\rangle$, and for each $i$, $\langle \sigma_i, R_i \parallel P\rangle \mathcal{R} \langle \sigma_i, R_i \parallel Q\rangle$ by definition of $\mathcal{R}$.
- If the reductions happens in $P$, it must be

  $$\langle \sigma, R \parallel M_{01}[q \rhd x].disc(q)\rangle \to \langle \frac{1}{p_0}\mathcal{E}_{0,q}(\sigma), R \parallel disc(q)\rangle \;{}_{p_0}\!\oplus \langle \frac{1}{p_1}\mathcal{E}_{1,q}(\sigma), R \parallel disc(q)\rangle$$

  where $\mathcal{E}_{0,q}(\rho) = (|0\rangle\langle 0| \otimes I)\rho(|0\rangle\langle 0| \otimes I)^\dagger$ is the trace non-increasing superoperator that projects qubit $q$ to $|0\rangle$, $p_0$ is the probability of obtaining outcome 0 from $\sigma$, and similarly for $\mathcal{E}_{1,q}$ and $p_1$. But then

  $$\langle \sigma, R \parallel M_{\pm}[q \rhd x].disc(q)\rangle \to \langle \frac{1}{p_+}\mathcal{E}_{+,q}(\sigma), R \parallel disc(q)\rangle \;{}_{+}\!\oplus \langle \frac{1}{p_-}\mathcal{E}_{-,q}(\sigma), R \parallel disc(q)\rangle$$

  Noticeably these two distributions are not probabilistic bisimilar, as it is evident in the case $\langle \Phi^+, P\rangle \to \langle |00\rangle\langle 00|\,, disc(\widetilde{q})\rangle \;{}_{\frac{1}{2}}\!\oplus \langle |11\rangle\langle 11|\,, disc(\widetilde{q})\rangle$ and $\langle \Phi^+, Q\rangle \to \langle |{+}{+}\rangle\langle {+}{+}|\,, disc(\widetilde{q})\rangle \;{}_{\frac{1}{2}}\!\oplus \langle |{-}{-}\rangle\langle {-}{-}|\,, disc(\widetilde{q})\rangle$. Thanks to the quantum equivalence relation, however, we have

  $$\langle \frac{1}{p_0}\mathcal{E}_{0,q}(\sigma), R \parallel disc(q)\rangle \;{}_{p_0}\!\oplus \langle \frac{1}{p_1}\mathcal{E}_{1,q}(\sigma), R \parallel disc(q)\rangle \equiv \overline{\langle \mathcal{E}_{0,q}(\sigma) + \mathcal{E}_{1,q}(\sigma), R \parallel disc(q)\rangle}$$

  $$\langle \frac{1}{p_+}\mathcal{E}_{+,q}(\sigma), R \parallel disc(q)\rangle \;{}_{p_+}\!\oplus \langle \frac{1}{p_-}\mathcal{E}_{-,q}(\sigma), R \parallel disc(q)\rangle \equiv \overline{\langle \mathcal{E}_{+,q}(\sigma) + \mathcal{E}_{-,q}(\sigma), R \parallel disc(q)\rangle}$$

  Observe that $\mathcal{E}_{0,q}(\sigma) + \mathcal{E}_{1,q}(\sigma)$ can be seen as $\mathcal{E}_{01,q}(\sigma)$, where $\mathcal{E}_{01,q}$ is the trace-preserving superoperator that measures the qubit $q$ in the computational basis and then discards the result. $\mathcal{E}_{01,q}(\sigma)$ is indeed a well defined superoperator, with $|0\rangle\langle 0| \otimes I$ and $|1\rangle\langle 1| \otimes I$ one of its Kraus decomposition. The same holds also for $\mathcal{E}_{+,q}(\sigma) + \mathcal{E}_{-,q}(\sigma) = \mathcal{E}_{\pm,q}(\sigma)$. So we can conclude

  $$\langle \mathcal{E}_{01,q}, R \parallel disc(q)\rangle \sim_{QS} \langle \mathcal{E}_{\pm,q}, R \parallel disc(q)\rangle$$

  from Theorem 4.3.4, since $tr_q(\mathcal{E}_{01,q}(\sigma)) = tr_q(\mathcal{E}_{\pm,q}(\sigma)) = tr_q(\sigma)$.

*Remark* 4.3.1. As a general result, note that for quantum saturated bisimilarity all the following processes are equivalent

$$U(q).disc(q) \sim_{QS} M[q \rhd x].disc(q) \sim_{QS} \mathcal{E}(q).disc(q) \sim_{QS} \tau.disc(q)$$

for any unitary $U$, measurement $M$ or superoperator $\mathcal{E}$.

## 4.4 Comparison

We summarize here the similarity and differences of lqCCS with the related works discussed in Chapter 3. In particular, we focus on QPALg and qCCS, that share with us a similar model. We will see that a relevant problem of QPALg is solved by our approach, that our bisimulations share some desired properties of qCCS, and finally we will show that starting from a qCCS-like calculus, we have establishd results similar to the ones that are peculiar of CQP.

### 4.4.1 QPALg

We show here, by means of an example, that lqCCS solve a relevant problem of qbit transmission in QPALg, resulting in a too much coarse-graned bisimilarity.

Consider the two configurations

$$\mathcal{C} = \langle \frac{1}{2} I \otimes \frac{1}{2} I, c!q_1 \parallel c!q_2 \rangle \qquad \mathcal{C}' = \langle |\Phi^+\rangle\langle\Phi^+| \, , c!q_1 \parallel c!q_2 \rangle$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} 11$. According to the labelled bisimulation of QPAlg, the two configurations are bisimilar, as they both send two qubits with reduced density operator $\frac{1}{2}I$ on channel $c$. For our definition instead it holds $\mathcal{C} \not\sim_{PS} \mathcal{C}'$, in accordance to what is prescribed by quantum theory, as the two configurations are distinguished by the context

$$B[-] = [-] \parallel c?x.c?y.M[x, y \rhd z].\textbf{if } z = 2 \textbf{ then } d!0 \parallel disc(x, y) \textbf{ else } \parallel disc(x, y)$$

where $M$ is the measurement on the 4-dimensional computational basis

$$M = \{ \, M_0 = \; |\, 00\rangle\langle 00 \,| \, , M_1 = \; |\, 01\rangle\langle 01 \,| \, , M_2 = \; |\, 10\rangle\langle 10 \,| \, , M_3 = \; |\, 11\rangle\langle 11 \,| \; \}$$

After receiving and measuring two unrelated mixed state qubits, $B[\mathcal{C}]$ will evolve in the distribution $\Delta$

$$\frac{1}{4}\langle |00\rangle\langle 00| \, , disc(\widetilde{q})\rangle + \frac{1}{4}\langle |01\rangle\langle 01| \, , disc(\widetilde{q})\rangle + \frac{1}{4}\langle |10\rangle\langle 10| \, , d!0 \parallel disc(\widetilde{q})\rangle + \frac{1}{4}\langle |11\rangle\langle 11| \, , disc(\widetilde{q})\rangle$$

where $\widetilde{q}$ is the couple $q_1, q_2$. After receiving and measuring two entangled qubits, instead, $B[\mathcal{C}']$ will evolve in the distribution $\Delta'$

$$\frac{1}{2}\langle |00\rangle\langle 00| \, , disc(\widetilde{q})\rangle + \frac{1}{2}\langle |11\rangle\langle 11| \, , disc(\widetilde{q})\rangle$$

We have that $\Delta \overset{\circ}{\not\sim}_{PS} \Delta'$, as there is no decomposition of $\Delta = \sum_{i \in I} p_i \mathcal{C}_i$ and $\Delta' = \sum_{i \in I} p_i \mathcal{C}'_i$ such that $\mathcal{C}_i \sim_{PS} \mathcal{C}'_i$ for each $i$, because $\Delta$ contains a configuration that expresses the barb $\downarrow_d$, while $\Delta'$ contains none.

### 4.4.2 qCCS

We compare here lqCCS with qCCS, showing that some defining properties of CCS is recovered in lqCCS. We omit here the main difference discussed above, which is the new bisimulation $\sim_{QS}$, shown to be more adequate to model behavioural equivalence in quantum processes.

Our probabilistic saturated bisimilarity is designed to be equivalent to open bisimilarity for qCCS, except for a few intended modification:

- Open bisimilarity requires bisimilar processes to have the same free variables, $\sim_{PS}$ requires bisimilar processes to have the same typing context.
- Open bisimilarity is superoperator-closed by definition, $\sim_{PS}$ is proven to be superoperator closed.
- Open bisimilarity requires bisimilar configurations to have the same environment, $\sim_{PS}$ implies that bisimilar configurations have the same environment.
- Open bisimilarity is contex closed as a property, $\sim_{PS}$ is context closed by definition.

In the following, by writing $\mathcal{E} \in \mathcal{TS}(\mathcal{H}_{\widetilde{q}})$, we intend a superoperator that acts only on the qubits $\widetilde{q}$, i.e. $\mathcal{E}(\rho) = \sum_{i \in I} (I_{\widetilde{p}} \otimes A_i)\rho(I_{\widetilde{p}} \otimes A_i)^\dagger$, where $\widetilde{p} = \mathrm{QN} \setminus \widetilde{q}$ are all the qubits *outside* $\widetilde{q}$. We also write $\mathcal{E}(\langle \rho, P \rangle)$ to denote the configuration $\langle \mathcal{E}(\rho), P \rangle$.

**Theorem 4.4.1.** *For any pair of configurations $\langle \rho, P \rangle, \langle \sigma, Q \rangle$ well-typed under $\Gamma; \Sigma$, $\langle \rho, P \rangle \sim_{PS} \langle \rho, P \rangle$ implies*

1. *for any $\mathcal{E} \in \mathcal{TS}(\mathcal{H}_{\widetilde{\Sigma}})$, $\mathcal{E}(\langle \rho, P \rangle) \ \sim_{PS} \ \mathcal{E}(\langle \rho, P \rangle)$*
2. *$tr_\Sigma(\rho) = tr_\Sigma(\sigma)$.*

*Proof.* To prove point 1, suppose $\langle \rho, P \rangle \sim_{QS} \langle \sigma, Q \rangle$, with $\rho, \sigma \in \mathcal{H}_{\widetilde{q},\widetilde{p}}$ and $\Gamma; \widetilde{p} \vdash P$, $\Gamma; \widetilde{p} \vdash Q$. For any superoperator $\mathcal{E} \in \mathcal{TS}(\mathcal{H}_{\widetilde{q}})$ we can construct a context

$$B[-] = [-] \parallel \mathcal{E}(\widetilde{q}).a!0 \parallel c!\widetilde{q}$$

where $a$ is a fresh channel. We know that $\langle \rho, B[P] \rangle$ and $\langle \sigma, B[Q] \rangle$ are bisimilar, and$\langle \rho, B[P] \rangle$ can evolve in $\langle \mathcal{E}(\rho), a!0 \parallel c!\widetilde{q} \parallel P \rangle$. Then $\langle \sigma, B[Q] \rangle$ must necessarily evolve in $\langle \mathcal{E}(\sigma), a!0 \parallel c!\widetilde{q} \parallel Q \rangle$, because it must match the $\downarrow_a$ barb, and $a$ is fresh. So we have that

$$\langle \mathcal{E}(\rho), a!0 \parallel c!\widetilde{q} \parallel P \rangle \sim_{QS} \langle \mathcal{E}(\sigma), a!0 \parallel c!\widetilde{q} \parallel Q \rangle$$

and from this it follows

$$\langle \mathcal{E}(\rho), P \rangle \sim_{QS} \langle \mathcal{E}(\sigma), Q \rangle$$

simply by contradiction: if there was a context capable of distinguishing $\mathcal{E}(\rho, P)$ from $\mathcal{E}(\rho, Q)$ then there would be a context able to distinguish also $\mathcal{E}(\rho, P \parallel a!0 \parallel c!\widetilde{q})$ from $\mathcal{E}(\sigma, Q \parallel a!0 \parallel c!\widetilde{q})$

To prove point 2 we proceed by contradiction, supposing $\langle \rho, P \rangle \sim_{QS} \langle \sigma, Q \rangle$ and $tr_{\widetilde{p}}(\rho) \neq tr_{\widetilde{p}}(\sigma)$, with a $\rho, \sigma \in \mathcal{H}_{\widetilde{q},\widetilde{p}}$ and $\Gamma; \widetilde{p} \vdash P$, $\Gamma; \widetilde{p} \vdash Q$. If $tr_{\widetilde{p}}(\rho) \neq tr_{\widetilde{p}}(\sigma)$, then there exists a measurement $M_{\widetilde{q}} = \{ M_1, \ldots, M_m \}$ that distinguishes them, i.e. such that $p_m(tr_{\widetilde{p}}(\rho)) = tr(M_m tr_{\widetilde{p}}(\rho) M_m^\dagger) \neq tr(M_m tr_{\widetilde{p}}(\sigma) M_m^\dagger) = p_m(tr_{\widetilde{p}}(\sigma))$ for some $m$. But for lemma 4.3.1, the same probabilities arise also from the measurement $M_{\widetilde{qp}} = \{ M_1 \otimes I_{\widetilde{p}}, \ldots, M_m \otimes I_{\widetilde{p}} \}$, that can therefore distinguish the whole state $\rho$ from $\sigma$. So, taken the context

$$[-] \parallel M[\widetilde{q} \triangleright x].\big(disc(\widetilde{q}) \parallel \textbf{if } x = 1 \textbf{ then } c_1!0 \textbf{ else } \ldots \textbf{if } x = m{-}1 \textbf{ then } c_{m-1}!0 \textbf{ else } c_m!0\big)$$

where $c_0 \ldots c_m$ are fresh channels, we have that $\langle \rho, B[P] \rangle$ should be bisimilar to $\langle \sigma, B[Q] \rangle$. But

$$\langle \rho, B[P] \rangle \to \sum_m p_m(\rho) \langle \rho_m, c_m!0 \rangle$$

and $\langle \sigma, B[Q] \rangle$ can perform only the transition

$$\langle \sigma, B[Q] \rangle \to \sum_m p_m(\sigma) \langle \sigma_m, c_m!0 \rangle$$

to match the barbs, but we know that $p_m(\rho) \neq p_m(\sigma)$ for at least one $m$. □

We can actually prove a stronger property, that in lqCCS the action of 'external' superoperators $\mathcal{E} \in \mathcal{TS}(\mathcal{H}_{\widetilde{\Sigma}})$ does not change the observable behaviour of a quantum system.

**Proposition 4.4.1.** *For any pair of configurations $\mathcal{C}, \mathcal{C}'$ well-typed under $\Gamma; \Sigma$, and for any $\mathcal{E} \in TSO(\mathcal{H}_{\widetilde{\Sigma}})$, $\mathcal{C} \to \Delta$ iff $\mathcal{E}(\mathcal{C}) \to \mathcal{E}(\Delta)$.*

*Proof.* The only non trivial rules are SemQOp and SemQMeas. Assume without loss of generality that $env(\mathcal{C}) \in \mathcal{H}_{\Sigma\otimes\overline{\Sigma}}$. By SemQOp, $\mathcal{C} = \langle \rho, \mathcal{E}(\widetilde{x}).P\rangle \longrightarrow \langle \mathcal{E}_{\widetilde{x}}(\rho), P\rangle = \Delta$. The type system ensures that $\tilde{x} \subseteq \Sigma$. We assume without loss of generality that $\tilde{x} = \Sigma$. We can also apply SemQOp as follows, $\mathcal{E}(\mathcal{C}) = \langle \mathcal{E}(\rho), \mathcal{E}(\widetilde{x}).P\rangle \longrightarrow \langle \mathcal{E}_{\widetilde{x}}(\mathcal{E}(\rho)), P\rangle$. We need to prove that $\langle \mathcal{E}_{\widetilde{x}}(\mathcal{E}(\rho)), P\rangle = \langle \mathcal{E}(\mathcal{E}_{\widetilde{x}}(\rho)), P\rangle = \mathcal{E}(\Delta)$, i.e., that $\mathcal{E}_{\widetilde{x}}(\mathcal{E}(\rho)) = \mathcal{E}(\mathcal{E}_{\widetilde{x}}(\rho))$. By definition, $\mathcal{E}_{\widetilde{x}}(\rho) = \sum_{i=1}^{n}(I_\Sigma \otimes A_i)\rho(I_\Sigma \otimes A_i)^\dagger$, and $\mathcal{E}(\rho) = \sum_{j=1}^{m}(B_j \otimes I_{\overline{\Sigma}})\rho(B_j \otimes I_{\overline{\Sigma}})^\dagger$.

By linearity

$$\begin{aligned}&\mathcal{E}_{\widetilde{x}}(\mathcal{E}(\rho)) = \\ &\sum_{i=1}^{n}(I_\Sigma \otimes A_i)(\sum_{j=1}^{m}(B_j \otimes I_{\overline{\Sigma}})\rho(B_j \otimes I_{\overline{\Sigma}})^\dagger)(I_\Sigma \otimes A_i)^\dagger = \\ &\sum_{i=1}^{n}\sum_{j=1}^{m}(I_\Sigma \otimes A_i)(B_j \otimes I_{\overline{\Sigma}})\rho(B_j \otimes I_{\overline{\Sigma}})^\dagger(I_\Sigma \otimes A_i)^\dagger,\end{aligned}$$

and

$$\begin{aligned}&\mathcal{E}(\mathcal{E}_{\widetilde{x}}(\rho)) = \\ &\sum_{j=1}^{m}(B_j \otimes I_{\overline{\Sigma}})(\sum_{i=1}^{n}(I_\Sigma \otimes A_i)\rho(I_\Sigma \otimes A_i)^\dagger)(B_j \otimes I_{\overline{\Sigma}})^\dagger = \\ &\sum_{i=1}^{n}\sum_{j=1}^{m}(B_j \otimes I_{\overline{\Sigma}})(I_\Sigma \otimes A_i)\rho(I_\Sigma \otimes A_i)^\dagger(B_j \otimes I_{\overline{\Sigma}})^\dagger.\end{aligned}$$

Thanks to conjugate properties, it is thus sufficient to show that

$$(B_{p\times p} \otimes I_{q\times q})(I_{p\times p} \otimes A_{q\times q}) = (I_{p\times p} \otimes A_{q\times q})(B_{p\times p} \otimes I_{q\times q}).$$

This is easily proven thanks to the mixed product property of the Kronecker product, telling us that

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

so in our case, we have

$$(B_{p\times p} \otimes I_{q\times q})(I_{p\times p} \otimes A_{q\times q}) = B_{p\times p} \otimes A_{q\times q} = (I_{p\times p} \otimes A_{q\times q})(B_{p\times p} \otimes I_{q\times q})$$

The proof for rule SemQMeas is the same, considering every $m \in \{0, \ldots, 2^{\widetilde{x}}\}$ separately. □

### 4.4.3 CQP

The main difference between our type system and CQP's type system is linearity. To transform an affine system in a linear system, is necessary to remove the *weakening* rule for Σ:

$$\frac{\Gamma; \Sigma \vdash P}{\Gamma; \Sigma, q \vdash P}\ \text{QWeak}$$

that allows to introduce a quantum name $q$ in $\Sigma$ even if it is not sent by $P$. In CQP, weakening is not an explicit rule of the typesystem, but is used implicitly in various rules, making it an affine type system.

As already said, our quantum saturated bisimilarity descends from the same quantum properties that are behind mixed configuration CQP bisimilarity. One feature of our language that is missing in CQP are superoperators, so only in our system is possible to prove that

$$Set_{|+\rangle\langle+|}(q).M_{01}(q \triangleright x).c!0 \sim Set_{|+\rangle\langle+|}.Set_{\frac{1}{2}I}(q).c!0$$

i.e. that a measurement of which we ignore the result is equivalent to the superoperator that sets all qubits to the maximmaly mixed state.

# Chapter 5

# Minimal Process Calculus

Given the difficulties of finding a good notion of behavioural equivalence in quantum process algebras, we consider to address the problem on a minimal setting, only focusing basic constructs.

## 5.1 Mathematical Preliminaries

A quantum distribution $\mathfrak{D} \in D(S)^{\mathcal{H}}$ over a set $S$ is a function from the finite-dimensional Hilbert space $\mathcal{H}$ of dimension $n$ to probability distributions $\Delta$ over $S$. In the following, we write $K_\Delta$ defined as the function that always returns $\Delta$ for every state $|\phi\rangle \in \mathcal{H}$.

Let $\{\, P_i \mid \sum_{i=1}^n P_i = I \,\}$ be a set of quantum projectors, and let $\mathfrak{D}_i$, $1 \leq i \leq n$, be a collection of quantum distributions. We use $\sum_{i=1}^n P_i\mathfrak{D}_i$ to denote the distribution determined by

$$\left(\sum_{i=1}^n P_i\mathfrak{D}_i\right)(|\phi\rangle) = \sum_{i=1}^n p_i(|\phi\rangle)\mathfrak{D}_i\left(\frac{P_i\,|\phi\rangle}{p_i(|\phi\rangle)}\right)$$

where $p_i(|\phi\rangle) = \langle\phi|\,P_i\,|\phi\rangle$.

Note that for any $|\phi\rangle$, $(\sum_{i=1}^n P_i\mathfrak{D}_i)(|\phi\rangle)$ is a legal probability distribution since $\mathfrak{D}_i(|\psi\rangle)$ is a probability distribution and

$$\sum_{i=1}^n p_i(|\phi\rangle) = \sum_{i=1}^n \langle\phi|\,P_i\,|\phi\rangle = \langle\phi|\,I\,|\phi\rangle = \langle\phi|\phi\rangle = 1.$$

When $n = 2$, $P_2$ is derivable as $I - P_1$, thus we write $\mathfrak{D}_1 \;{}_{P_1}\!\boxplus\, \mathfrak{D}_2$ for $\sum_{i=1}^n P_i\mathfrak{D}_i$. The operator $- \;{}_P\!\boxplus -$ can be defined from $- \;{}_p\!\oplus -$ as follows:

$$(\mathfrak{D} \;{}_{P_1}\!\boxplus\, \mathfrak{T})(|\phi\rangle) = \mathfrak{D}\left(\frac{P_1\,|\phi\rangle}{p_1(|\phi\rangle)}\right) \;{}_{p_1(|\phi\rangle)}\!\oplus\, \mathfrak{T}\left(\frac{P_2\,|\phi\rangle}{p_2(|\phi\rangle)}\right)$$

We define the common notions of linearity and decomposability as usual.

**Definition 5.1.1.** *We say that a relation* $\mathcal{R} \subseteq D(S)^{\mathcal{H}} \times D(S)^{\mathcal{H}}$ *is* linear *over* $- \boxplus -$ *if* $\mathfrak{D}_i \,\mathcal{R}\, \mathfrak{T}_i$, $i = 1, 2$, *implies* $(\mathfrak{D}_1 \;{}_P\!\boxplus\, \mathfrak{D}_2) \,\mathcal{R}\, (\mathfrak{T}_1 \;{}_P\!\boxplus\, \mathfrak{T}_2)$ *for any* $P$. *We say that a relation* $\mathcal{R} \subseteq D(S)^{\mathcal{H}} \times D(S)^{\mathcal{H}}$ *is* left-decomposable *over* $- \boxplus -$ *if* $(\mathfrak{D}_1 \;{}_P\!\boxplus\, \mathfrak{D}_2) \;\mathcal{R}\; \mathfrak{T}$ *implies* $\mathfrak{T} = (\mathfrak{T}_1 \;{}_P\!\boxplus\, \mathfrak{T}_2)$ *where* $\mathfrak{D}_i \;\mathcal{R}\; \mathfrak{T}_i$, *for* $i = 1, 2$. Right-decomposable *relations are defined as expected, and a relation is* decomposable *if it is both left- and right-decomposable.*

The quantum lifting of a relation is defined as follows.

**Definition 5.1.2.** *Let $\mathcal{R}$ be a relation in $S \times S$, we define its quantum lifting $\overset{\boxplus}{\mathcal{R}}$ as a relation in $D(S)^{\mathcal{H}} \times D(S)^{\mathcal{H}}$ as the minimal relation such that*

1. *$s \; \mathcal{R} \; s'$ implies $K_{\overline{s}} \overset{\boxplus}{\mathcal{R}} K_{\overline{s'}}$; and*

2. *$\mathfrak{D}_i \overset{\boxplus}{\mathcal{R}} \mathfrak{T}_i$, $i = 1, 2$, implies $\mathfrak{D}_1 \; {}_P\!\boxplus \; \mathfrak{D}_2 \overset{\boxplus}{\mathcal{R}} \mathfrak{T}_1 \; {}_P\!\boxplus \; \mathfrak{T}_2$ for any projector $P$.*

**Proposition 5.1.1.** *Let $\mathcal{R}$ be a relation in $S \times S$, and let $\mathfrak{D}, \mathfrak{T}$ be quantum distributions such that $\mathfrak{D} \overset{\boxplus}{\mathcal{R}} \mathfrak{T}$. Then, for any $|\phi\rangle$, $\mathfrak{D}(|\phi\rangle) \overset{\circ}{\mathcal{R}} \mathfrak{T}(|\phi\rangle)$.*

*Proof.* We proceed by induction on the derivation of $\mathfrak{D} \overset{\boxplus}{\mathcal{R}} \mathfrak{T}$. Case *1.* is trivial, for any $|\phi\rangle$, $K_{\overline{s}}(|\phi\rangle) = \overline{s}$, and $K_{\overline{s'}}(|\phi\rangle) = \overline{s'}$, and $s \; \mathcal{R} \; s'$ implies $\overline{s} \overset{\circ}{\mathcal{R}} \overline{s'}$. For case *2.*, we have that

$$(\mathfrak{D}_1 \; {}_{P_1}\!\boxplus \; \mathfrak{D}_2)(|\phi\rangle) = \mathfrak{D}_1 \left( \frac{P_1 |\phi\rangle}{p_1(|\phi\rangle)} \right) \; {}_{p_1(|\phi\rangle)}\!\oplus \; \mathfrak{D}_2 \left( \frac{P_2 |\phi\rangle}{p_2(|\phi\rangle)} \right)$$
$$(\mathfrak{T}_1 \; {}_{P_1}\!\boxplus \; \mathfrak{T}_2)(|\phi\rangle) = \mathfrak{T}_1 \left( \frac{P_1 |\phi\rangle}{p_1(|\phi\rangle)} \right) \; {}_{p_1(|\phi\rangle)}\!\oplus \; \mathfrak{T}_2 \left( \frac{P_2 |\phi\rangle}{p_2(|\phi\rangle)} \right)$$

By induction hypothesis we know that $\mathfrak{D}_i \left( \frac{P_i|\phi\rangle}{p_i(|\phi\rangle)} \right) \overset{\circ}{\mathcal{R}} \mathfrak{T}_i \left( \frac{P_i|\phi\rangle}{p_i(|\phi\rangle)} \right)$, for $i = 1, 2$, and the thesis holds by linearity. □

## 5.2 Quantum Labeled Transition Systems

A quantum labeled transition system QLTS on an Hilbert space $\mathcal{H}$ is a triple $(S, Act_\tau, \rightarrow)$ where

- $S$ is a set of states $s, s_1, \ldots$;
- $Act_\tau$ is a set of transition labels with $\tau$ a distinguished element;
- $\rightarrow \subseteq S \times Act_\tau \times D(S)^{\mathcal{H}}$ is the transition relation.

We define a minimal quantum process algebra (mQPA) for describing quantum processes. A quantum process $Q$ is defined as

$$Q ::= \mathbf{0} \mid \mu.Q \mid Q + Q \mid U \circ Q \mid Q \; {}_P\!\boxplus \; Q$$

where $U$ is a unitary transformation over $\mathcal{H}$.

We give the semantics of mQPA in terms of QLTS. Some terms are taken as states $s \in S$, in particular the ones where unitary operators and $- \boxplus -$ are guarded.

$$s ::= \mathbf{0} \mid \mu.Q \mid s + s$$

The interpretation of an arbitrary term $Q$ as quantum distribution $[\![Q]\!]$ over S is given by the function $[\![-]\!]$:

$$\begin{aligned}
&[\![\mathbf{0}]\!](|\phi\rangle) = \overline{\mathbf{0}} \\
&[\![\mu.Q]\!](|\phi\rangle) = \overline{\mu.Q} \\
&[\![Q_1 + Q_2]\!](|\phi\rangle)(s) = \begin{cases} [\![Q_1]\!](|\phi\rangle)(s_1) \cdot [\![Q_2]\!](|\phi\rangle)(s_2) & \text{if } s = s_1 + s_2 \\ 0 & \text{otherwise} \end{cases} \\
&[\![U \circ Q]\!](|\phi\rangle) = [\![Q]\!](U |\phi\rangle) \\
&[\![Q_1 \; {}_P\!\boxplus \; Q_2]\!] = [\![Q_1]\!] \; {}_P\!\boxplus \; [\![Q_2]\!]
\end{aligned}$$

The following proposition is trivially derivable by definition.

**Proposition 5.2.1.** *For any $s \in S$, $[\![s]\!] = K_{\bar{s}}$.*

The transition relation $\rightarrow$ is defined as follows, with $s \xrightarrow{\mu} \Delta$ as notation for $(s, \mu, \Delta) \in \rightarrow$.

$$\frac{}{\mu.Q \xrightarrow{\mu} [\![Q]\!]}\ \textsc{Action} \qquad \frac{Q_1 \xrightarrow{\mu} \Delta}{Q_1 + Q_2 \xrightarrow{\mu} \Delta}\ \textsc{Ext.L} \qquad \frac{Q_2 \xrightarrow{\mu} \Delta}{Q_1 + Q_2 \xrightarrow{\mu} \Delta}\ \textsc{Ext.R}$$

We define bisimularity on QLTS as usual.

**Definition 5.2.1.** *A symmetric relation $\mathcal{R} : S \times S$ is called a QLTS* bisimulation *if it's symmetric and for each pair of states $s, s' \in S$ such that $s\mathcal{R}s'$, if $s \xrightarrow{\mu} \Delta$ then $s' \xrightarrow{\mu} \Delta'$ and $\Delta \overset{\boxplus}{\mathcal{R}} \Delta'$, for some quantum distributions $\Delta' \in D(S)$.* Q-bisimilarity *$\sim_Q$ is the largest QLTS bisimulation.*

### 5.2.1 Testing Bisimilarity over problematic Cases

We take the example 6, 7, 8, and show that they behave as expected in mQPA.

For examples 6 and 7 consider the following.

*Example* 5.2.1. A qbit which is in a mixed state of $|0\rangle$ and $|1\rangle$ with equal probability behaves exactly as a qbit which is in a mixed state of $|+\rangle$ and $|-\rangle$. Consider the two following processes.

$$\begin{aligned} Q &= (s \;{}_{|0\rangle\langle 0|}\boxplus\; s') \;{}_{|+\rangle\langle +|}\boxplus\; (s \;{}_{|0\rangle\langle 0|}\boxplus\; s') \\ Q' &= (s \;{}_{|+\rangle\langle +|}\boxplus\; s') \;{}_{|0\rangle\langle 0|}\boxplus\; (s \;{}_{|+\rangle\langle +|}\boxplus\; s') \end{aligned}$$

Note that in $Q$ (in $Q'$ resp.), after the nested measure, the qbit is in state $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|-\rangle$ resp.) with equal probability. Indeed, $Q$ and $Q'$ stand for the same quantum distribution: $[\![Q]\!] = [\![Q']\!] = K_{\bar{s}}$.

Example 8 is addressed as follows.

*Example* 5.2.2. Consider the bell pair $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. Let $Q$, $Q'$, $Q_0$ and $Q_+$ be as follows

$$\begin{aligned} Q &= z \;{}_{P_{\text{-}0}}\boxplus\; u \\ Q' &= p \;{}_{P_{\text{-}+}}\boxplus\; m \\ Q_0 &= ((Q + Q') \;{}_{P_{\text{-}0}}\boxplus\; (Q + Q')) \;{}_{P_{|\Phi^+\rangle\langle\Phi^+|}}\boxplus\; \mathbf{0} \\ Q_+ &= ((Q + Q') \;{}_{P_{\text{-}+}}\boxplus\; (Q + Q')) \;{}_{P_{|\Phi^+\rangle\langle\Phi^+|}}\boxplus\; \mathbf{0} \end{aligned}$$

Where $P_{\text{-}0}$ and $P_{\text{-}+}$ are defined as $|00\rangle\langle 00| + |10\rangle\langle 10|$ and $|0+\rangle\langle 0+| + |1+\rangle\langle 1+|$ respectively. Note that $[\![P_0]\!] \overset{\boxplus}{\sim} [\![P_+]\!]$ iff they behave the same on $|\Phi^+\rangle$, and they should, because the mixed states obtained by measuring a single qbit on the computational basis, and on the Hadamard basis are the same.

Indeed $[\![P_0]\!] = [\![P_+]\!]$. Take any $|\phi\rangle$,

$$\begin{aligned} [\![P_0]\!](|\phi\rangle) &= [\![((Q + Q') \;{}_{P_{\text{-}0}}\boxplus\; (Q + Q'))]\!](|\Phi^+\rangle) \;{}_{p}\oplus\; \bar{\mathbf{0}} \\ &= ([\![Q + Q']\!](|00\rangle) \;{}_{1/2}\oplus\; [\![Q + Q']\!](|11\rangle)) \;{}_{p}\oplus\; \bar{\mathbf{0}} \\ &= (((\bar{z} + \bar{p}) \;{}_{1/2}\oplus\; (\bar{z} + \bar{m})) \;{}_{1/2}\oplus\; ((\bar{u} + \bar{p}) \;{}_{1/2}\oplus\; (\bar{u} + \bar{m}))) \;{}_{p}\oplus\; \bar{\mathbf{0}} \\ &= (((\bar{z} + \bar{p}) \;{}_{1/2}\oplus\; (\bar{u} + \bar{p})) \;{}_{1/2}\oplus\; ((\bar{z} + \bar{m}) \;{}_{1/2}\oplus\; (\bar{u} + \bar{m}))) \;{}_{p}\oplus\; \bar{\mathbf{0}} \\ &= ([\![Q + Q']\!](|{+}{+}\rangle) \;{}_{1/2}\oplus\; [\![Q + Q']\!](|{-}{-}\rangle)) \;{}_{p}\oplus\; \bar{\mathbf{0}} \\ &= [\![((Q + Q') \;{}_{P_{\text{-}+}}\boxplus\; (Q + Q'))]\!](|\Phi^+\rangle) \;{}_{p}\oplus\; \bar{\mathbf{0}} = [\![P_+]\!](|\phi\rangle). \end{aligned}$$

### 5.2.2 Alternative

We define an alternative characterization of a quantum transition system that is more in-line with preexisting quantum transition systems like [13, 10]. A quantum labeled transition system qLTS on an Hilbert space $\mathcal{H}$ is a triple $(S, Act_\tau, \hookrightarrow)$ where

- $S$ is a set of states $s, s_1, \dots$;
- $Act_\tau$ is a set of transition labels with $\tau$ a distinguished element;
- $\hookrightarrow \subseteq (\mathcal{H} \times S) \times Act_\tau \times D(\mathcal{H} \times S)$ is the transition relation.

To simplify our presentation, we reduce to $Q$ and $S$ of a specific form, namely where the branches of non-deterministic choices are always guarded by a transition, like in $(\tau.U \circ \mathbf{0}) + (\alpha.U' \circ \mathbf{0})$. Note that this is consistent with the behaviour of preexisting quantum process algebras like qCCS. We stress that a term is in this specific form by writing $\hat{Q}$ or $\hat{S}$.

We define the interpretation of a pair $(\left|\phi\right\rangle, \hat{Q})$ as a distribution as given by the function $\llparenthesis - \rrparenthesis : (\mathcal{H} \times S) \to D(\mathcal{H} \times S)$:

$$\begin{aligned}
&\llparenthesis \left|\phi\right\rangle, s \rrparenthesis = \overline{(\left|\phi\right\rangle, s)} \\
&\llparenthesis \left|\phi\right\rangle, U \circ \hat{Q} \rrparenthesis = \llparenthesis U \left|\phi\right\rangle, \hat{Q} \rrparenthesis \\
&\llparenthesis \left|\phi\right\rangle, \hat{Q}_1 \;{}_P\!\boxplus\, \hat{Q}_2 \rrparenthesis = \llparenthesis P \left|\phi\right\rangle, \hat{Q}_1 \rrparenthesis \;{}_{p(P, \left|\phi\right\rangle)}\!\oplus \llparenthesis P^\perp \left|\phi\right\rangle, \hat{Q}_2 \rrparenthesis
\end{aligned}$$

The transition relation $\hookrightarrow$ is defined as follows, with $s \overset{\mu}{\hookrightarrow} \Delta$ as notation for $(s, \mu, \Delta) \in \hookrightarrow$.

$$\frac{}{(\left|\phi\right\rangle, \mu.Q) \overset{\mu}{\hookrightarrow} \llparenthesis \left|\phi\right\rangle, Q \rrparenthesis}\ \textsc{Action}$$

$$\frac{(\left|\phi\right\rangle, Q_1) \overset{\mu}{\hookrightarrow} \Delta}{(\left|\phi\right\rangle, Q_1 + Q_2) \overset{\mu}{\hookrightarrow} \Delta}\ \textsc{Ext.L} \qquad \frac{(\left|\phi\right\rangle, Q_2) \overset{\mu}{\hookrightarrow} \Delta}{(\left|\phi\right\rangle, Q_1 + Q_2) \overset{\mu}{\hookrightarrow} \Delta}\ \textsc{Ext.R}$$

**Definition 5.2.2.** *A symmetric relation $\mathcal{R} : (\mathcal{H} \times S) \times (\mathcal{H} \times S)$ is a qLTS* bisimulation *if for each pair $(\left|\phi\right\rangle, s), (\left|\phi'\right\rangle, s)$ such that $(\left|\phi\right\rangle, s)\mathcal{R}(\left|\phi'\right\rangle, s)$, if $(\left|\phi\right\rangle, s) \xrightarrow{\mu} \Delta$ then $(\left|\phi\right\rangle', s') \xrightarrow{\mu} C'$ and $C \mathrel{\mathring{\mathcal{R}}} \Delta'$.* q-bisimilarity *$\sim_q$ is the largest qLTS bisimulation.*

# Chapter 6

# Conclusions and Future work

We have explored the main quantum process calculi proposed in the literature, focusing on the quantum-related design choices underlying them, which lead to fairly different notions of behavioural equivalence.

One of the discriminating factor between calculi, namely the visibility of qubits, stems from the intrinsic ambiguity of the proposed syntaxes, and on how it affects the modelling of real systems. We have enriched lqCCS with a linear type system, that eliminates this ambiguity. Thanks to this result, lqCCS processes are interpreted in the same way by all the considered proposed calculi, allowing us to compare the behavioural equivalences they propose. Probabilistic saturated bisimilarity has been introduced, to capture what can or cannot be distinguished by an external observer.

Another discriminating factor, i.e. how to compare quantum values, has instead proven to be a significant quantum related detail that cannot be reduced to a syntactical ambiguity, as it reflects foundational assumptions on observable properties of quantum systems. Perhaps surprisingly, the crucial detail that separates qCCS and CQP is not in how they specify quantum properties of a configuration, but in how these quantum properties are lifted to properties of probabilistic distributions. Indeed the peculiar characteristics of quantum computing allows different distributions (i.e. ensembles) to have the same observable properties (i.e. mixed states). To model these defining properties of quantum theory, we have relaxed the conditions of Larsen-Skou bisimilarity, introducing a quantum equivalence relation between distributions. Thanks to this novelty, Quantum Saturated Bisimilarity satisfies some expected properties that were absent in qCCS. For example, measurements and superoperator have different semantics, but may yield bisimilar transition systems.

We have also proposed a minimal process algebra that abstracts away from most classical details and only focus on quantum behaviour. In this simplified setting, we give an entirely new, purely quantum-based notion of semantics and bisimilarity, and we prove it behaves well in some previously discussed problematic cases.

### Future Work

Linear qCCS and probabilistic/quantum saturated bisimilarity have raised a number of interesting questions and challenges, on both practical and foundational aspects of quantum process calculus.

We only focused on strong saturated bisimilarity, while the other calculi in the literature propose also weak and branching bisimilarity. We leave the extension of our work to the non strong case as a future work. To define the needed transitive closure of the $\rightarrow$ transition relation, we could adopt the distribution transformer approach of qCCS, yielding to a Segala-style probabilistic weak saturated bisimilarity. The resulting bisimilarity could be formulated as a bisimilarity between distributions, like in [18], instead of a bisimilarity between configurations. Distribution bisimilarity will allow us to avoid basing our future extension on the supposed problematic Larsen-Skou lifting, but the tricky interaction between non-determinism and quantum probabilistic behaviour would still be relevant, and so we still expect probabilistic and quantum saturated bisimilarity not to coincide.

One disadvantage of quantum bisimilarity over probabilistic bisimilarity is that it is not an equivalence relation, as bisimulations are not closed for composition. One possible solution would be to define both the transition system and the bisimulation as relations on *equivalence classes* of distributions, just like [18] defines transitions and bisimulation between distributions. In such a system, quantum saturated bisimilarity is an equivalence relation, and it should be possible to recover the same results obtained in this thesis.

Supposing that two configurations are saturated bisimilar is a strong hypothesis, not always easy to compare with labeled bisimlarity. Actually, lots of properties descend from saturated bisimilarity, but as a drawback it is also cumbersome to prove the bisimilairty between two arbitrary configurations. One of the most successful technique to help in this task is based on the definition of an equivalent Context-LTS, a labeled transition system with contexts as labels [5]. An intricacy is that, due to the inherently stateful nature of quantum computations, there are two different ways in which a process $P$ can interact with a context $B[-]$: they can synchronize on some channel, as in a classical process algebra, or one of the two can manipulates some (possibly entangled) qubits in the shared underlying quantum state. Hence the results of [5] need to be adapted for the quantum case. In general, it would be interesting to explore which proof techniques for saturated bisimilarity would still be sound for a probabilistic quantum process calculus.

# Bibliography

[1] Roberto M. Amadio, Ilaria Castellani, and Davide Sangiorgi. “On Bisimulations for the Asynchronous $\pi$-Calculus”. In: *Theoretical Computer Science*. Concurrency Theory 195.2 (Mar. 1998), pp. 291–324. ISSN: 0304-3975. DOI: 10.1016/S0304-3975(97)00223-5.

[2] Paul Benioff. “Quantum mechanical hamiltonian models of turing machines”. en. In: *Journal of Statistical Physics* 29.3 (Nov. 1982), pp. 515–546. ISSN: 1572-9613. DOI: 10.1007/BF01342185. URL: https://doi.org/10.1007/BF01342185 (visited on 09/20/2022).

[3] J. A. Bergstra and J. W. Klop. “Algebra of Communicating Processes with Abstraction”. In: *Theoretical Computer Science* 37 (Jan. 1985), pp. 77–121. ISSN: 0304-3975. DOI: 10.1016/0304-3975(85)90088-X.

[4] Gerard Berry and Gerard Boudol. “The Chemical Abstract Machine”. In: *Proceedings of the 17th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. POPL ’90. New York, NY, USA: Association for Computing Machinery, Dec. 1989, pp. 81–94. ISBN: 978-0-89791-343-0. DOI: 10.1145/96709.96717.

[5] Filippo Bonchi, Fabio Gadducci, and Giacoma Valentina Monreale. “A General Theory of Barbs, Contexts, and Labels”. In: *ACM Transactions on Computational Logic* 15.4 (Aug. 2014), pp. 1–27. ISSN: 1529-3785, 1557-945X. DOI: 10.1145/2631916.

[6] Gérard Boudol. “Asynchrony and the Pi-calculus”. Report. INRIA, 1992, p. 15.

[7] John Clarke and Frank K. Wilhelm. “Superconducting quantum bits”. en. In: *Nature* 453.7198 (June 2008). Number: 7198 Publisher: Nature Publishing Group, pp. 1031–1042. ISSN: 1476-4687. DOI: 10.1038/nature07128. URL: https://www.nature.com/articles/nature07128 (visited on 09/22/2022).

[8] Timothy AS Davidson. “Formal Verification Techniques Using Quantum Process Calculus”. PhD thesis. University of Warwick, 2012.

[9] Yuxin Deng and Wenjie Du. *Logical, Metric, and Algorithmic Characterisations of Probabilistic Bisimulation*. Mar. 2011. arXiv: 1103.4577 [cs].

[10] Yuxin Deng and Yuan Feng. “Open Bisimulation for Quantum Processes”. In: *Theoretical Computer Science*. Ed. by Jos C. M. Baeten, Tom Ball, and Frank S. de Boer. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2012, pp. 119–133. ISBN: 978-3-642-33475-7. DOI: 10.1007/978-3-642-33475-7_9.

[11] Josée Desharnais, Abbas Edalat, and Prakash Panangaden. “Bisimulation for Labelled Markov Processes”. In: *Information and Computation* 179.2 (Dec. 2002), pp. 163–193. ISSN: 0890-5401. DOI: 10.1006/inco.2001.2962.

[12] Yuan Feng, Yuxin Deng, and Mingsheng Ying. “Symbolic Bisimulation for Quantum Processes”. In: *ACM Transactions on Computational Logic* 15.2 (May 2014), 14:1–14:32. ISSN: 1529-3785. DOI: 10.1145/2579818.

[13] Yuan Feng, Runyao Duan, and Mingsheng Ying. “Bisimulation for Quantum Processes”. In: *ACM Transactions on Programming Languages and Systems* 34.4 (Dec. 2012), 17:1–17:43. ISSN: 0164-0925. DOI: 10.1145/2400676.2400680.

[14] Yuan Feng et al. “Probabilistic Bisimulations for Quantum Processes”. In: *Information and Computation* 205.11 (Nov. 2007), pp. 1608–1639. ISSN: 08905401. DOI: 10.1016/j.ic.2007.08.001.

[15] Simon J. Gay and Rajagopal Nagarajan. “Communicating Quantum Processes”. In: *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages.* POPL ’05. New York, NY, USA: Association for Computing Machinery, Jan. 2005, pp. 145–157. ISBN: 978-1-58113-830-6. DOI: 10.1145/1040305.1040318.

[16] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. “Quantum Algorithm for Linear Systems of Equations”. In: *Physical Review Letters* 103.15 (Oct. 2009). Publisher: American Physical Society, p. 150502. DOI: 10.1103/PhysRevLett.103.150502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.103.150502 (visited on 09/20/2022).

[17] M. Hennessy and A. Ingolfsdottir. “A Theory of Communicating Processes with Value Passing”. In: *Information and Computation* 107.2 (Dec. 1993), pp. 202–236. ISSN: 0890-5401. DOI: 10.1006/inco.1993.1067.

[18] Matthew Hennessy. “Exploring Probabilistic Bisimulations, Part I”. In: *Formal Aspects of Computing* 24.4-6 (July 2012), pp. 749–768. ISSN: 0934-5043, 1433-299X. DOI: 10.1007/s00165-012-0242-7.

[19] Holger Hermanns, Jan Krčál, and Jan Křetínskỳ. “Probabilistic Bisimulation: Naturally on Distributions”. In: *International Conference on Concurrency Theory.* Springer, 2014, pp. 249–265.

[20] C. A. R. Hoare. “Communicating Sequential Processes”. In: *Communications of the ACM* 21.8 (Aug. 1978), pp. 666–677. ISSN: 0001-0782. DOI: 10.1145/359576.359585.

[21] Vijay Anand Korthikanti et al. “Reasoning about MDPs as Transformers of Probability Distributions”. In: *2010 Seventh International Conference on the Quantitative Evaluation of Systems.* IEEE, 2010, pp. 199–208.

[22] Marta Kwiatkowska, Gethin Norman, and David Parker. “PRISM 4.0: Verification of Probabilistic Real-Time Systems”. In: *Computer Aided Verification.* Ed. by Ganesh Gopalakrishnan and Shaz Qadeer. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2011, pp. 585–591. ISBN: 978-3-642-22110-1. DOI: 10.1007/978-3-642-22110-1_47.

[23] Marie Lalire. *Relations among Quantum Processes: Bisimilarity and Congruence.* Mar. 2006. arXiv: quant-ph/0603274.

[24] Marie Lalire and Philippe Jorrand. *A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics.* July 2004. arXiv: quant-ph/0407005.

[25] Kim G. Larsen and Arne Skou. “Bisimulation through Probabilistic Testing”. In: *Information and Computation* 94.1 (Sept. 1991), pp. 1–28. ISSN: 0890-5401. DOI: 10.1016/0890-5401(91)90030-6.

[26] Robin Milner. *A Calculus of Communicating Systems.* Springer, 1980.

[27] Robin Milner. “Functions as Processes”. In: *Automata, Languages and Programming*. Ed. by Michael S. Paterson. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1990, pp. 167–180. ISBN: 978-3-540-47159-2. DOI: 10.1007/BFb0032030.

[28] Robin Milner. *Communicating and Mobile Systems: The Pi Calculus*. Cambridge University Press, May 1999. ISBN: 978-0-521-65869-0.

[29] Robin Milner and Davide Sangiorgi. “Barbed Bisimulation”. In: *Automata, Languages and Programming*. Ed. by G. Goos, J. Hartmanis, and W. Kuich. Vol. 623. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 685–695. ISBN: 978-3-540-55719-7 978-3-540-47278-0. DOI: 10.1007/3-540-55719-9_114.

[30] Michael A. Nielsen and Isaac L. Chuang. “Quantum Computation and Quantum Information”. In: *Phys. Today* 54.2 (2001), p. 60.

[31] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010. ISBN: 978-1-107-00217-3.

[32] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. en. Cambridge University Press, 2010. ISBN: 978-0-511-97666-7. DOI: 10.1017/CBO9780511976667.

[33] I. Pogorelov et al. “Compact Ion-Trap Quantum Computing Demonstrator”. In: *PRX Quantum* 2.2 (June 2021). Publisher: American Physical Society, p. 020343. DOI: 10.1103/PRXQuantum.2.020343. URL: https://link.aps.org/doi/10.1103/PRXQuantum.2.020343 (visited on 09/22/2022).

[34] A. Poppe et al. “Practical Quantum Key Distribution with Polarization-Entangled Photons”. In: *Optics Express* 12.16 (2004). arXiv:quant-ph/0404115, p. 3865. ISSN: 1094-4087. DOI: 10.1364/OPEX.12.003865. URL: http://arxiv.org/abs/quant-ph/0404115 (visited on 09/17/2022).

[35] Roberto Segala and Nancy Lynch. “Probabilistic Simulations for Probabilistic Processes”. In: *CONCUR ’94: Concurrency Theory*. Ed. by Bengt Jonsson and Joachim Parrow. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1994, pp. 481–496. ISBN: 978-3-540-48654-1. DOI: 10.1007/978-3-540-48654-1_35.

[36] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. In: *Physical Review Letters* 85.2 (July 2000). Publisher: American Physical Society, pp. 441–444. DOI: 10.1103/PhysRevLett.85.441. URL: https://link.aps.org/doi/10.1103/PhysRevLett.85.441 (visited on 09/22/2022).

[37] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[38] Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. “Exact Quantum Algorithms for the Leader Election Problem”. In: *ACM Transactions on Computation Theory* 4.1 (Mar. 2012), 1:1–1:24. ISSN: 1942-3454. DOI: 10.1145/2141938.2141939. URL: https://doi.org/10.1145/2141938.2141939 (visited on 09/20/2022).

[39] Yong Wang. “Probabilistic Process Algebra to Unifying Quantum and Classical Computing in Closed Systems”. In: *International Journal of Theoretical Physics* 58.10 (Oct. 2019), pp. 3436–3509. ISSN: 0020-7748, 1572-9575. DOI: 10.1007/s10773-019-04216-2.

[40] Mingsheng Ying et al. *An Algebra of Quantum Processes*. Sept. 2010. arXiv: 0707.0330 [quant-ph].