Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-deterministic Observers

LORENZO CERAGIOLI, IMT School for Advanced Studies Lucca, Italy
FABIO GADDUCCI, University of Pisa, Italy
GIUSEPPE LOMURNO, University of Pisa, Italy
GABRIELE TEDESCHI, University of Pisa, Italy

Past years have seen the development of a few proposals for quantum extensions of process calculi. The rationale is clear: with the development of quantum communication protocols, there is a need to abstract and focus on the basic features of quantum concurrent systems, like CCS and CSP have done for their classical counterparts. So far, though, no accepted standard has emerged, neither for the syntax nor for the behavioural semantics. Indeed, the various proposals do not agree on what should be the observational properties of quantum values, and as a matter of fact, the soundness of such properties has never been validated against the prescriptions of quantum theory.

To this aim, we introduce a new calculus, Linear Quantum CCS (lqCCS), and investigate the features of behavioural equivalences based on barbs and contexts. Our calculus can be thought of as an asynchronous, linear version of qCCS, which is in turn based on value-passing CCS. The combination of linearity and asynchronous communication fits well with the properties of quantum systems (e.g. the no-cloning theorem), since it ensures that each qubit is sent exactly once, precisely specifying which qubits of a process interact with the context.

We exploit contexts to examine how bisimilarities relate to quantum theory. We show that the observational power of general contexts is incompatible with quantum theory: roughly, they can perform non-deterministic moves depending on quantum values without measuring (hence perturbing) them.

Therefore, we refine the operational semantics in order to prevent contexts from performing unfeasible non-deterministic choices. This induces a coarser bisimilarity that better fits the quantum setting: (*i*) it lifts the indistinguishability of quantum states to the distributions of processes and, despite the additional constraints, (*ii*) it preserves the expressiveness of non-deterministic choices based on classical information. To the best of our knowledge, our semantics is the first one that satisfies the two properties above.

CCS Concepts: • **Theory of computation** → **Process calculi**; **Quantum computation theory**; Probabilistic computation; • **Software and its engineering** → **Formal software verification**; • **Networks** → Protocol correctness.

Additional Key Words and Phrases: Quantum Communication, Linear Process Calculi, Behavioural Equivalence, Probabilistic Bisimulation.

ACM Reference Format:
Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024. Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-deterministic Observers. *Proc. ACM Program. Lang.* 8, POPL, Article 43 (January 2024), 29 pages. https://doi.org/10.1145/3632885

Authors' addresses: Lorenzo Ceragioli, IMT School for Advanced Studies Lucca, Italy, lorenzo.ceragioli@imtlucca.it; Fabio Gadducci, University of Pisa, Italy, fabio.gadducci@unipi.it; Giuseppe Lomurno, University of Pisa, Italy, giuseppe.lomurno@phd.unipi.it; Gabriele Tedeschi, University of Pisa, Italy, gabriele.tedeschi@phd.unipi.it.

ACM 2475-1421/2024/1-ART43
https://doi.org/10.1145/3632885

1 INTRODUCTION

Quantum computing is a promising emerging technology that exploits non-classical phenomena described by quantum mechanics, such as entanglement and superposition. The basic component of quantum algorithms and protocols is the *qubit*, a system that can be in one of two basis states $|0\rangle$ and $|1\rangle$, as well as in any linear combination of them, called a *superposition*. The state of a quantum system is modelled as a set of qubits on which the programmer applies various transformations. Differently from classical systems, the state of a composite quantum system can be *entangled*, i.e. the subsystems cannot be described separately. Moreover, reading the state of a qubit ("measuring" it, in quantum jargon), causes its state to probabilistically change to one of the basis states. Finally, the *no-cloning theorem* forbids copying qubits and thus poses serious constraints to programmers.

Both theory and implementations of quantum computing attracted considerable research efforts in the last decades, leading to quantum algorithms with more than polynomial speedup over classical counterparts [Harrow et al. 2009; Shor 1994] and quantum protocols, e.g. for key distribution [Bennet and Brassard 2014; Poppe et al. 2004] and leader election [Tani et al. 2012]. Practical applications, though, require quantum computers with large enough memories. This is a challenging task, as it is difficult to maintain quantum properties among a big number of qubits. A solution seems to lie on distributed computing, by suitably linking multiple quantum computers [Kimble 2008].

With the recent advances, the need has emerged for verification techniques applicable to quantum distributed algorithms and protocols. Concerning purely probabilistic systems, several models have been proposed so far: some only target the probabilistic behaviour, like Markov Chains [Sokolova 2011], while others also take into account pure non-determinism, like Segala Automata [Segala 1995] and Probabilistic Transition Systems [Hennessy 2012]. This second approach appears to be more adequate to model protocols where actors can perform their choices freely, and not only according to some predefined probability distribution. Process calculi and bisimilarity have been successful in modelling and verifying classical concurrent systems characterized by probabilistic and non-deterministic behaviours. We expect the same will hold in the quantum case, where different process calculi and behavioural equivalences have been proposed that display both quantum and non-deterministic features. While the features of these calculi are mostly comparable, the proposed bisimilarities greatly vary from one work to the other, and are seldom compared with each other and with quantum theory. Indeed, they turn out to disagree on several simple cases which naturally occur when modelling real-world protocols. Moreover, such discrepancies are partially due to the fact that some proposed bisimilarities do not fit what is prescribed by quantum theory. In fact, Davidson [2012] and Kubota et al. [2012] prove that processes sending indistinguishable quantum values are spuriously discriminated. This discrepancy is yet to be investigated in depth, and there are no correctness results relating bisimilarity to indistinguishability in quantum theory. We exemplify in Table 1 some cases on which the current proposals diverge, and investigate the underlying causes. The works we compare are QPAlg by Lalire [2006], CQP by Davidson [2012] and qCCS, which comes with two different bisimilarities: $\sim_p$ proposed by Deng and Feng [2012], and $\sim_d$ by Feng and Ying [2015]. For each row of the table, we discuss the prescriptions of quantum theory, reporting violations and proposing a possible solution.

In fact, to tackle these foundational issues, we introduce a new process calculus, namely *linear quantum CCS* (lqCCS), which offers the main features common to the previous proposals, and use it as a framework for exploring behavioural equivalence for quantum systems. Our calculus builds up on qCCS (in turn inspired by value-passing CCS [Hennessy 1991]), yet offers asynchronous communication and a linear type system. Quantum systems are modelled as *configurations* in a stateful manner, with the state of the qubits alongside the processes. Furthermore, the no-cloning theorem prescribes that once a qubit has been sent, the sender cannot use it any more. To comply

Table 1. Recap of the main differences between the proposed bisimilarities.

PAIR OF PROCESSES (in lqCCS syntax)	QPAlg	CQP	qCCS	lqCCS
$c?x.\mathrm{H}(x).\mathbf{0}$ **and** $c?x.\mathrm{X}(x).\mathbf{0}$	$\sim$	$\sim$	$\nsim_p$, $\nsim_d$	illegal
$c?x.\mathrm{H}(x).\mathbf{0}_x$ **and** $c?x.\mathrm{X}(x).\mathbf{0}_x$	$\sim$	$\sim$	$\sim_p$, $\sim_d$	$\sim_s$, $\sim_{cs}$
$c?x.\mathrm{H}(x).d!x$ **and** $c?x.\mathrm{X}(x).d!x$	$\nsim$	$\nsim$	$\nsim_p$, $\nsim_d$	$\nsim_s$, $\nsim_{cs}$
$\mathrm{Set}_{\frac{1}{4}I}(q_1, q_2).(c!q_1 \parallel c!q_2)$ **and** $\mathrm{Set}_{\lvert\Phi^+\rangle\langle\Phi^+\rvert}(q_1, q_2).(c!q_1 \parallel c!q_2)$	$\sim$	$\nsim$	$\nsim_p$, $\nsim_d$	$\nsim_s$, $\nsim_{cs}$
$\mathrm{Set}_{\lvert+\rangle\langle+\rvert}(q).M_{01}(q \triangleright x).c!q$ **and** $\mathrm{Set}_{\lvert0\rangle\langle0\rvert}(q).M_{\pm}(q \triangleright x).c!q$	$\nsim$	$\sim$	$\nsim_p$, $\sim_d$	$\nsim_s$, $\sim_{cs}$
$\mathrm{Set}_{\lvert+\rangle\langle+\rvert}(q).M_{01}(q \triangleright x).(c!q + d!q)$ **and** $\mathrm{Set}_{\lvert0\rangle\langle0\rvert}(q).M_{\pm}(q \triangleright x).(c!q + d!q)$	$\nsim$	$\sim$	$\nsim_p$, $\sim_d$	$\nsim_s$, $\nsim_{cs}$

with this requirement, quantum process calculi usually enforce *affinity*, guaranteeing that each qubit is sent at most once. We go one step further by requiring each qubit to be sent or discarded (i.e. sent on a restricted channel) *exactly* once, thus forcing the observability of each qubit to be clearly defined. This allows us to resolve a superficial discrepancy of the proposed behavioural equivalences, focusing on unambiguous cases only. Take as example the pair of processes of the first row of Table 1. Both receive a qubit on channel c (with $c?x$), modify it (with either $H(x)$ or $X(x)$), and then terminate ($\mathbf{0}$). The two processes apply different transformations, resulting in different quantum states. Both CQP and QPAlg assume unsent qubits are not visible and deem P and Q bisimilar, while the bisimilarities for qCCS do the opposite. The linear typing of lqCCS forces to specify visibility, and allows matching these different results employing an appropriate discarding discipline (i.e. the processes are equivalent if the qubit is discarded using $\mathbf{0}_x$ as in the second row of Table 1, they are distinguishable if it is sent on a visible channel as in the third row).

We define a saturated probabilistic bisimilarity for lqCCS, denoted as $\sim_s$, which relies on contexts for distinguishing quantum processes [Bonchi et al. 2014]. This seems a fruitful choice, because the notion of observable property of a visible quantum value is not straightforward, as witnessed by the variety of labelled bisimulations proposed so far. On the contrary, available operations over quantum values are well known (unitaries and measurements), and thus contexts are easily defined and uniquely determined (at least as far as quantum properties are concerned). Take the fourth row of Table 1 as an example, where both processes prepare and send a pair of qubits, but only the latter is entangled. Remarkably, in both cases, the sent qubits are in the same state when taken separately. QPAlg uses the value of each sent qubit as labels, thus incorrectly equating the two processes. Indeed, detecting the entanglement requires considering the pair of qubits as a whole.

We also suffer from the problem highlighted by Davidson and Kubota et al., as our saturated bisimilarity spuriously discriminates between equivalent quantum values. More in detail, quantum theory prescribes that certain probability distributions of quantum states should be indistinguishable (namely if they are represented by the same density operator). Consider the processes of the fifth row of Table 1. After setting and measuring the qubits, the state of the sent qubit of both processes is in a fair distribution, respectively of $|0\rangle$ and $|1\rangle$, and of $|+\rangle$ and $|-\rangle$. Such distributions are prescribed to be indistinguishable. Nonetheless, the two processes are not bisimilar according to QPAlg and $\sim_p$ of qCCS. Also $\sim_s$ suffers from the same issue, but the use of contexts allow us to precisely pinpoint the cause of the problem in the interaction between non-determinism and quantum features. Indeed, unconstrained non-determinism allows contexts to choose a move based on the (in principle unknown) current quantum state, without performing a measurement (and thus, without perturbing the state, violating a defining feature of quantum objects). Non-determinism must be constrained for contexts to fit the limitations of quantum theory.

We give a new enhanced semantics and proper contexts, forbidding ill-formed moves where the non-deterministic choices depend on unknown quantum values. Moreover, we define *constrained* saturated bisimilarity, denoted as $\sim_{cs}$, which is strictly coarser than $\sim_s$. We prove two main properties: $\sim_{cs}$ recovers the indistinguishability of quantum values prescribed by quantum theory, and, even if constrained, non-deterministic sum can still simulate boolean conditional statements. Theorem 4.8 shows that our constraints suffice to equate lqCCS configurations with indistinguishable quantum states. Notice indeed that the processes of the fifth row of Table 1 are correctly deemed bisimilar by $\sim_{cs}$. We argue that our constraints are not overly restrictive. To confirm this, Theorem 4.12 shows that non-deterministic choices can always perform different moves according to known classical values, thus replicating the behaviour of boolean guards. This is an expected property that was missing in previous bisimilarities like the one of CQP and $\sim_d$ of qCCS, which also indirectly constrain non-determinism. Consider the last row of Table 1 where both processes send a qubit, choosing non-deterministically over two possible channels. Remarkably, for each channel, the state of the sent qubits is represented by the same density operator, but the two processes could be distinguished if they had chosen the channel according to the outcome of the measurement (e.g. by using a boolean guard). Since non-deterministic sum simulates such behaviour in our enhanced semantics, the two processes are correctly distinguished. On the contrary, all the previous works that correctly equates the processes of the fifth row of the table fails in distinguishing the ones in the last row: indeed, they overly constrain non-determinism.

As a final contribution, we provide a few proof techniques and employ them to analyse three real-world protocols: quantum teleportation, super-dense coding and quantum coin-flipping.

Synopsis. In section 2 we give some background about probability distributions and quantum theory. In section 3 we present lqCCS, we discuss probabilistic bisimilarity and its interaction with non-determinism. In section 4 we propose our novel semantics and bisimilarity equivalence. In section 5 we describe the capabilities of the novel bisimilarity through the lenses of well-known quantum protocols. Finally, we compare with related works in section 6, and we conclude in section 7. For the full proofs we refer to the extended version [Ceragioli et al. 2023].

2 BACKGROUND

We recall some background on probability distributions and introduce quantum computing. Finally, we present density operators that model probability distributions of quantum systems and their evolution. We refer to Nielsen and Chuang [2010] for further reading on quantum computing.

2.1 Probability Distributions

A *probability distribution* over a set S is a function $\Delta : S \longrightarrow [0,1]$ such that $\sum_{s \in S} \Delta(s) = 1$. We call the *support* of a distribution Δ, written $\lceil \Delta \rceil$, the set $\{s \in S \mid \Delta(s) > 0\}$. We write $\mathcal{D}(S)$ for the set of distributions over S, and restrict ourselves to distributions with finite support.

For each $s \in S$, we let $\overline{s}$ be the *point distribution* that assigns 1 to s. Given a finite set of non-negatives reals $\{p_i\}_{i \in I}$ such that $\sum_{i \in I} p_i = 1$, we write $\sum_{i \in I} p_i \bullet \Delta_i$ for the distribution determined by $(\sum_{i \in I} p_i \bullet \Delta_i)(s) = \sum_{i \in I} p_i \Delta_i(s)$. Sometimes, we will use the notation above to write the distributions "explicitly" by listing the elements of the support with their probability as in $\Delta = \sum_{s \in \lceil S \rceil} p_s \bullet \overline{s}$. Finally, the notation $\Delta_1 \ {}_p\!\oplus \Delta_2$ is a shorthand for $p \bullet \Delta_1 + (1-p) \bullet \Delta_2$.

A relation $\mathcal{R} \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$ is said to be *linear* if $(\Delta_1 \ {}_p\!\oplus \Delta_2) \ \mathcal{R} \ (\Theta_1 \ {}_p\!\oplus \Theta_2)$ for any $p \in [0,1]$ whenever $\Delta_i \ \mathcal{R} \ \Theta_i$ for $i = 1, 2$. $\mathcal{R}$ is said to be *left-decomposable* if $(\Delta_1 \ {}_p\!\oplus \Delta_2) \ \mathcal{R} \ \Theta$ implies $\Theta = (\Theta_1 \ {}_p\!\oplus \Theta_2)$ for some Θ_1, Θ_2 with $\Delta_i \ \mathcal{R} \ \Theta_i$ for $i = 1, 2$ and for any $p \in [0,1]$. Right-decomposability is defined symmetrically, and a relation is *decomposable* when it is both left- and right-decomposable.

Given $\mathcal{R} \subseteq S \times \mathcal{D}(S)$, its *lifting* $\text{lift}(\mathcal{R}) \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$ is the smallest linear relation such that $\overline{s}\ \text{lift}(\mathcal{R})\ \Theta$ when $s\ \mathcal{R}\ \Theta$.

2.2 State Space

A (finite-dimensional) *Hilbert space*, denoted as $\mathcal{H}$, is a complex vector space equipped with a binary operator $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ called *inner product*, defined as $\langle \psi | \phi \rangle = \sum_i \alpha_i^* \beta_i$, where $|\psi\rangle = (\alpha_1, \dots, \alpha_i)^T$ and $|\phi\rangle = (\beta_1, \dots, \beta_i)^T$. We indicate column vectors as $|\psi\rangle$ and their conjugate transpose as $\langle\psi| = |\psi\rangle^\dagger$. The state of an isolated physical system is represented as a *unit vector* $|\psi\rangle$ (called *state vector*), i.e. a vector such that $\langle\psi|\psi\rangle = 1$. The simplest example of a quantum physical system is a *qubit*, which is associated with the two-dimensional Hilbert Space $\widehat{\mathcal{H}} = \mathbb{C}^2$. The vectors $\{|0\rangle = (1,0)^T, |1\rangle = (0,1)^T\}$ form an orthonormal basis of $\widehat{\mathcal{H}}$, called the *computational basis*. Other important vectors in $\widehat{\mathcal{H}}$ are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which form the *diagonal basis*, or Hadamard basis.

Intuitively, different bases represent different observable properties of a quantum system. Note that $|+\rangle$ and $|-\rangle$ are non-trivial linear combinations of $|0\rangle$ and $|1\rangle$, roughly meaning that the property associated with the computational basis is undetermined in $|+\rangle$ and $|-\rangle$. In the quantum jargon, the states in the diagonal basis are *superpositions* with respect to the standard basis. Symmetrically, $|0\rangle$ and $|1\rangle$ are themselves superpositions with respect to the diagonal basis.

2.3 Unitary Transformations

For each linear operator A on a Hilbert space $\mathcal{H}$, there is a linear operator $A^\dagger$, the *adjoint* of A, which is given by the conjugate transpose of A and is the unique operator such that $\langle\psi|A|\phi\rangle = \langle A^\dagger\psi|\phi\rangle$. A linear operator U is said to be *unitary* when $UU^\dagger = U^\dagger U = I$. In quantum physics, the evolution of a closed system is described by a unitary transformation: the state $|\psi\rangle$ at time t_0 is related to $|\psi'\rangle$ at time t_1 by a unitary operator U, which only depends on t_0 and t_1, i.e. $|\psi'\rangle = U|\psi\rangle$.

In quantum computing, the programmer manipulates the state of qubits by applying unitary transformations. Some of the most common transformations on single qubits are: X that transforms the qubit $|0\rangle$ into $|1\rangle$ and vice-versa (corresponding to the classical logical not); Z that given $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ returns $\alpha|0\rangle - \beta|1\rangle$; and H that maps $|0\rangle$ and $|1\rangle$ into $|+\rangle$ and $|-\rangle$ respectively.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

2.4 Measurement

Quantum measurements are needed for describing systems that exchange information with the environment. Performing a measurement on a quantum state returns a classical result and causes the quantum state to change (i.e. to *decay*). Thus, measurements alter the state of the qubits. Moreover, the result of a measurement is intrinsically probabilistic.

A *measurement operator* is a linear transformation that associates each input quantum state with a probability and a resulting quantum state. A *measurement* is then a set of possible classical outcomes: each of them is associated with a *measurement operator* that encodes how the probability of the outcome and the resulting quantum state depends on the current state $|\psi\rangle$.

Formally, a measurement is a set $\{M_m\}_m$ of measurement operators, where m refers to the classical outcomes, such that the *completeness* equation $\sum_m M_m^\dagger M_m = I$ holds. If the state of the system is $|\psi\rangle$ before the measurement, then the probability of m occurring is $p_m = \langle\psi| M_m^\dagger M_m |\psi\rangle$. If m is the outcome, then the state after the measurement will be $\frac{1}{\sqrt{p_m}} M_m |\psi\rangle$.

The simplest measurements project a state into one of the basis of $\mathcal{H}$, e.g. $M_{01} = \{M_0, M_1\}$ with $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$ in the computational basis of $\widehat{\mathcal{H}}$, and $M_\pm = \{M_+, M_-\}$ with $M_+ = |+\rangle\langle +|, M_- = |-\rangle\langle -|$ in the Hadamard basis.

As expected, applying the measurement M_{01} on $|0\rangle$ returns the classical outcome 0 and the state $|0\rangle$ with probability 1. When applying the same measurement on $|+\rangle$, instead, the result may be 0 and $|0\rangle$, or 1 and $|1\rangle$ with equal probability. Note also that measuring $|0\rangle$ with $M_\pm$ leads to either 0 and $|+\rangle$, or 1 and $|-\rangle$, also with equal probability.

2.5 Composite Quantum Systems

We represent the state space of a composite physical system as the *tensor product* of the state spaces of its components. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be n and m-dimensional Hilbert spaces: their tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ is an $n \cdot m$ Hilbert space. Moreover, if $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ and $\{|\phi_1\rangle, \dots, |\phi_m\rangle\}$ are bases of respectively $\mathcal{H}_A$ and $\mathcal{H}_B$, then $\{|\psi_i\rangle \otimes |\phi_j\rangle \mid i = 1, \dots, n, j = 1, \dots, m\}$ is a basis of $\mathcal{H}_A \otimes \mathcal{H}_B$, where $|\psi\rangle \otimes |\phi\rangle$ is the Kronecker product, defined as

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{m,n} \end{bmatrix} \otimes A = \begin{bmatrix} x_{1,1}A & \cdots & x_{1,n}A \\ \vdots & \ddots & \vdots \\ x_{m,1}A & \cdots & x_{m,n}A \end{bmatrix}$$

We often omit the tensor product and write $|\psi\rangle\,|\phi\rangle$ or $|\psi\phi\rangle$. We write $\widehat{\mathcal{H}}^{\otimes n}$ for the 2^n-dimensional Hilbert space defined as the tensor product of n copies of $\widehat{\mathcal{H}}$ (i.e. the possible states of n qubits).

What is said above about unitary transformations and measurements also applies to composite systems. Given a list of single-qubits unitaries $U_1, U_2 \dots U_n$, their tensor product $U_1 \otimes U_2 \cdots \otimes U_n$ is a unitary transformation over n qubits. Not all unitaries on n qubits can be obtained in this way: the most used that cannot be obtained via tensor product are the SWAP operator exchanging the state of two qubits, i.e. SWAP $|\psi\phi\rangle = |\phi\psi\rangle$, and the controlled not (CNOT) over two qubits, defined as

$$\text{CNOT}\,|00\rangle = |00\rangle, \quad \text{CNOT}\,|01\rangle = |01\rangle, \quad \text{CNOT}\,|10\rangle = |11\rangle, \quad \text{CNOT}\,|11\rangle = |10\rangle.$$

A measurement for a composite system may measure only some of the qubits and leave others unaltered, e.g. $\{M_0 \otimes I, M_1 \otimes I\}$ measures (in the computational basis) the first qubit of a pair.

A quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is *separable* when it can be expressed as the Kronecker product of two vectors of $\mathcal{H}_A$ and $\mathcal{H}_B$. Otherwise, it is *entangled*, like the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. When two qubits are entangled, the evolution of the one depends on the transformations applied to the other. Measuring e.g. the first qubit of $|\Phi^+\rangle$ in the computational basis causes the state to decay into either $|00\rangle$ or $|11\rangle$ with equal probability, where also the state of the second qubit is updated.

The Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ form the Bell basis for $\widehat{\mathcal{H}}^{\otimes 2}$, with

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

A defining feature of quantum computing is that qubits cannot be duplicated.

Proposition 2.1 (No-Cloning Theorem). *There is no unitary operation U on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ for all states $|\psi\rangle \in \mathcal{H}_A$ and $|\phi\rangle \in \mathcal{H}_B$.*

As a result, qubits cannot be stored in multiple locations or broadcast to multiple receivers.

2.6 Density Operator Formalism

The density operator formalism puts together quantum systems and probability distributions by considering mixed states, i.e. *probabilistic mixture of quantum states.* A point distribution $\overline{|\psi\rangle}$ (called a pure state) is represented by the matrix $|\psi\rangle\!\langle\psi|$. In general, a mixed state $\Delta \in \mathcal{D}(\widehat{\mathcal{H}}^{\otimes n})$ for n qubits is represented as the matrix $\rho \in \mathbb{C}^{2^n \times 2^n}$, known as its *density operator*, with $\rho = \sum_i \Delta(\psi_i)\, |\psi_i\rangle\!\langle\psi_i|$. We write $\mathcal{DO}(\mathcal{H})$ for the set of density operators of $\mathcal{H}$.

For example, the mixed state $\overline{|0\rangle}\ {}_{1/3}\!\oplus \overline{|+\rangle}$ being $|0\rangle$ with probability $1/3$ and in $|+\rangle$ with probability $2/3$ is represented as

$$\frac{1}{3}\,|0\rangle\!\langle 0| + \frac{2}{3}\,|+\rangle\!\langle +| = \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Note that the encoding of probabilistic mixtures of quantum states as density operators is not injective. For example, $\frac{1}{2}I$ is called the *maximally mixed state* and represents both the distribution $\Delta_C = \overline{|0\rangle}\ {}_{1/2}\!\oplus \overline{|1\rangle}$ and $\Delta_H = \overline{|+\rangle}\ {}_{1/2}\!\oplus \overline{|-\rangle}$. This is a desired feature, as the laws of quantum mechanics deem indistinguishable all the distributions that result in the same density operator.

The evolution of mixed states is given as a *trace-preserving superoperator* $\mathcal{E} : \mathcal{DO}(\mathcal{H}) \to \mathcal{DO}(\mathcal{H})$, a function defined by its *Kraus operator sum decomposition* $\{E_i\}_i$ for $i = 1, \dots, \dim(\mathcal{H})^2$, satisfying that $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ and $\sum_i E_i^\dagger E_i = I_{\mathcal{H}}$, where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$. Notice that the operators E_i are not unitaries in general, see Nielsen and Chuang [2010, Section 8.2.3]. We write $\mathcal{TS}(\mathcal{H})$ for the set of trace-preserving superoperators on $\mathcal{H}$.

The tensor product of density operators $\rho \otimes \sigma$ is defined as their Kronecker product, and of superoperators $\mathcal{E} \otimes \mathcal{F}$ as the superoperator having Kraus decomposition $\{E_i \otimes F_j\}_{i,j}$ with $\{E_i\}_i$ and $\{F_j\}_j$ Kraus decompositions of $\mathcal{E}$ and $\mathcal{F}$. Superoperators represent unitary transformations U as $\mathcal{E}_U$ with $\{U\}$ its Kraus decomposition. Other transformations are possible, like the constant Set_ρ superoperators, transforming any input state in the given state ρ; and the probabilistic combination of unitaries having Kraus decomposition $\{\sqrt{p_i}U_i\}_i$ with $\sum_i p_i = 1$ and U_i a unitary transformation (each U_i is applied with a given probability, which is useful for modelling noisy channels and gates).

Density operators can be used to describe the state of a subsystem of a composite quantum system. Let $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ represents a composite system, with subsystems A and B. Given a (not necessarily separable) $\rho^{AB} \in \mathcal{H}_{AB}$, the *reduced density operator* of system A, $\rho^A = \mathrm{tr}_B(\rho^{AB})$, describes the state of the subsystem A, with tr_B the *partial trace over* B, defined as the linear transformation such that $\mathrm{tr}_B(|\psi\rangle\!\langle\psi'| \otimes |\phi\rangle\!\langle\phi'|) = |\psi\rangle\!\langle\psi'|\,\mathrm{tr}(|\phi\rangle\!\langle\phi'|)$. When applied to pure separable states, the partial trace returns the actual state of the subsystem. When applied to an entangled state, instead, it produces a probability distribution of states, because "forgetting" the information on the subsystem B leaves us with only partial information on subsystem A. As an example, the partial trace over the first qubit of $\rho = |\Phi^+\rangle\!\langle\Phi^+|$ is the maximally mixed state.

3 A LINEAR PROCESS ALGEBRA

In the following sections we describe the syntax and the type system of lqCCS processes, as well as a reduction-style semantics and a first notion of bisimilarity. Our process calculus is enriched with a linear type system both for reflecting the no-cloning theorem (see Proposition 2.1) and for resolving the minor discrepancy on qubit visibility summarized in the first three rows of Table 1.

3.1 Syntax and Type System

The syntax of lqCCS is defined as follows

$$\begin{aligned} P &::= K \mid P \parallel P \mid P \setminus c \mid \textbf{if } e \textbf{ then } P \textbf{ else } P \\ K &::= \mathbf{0}_{\tilde{e}} \mid \tau.P \mid \mathcal{E}(\tilde{e}).P \mid M(\tilde{e} \rhd x).P \mid c?x.P \mid c!e \mid K + K \\ e &::= x \mid b \mid n \mid q \mid \neg e \mid e \vee e \mid e \leq e \end{aligned}$$

where $b \in \mathbb{B}$, $n \in \mathbb{N}$, $q \in \mathcal{Q}$, $x \in \mathrm{Var}$, $c \in \mathrm{Chan}$ with $\mathcal{Q}$, Var, Chan denumerable sets of respectively qubit names, variables and channels, each typed. We use $\tilde{e}$ to denote a (possibly empty) tuple

$$\frac{\tilde{e} \in \tilde{\Sigma}}{\Sigma \vdash \mathbf{0}_{\tilde{e}}}\ \textsc{Nil} \qquad \frac{\Sigma \vdash P}{\Sigma \vdash \tau.P}\ \textsc{Tau} \qquad \frac{M : \mathrm{Meas}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad y : \mathbb{N} \quad \Sigma \vdash P}{\Sigma \vdash M(\tilde{e} \triangleright y).P}\ \textsc{QMeas}$$

$$\frac{\Sigma \vdash P}{\Sigma \vdash P \setminus c}\ \textsc{Restrict} \qquad \frac{\Sigma \vdash P \quad \Sigma \vdash Q}{\Sigma \vdash P + Q}\ \textsc{Sum} \qquad \frac{\mathcal{E} : \mathrm{Op}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad \Sigma \vdash P}{\Sigma \vdash \mathcal{E}(\tilde{e}).P}\ \textsc{QOp}$$

$$\frac{c : \widehat{T} \quad x : T \in \{\mathbb{B}, \mathbb{N}\} \quad \Sigma \vdash P}{\Sigma \vdash c?x.P}\ \textsc{CRecv} \qquad \frac{c : \widehat{\mathcal{Q}} \quad x : \mathcal{Q} \quad \Sigma \cup \{x\} \vdash P}{\Sigma \vdash c?x.P}\ \textsc{QRecv} \qquad \frac{c : \widehat{\mathcal{Q}} \quad e : \mathcal{Q}}{\{e\} \vdash c!e}\ \textsc{QSend}$$

$$\frac{c : \widehat{T} \quad e : T \in \{\mathbb{B}, \mathbb{N}\}}{\emptyset \vdash c!e}\ \textsc{CSend} \qquad \frac{e : \mathbb{B} \quad \Sigma \vdash P_1 \quad \Sigma \vdash P_2}{\Sigma \vdash \mathbf{if}\ e\ \mathbf{then}\ P_1\ \mathbf{else}\ P_2}\ \textsc{ITE} \qquad \frac{\Sigma_1 \cap \Sigma_2 = \emptyset \quad \Sigma_1 \vdash P_1 \quad \Sigma_2 \vdash P_2}{\Sigma_1 \cup \Sigma_2 \vdash P_1 \parallel P_2}\ \textsc{Par}$$

Fig. 1. Typing rules for lqCCS

$e_1, \dots, e_n$ of expressions. The process $\mathbf{0}_{\tilde{e}}$ *discards* the qubits in $\tilde{e}$. It behaves as a deadlock process that maintains ownership of the qubits in $\tilde{e}$ and makes them inaccessible to other processes. As we will see, discard processes are semantically equivalent to any deadlock process using the same qubits. The process $\mathbf{0}_{q_1,q_2}$ is e.g. equivalent to $\mathbf{0}_{q_2,q_1}$ and to $c?x.(c!q_1 \parallel c!q_2 \parallel c!x) \setminus c$, since q_1 and q_2 will never be available. When $\tilde{e}$ is the empty sequence, we simply write $\mathbf{0}$ to stress the equivalence with the nil process of standard CCS. This feature of lqCCS allows to clearly mark which qubits are hidden to the environment, thus relieving bisimilar processes to agree on them. Note that "discard-like" processes can be written also in qCCS, but are never used in the literature. A symbol $\mathcal{E}$ denotes a trace-preserving superoperator on $\widehat{\mathcal{H}}^{\otimes n}$ for some $n > 0$, and we write $\mathcal{E} : \mathrm{Op}(n)$ to indicate that $\mathcal{E}$ is a superoperator with arity n. A symbol M denotes a measurement $\{M_0, \dots, M_{k-1}\}$ with such operators acting on n qubits and with k different outcomes: we write $M : \mathrm{Meas}(n)$ to indicate that M is a measurement operator with arity n, and denote as $|M|$ the cardinality k of M. We let M_{01} and $M_{\pm}$ be the projective measurement over the computational and Hadamard basis respectively. We say that the channel name c is *bound* in $P \setminus c$ and *free* otherwise. We denote with $\mathrm{fc}(P)$ the set of free channels and with $\mathrm{fv}(P)$ the set of free classical variables of P, defined as usual.

Affinity is often enforced in quantum process calculi for preventing qubits from being broadcast, which is forbidden by the no-cloning theorem. We decided to go one step further and to impose a linear type system, which forces the processes to either send or explicitly discard each qubit that they own. Therefore, the visibility of qubits is explicitly stated, relieving us from performing an arbitrary choice about the visibility of those qubits that are neither sent nor discarded.

Typing judgments are of the form $\Sigma \vdash P$. The use of quantum names is subject to linearity and those in use are collected in $\Sigma \subseteq \mathcal{Q}$. The set of types is $\{\mathcal{Q}, \mathbb{N}, \mathbb{B}\}$, respectively the type of quantum names, naturals and booleans. The set of channel types is $\{\widehat{\mathcal{Q}}, \widehat{\mathbb{N}}, \widehat{\mathbb{B}}\}$. From now on we will assume that channels and variables are typed, and expressions involving natural and booleans are typed as standard. The typing system is in Figure 1, where for a set A we use $\tilde{A}$ to denote the set of tuples $\tilde{a}$ such that any element of A occurs exactly once in $\tilde{a}$. Linearity is enforced by the combination of rules Nil, QSend and Par. In particular, the former two are the only rules that introduce new qubits into the quantum context, therefore each quantum name must be sent along some channel or discarded; while the latter ensures that each qubit is not shared between parallel processes.

It is easy to show that the typing of processes is unique, therefore in the following we will simply write Σ_P for the unique set of quantum names such that $\Sigma_P \vdash P$.

Proposition 3.1 (Unique Type). *If $\Sigma \vdash P$ and $\Sigma' \vdash P$ then $\Sigma = \Sigma'$.*

Proof sketch. By induction on the derivations of $\Sigma \vdash P$ and $\Sigma' \vdash P$. □

$$\frac{}{P \parallel \mathbf{0} \equiv P}\ \textsc{SCParNil} \qquad \frac{}{P \parallel Q \equiv Q \parallel P}\ \textsc{SCParComm} \qquad \frac{}{P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R}\ \textsc{SCParAssoc}$$

$$\frac{}{P + \mathbf{0}_{\tilde{e}} \equiv P}\ \textsc{SCSumNil} \qquad \frac{}{P + Q \equiv Q + P}\ \textsc{SCSumComm} \qquad \frac{}{P + (Q + R) \equiv (P + Q) + R}\ \textsc{SCSumAssoc}$$

$$\frac{}{\mathbf{if}\ f\!f\ \mathbf{then}\ P\ \mathbf{else}\ Q \equiv Q}\ \textsc{SCIteF} \qquad \frac{}{\mathbf{if}\ tt\ \mathbf{then}\ P\ \mathbf{else}\ Q \equiv P}\ \textsc{SCIteT} \qquad \frac{e \Downarrow v}{P \equiv P[{}^{v}/_{e}]}\ \textsc{SCValExpr}$$

$$\frac{}{\mathbf{0}_{\tilde{e}} \setminus c \equiv \mathbf{0}_{\tilde{e}}}\ \textsc{SCRestrNil} \qquad \frac{}{P \setminus c \setminus d \equiv P \setminus d \setminus c}\ \textsc{SCRestrOrd} \qquad \frac{c \notin \mathrm{fc}(P)}{(P \parallel Q) \setminus c \equiv P \parallel (Q \setminus c)}\ \textsc{SCRestrPar}$$

Fig. 2. Structural congruence

As a simple example of lqCCS, we present the following quantum lottery protocol **QL**, which uses a qubit to randomly select a winner between two competitors.

Example 3.2. Let $\mathbf{QL} = H(q).M_{01}(q \triangleright x).((\mathbf{if}\ x = 0\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1) \parallel \mathbf{0}_q)$. The qubit q is firstly transformed with H and then measured in the computational basis. Depending on the outcome, stored in x, either Alice or Bob is announced as the winner (through $a!1$ and $b!1$ respectively). Finally, the qubit is discarded as it is no longer needed. The unique typing of **QL** is given by $\{q\} \vdash \mathbf{QL}$, with $a : \widehat{\mathbb{N}}$, $b : \widehat{\mathbb{N}}$, $x : \mathbb{N}$, and $q : \mathcal{Q}$.

3.2 Operational Semantics

The operational semantics of lqCCS is defined as a probabilistic reduction system $(\mathit{Conf}_\perp, \to)$ over closed processes (i.e., processes P such that $\mathrm{fv}(P) = \emptyset$), where

- $\mathit{Conf}_\perp$ is $\mathit{Conf} \cup \{\perp\}$, with Conf the set of configurations of the form $\langle \rho, P \rangle$, and $\perp$ the "deadlock" configuration that always evolves in $\overline{\perp}$;
- $\to \subseteq \mathit{Conf}_\perp \times \mathcal{D}(\mathit{Conf}_\perp)$ is the probabilistic transition relation.

Given a set $\Sigma = \{q_1, \ldots, q_n\} \subseteq \mathcal{Q}$, a global quantum state ρ is a density operator over $\mathcal{H}_\Sigma = \widehat{\mathcal{H}}^{\otimes n}$, where q_i refers to the i-th qubit in ρ. Expressions e are evaluated through a big step semantics $e \Downarrow v$ with v a value, i.e. either $n \in \mathbb{N}$, $b \in \mathbb{B}$, or $x \in \mathrm{Var}$. We restrict ourselves to standard boolean and arithmetic operations, and therefore omit the rules and assume free variables are not evaluated.

The type system is extended to configurations by considering the qubits of the underlying quantum state. In the following, we denote as Σ_ρ the set of qubits appearing in ρ.

Definition 3.3. Let $\langle \rho, P \rangle \in \mathit{Conf}$ and $\Delta \in \mathcal{D}(\mathit{Conf}_\perp)$. We let $(\Sigma_\rho, \Sigma_P) \vdash \langle \rho, P \rangle$ if $\Sigma_P \subseteq \Sigma_\rho$. We let $(\Sigma, \Sigma') \vdash \perp$ for any Σ and Σ', and $(\Sigma, \Sigma') \vdash \Delta$ if $(\Sigma, \Sigma') \vdash C$ for any C in $\lceil \Delta \rceil$.

Hereafter, we restrict ourselves to well-typed distributions. We extend the standard structural congruence relation for CCS [Milner 1992] as presented in Figure 2, and we impose congruent processes to be typed by the same Σ. The new rules allow the evaluation of expressions and reduction of $\mathbf{if} \cdot \mathbf{then} \cdot \mathbf{else} \cdot$ occurrences. We lift the congruence to distributions of configurations by linearity and imposing $\overline{\perp} \equiv \overline{\perp}$ and $\overline{\langle \rho, P \rangle} \equiv \overline{\langle \rho, P' \rangle}$ whenever $P \equiv P'$.

The transition relation $\to$ is the smallest relation that satisfies the rules in Figure 3, augmented with $C \to \overline{\perp}$ if there is no Δ such that $C \to \Delta$ [Deng 2018]. We have the standard rules for CCS operators, so for example a process $\tau.P$ performs a silent action that does not affect the quantum state, and then continues its evolution as P, while $P \setminus c$ behaves as P but the channel c is *restricted*, i.e. P cannot synchronize with other processes on that channel. Along them we introduce rules for superoperators and measurements. Since the arity of $\mathcal{E}$ can be smaller than the number of qubits in the quantum state ρ, we define $\mathcal{E}_{\tilde{q}}$ as the superoperator obtained by composing (i) a suitable set of SWAP unitaries to bring the qubits $\tilde{q}$ in the first positions; (ii) the tensor product

$$\frac{}{\langle \rho, \tau.P + Q\rangle \longrightarrow \overline{\langle \rho, P\rangle}}\ \textsc{Tau} \qquad \frac{\langle \rho, P\rangle \longrightarrow \Delta}{\langle \rho, P \setminus c\rangle \longrightarrow \Delta \setminus c}\ \textsc{Restrict} \qquad \frac{}{\langle \rho, \mathcal{E}(\tilde{q}).P + Q\rangle \longrightarrow \overline{\langle \mathcal{E}_{\tilde{q}}(\rho), P\rangle}}\ \textsc{QOp}$$

$$\frac{\rho_m = (M_m)_{\tilde{q}}(\rho) \quad p_m = \mathrm{tr}(\rho_m)}{\langle \rho, M(\tilde{q} \rhd y).P + Q\rangle \longrightarrow \sum_{m=0}^{|M|-1} p_m \bullet \overline{\langle \frac{\rho_m}{p_m}, P[{}^{m}\!/\!{}_{y}]\rangle}}\ \textsc{QMeas} \qquad \frac{\langle \rho, P\rangle \longrightarrow \Delta}{\langle \rho, P \parallel Q\rangle \longrightarrow \Delta \parallel Q}\ \textsc{Par}$$

$$\frac{}{\langle \rho, (c!v + R) \parallel ((c?x.P) + Q)\rangle \longrightarrow \overline{\langle \rho, P[{}^{v}\!/\!{}_{x}]\rangle}}\ \textsc{Reduce} \qquad \frac{P \equiv Q \quad \langle \rho, Q\rangle \longrightarrow \Delta \quad \Delta \equiv \Delta'}{\langle \rho, P\rangle \longrightarrow \Delta'}\ \textsc{Congr}$$

Fig. 3. lqCCS Semantics

of the superoperator $\mathcal{E}$ with the identity on untouched qubits on the right; and (iii) the inverse of the SWAP operators of point (i) to recover the original order of qubits [Lalire 2006]. The same mechanism is applied to measurements to obtain $(M_m)_{\tilde{q}}$ from M_m. If $\Delta = \sum_i p_i \bullet \overline{\langle \rho_i, P_i\rangle}$, we let $\Delta \setminus c$ and $\Delta \parallel Q$ denote distributions $\sum_i p_i \bullet \overline{\langle \rho_i, P_i \setminus c\rangle}$ and $\sum_i p_i \bullet \overline{\langle \rho_i, P_i \parallel Q\rangle}$. In the following, we lift $\longrightarrow$ to distributions, writing $\longrightarrow$ for $\mathrm{lift}(\longrightarrow) \in \mathcal{D}(\mathit{Conf}_\bot) \times \mathcal{D}(\mathit{Conf}_\bot)$.

Noteworthy, the typing is preserved by the transition relation.

Theorem 3.4 (Typing Preservation). *If* $(\Sigma_\rho, \Sigma_P) \vdash \langle \rho, P\rangle$ *and* $\langle \rho, P\rangle \longrightarrow \Delta$ *then* $(\Sigma_\rho, \Sigma_P) \vdash \Delta$.

Proof sketch. By induction on the derivation of $\langle \rho, P\rangle \longrightarrow \Delta$. The only interesting case is for Reduce, for which we prove that substitution works if the new name is not in the typing context of the process, i.e. that if $\Sigma \cup \{x\} \vdash P$ and $v \notin \Sigma$ then $\Sigma \cup \{v\} \vdash P[{}^{v}\!/\!{}_{x}]$. Then it suffices to note that $v \notin \Sigma$ is guaranteed by the typing of parallel processes. Note also that Σ_ρ is not impacted by any rule, therefore it is trivially preserved. □

Example 3.5. The semantics of **QL** from Example 3.2 on quantum state $|0\rangle\langle 0|$ is as follows

$$\begin{aligned}
&\overline{\langle |0\rangle\langle 0|, \mathbf{QL}\rangle} \to \overline{\langle\, |+\rangle\langle +|, M_{01}(q \rhd x).((\mathbf{if}\ x = 0\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1) \parallel \mathbf{0}_q)\rangle} \\
&\quad \to \left(\overline{\langle |0\rangle\langle 0|, \mathbf{if}\ 0 = 0\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1\rangle}\ {}_{1/2}\!\oplus \overline{\langle |1\rangle\langle 1|, \mathbf{if}\ 1 = 0\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1\rangle}\right) \parallel \mathbf{0}_q \\
&\quad \equiv \left(\overline{\langle |0\rangle\langle 0|, a!1\rangle}\ {}_{1/2}\!\oplus \overline{\langle |1\rangle\langle 1|, b!1\rangle}\right) \parallel \mathbf{0}_q
\end{aligned}$$

3.3 A First Notion of Behavioural Equivalence

Since quantum mechanics is intrinsically probabilistic, quantum processes are commonly compared by using some probabilistic version of bisimilarity [Deng and Feng 2012; Feng et al. 2007, 2012; Lalire 2006; Lalire and Jorrand 2004]. We follow the approach of Hennessy [2012], defining bisimulations directly on distributions. Differently from the previous proposals, we do not use labels but rely instead on contexts and barbs, i.e. defining a saturated bisimilarity à la Bonchi et al. [2014].

We start by defining barbs, i.e. atomic observable properties of the lqCCS processes.

Definition 3.6. A *process barb* is a predicate $\downarrow_c$ on processes satisfied by P (written $P\downarrow_c$) if $P \equiv (c!e + R) \parallel Q$ for some Q, R. A *distribution barb* is a predicate $\downarrow_b^p$ on distributions such that

- Δ satisfies $\downarrow_c^p$, written $\Delta\downarrow_c^p$, if $\sum_{P\downarrow_c} \Delta(\langle \rho, P\rangle) = p$;
- Δ satisfies $\downarrow_\bot^p$, written $\Delta\downarrow_\bot^p$, if $\Delta(\bot) = p$.

Intuitively, the barbs of a process are the visible channels on which a value is ready to be sent, while the barbs of a distribution are defined as the probability of having a process capable to send on a given channel, or as the probability of having a deadlocked process. Notice that if $\Delta{\downarrow}^{p}_{\bot}$, then it must be $\Delta = \overline{\bot}\ {}_{p}{\oplus}\ \Delta'$ for some Δ' such that $\Delta'(\bot) = 0$. Note also that barbs are purely classical.

In saturated bisimilarities, contexts $B[\,\cdot\,]$ play the role of observers that are used for discriminating processes. In this first version of bisimilarity, they are defined as lqCCS processes with a typed hole.

Definition 3.7. A context $B[\,\cdot\,]_{\Sigma}$ is generated by the production $B[\,\cdot\,]_{\Sigma} ::= [\,\cdot\,]_{\Sigma} \parallel P$, up to structural congruence and typed according to the rules in Figure 1 and to the following one

$$\frac{\Sigma' \setminus \Sigma \vdash P \quad \Sigma \subseteq \Sigma'}{\Sigma' \vdash [\,\cdot\,]_{\Sigma} \parallel P}\ \textsc{Hole}$$

A process P is applied to contexts by replacing the hole with P. Intuitively, a context $\Sigma' \vdash B[\,\cdot\,]_{\Sigma}$ is a function that given a process P returns a process $B[P]$ obtained by replacing P for $[\,\cdot\,]$, where Σ is the typing context of the valid inputs and Σ' the one of the outputs. Note that a context can own some qubits and each qubit cannot be referred to in both P and $B[\,\cdot\,]$. We apply $\Sigma' \vdash B[\,\cdot\,]_{\Sigma}$ to configurations $(\Sigma_{\rho}, \Sigma_{P}) \vdash \langle \rho, P \rangle$ obtaining $(\Sigma_{\rho}, \Sigma') \vdash \langle \rho, B[P] \rangle$ when $\Sigma' \subseteq \Sigma_{\rho}$ and $\Sigma = \Sigma_{P}$, i.e. when the qubits referred by $B[\,\cdot\,]$ are defined in ρ and the process P is as prescribed by $B[\,\cdot\,]$. We write $B[\langle \rho, P \rangle]$ for $\langle \rho, B[P] \rangle$, $B[\bot]$ for $\bot$, and $B[\Delta]$ for the distribution obtained by applying $B[\,\cdot\,]$ to the support of Δ. It is trivial to show that if Δ and Θ are typed by the same typing context, then $B[\Delta]$ is defined if and only if $B[\Theta]$ is defined, and that their typing is unique.

In the following, we only consider well-typed distributions and contexts, and we impose bisimulations to be over distributions of the same type (thus we avoid specifying types).

Definition 3.8 (s-bisimilarity). A relation $\mathcal{R} \subseteq \mathcal{D}(\mathit{Conf}_{\bot}) \times \mathcal{D}(\mathit{Conf}_{\bot})$ is a *saturated bisimulation* if $\Delta \mathcal{R} \Theta$ implies that for any context $B[\,\cdot\,]$ it holds

- $\Delta{\downarrow}^{p}_{b}$ if and only if $\Theta{\downarrow}^{p}_{b}$;
- whenever $B[\Delta] \longrightarrow \Delta'$, there exists Θ' such that $B[\Theta] \longrightarrow \Theta'$ and $\Delta'\ \mathcal{R}\ \Theta'$;
- whenever $B[\Theta] \longrightarrow \Theta'$, there exists Δ' such that $B[\Delta] \longrightarrow \Theta'$ and $\Delta'\ \mathcal{R}\ \Theta'$.

Let *saturated bisimilarity* $\sim_{s}$ be the largest saturated bisimulation.

We say that two processes P, Q are saturated bisimilar if $\overline{\langle \rho, P \rangle} \sim_{s} \overline{\langle \rho, Q \rangle}$ for any ρ.

When encoding a protocol or its specification in lqCCS, each qubit must be sent on a visible channel if its value is a relevant aspect of the given protocol, discarded otherwise. Notice that, thanks to linearity, the visibility of qubits cannot be ambiguous, and that $\sim_{s}$ replicates the results of the previous proposals in the unambiguous cases (see the first three rows of Table 1).

Example 3.9. Consider **QL** of Example 3.2. It is not difficult to show that $\overline{\langle |0\rangle\langle 0|\,, \mathbf{QL} \rangle}$ is bisimilar to $\Delta_{\mathbf{QL}} = \left(\overline{\langle \rho, \tau.\tau.a!1 \rangle}\ {}_{1/2}{\oplus}\ \overline{\langle \rho, \tau.\tau.b!1 \rangle}\right) \parallel \mathbf{0}_{q}$ for any $\rho \in \widehat{\mathcal{H}}$. Note that $\Delta_{\mathbf{QL}} \longrightarrow \Delta'_{\mathbf{QL}} \longrightarrow \Delta''_{\mathbf{QL}}$ with $\Delta'_{\mathbf{QL}} = \left(\overline{\langle \rho, \tau.a!0 \rangle}\ {}_{1/2}{\oplus}\ \overline{\langle \rho, \tau.b!1 \rangle}\right) \parallel \mathbf{0}_{q}$ and $\Delta''_{\mathbf{QL}} = \left(\overline{\langle \rho, a!0 \rangle}\ {}_{1/2}{\oplus}\ \overline{\langle \rho, b!1 \rangle}\right) \parallel \mathbf{0}_{q}$. It suffices then to give the relation $\mathcal{R}$ below, which is a bisimulation once closed for congruence and contexts

$$\mathcal{R} = \left\{ \left(\overline{\langle |0\rangle\langle 0|\,, \mathbf{QL} \rangle}, \Delta_{\mathbf{QL}} \right), \left(\overline{\langle |+\rangle\langle +|\,, M_{01}(q \rhd x).(c!x \parallel \mathbf{0}_{q}) \rangle}, \Delta'_{\mathbf{QL}} \right), \left(\Delta''_{\mathbf{QL}}, \Delta''_{\mathbf{QL}} \right), \left(\overline{\bot}, \overline{\bot} \right) \right\}$$

Finally, note that this result depends on the use of discard, meaning that the messages over a and b are the outcome of the protocol, and not the resulting quantum state. For example, the distribution $\overline{\langle |0\rangle\langle 0|\,, H(q).M_{01}(q \rhd x).((\mathbf{if}\ x = 0\ \mathbf{then}\ a!1\ \mathbf{else}\ b!1) \parallel c!q) \rangle}$ is not bisimilar to $\overline{\langle |0\rangle\langle 0|\,, \tau.\tau.a!1 \parallel c!q \rangle}\ {}_{1/2}{\oplus}\ \overline{\langle |0\rangle\langle 0|\,, \tau.\tau.b!1 \parallel c!q \rangle}$. To prove that, it suffices to consider the context $B[\,\cdot\,] = [\,\cdot\,] \parallel c?x.M_{01}(x \rhd y).\mathbf{if}\ y = 0\ \mathbf{then}\ \mathbf{0}_{x}\ \mathbf{else}\ \mathit{fail}!x$, which will eventually exhibit the barb *fail* with the former distribution only.

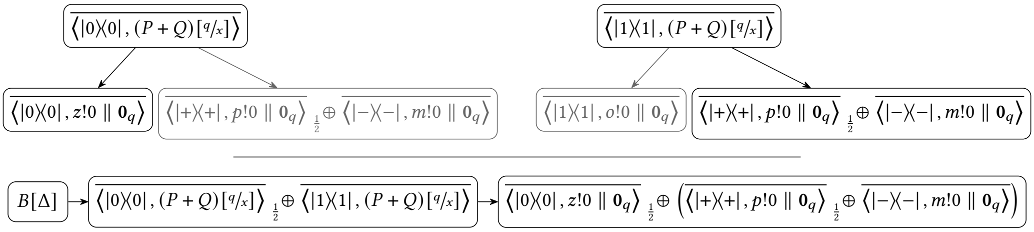
$\overline{\langle |0\rangle\langle 0|, (P+Q)[q/x] \rangle}$
$\overline{\langle |1\rangle\langle 1|, (P+Q)[q/x] \rangle}$
$\overline{\langle |0\rangle\langle 0|, z!0 \parallel \mathbf{0}_q \rangle}$
$\overline{\langle |+\rangle\langle +|, p!0 \parallel \mathbf{0}_q \rangle} \; {}_{\frac{1}{2}}\!\oplus \overline{\langle |-\rangle\langle -|, m!0 \parallel \mathbf{0}_q \rangle}$
$\overline{\langle |1\rangle\langle 1|, o!0 \parallel \mathbf{0}_q \rangle}$
$\overline{\langle |+\rangle\langle +|, p!0 \parallel \mathbf{0}_q \rangle} \; {}_{\frac{1}{2}}\!\oplus \overline{\langle |-\rangle\langle -|, m!0 \parallel \mathbf{0}_q \rangle}$
$B[\Delta]$
$\overline{\langle |0\rangle\langle 0|, (P+Q)[q/x] \rangle} \; {}_{\frac{1}{2}}\!\oplus \overline{\langle |1\rangle\langle 1|, (P+Q)[q/x] \rangle}$
$\overline{\langle |0\rangle\langle 0|, z!0 \parallel \mathbf{0}_q \rangle} \; {}_{\frac{1}{2}}\!\oplus \left(\overline{\langle |+\rangle\langle +|, p!0 \parallel \mathbf{0}_q \rangle} \; {}_{\frac{1}{2}}\!\oplus \overline{\langle |-\rangle\langle -|, m!0 \parallel \mathbf{0}_q \rangle} \right)$

Fig. 4. On the bottom, the evolution of $B[\Delta]$ into Δ' and then Δ''. The last step is built by convex combination of two freely chosen moves of the subdistributions, which are displayed above. It is clear that observers can make different non-deterministic choices for each subdistribution, also based on quantum states.

As a result of our saturated approach, entangled pairs are correctly distinguished from separable states with the same partial trace (see the fourth row of the same table).

Example 3.10. The processes in the fourth row of Table 1 are distinguished by the context $B[\,\cdot\,] = [\,\cdot\,] \parallel c?x.c?y.M(x, y \triangleright z).(\mathbf{if}\ z = (01)_2\ \mathbf{then}\ d!0\ \mathbf{else}\ \mathbf{0} \parallel \mathbf{0}_{x,y})$, because it will eventually exhibit the barb d if the state decays in $|01\rangle$ (which is only possible for $\frac{1}{4}I$).

Finally, notice that saturated bisimilarity equates the discard process $\mathbf{0}_{q_1,q_2}$ with both $\mathbf{0}_{q_2,q_1}$ and $c?x.(c!q_1 \parallel c!q_2 \parallel c!x) \setminus c$. To prove that, it suffices to give the relation associating Δ with $\Delta[P/Q]$ for any choice of P and Q among the processes above. This is clearly a bisimulation, once closed for contexts and congruence: for any context $B[\,\cdot\,]$, if $B[P] \longrightarrow \Delta$ then $B[Q] \longrightarrow \Delta[P/Q]$.

4 CURBING THE POWER OF NON-DETERMINISTIC CONTEXTS

The example in the fifth row of Table 1, shows that saturated bisimilarity is inadequate for the quantum case (similarly to QPAlg [Lalire 2006] and qCCS [Deng and Feng 2012]). Moreover, we trace the cause of this problem to the interaction between probabilistic and non-deterministic behaviour. We define a new semantics where non-determinism in contexts is constrained. These constraints solve the problem above, matching a defining feature of quantum systems, i.e. that states cannot be observed without being affected. Nonetheless, processes can still perform different non-deterministic choices upon known classical values. As a result of that, processes in the sixth row of Table 1 are distinguished.

4.1 Non-deterministic Issues

In quantum theory, the encoding of probability distributions of quantum states as density operators is not injective. Formally, a density operator represents an equivalence class of distributions of quantum states that behave the same according to quantum theory. They are defined by the relation $\mathcal{R} \subseteq \mathcal{D}(\mathcal{H}) \times \mathcal{D}(\mathcal{H})$ such that $\Delta \mathcal{R} \Theta$ whenever $\sum_{|\psi\rangle} \Delta(|\psi\rangle) |\psi\rangle\langle\psi| = \sum_{|\psi\rangle} \Theta(|\psi\rangle) |\psi\rangle\langle\psi|$.

Consider a pair of non-biased random qubit sources, the first sending a qubit in state $|0\rangle$ or $|1\rangle$, the second in state $|+\rangle$ or $|-\rangle$. Quantum theory prescribes that such two sources cannot be distinguished by any observer, as the received qubit behaves the same (see Nielsen and Chuang [2010, Section 2.4.2]). Indeed, the (mixed) states of the qubits sent by the two sources are represented by the same density operator $\frac{1}{2}I$. One expects the lqCCS encoding of these sources to be bisimilar. Somewhat surprisingly, this is not the case.

Example 4.1. Take the fifth row of Table 1. After two steps with empty contexts, the two distributions evolve into $\Delta = \overline{\langle |0\rangle\langle 0|, c!q \rangle} \; {}_{1/2}\!\oplus \overline{\langle |1\rangle\langle 1|, c!q \rangle}$ and $\Theta = \overline{\langle |+\rangle\langle +|, c!q \rangle} \; {}_{1/2}\!\oplus \overline{\langle |-\rangle\langle -|, c!q \rangle}$,

$$\frac{}{\left\langle \rho, P, \mathcal{E}(\tilde{q}).R \right\rangle \rightsquigarrow_{\varepsilon} \overline{\left\langle \mathcal{E}_{\tilde{q}}(\rho), P, R \right\rangle}}\ \textsc{OQOp} \qquad \frac{\rho_m = (M_m)_{\tilde{q}}(\rho) \quad p_m = \mathrm{tr}(\rho_m)}{\left\langle \rho, P, M(\tilde{q} \rhd y).R \right\rangle \rightsquigarrow_{\varepsilon} \sum_{m=0}^{|M|-1} p_m \bullet \overline{\left\langle \frac{\rho_m}{p_m}, P, R[{}^{m}/_{y}] \right\rangle}}\ \textsc{OQMeas}$$

$$\frac{c \notin D}{\left\langle \rho, ((c!v + P) \parallel Q) \setminus D, c?x.R + S \right\rangle \rightsquigarrow_{\varepsilon} \overline{\left\langle \rho, Q \setminus D, R[{}^{v}/_{x}] \right\rangle}}\ \textsc{Input}$$

$$\frac{c \notin D}{\left\langle \rho, (((c?x.P) + P') \parallel Q) \setminus D, c!v \right\rangle \rightsquigarrow_{\varepsilon} \overline{\left\langle \rho, (P[{}^{v}/_{x}] \parallel Q) \setminus D, \mathbf{0} \right\rangle}}\ \textsc{Output}$$

$$\frac{\left\langle \rho, P \right\rangle \longrightarrow \Delta}{O[\left\langle \rho, P \right\rangle] \rightsquigarrow_{\diamond} O[\Delta]}\ \textsc{Process} \qquad \frac{\left\langle \rho, P, R \right\rangle \rightsquigarrow_{\lambda} \Delta}{\left\langle \rho, P, R \parallel S \right\rangle \rightsquigarrow_{\ell \cdot \lambda} \Delta \parallel S}\ \textsc{ParL} \qquad \frac{\left\langle \rho, P, S \right\rangle \rightsquigarrow_{\lambda} \Delta}{\left\langle \rho, P, R \parallel S \right\rangle \rightsquigarrow_{r \cdot \lambda} R \parallel \Delta}\ \textsc{ParR}$$

$$\frac{P \equiv P' \quad R \equiv_o R' \quad \left\langle \rho, P', R' \right\rangle \rightsquigarrow_{\pi} \Delta' \quad \Delta' \equiv_o \Delta}{\left\langle \rho, P, R \right\rangle \rightsquigarrow_{\pi} \Delta}\ \textsc{Congr}$$

Fig. 5. lqCCS enhanced semantics

encoding the qubit sources above. To see that $\Delta \not\sim_s \Theta$, take $B[\,\cdot\,] = [\,\cdot\,] \parallel c?x.(P + Q)$ where

$$\begin{aligned} P &= M_{01}(x \rhd y).((\textbf{if } y = 0 \textbf{ then } z!0 \textbf{ else } o!0) \parallel \mathbf{0}_x), \text{ and} \\ Q &= M_{\pm}(x \rhd y).((\textbf{if } y = 0 \textbf{ then } p!0 \textbf{ else } m!0) \parallel \mathbf{0}_x). \end{aligned}$$

$B[\Delta]$ reduces to $\Delta' = \left(\overline{\left\langle |0\rangle\langle 0|, P + Q \right\rangle}\ {}_{1/2}{\oplus}\ \overline{\left\langle |1\rangle\langle 1|, P + Q \right\rangle}\right)[{}^{q}/_{x}]$, and $B[\Theta]$ can only reduce to $\Theta' = \left(\overline{\left\langle |+\rangle\langle +|, P + Q \right\rangle}\ {}_{1/2}{\oplus}\ \overline{\left\langle |-\rangle\langle -|, P + Q \right\rangle}\right)[{}^{q}/_{x}]$ to match this move. By choosing P and Q respectively in the left and right part, Δ' reduces to $\Delta'' = \left(\overline{\left\langle |0\rangle\langle 0|, z!0 \right\rangle}\ {}_{1/2}{\oplus} \left(\overline{\left\langle |+\rangle\langle +|, p!0 \right\rangle}\ {}_{1/2}{\oplus}\ \overline{\left\langle |-\rangle\langle -|, m!0 \right\rangle}\right)\right) \parallel \mathbf{0}_q$ that exhibits the barb z but not o. It is easy to check that Θ cannot replicate this behaviour: for any choice of P and Q it will either express both z and o, or none of them.

This result is paradigmatic, where different mixtures of quantum states are discriminated by a non-deterministic context that chooses how to reduce based on the value of the received qubit, which in theory should be unknown (see Figure 4). Note also that the two sources above have a deterministic behaviour, while non-determinism is only introduced by the context.

We argue that unconstrained non-deterministic contexts are too strong for representing the real capacity of discriminating quantum processes. Therefore, in the following, we give a new semantics that constrains non-deterministic contexts so that they cannot apply the strategy above to discriminate between processes. Note that removing + from the contexts is not sufficient, as we can replicate the same non-deterministic behaviour of Example 4.1 with just the parallel composition, e.g. with $B'[\,\cdot\,] = [\,\cdot\,] \parallel c?x.P \parallel c?x.Q$.

4.2 Constrained Bisimilarity

We consider a special set of processes, called *observers*, that are used as constrained contexts for lqCCS. An observer R is a process without silent action, restrictions and with non-deterministic choice limited to sums of receptions. We constrain non-deterministic choices for matching the observational limitations prescribed by quantum theory, while silent actions and restrictions are safely omitted for convenience, as they do not increase the discriminating capabilities of contexts (as proved by Bonchi et al. [2014]).

$$\frac{}{P + \mathbf{0}_{\tilde{e}} \equiv_o P}\ \textsc{SCCSumNil} \qquad \frac{}{P + Q \equiv_o Q + P}\ \textsc{SCCSumComm} \qquad \frac{}{P + (Q + R) \equiv_o (P + Q) + R}\ \textsc{SCCSumAssoc}$$

$$\frac{}{\mathbf{if}\ \mathit{ff}\ \mathbf{then}\ P\ \mathbf{else}\ Q \equiv_o Q}\ \textsc{SCCIteF} \qquad \frac{}{\mathbf{if}\ \mathit{tt}\ \mathbf{then}\ P\ \mathbf{else}\ Q \equiv_o P}\ \textsc{SCCIteT} \qquad \frac{e \Downarrow v}{P \equiv_o P[{}^{v}/_{e}]}\ \textsc{SCCValExpr}$$

Fig. 6. Structural congruence of lqCCS observers

Formally, an observer is defined by taking the pre-terms generated by the following grammar and by imposing additional constraints over parallel composition

$$\begin{aligned} R &::= \mathbf{0}_{\tilde{e}} \mid c!e \mid T \mid R \parallel R \mid \mathbf{if}\ e\ \mathbf{then}\ R\ \mathbf{else}\ R \mid \mathcal{E}(\tilde{x}).R \mid M(\tilde{x} \triangleright y).R \\ T &::= c?x.R \mid T + T \end{aligned}$$

A pre-term R is an observer if $T \not\equiv c?x.R' + c?y.R'' + T'$ for any T appearing in R. This additional constraint forbids parallel processes in R from performing non-deterministic choices upon reception, and it could be decided by a suitable extension of our type system.

Despite the syntactical constraints, the major difference between a process P and an observer R is their treatment in our enhanced semantics, which is given on extended configurations: triples with an observer as the third element. In the following, we sometimes write $\langle \rho, P \rangle$ for $\langle \rho, P, \mathbf{0} \rangle$. We say that $(\Sigma_\rho, \Sigma) \vdash \langle \rho, P, R \rangle$ if $\Sigma = \Sigma_P \cup \Sigma_R$, $\Sigma_P \cap \Sigma_R = \emptyset$, and $\Sigma \subseteq \Sigma_\rho$. Distributions of configurations are typed as usual. Contexts $O[\,\cdot\,]_\Sigma$ are defined from observers R up to structural congruence as $O[\,\cdot\,]_\Sigma ::= [\,\cdot\,]_\Sigma \parallel R$. Context application $O\big[\langle \rho, P, R \rangle\big]$ is defined over configurations as $\langle \rho, P, O[R] \rangle$.

We define a new congruence for observers, named $\equiv_o$, based on $\equiv$ but lacking rules for parallel and restriction operators (see Figure 6). We lift $\equiv_o$ to distributions by linearity and imposing $\overline{\bot} \equiv_o \overline{\bot}$ and $\overline{\langle \rho, P, R \rangle} \equiv_o \overline{\langle \rho, P', R' \rangle}$ if $P \equiv P'$ and $R \equiv_o R'$. Note that the commutativity of the parallel operator is preserved for processes, while it does not hold for observers: we want to distinguish the locus of the reductions for properly constraining the non-deterministic evolution of distributions. We give an *enhanced semantics* for lqCCS in Figure 5, adopting the style of Degano and Priami [2001]: an arrow $\rightsquigarrow_\pi \subseteq \mathit{Conf}_\bot \times \mathcal{D}(\mathit{Conf}_\bot)$ for any index π, which encodes the non-deterministic choice of the observer (or $\diamond$ if only the process evolves). Indices are strings in $\{\ell, r\}^* \cup \{\diamond\}$, and we write ε for the empty string, $\cdot$ for string concatenation, and λ for indices different from $\diamond$.

In the rules In and Out, we write $\backslash D$ for any sequence of restrictions. We also write $\Delta \parallel R$ and $R \parallel \Delta$ meaning that R is composed with the observers of Δ. As for the probabilistic semantics, the $\rightsquigarrow_\pi$ is extended by imposing that $C \rightsquigarrow_\pi \overline{\bot}$ if there is no Δ such that $C \rightsquigarrow_\pi \Delta$ In the following, we lift semantic transitions, and write $\rightsquigarrow_\pi$ instead of $\mathrm{lift}(\rightsquigarrow_\pi) \in \mathcal{D}(\mathit{Conf}_\bot) \times \mathcal{D}(\mathit{Conf}_\bot)$. The observational power is limited by the indexing as the lifting of $\rightsquigarrow_\pi$ allows a distribution to evolve only when all its configurations reduce by performing the same choice. The absence of rules for observer synchronization does not limit the observational power [Bonchi et al. 2014]. Note that the transition system is still non-deterministic, but different non-deterministic choices produce different indices. Nevertheless, the observer is still capable to behave differently in different configurations of the same distribution, but only through the $\mathbf{if} \cdot \mathbf{then} \cdot \mathbf{else} \cdot$ construct or because of a sum of receptions (where the choice is performed by the sending process and not by the observer). This ensures that the observer choices are based on *classical information* obtained from the process.

We say that a configuration satisfies the barb c, written $\langle \rho, P, R \rangle \downarrow_c$, if $P \equiv (c!v + S) \parallel Q$ or $R \equiv c!v \parallel S$ (notice that we use $\equiv$ instead of $\equiv_o$ for R, thus considering also commutativity, associativity, and identity). The extension of barbs to distributions is as usual.

We now define constrained saturated bisimulation with the usual assumption that it is defined over distributions of the same type, and that contexts are taken accordingly.

Definition 4.2 (cs-bisimilarity). A relation $\mathcal{R} \subseteq \mathcal{D}(Conf_\perp) \times \mathcal{D}(Conf_\perp)$ is a *constrained saturated bisimulation* if $\Delta \mathcal{R} \Theta$ implies that for any context $O[\,\cdot\,]$ it holds

- $\Delta{\downarrow}^p_b$ if and only if $\Theta{\downarrow}^p_b$;
- whenever $O[\Delta] \rightsquigarrow_\pi \Delta'$, there exists Θ' such that $O[\Theta] \rightsquigarrow_\pi \Theta'$ and $\Delta' \mathcal{R} \Theta'$;
- whenever $O[\Theta] \rightsquigarrow_\pi \Theta'$, there exists Δ' such that $O[\Delta] \rightsquigarrow_\pi \Theta'$ and $\Delta' \mathcal{R} \Theta'$.

Let *constrained saturated bisimilarity* $\sim_{cs}$ be the largest constrained saturated bisimulation. We say that two processes P, Q are constrained bisimilar if $\overline{\langle \rho, P, \mathbf{0} \rangle} \sim_{cs} \overline{\langle \rho, Q, \mathbf{0} \rangle}$ for each ρ.

Example 4.3. Consider Δ, P, Q from Example 4.1 and take $O[\,\cdot\,] = [\,\cdot\,] \parallel c?x.P \parallel c?x.Q$ (notice that it emulates the context distinguishing Δ from Θ in Example 4.1). In the enhanced semantics, $O[\Delta]$ only performs $O[\Delta] \rightsquigarrow_\ell (\overline{\langle |0\rangle\langle 0|\,, \mathbf{0}, P[{}^q/_x] \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |1\rangle\langle 1|\,, \mathbf{0}, P[{}^q/_x] \rangle}) \parallel c?x.Q$ or $O[\Delta] \rightsquigarrow_r (\overline{\langle |0\rangle\langle 0|\,, \mathbf{0}, Q[{}^q/_x] \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |1\rangle\langle 1|\,, \mathbf{0}, Q[{}^q/_x] \rangle}) \parallel c?x.P$, as the indices must coincide for any configuration in the support of Δ. Indeed, we will later prove that $\Delta \sim_{cs} \Theta$.

4.3 Behavioural Assessment of Constrained Bisimilarity

In the following, we state some important properties of $\sim_{cs}$. A first result recovers the linearity of the relation. We then prove that $\sim_{cs}$ is strictly coarser than the previously defined $\sim_s$. Furthermore, we show that our constraints are strong enough to agree with the limitations of the observational power prescribed by quantum theory. More precisely, we consider the equivalence classes over distributions of quantum states implicitly represented by density operators, and we generalize them as classes of bisimilar distributions of lqCCS configurations. An undue curbing of contexts is not better than a deficient one, therefore, we finally prove that the expressivity of the non-deterministic sum of processes is preserved when justified by classical information.

Theorem 4.4. *If $\Delta_i \sim_{cs} \Theta_i$ for $i = 1, 2$, then $\Delta_1 \;{}_p{\oplus}\; \Delta_2 \sim_{cs} \Theta_1 \;{}_p{\oplus}\; \Theta_2$ for any $p \in [0, 1]$.*

Proof sketch. It follows from the linearity of barbs and the decomposability of $\rightsquigarrow_\pi$, which hold by definition. □

Regarding quantum properties, the enhanced semantics limits the capability of the observer to perform different choices in different configurations of the same distribution. As a result, cs-bisimilarity is strictly broader than s-bisimilarity, as observers are less powerful.

Theorem 4.5. $\sim_s \subsetneq \sim_{cs}$.

Proof sketch. Example 4.6 shows that $\sim_{cs} \not\subseteq \sim_s$. For $\sim_s \subseteq \sim_{cs}$ we provide a translation $(\!|\,\cdot\,|\!)$ that annotates a given R with fresh barbs encoding the non-deterministic choices. We prove by induction that the enhanced semantics of $\langle \rho, P, R \rangle$ corresponds to the standard semantics of $\langle \rho, P || (\!| R |\!) \rangle$, where $(\!| R |\!)$ is composed with the parallel operator (as required by $\sim_s$). In particular, $\langle \rho, P, R \rangle \rightsquigarrow_\pi \Delta$ if and only if $(\!| R |\!) \downarrow_\pi$ and $\langle \rho, P || (\!| R |\!) \rangle \longrightarrow \Delta'$ with $\Delta' {\downarrow}^0_\pi$ (roughly, a $\rightsquigarrow_\pi$ move corresponds to a $\longrightarrow$ one where the barb π is "consumed"). This allows us to prove that $\sim_s$ is a cs-bisimulation. □

From the proof above it follows that the enhanced semantics does not give cs-bisimilarity any additional discriminating power with respect to the standard semantics. In other words, we could have defined $\sim_{cs}$ without changing the semantics, just requiring instead that contexts express their non-deterministic choices as barbs. The enhanced semantics — as well as the absence of congruence rules for parallel observers — is then just a convenient way to assign a name to each possible non-deterministic choice, which fits well with the SOS-style rules.

We discuss now how cs-bisimilarity deals with the issue presented in subsection 4.1.

Example 4.6. Let $\Delta = \overline{\langle |+\rangle\langle+| \, , M_{01}(q \rhd x).c!q, \mathbf{0} \rangle}$, and $\Theta = \overline{\langle |0\rangle\langle 0| \, , M_{\pm}(q \rhd x).c!q, \mathbf{0} \rangle}$. For each $O[\,\cdot\,]$, $O[\Delta]$ evolves in $O[\Delta']$ with $\Delta' = \overline{\langle |0\rangle\langle 0| \, , c!q, \mathbf{0} \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |1\rangle\langle 1| \, , c!q, \mathbf{0} \rangle}$, and $O[\Theta]$ in $O[\Theta']$ with $\Theta' = \overline{\langle |+\rangle\langle+| \, , c!q, \mathbf{0} \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |-\rangle\langle-| \, , c!q, \mathbf{0} \rangle}$. As detailed in subsection 4.1, one would expect $\Delta' \sim_{cs} \Theta'$, as they send indistinguishable quantum states. We prove that this is the case, in particular, because the process $c!q$ is deterministic.

A distribution Δ is *deterministic* if its evolution is fully probabilistic, i.e. if it evolves in a single distribution up to bisimilarity. For example, distributions without parallel operators and non-deterministic sums are trivially deterministic.

Definition 4.7 (Deterministic processes). A set of distributions $\mathcal{A}$ is deterministic if $\Delta \in \mathcal{A}$ implies that for any $O[\,\cdot\,], \Delta', \Delta''$, if $O[\Delta] \rightsquigarrow_{\pi} \Delta'$ and $O[\Delta] \rightsquigarrow_{\pi} \Delta''$ then $\Delta' \sim_{cs} \Delta''$ and $\Delta', \Delta'' \in \mathcal{A}$. A distribution Δ is called deterministic if it is contained in a deterministic set. A process P is deterministic if $\overline{\langle \rho, P, \mathbf{0} \rangle}$ is deterministic for any state ρ.

As previously stated, mixed states represented by the same density operator are indistinguishable. We recover an analogous result for lqCCS. Roughly, quantum states can be combined into a point distribution when paired with identical deterministic processes.

Theorem 4.8. *If P is deterministic, then for any ρ, σ, p, R, $\overline{\langle \rho, P, R \rangle} \;{}_{p}{\oplus}\; \overline{\langle \sigma, P, R \rangle} \sim_{cs} \overline{\langle \rho \;{}_{p}{\oplus}\; \sigma, P, R \rangle}$ where $\rho \;{}_{p}{\oplus}\; \sigma$ is defined as the density operator $p\rho + (1-p)\sigma$.*

Proof sketch. For any deterministic P, we prove by structural induction that

$$\mathcal{R} = \{\, (\bot, \bot) \,\} \cup \left\{ \left(\overline{\langle \rho \;{}_{p}{\oplus}\; \sigma, P, R \rangle} \, , \, \overline{\langle \rho, P, R \rangle} \;{}_{p}{\oplus}\; \overline{\langle \sigma, P, R \rangle} \right) \mid \rho, \sigma, p, R \right\}$$

is a bisimulation up to convex hull [Bonchi et al. 2017] and up to bisimilarity (the soundness of which is given by Proposition 4.19 and according to Pous and Sangiorgi [2011]).

The result mainly follows from the fact that the classical components of the distributions are identical, while the quantum components are indistinguishable, as superoperators and measurements are convex, i.e. $\mathcal{F}(\rho) \;{}_{p}{\oplus}\; \mathcal{F}(\sigma) = \mathcal{F}(\rho \;{}_{p}{\oplus}\; \sigma)$ for any superoperator or measurement $\mathcal{F}$. The hypothesis of determinism is required for the cases of non-deterministic sums and parallel compositions. Indeed, $\Delta = \overline{\langle \rho, P \parallel Q, \mathbf{0} \rangle} \;{}_{p}{\oplus}\; \overline{\langle \sigma, P \parallel Q, \mathbf{0} \rangle}$ may evolve differently with the left and right component, e.g. choosing P in the left and Q in the right. The hypothesis of the process being deterministic ensures that no information is leaked about ρ and σ, and ensures that the choice of Δ is irrelevant, allowing $\overline{\langle \rho \;{}_{p}{\oplus}\; \sigma, P, \mathbf{0} \rangle}$ to replicate its move. This is not possible in general, as shown in Example 4.10. □

Remarkably, transitivity of $\sim_{cs}$ suffices for proving the bisimilarity of deterministic processes paired with distributions of quantum states that are represented by the same density operator. Note for example that $\overline{\langle |0\rangle\langle 0| \, , c!q \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |1\rangle\langle 1| \, , c!q \rangle}$ and $\overline{\langle |+\rangle\langle+| \, , c!q \rangle} \;{}_{1/2}{\oplus}\; \overline{\langle |-\rangle\langle-| \, , c!q \rangle}$ of Example 4.6 and 4.1 are both bisimilar to $\overline{\langle \frac{1}{2} I, c!q \rangle}$. More in general, the equivalence classes represented by density operators are lifted to lqCCS distributions, yielding the equivalence $\mathcal{R} \subseteq \sim_{cs}$ relating Δ and Θ deterministic whenever $\sum_{\rho} \Delta(\langle \rho, P, R \rangle)\rho = \sum_{\rho} \Theta(\langle \rho, P, R \rangle)\rho$ for all P, R. Note also that, thanks to the linearity of $\sim_{cs}$, the property above is not limited to syntactically identical processes.

A consequence of Theorem 4.8 is that $\sim_{cs}$ is not decomposable, similarly to other proposals addressing the limitations of probabilistic bisimilarity [Deng 2018; Feng and Ying 2015].

Corollary 4.9. *cs-bisimilarity is not a decomposable relation.*

$$\frac{P' \leq P \quad Q' \leq Q}{P' \mathbin{\square} Q' \leq P \mathbin{\square} Q}\ \square \in \{\|, +\} \qquad \frac{P' \leq P}{\mu.P' \leq \mu.P}\ \mu \in \{\tau, c?x, \mathcal{E}(\tilde{e}), M(\tilde{e} \triangleright x)\} \qquad \frac{P' \leq P}{P' \leq P + Q} \qquad \frac{Q' \leq Q}{Q' \leq P + Q}$$

$$\frac{P' \leq P}{P' \setminus c \leq P \setminus c} \qquad \frac{P' \leq P \quad Q' \leq Q}{\textbf{if } e \textbf{ then } P' \textbf{ else } Q' \leq P + Q} \qquad \frac{P' \leq P \quad Q' \leq Q}{\textbf{if } e \textbf{ then } P' \textbf{ else } Q' \leq \textbf{if } e \textbf{ then } P \textbf{ else } Q}$$

Fig. 7. Refinement relation over lqCCS processes.

Proof sketch. Take $\Delta = \overline{\langle |0\rangle\langle 0|, c!q \rangle} \ {}_{1/2}{\oplus}\ \overline{\langle |1\rangle\langle 1|, c!q \rangle}$ and $\Theta = \overline{\langle |+\rangle\langle +|, c!q \rangle} \ {}_{1/2}{\oplus}\ \overline{\langle |-\rangle\langle -|, c!q \rangle}$. Notice that $\Delta \sim_{cs} \Theta$ by Theorem 4.8. Then, for $\sim_{cs}$ to be decomposable, Θ should be equal to $\Theta_1 \ {}_{1/2}{\oplus}\ \Theta_2$ for some $\Theta_1 \sim_{cs} \overline{\langle |0\rangle\langle 0|, c!q \rangle}$. But since Θ_1 can only be either $\overline{\langle |+\rangle\langle +|, c!q \rangle}$, $\overline{\langle |-\rangle\langle -|, c!q \rangle}$ or a combination of them, $\Theta_1 \nsim_{cs} \overline{\langle |0\rangle\langle 0|, c!q \rangle}$ as they send observably different quantum values. □

Theorem 4.8 targets deterministic processes because they represent fully defined physical processes, e.g., where all the choices are performed by boolean conditions. Indeed, there is no reason to expect the property to hold for processes expressing non-determinism à la CCS, as it does not encode any physical behaviour considered in quantum theory. More in detail, an extension of this theorem for general processes can only hold with overly constrained non-deterministic sums, and it would contradict Theorem 4.12 below, attesting to the preservation of the expressiveness of non-determinism in processes. We show an example of a non-deterministic process, derived from the sixth row of Table 1, for which Theorem 4.8 does not apply.

Example 4.10. Consider the following pair of processes of the last line of Table 1

$$\mathrm{Set}_{|+\rangle\langle+|}(q).M_{01}(q \triangleright x).(c!q + d!q) \text{ and } \mathrm{Set}_{|0\rangle\langle 0|}(q).M_{\pm}(q \triangleright x).(c!q + d!q)$$

We will later show that the distributions $\Delta = \overline{\langle |+\rangle\langle +|, M_{01}(q \triangleright x).\textbf{if } x = 0 \textbf{ then } P \textbf{ else } Q, \mathbf{0} \rangle}$ and $\Theta = \overline{\langle |0\rangle\langle 0|, M_{\pm}(q \triangleright x).\textbf{if } x = 0 \textbf{ then } P \textbf{ else } Q, \mathbf{0} \rangle}$ to which the two processes reduce are not bisimilar.

As discussed previously, this is expected as we want to restrict the non-determinism of observers only. Non-deterministic sum is typically used in processes to model unspecified behaviour, to be instantiated in future refinements. Thus, we do not want to constrain non-determinism to the point that + cannot replicate the behaviour of its refinements like boolean conditions.

We say that P' refines P, if P' can be obtained from P by substituting some occurrences of $Q + Q'$ with either Q, Q', or **if** e **then** Q **else** Q' for an arbitrary e.

Definition 4.11. The refinement relation $P' \leq P$ is the smallest reflexive relation satisfying the rules in Figure 7. We say that P' refines P, and that a configuration $\langle \rho, P' \rangle$ refines $\langle \rho, P \rangle$, if $P' \leq P$. We let $\perp$ refine all the configurations, and define distribution refinement by linearity.

A process is expected to be capable of matching any move of its refinements, thus, when considering $P = M_{01}(q \triangleright x).(Q + Q')$, the moves of all $P' \leq P$ should be available for P, included the ones of $M_{01}(q \triangleright x).\textbf{if } x = 0 \textbf{ then } Q \textbf{ else } Q'$ where the choice between Q and Q' depends on the outcome of the measurement.

We prove in the following that our constraints on non-determinism are not too restrictive, namely, that a distribution can simulate all its refinements.

Theorem 4.12. *Let $\Delta' \leq \Delta$. If $\Delta' \rightsquigarrow_{\pi} \Theta'$ then $\Delta \rightsquigarrow_{\pi} \Theta$ for some Θ such that $\Theta' \leq \Theta$.*

Proof sketch. We prove by rule induction that whenever $P' \leq P$ and $\langle \rho, P', R \rangle \rightsquigarrow_{\pi} \Delta'$ then $\langle \rho, P, R \rangle \rightsquigarrow_{\pi} \Delta$ for some Δ such that $\Delta' \leq \Delta$. The proof for Congr relies on the fact that refinement

$$\begin{tikzcd}
\boxed{\overline{\left\langle |+\rangle\langle+| , M_{01}(q \triangleright x).\mathbf{if}\ x = 0\ \mathbf{then}\ c!q\ \mathbf{else}\ d!q, \mathbf{0} \right\rangle}} \arrow[r, phantom, "\leq"] \arrow[d, squiggly, "\diamond"] & \boxed{\overline{\left\langle |+\rangle\langle+| , M_{01}(q \triangleright x).(c!q + d!q), \mathbf{0} \right\rangle}} \arrow[d, squiggly, dashed, "\diamond"] \\
\boxed{\overline{\left\langle |0\rangle\langle0| , c!q, \mathbf{0} \right\rangle} \;{}_{\frac{1}{2}}\!\oplus \overline{\left\langle |1\rangle\langle1| , d!q, \mathbf{0} \right\rangle}} \arrow[r, phantom, "="] & \boxed{\overline{\left\langle |0\rangle\langle0| , c!q, \mathbf{0} \right\rangle} \;{}_{\frac{1}{2}}\!\oplus \overline{\left\langle |1\rangle\langle1| , d!q, \mathbf{0} \right\rangle}}
\end{tikzcd}$$

Fig. 8. The existence of the dashed arrow on the right is guaranteed by the solid one on the left by Theorem 4.12.

and structural congruence works well together. In detail, we show that given $P' \preceq P$ with $P' \equiv Q'$ we can find some Q such that $Q' \preceq Q$ and $P \equiv Q$. In the other cases it suffices to use the induction hypothesis. The theorem then holds by decomposability of $\rightsquigarrow_\pi$. □

As a result of this property, the distributions Δ and Θ of Example 4.10 are distinguishable.

Example 4.13. Consider Δ and Θ of Example 4.10, and notice that $\Delta' \preceq \Delta$, where Δ' sends on c if and only if the qubit is in $|0\rangle$. Formally $\Delta' = \overline{\left\langle |+\rangle\langle+| , M_{01}(q \triangleright x).\mathbf{if}\ x = 0\ \mathbf{then}\ c!q\ \mathbf{else}\ d!q, \mathbf{0} \right\rangle}$ (see Figure 8). By performing this choice, Δ' is implicitly communicating the outcome of the measurement to the observer (through a side-channel, we could say). Consider the context

$$O[\,\cdot\,] = [\,\cdot\,] \parallel (c?x.M_{01}(x \triangleright y).(\mathbf{if}\ y = 0\ \mathbf{then}\ z!0\ \mathbf{else}\ o!0 \parallel \mathbf{0}_x)) + (d?x.\tau.\mathbf{0}_x)$$

and note that, after two steps, $O[\Delta']$ reduces to a distribution expressing barb z but not o, which is impossible for $O[\Theta]$. As a result of Theorem 4.12, Δ can replicate this move of Δ', hence $\Delta \not\sim_{cs} \Theta$.

Our constrained bisimilarity is the first one to verify both Theorem 4.8 and 4.12, while all the previously proposed ones either fail in equating indistinguishable quantum states, or overly constrain non-determinism (see Table 1 for an in-depth comparison).

4.4 Properties of Constrained Bisimilarity

We now investigate our cs-bisimilarity. We first recover two defining properties of [Deng and Feng 2012], namely that $\sim_{cs}$ is closed for superoperator application on qubits not appearing in the processes, and that the state of such qubits is required to match in bisimilar distributions. Then we show that discarded qubits can be "traced out" from the quantum state without affecting bisimilarity. Finally, we discuss up-to techniques for proving constrained bisimilarity.

We start by recovering trace-identity and closure over superoperator application.

Proposition 4.14. *Let $\overline{\langle \rho, P, \mathbf{0} \rangle} \sim_{cs} \overline{\langle \sigma, Q, \mathbf{0} \rangle}$, then*

(1) $\overline{\langle \mathcal{E}_{\tilde{q}}(\rho), P, \mathbf{0} \rangle} \sim_{cs} \overline{\langle \mathcal{E}_{\tilde{q}}(\sigma), Q, \mathbf{0} \rangle}$*, for any $\mathcal{E}_{\tilde{q}}$ and $\tilde{q}$ not in $\tilde{\Sigma}_P$;*
(2) $\mathrm{tr}_{\Sigma_P}(\rho) = \mathrm{tr}_{\Sigma_P}(\sigma)$.

Proof sketch. For the first point, take any superoperator $\mathcal{E}_{\tilde{q}}$, then there is a context that performs such transformation, so a context-closed relation is necessarily superoperator-closed. For the second one, we proceed by contradiction: if the reduced density operators of two configurations are different, then we can build a context which measures such qubits obtaining a different distribution of outcomes and thus distinguishing the configurations via fresh barbs. □

Note that this is a useful result for disproving bisimilarity, as e.g., distributions with different partial trace are immediately deemed distinguishable.

A result that helps instead in proving bisimilarity is that the state of discarded qubits can be ignored. In order to prove this in general, we extend the partial trace as follows.

Definition 4.15. The partial trace $\mathrm{tr}_{\tilde{q}}\left(\left\langle \rho, P, R \right\rangle\right)$ over $\tilde{q}$ of a configuration is $\left\langle \mathrm{tr}_{\tilde{q}}(\rho), P', R \right\rangle$ when $P \equiv P' \parallel \mathbf{0}_{\tilde{q}}$. We let $\mathrm{tr}_{\tilde{q}}(\bot) = \bot$, and define the partial trace of distributions by linearity.

Intuitively, we remove the discarded qubits *together with* the discard processes. Note that such an operation is defined only on distributions of configurations that discard the same qubits.

Proposition 4.16. *Let Δ, Θ be distributions such that $\mathrm{tr}_{\tilde{q}}(\Delta)$ and $\mathrm{tr}_{\tilde{q}}(\Theta)$ are well-defined for a given $\tilde{q}$. If $\mathrm{tr}_{\tilde{q}}(\Delta) \sim_{cs} \mathrm{tr}_{\tilde{q}}(\Theta)$ then $\Delta \sim_{cs} \Theta$.*

Proof sketch. We show, by induction on $\rightsquigarrow_{\pi}$, that the semantics of C and of $\mathrm{tr}_{\tilde{q}}(C)$ are equivalent, and since the partial trace does not affect barbs, the desired property follows. □

Note that, even if this property is given for the process $\mathbf{0}_{\tilde{q}}$, we can apply it to any "discard-like" process thanks to the linearity of $\sim_{cs}$, i.e. to any process bisimilar to $\mathbf{0}_{\tilde{q}}$.

The capacity to ignore discarded qubit is useful in a lot of proofs, as for the example below.

Example 4.17. The two distributions below are bisimilar

$$\Delta = \overline{\left\langle |\Phi^+\rangle\langle\Phi^+|\,, M_{01}(q_1 \rhd x).c!q_1 \parallel \mathbf{0}_{q_2}, \mathbf{0} \right\rangle} \text{ and } \Theta = \overline{\left\langle |\Phi^+\rangle\langle\Phi^+|\,, M_{\pm}(q_1 \rhd x).c!q_1 \parallel \mathbf{0}_{q_2}, \mathbf{0} \right\rangle}$$

Taken any $O[\,\cdot\,]$, they evolve in $O[\Delta']$ with $\Delta' = \left(\overline{\left\langle |00\rangle\langle 00|\,, c!q_1, \mathbf{0} \right\rangle} \;{}_{1/2}\!\oplus\; \overline{\left\langle |11\rangle\langle 11|\,, c!q_1, \mathbf{0} \right\rangle}\right) \parallel \mathbf{0}_{q_2}$ and $O[\Theta']$ with $\Theta' = \left(\overline{\left\langle |{+}{+}\rangle\langle{+}{+}|\,, c!q_1, \mathbf{0} \right\rangle} \;{}_{1/2}\!\oplus\; \overline{\left\langle |{-}{-}\rangle\langle{-}{-}|\,, c!q_1, \mathbf{0} \right\rangle}\right) \parallel \mathbf{0}_{q_2}$.

Finally, $\mathrm{tr}_{q_2}(\Delta') \sim_{cs} \mathrm{tr}_{q_2}(\Theta')$ holds because $\mathrm{tr}_{q_2}(\Delta') = \overline{\left\langle |0\rangle\langle 0|\,, c!q_1, \mathbf{0} \right\rangle} \;{}_{1/2}\!\oplus\; \overline{\left\langle |1\rangle\langle 1|\,, c!q_1, \mathbf{0} \right\rangle}$ and $\mathrm{tr}_{q_2}(\Theta') = \overline{\left\langle |+\rangle\langle +|\,, c!q_1, \mathbf{0} \right\rangle} \;{}_{1/2}\!\oplus\; \overline{\left\langle |-\rangle\langle -|\,, c!q_1, \mathbf{0} \right\rangle}$, and the two are equated by Theorem 4.8.

Finally, we report a general proof technique. While proving bisimilarity of two distributions usually requires giving a bisimulation relating the two, up-to techniques allows using smaller relations in place of proper bisimulations. Given a relation $\mathcal{R} \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$, its *convex hull* $Cv(\mathcal{R})$ is the least relation such that $(\sum_{i \in I} p_i \bullet \Delta_i)\ Cv(\mathcal{R})\ (\sum_{i \in I} p_i \bullet \Theta_i)$ whenever $\Delta_i\ \mathcal{R}\ \Theta_i$ for all $i \in I$. Bisimulations up to Cv [Bonchi et al. 2017] are then defined as follows.

Definition 4.18 (Bisimulation up to convex hull). A relation $\mathcal{R} \subseteq \mathcal{D}(Conf_{\bot}) \times \mathcal{D}(Conf_{\bot})$ is a *cs-bisimulation up to Cv* if $\Delta\, \mathcal{R}\, \Theta$ implies that for any context $O[\,\cdot\,]$ it holds

- $\Delta \downarrow_b^p$ if and only if $\Theta \downarrow_b^p$;
- whenever $O[\Delta] \rightsquigarrow_{\pi} \Delta'$, there exists Θ' such that $O[\Theta] \rightsquigarrow_{\pi} \Theta'$ and $\Delta'\ Cv(\mathcal{R})\ \Theta'$;
- whenever $O[\Theta] \rightsquigarrow_{\pi} \Theta'$, there exists Δ' such that $O[\Delta] \rightsquigarrow_{\pi} \Theta'$ and $\Delta'\ Cv(\mathcal{R})\ \Theta'$.

Giving a bisimulation up to convex hull is a sound proof technique for $\sim_{cs}$.

Proposition 4.19. *If $\Delta\ \mathcal{R}\ \Theta$ with $\mathcal{R}$ a bisimulation up to convex hull, then $\Delta \sim_{cs} \Theta$.*

Proof sketch. We need to show that *Cv* is *compatible* [Pous and Sangiorgi 2011], which follows from the linearity of barbs and from the fact that $\rightsquigarrow_{\pi}$ is decomposable. □

5 CONSTRAINED BISIMILARITY AT WORK

We discuss real-world protocols: quantum teleportation, superdense coding and quantum coin flipping. We show how lqCCS models them, and how $\sim_{cs}$ is used for proving their properties.

5.1 Quantum Teleportation

The objective of quantum teleportation [Bennett et al. 1993] is to allow Alice to send quantum information to Bob without a quantum channel. Alice and Bob must have each a qubit of an entangled pair $|\Phi^+\rangle$. The protocol works as follows: Alice performs a fixed set of unitaries to the qubit to transfer and to their part of the entangled pair; then Alice measures the qubits and sends the classical outcome to Bob, which applies different unitaries to their own qubit according to the received information. In the end, the qubit of Bob will be in the state of Alice's one, and the entangled pair is discarded. Note that Alice is not required to know the state of the qubit to send.

Consider the following encoding of the protocol where we assume that Alice (**A**) and Bob (**B**) already share an entangled pair (q_1, q_2) (we write $(n)_2$ to stress that n is in binary representation)

$$\begin{aligned}
\mathbf{A} &= \mathrm{CNOT}(q_0, q_1).\mathrm{H}(q_0).M_{01}(q_0, q_1 \triangleright x).(m!x \parallel \mathbf{0}_{q_0,q_1}) \\
\mathbf{B} &= m?y.\mathbf{if}\ y = (00)_2\ \mathbf{then}\ \mathrm{I}(q_2).out!q_2\ \mathbf{else}\ (\mathbf{if}\ y = (01)_2\ \mathbf{then}\ \mathrm{X}(q_2).out!q_2 \\
&\qquad \mathbf{else}\ (\mathbf{if}\ y = (10)_2\ \mathbf{then}\ \mathrm{Z}(q_2).out!q_2\ \mathbf{else}\ \mathrm{ZX}(q_2).out!q_2)) \\
\mathbf{Tel} &= (\mathbf{A} \parallel \mathbf{B}) \setminus m
\end{aligned}$$

We let $\Delta = \overline{\langle |\psi\Phi^+\rangle\!\langle\psi\Phi^+| , \mathbf{Tel}, \mathbf{0} \rangle}$, with $\Theta = \overline{\langle |\psi\Phi^+\rangle\!\langle\psi\Phi^+| , \mathrm{SWAP}(q_0, q_2).\tau.\tau.\tau.\tau.(out!q_2 \parallel \mathbf{0}_{q_0,q_1}, \mathbf{0} \rangle}$ its specification, for $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, and sketch the proof for $\Delta \sim_{cs} \Theta$ below.

Since there is no qubit in $|\psi\Phi^+\rangle\!\langle\psi\Phi^+|$ apart from the ones in $\Sigma_{\mathbf{Tel}}$, R is in deadlock for any context $O[\,\cdot\,] = [\,\cdot\,] \parallel R$. Thus, all subsequent transitions are of the kind $O[\Delta] \rightsquigarrow_{\diamond} O[\Delta']$ with $\Delta \rightsquigarrow_{\diamond} \Delta'$ until a send operation on an unrestricted channel is reached (and the same for Θ). For simplicity, we will therefore omit the contexts in the first steps

$$\begin{aligned}
\Delta &\rightsquigarrow_{\diamond}^{3} \sum_{i=0}^{3} \frac{1}{4} \bullet \overline{\langle |i\rangle\!\langle i| \otimes |\psi_i\rangle\!\langle\psi_i| , (m!i \parallel \mathbf{0}_{q_0,q_1} \parallel \mathbf{B}) \setminus m, \mathbf{0} \rangle} \\
&\rightsquigarrow_{\diamond}^{2} \Delta' = \sum_{i=0}^{3} \frac{1}{4} \bullet \overline{\langle |i\rangle\!\langle i| \otimes |\psi_i\rangle\!\langle\psi_i| , (\mathbf{0}_{q_0,q_1} \parallel out!q_2) \setminus m, R \rangle} \\
\Theta &\rightsquigarrow_{\diamond} \overline{\langle |\Phi^+\psi\rangle\!\langle\Phi^+\psi| , \tau.\tau.\tau.\tau.(out!q_2 \parallel \mathbf{0}_{q_0,q_1}), \mathbf{0} \rangle} \rightsquigarrow_{\diamond}^{4} \Theta' = \overline{\langle |\Phi^+\psi\rangle\!\langle\Phi^+\psi| , out!q_2 \parallel \mathbf{0}_{q_0,q_1}, R \rangle}
\end{aligned}$$

where $|\psi_0\rangle = |\psi\rangle$, $|\psi_1\rangle = \beta\,|0\rangle + \alpha\,|1\rangle$, $|\psi_2\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$, $|\psi_3\rangle = \beta\,|0\rangle - \alpha\,|1\rangle$, and where, abusing notation, we use $|0\rangle = |00\rangle, |1\rangle = |01\rangle, |2\rangle = |10\rangle$ and $|3\rangle = |11\rangle$ when speaking of pairs of qubits. All intermediate steps happen with the same label ($\diamond$) and no barb is expressed, as the channel m is restricted. Finally, since $out!q_2$ is a deterministic process, it is immediate to prove that $\mathrm{tr}_{q_0,q_1}(O[\Delta']) \sim_{cs} \langle |\psi\rangle\!\langle\psi| , out!q_2, R \rangle = \mathrm{tr}_{q_0,q_1}(O[\Theta'])$ by applying Theorem 4.8. The bisimilarity of Δ' and Θ' then follows from Proposition 4.16, therefore $\Delta \sim_{cs} \Theta$.

5.2 Superdense Coding

We consider a generalization of the superdense coding protocol [Bennett and Wiesner 1992]. Assume Alice and Bob have each a qubit of a Bell pair $|\Psi^+\rangle$. The protocol allows Alice to communicate a distribution of two-bit integers to Bob by sending their single qubit to Bob.

The protocol works as follows: Alice chooses a distribution of integers in $[0, 3]$ and encode it by performing suitable transformations to their qubit, which is then sent to Bob; Bob receives the qubit and decodes the distribution by performing CNOT and $\mathrm{H} \otimes \mathrm{I}$ on the pair of qubits (the received qubit and their original one), and then a measurement on the standard basis. By measuring the qubits, Bob recovers the distribution chosen by Alice, and can use it as they like.

We consider the following instantiation of the protocol, where Bob uses the received value to decide (in an unspecified way) on which channel to send the received qubit (either channel *a* or *b*)

$$\begin{aligned} \mathbf{A} &= \mathcal{E}(q_0).c!q_0 \\ \mathbf{B} &= c?x.\mathrm{CNOT}(x, q_1).\mathrm{H}(x).M(x, q_1 \rhd y).((a!x + b!x) \parallel \mathbf{0}_{q_1}) \\ \mathbf{SDC} &= \mathbf{A} \parallel \mathbf{B} \setminus c \end{aligned}$$

More in detail, Alice encodes: the point distribution $\bar{0}$ by applying the unitary I, $\bar{1}$ with X, $\bar{2}$ with Z, and $\bar{3}$ with ZX. In general, they apply a superoperator $\mathcal{E}$ with Kraus decomposition

$$\{\sqrt{p_0}I, \sqrt{p_1}X, \sqrt{p_2}Z, \sqrt{p_3}ZX\} \quad \text{for some } p_i \in [0,1] \text{ such that } \sum\nolimits_i p_i = 1$$

Consider now the following where Rob (in place of Bob) forgets to measure the qubits

$$\mathbf{R} = c?x.\mathrm{CNOT}(x, q_1).\mathrm{H}(x).\tau.((a!x + b!x) \parallel \mathbf{0}_{q_1})$$

Ideally, Rob cannot base their decision on the value sent by Alice, hence we expect **SDC** to be distinguishable from the case where **R** is substituted for *Bob*. Indeed, $\overline{\langle |\Psi^+\rangle\langle\Psi^+|, \mathbf{A} \parallel \mathbf{B} \setminus c \rangle}$ and $\overline{\langle |\Psi^+\rangle\langle\Psi^+|, \mathbf{A} \parallel \mathbf{R} \setminus c \rangle}$ are not constrained bisimilar in general. Consider, for example, $\mathcal{E}$ with Kraus decomposition $\{\frac{1}{2}\mathrm{I}, \frac{1}{2}\mathrm{X}, \frac{1}{2}\mathrm{Z}, \frac{1}{2}\mathrm{ZX}\}$ (i.e. Alice encodes a fair distribution of all the possible values).

Assume we always take the empty observer $O[\cdot] = [\cdot]$ whenever we do not specify otherwise, and note that the following steps are forced

$$\begin{aligned} \overline{\langle |\Psi^+\rangle\langle\Psi^+|, \mathbf{SDC} \rangle} &\rightsquigarrow_{\diamond} \overline{\langle \rho, c!q_0 \parallel \mathbf{B} \setminus c \rangle}, \text{ with } \rho = \frac{1}{4}\left(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right) \\ &\rightsquigarrow_{\diamond} \overline{\langle \rho, \mathrm{CNOT}(q_0, q_1).\mathrm{H}(q_0).M(q_0, q_1 \rhd y).((a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1}) \setminus c \rangle} \\ &\rightsquigarrow_{\diamond}^{2} \overline{\langle \frac{1}{4}I, M(q_0, q_1 \rhd y).((a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1}) \setminus c \rangle} \rightsquigarrow_{\diamond} \Delta_{\mathbf{B}} \end{aligned}$$

where $\Delta_{\mathbf{B}}$ is defined as

$$\sum\nolimits_{j=0}^{3} \frac{1}{4} \bullet \overline{\langle |j\rangle\langle j|, (a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1} \rangle}$$

Similarly, for Rob we have that the following are forced

$$\begin{aligned} \overline{\langle |\Psi^+\rangle\langle\Psi^+|, \mathbf{A} \parallel \mathbf{R} \setminus c \rangle} &\rightsquigarrow_{\diamond} \overline{\langle \rho, c!q_0 \parallel \mathbf{R} \setminus c \rangle} \\ &\rightsquigarrow_{\diamond} \overline{\langle \rho, \mathrm{CNOT}(q_0, q_1).\mathrm{H}(q_0).\tau.((a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1}) \setminus c \rangle} \\ &\rightsquigarrow_{\diamond}^{2} \overline{\langle \frac{1}{4}I, \tau.((a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1}) \setminus c \rangle} \rightsquigarrow_{\diamond} \Delta_{\mathbf{R}} = \overline{\langle \frac{1}{4}I, (a!q_0 + b!q_0) \parallel \mathbf{0}_{q_1} \rangle} \end{aligned}$$

Take now the following context

$$O'[\cdot] = [\cdot] \parallel a?z.M(z \rhd res)(\textbf{if } res = 0 \textbf{ then } success!z \textbf{ else } fail!z + b?z.\tau.\mathbf{0}_z)$$

and assume $O'[\Delta_{\mathbf{B}}]$ evolves as

$$\begin{aligned} &\frac{1}{4} \bullet \overline{\langle |00\rangle\langle 00|, \mathbf{0}_{q_1}, \mathbf{0} \parallel M(q_0 \rhd res)(\textbf{if } res = 0 \textbf{ then } success!z \textbf{ else } fail!z \rangle} \\ +\, &\frac{1}{4} \bullet \overline{\langle |01\rangle\langle 01|, \mathbf{0}_{q_1}, \mathbf{0} \parallel M(q_0 \rhd res)(\textbf{if } res = 0 \textbf{ then } success!z \textbf{ else } fail!z \rangle} \\ +\, &\frac{1}{4} \bullet \overline{\langle |10\rangle\langle 10|, \mathbf{0}_{q_1}, \mathbf{0} \parallel \tau.\mathbf{0}_{q_0} \rangle} + \frac{1}{4} \bullet \overline{\langle |11\rangle\langle 11|, \mathbf{0}_{q_1}, \mathbf{0} \parallel \tau.\mathbf{0}_{q_0} \rangle} \end{aligned}$$

After a reduction, $O'[\Delta_{\mathbf{B}}]$ expresses the barbs *success* and *fail* with probability 1/2 and 0 respectively.

On the contrary, $O'[\Delta_{\mathbf{R}}]$ may only evolve as either

$$\overline{\left\langle \frac{1}{4}I, \mathbf{0}_{q_1}, \mathbf{0} \parallel M(q_0 \rhd \text{res})(\mathbf{if}\ \text{res} = 0\ \mathbf{then}\ \mathit{success}!z\ \mathbf{else}\ \mathit{fail}!z \right\rangle} \quad \text{or} \quad \overline{\left\langle \frac{1}{4}I, \mathbf{0}_{q_1}, \mathbf{0} \parallel \tau.\mathbf{0}_{q_0} \right\rangle},$$

and, after a reduction, must express both the barbs *success* and *fail* with either probability 1/2 or 0.

This important result is due to the Theorem 4.12, which allows **B** to behave as if any boolean conditional was in place of +, thus to send the qubit on a if the outcome of the measurement is strictly lower than 2, and on b otherwise. The other proposed behavioural equivalences for addressing the problem of the standard probabilistic bisimilarity deem the two distributions indistinguishable (see section 6 for an in depth comparison).

5.3 Quantum Coin Flipping

We present now a more complex example, namely the Quantum Coin Flipping (QCF) protocol. Suppose Alice and Bob do not trust each other, and want to randomly select a winner between them. Bennet and Brassard [2014] propose a protocol in which Alice chooses either the 01 or ± basis at random, then generates a sequence of random bits and encodes them into a sequence of qubits in the selected basis (the first element of the basis stands for bit 0, the second for 1). The qubits are then sent to Bob, who measures each of them in a random basis (01 or ±). Finally, Bob tries to guess the basis chosen by Alice: Bob wins if the guess is correct.

Bob has no way to find Alice's basis from the received qubits, so the guess will be correct or wrong with equal probability. Alice could cheat, lying about their basis. To protect Bob, at the end of the protocol, Alice must reveal their basis and the original bit sequence. Bob then compares the original sequence with the previously stored outcomes of the measurements. For qubits where Alice's basis coincides with Bob's one, the outcomes must coincide with the original bit sequence.

Hereafter, we let x_i be the i-th bit of the integer x, and resort to some minor extensions of lqCCS

- $\langle \rho, \mathit{RandBit}(x).P \rangle$ evolves as $\overline{\langle \rho, P[0/x] \rangle}\ {}_{1/2}{\oplus}\ \overline{\langle \rho, P[1/x] \rangle}$, and could be implemented with an additional qubit.
- We assume a mapping β from bit to bases with $\beta(0)$ and $\beta(1)$ the 01 and ± basis.
- We assume a polyadic extension of lqCCS type system and semantics where $c!\tilde{v}$ and $c?\tilde{x}$ allow substituting tuples of values $\tilde{v} = v_1, \ldots, v_n$ for variables $\tilde{x} = x_1, \ldots, x_n$.

We formalize QCF as follows, where n is the number of qubits, and the outcome is sent on a and b (1 if Bob wins and 0 otherwise). We use $b =_{int} b'$ for comparing digits, defined as $(1-b)(1-b')+bb'$.

$$\begin{aligned}
\mathbf{Alice} &= \mathit{Rand}(\text{secretvalue}).\mathbf{Alice}_{\beta(\text{secretvalue})}\\
\mathbf{Alice}_{01} &= \mathrm{H}(\tilde{q}).M_{01}(\tilde{q} \rhd w).(\mathit{AtoB}!\tilde{q} \parallel \mathit{guess}?g.(a!(g =_{int} 0) \parallel \mathit{secret}!0 \parallel \mathit{witness}!w))\\
\mathbf{Alice}_{\pm} &= I(\tilde{q}).M_{\pm}(\tilde{q} \rhd w).(\mathit{AtoB}!\tilde{q} \parallel \mathit{guess}?g.(a!(g =_{int} 1) \parallel \mathit{secret}!1 \parallel \mathit{witness}!w))\\
\mathbf{Bob} &= \mathit{AtoB}?\tilde{z}.\left(\left(\left(\Big\|_{i=1}^{n} \mathbf{Server}_i\right) \parallel \mathbf{Bob}'\right) \setminus \{\mathit{base}_i\}_{i=1}^{n} \setminus \{\text{bit}_i\}_{i=1}^{n}\right)\\
\mathbf{Bob}' &= \mathit{base}_1?b_1 \ldots \mathit{base}_n?b_n.\mathit{bit}_1?x_1 \ldots \mathit{bit}_n?x_n.\mathit{Rand}(g).(\mathit{guess}!g \parallel \mathbf{Bob}'')\\
\mathbf{Bob}'' &= \mathit{secret}?g'.\mathit{witness}?w.\left(b!(g =_{int} g') \parallel \left(\Big\|_{i=1}^{n} \mathbf{if}\ (b_i = g' \wedge x_i \neq w_i\ \mathbf{then}\ \mathit{cheat}!0\ \mathbf{else}\ \mathbf{0}\right)\right)\\
\mathbf{Server}_i &= \mathit{Rand}(b).M_{\beta(b)}(z_i \rhd x).(\mathit{base}_i!b \parallel \mathit{bit}_i!x \parallel \mathbf{0}_{z_i})\\
\mathbf{QCF} &= (\mathbf{Alice} \parallel \mathbf{Bob}) \setminus \{\mathit{AtoB}, \mathit{guess}, \mathit{secret}, \mathit{witness}\}
\end{aligned}$$

Thanks to cs-bisimilarity, we can analyse three properties of QCF, namely that the outcome is fair, that Bob cannot cheat, and neither Alice can. As reported by Bennet and Brassard [2014], the first two properties hold, but an attack exists allowing Alice to decide the outcome of the protocol.

Fairness. We show that $\langle |0^n\rangle\langle 0^n| , \mathbf{QCF} \rangle \sim_{cs} \langle |0^n\rangle\langle 0^n| , \mathbf{FairCoin} \rangle$, with **FairCoin** defined as $\tau^{4n+5}.Rand(x).(a!x \parallel \tau.\tau.b!x \parallel \mathbf{0}_{\tilde{q}})$. As before, it suffices to consider the empty context, and we show the evolution of the protocol for $n = 1$, as the other cases follow the same pattern.

$$\langle |0\rangle\langle 0| , \mathbf{QCF} \rangle \rightsquigarrow_{\diamond} \left(\overline{\langle |0\rangle\langle 0| , \mathbf{Alice}_{01} \parallel \mathbf{Bob} \rangle} \;{}_{\frac{1}{2}}\!\oplus \overline{\langle |0\rangle\langle 0| , \mathbf{Alice}_{\pm} \parallel \mathbf{Bob} \rangle} \right) \setminus C$$

where $C = \{AtoB, guess, secret, witness\}$. We will focus just on the execution of $Alice_{01}$, as the other one is symmetrical. The first actions of Alice are to prepare the qubit at random and send it to Bob. The latter will then measure it in a random basis and record the result. Formally

$$\begin{aligned}
&\langle |0\rangle\langle 0| , \mathbf{Alice}_{01} \parallel \mathbf{Bob} \rangle \\
&\rightsquigarrow_{\diamond}^{3} \sum\nolimits_{j\in\{0,1\}} \frac{1}{2} \bullet \overline{\langle |j\rangle\langle j| , \mathbf{Alice}'_{01}[j/w] \parallel \mathbf{Bob}' \parallel \mathbf{Server} \rangle} \\
&\rightsquigarrow_{\diamond}^{2} \quad \frac{1}{2} \bullet \left(\sum\nolimits_{j\in\{0,1\}} \frac{1}{2} \bullet \overline{\langle |j\rangle\langle j| , \mathbf{Alice}'_{01}[j/w] \parallel \mathbf{Bob}' \parallel (base!0 \parallel bit!j \parallel \mathbf{0}_q) \rangle} \right) \\
&\qquad + \frac{1}{2} \bullet \left(\sum\nolimits_{j\in\{0,1\}} \frac{1}{2} \bullet \overline{\langle H\,|j\rangle\langle j|\,H, \mathbf{Alice}'_{01}[j/w] \parallel \mathbf{Bob}' \parallel (base!1 \parallel bit!j \parallel \mathbf{0}_q) \rangle} \right)
\end{aligned}$$

where $\mathbf{Alice}'_{01} = guess?g.(a!(g =_{int} 0) \parallel secret!0 \parallel witness!w)$. After the measurement (and after synchronsing with the server processes) Bob send their random guess of the secret basis to Alice, who reveals the correct one. Bob checks the consistency of Alice response, and if the protocol is executed correctly the two parties will agree on the outcome: either 0 or 1 with equal probability.

$$\begin{aligned}
&\frac{1}{2} \bullet \left(\sum\nolimits_{j,k\in\{0,1\}} \frac{1}{4} \bullet \overline{\langle |j\rangle\langle j| , \mathbf{0}_q \parallel \mathbf{Alice}'_{01}[j/w] \parallel guess!k \parallel \mathbf{Bob}''[0/b][j/x][k/g] \rangle} \right) \\
&+ \frac{1}{2} \bullet \left(\sum\nolimits_{j,k\in\{0,1\}} \frac{1}{4} \bullet \overline{\langle H\,|j\rangle\langle j|\,H, \mathbf{0}_q \parallel \mathbf{Alice}'_{01}[j/w] \parallel guess!k \parallel \mathbf{Bob}''[1/b][j/x][k/g] \rangle} \right) \\
&\rightsquigarrow_{\diamond}^{3} \left(\sum\nolimits_{j,k\in\{0,1\}} \frac{1}{4} \bullet \overline{\langle |j\rangle\langle j| , \mathbf{0}_q \parallel a!k \parallel b!k \rangle} \right) {}_{\frac{1}{2}}\!\oplus \left(\sum\nolimits_{j,k\in\{0,1\}} \frac{1}{4} \bullet \overline{\langle H\,|j\rangle\langle j|\,H, \mathbf{0}_q \parallel a!k \parallel b!k \rangle} \right)
\end{aligned}$$

It is easy to see that in this last step **QCF** expresses the barbs $\downarrow a$ and $\downarrow b$, sending the same values as the specification **FairCoin**, and the two are indeed bisimilar.

Dishonest Bob. In order to cheat, Bob needs to discover Alice's secret from the sent qubits alone. This is impossible, because Theorem 4.8 deems the initial prefixes of $\mathbf{Alice}_{01}$ and $\mathbf{Alice}_{\pm}$ bisimilar.

$$\mathbf{A}_{01} = \sum\nolimits_{j=0}^{2^n-1} \frac{1}{2^n} \bullet \langle |j\rangle\langle j| , AtoB!\tilde{q} \rangle \quad \sim_{cs} \quad \sum\nolimits_{j=0}^{2^n-1} \frac{1}{2^n} \bullet \langle H^{\otimes n}\,|j\rangle\langle j|\,H^{\otimes n}, AtoB!\tilde{q} \rangle = \mathbf{A}_{\pm}$$

Note that $A_{01} \nsim_s A_{\pm}$, as shown in Example 4.1. Traditional probabilistic bisimilarity à la Hennessy [2012] fails in analysing Quantum Coin Flipping and similar protocols.

Dishonest Alice. Interestingly, Alice can cheat by using additional qubits entangled with the ones they sends to Bob. By measuring their entangled qubits in Bob's chosen basis, Alice forges a fake witness for deceiving Bob (in the process, Alice wins and 0 is sent on a and b). We call this attacker Alison, and show that $\langle |0^{2n}\rangle\langle 0^{2n}| , (\mathbf{Alison} \parallel \mathbf{Bob}) \setminus C \rangle \sim_{cs} \langle |0^{2n}\rangle\langle 0^{2n}| , \mathbf{UnfairCoin} \rangle$.

$$\begin{aligned}
\mathbf{Alison} &= Set_{\Phi^+}(q_1, q'_1) \ldots Set_{\Phi^+}(q_n, q'_n).\, (AtoB!\tilde{q} \parallel \mathbf{Alison}') \\
\mathbf{Alison}' &= guess?g.(a!0 \parallel secret!(1-g) \parallel M_{\beta(1-g)}(q' \rhd x').(witness!x' \parallel \mathbf{0}_{\tilde{q}'})) \\
\mathbf{UnfairCoin} &= \tau^{5n+3}.(a!0 \parallel \tau.\tau.\tau.b!0 \parallel \mathbf{0}_{\tilde{q}} \parallel \mathbf{0}_{\tilde{q}'})
\end{aligned}$$

The **UnfairCoin** specification always selects Alison as the winner, and never expresses the $\downarrow_{cheat}$ barb. In other words, $(\mathbf{Alison} \parallel \mathbf{Bob}) \setminus C \sim_{cs} \mathbf{UnfairCoin}$ means that Alison is always capable of tricking Bob without being discovered.

The behaviour of Bob is identical to the previous case. Indeed, the reduced density operator of the qubits sent by Alison is indistinguishable from the one of the honest Alice. But after receiving Bob's guess, Alison can measure their own qubits, which have decayed as the ones of Bob. In this way, her fake witness w' will always be correct, as we show for the case $n = 1$

$$\begin{aligned}&\langle |00\rangle\langle 00|, (\mathbf{Alison} \parallel \mathbf{Bob}) \setminus C \rangle \\ &\rightsquigarrow^{11}_{\diamond} \left(\sum_{j \in \{0,1\}} \frac{1}{2} \bullet \overline{\langle |jj\rangle\langle jj|, \mathbf{0}_q \parallel a!0 \parallel b!0 \rangle} \right) {}_{\frac{1}{2}}\!\oplus \left(\sum_{j \in \{+,-\}} \frac{1}{2} \bullet \overline{\langle |jj\rangle\langle jj|, \mathbf{0}_q \parallel a!0 \parallel b!0 \rangle} \right)\end{aligned}$$

6 RELATED WORKS

We focus on the quantum process calculi most similar to our proposal, as well as likely the better established and developed, namely QPAlg [Lalire 2006; Lalire and Jorrand 2004], CQP [Davidson 2012; Gay and Nagarajan 2005, 2006], and qCCS [Deng 2018; Deng and Feng 2012; Feng et al. 2014, 2007, 2012; Feng and Ying 2015; Ying et al. 2009]. When comparing the proposed behavioural equivalences, we abstract from the "classical" details and focus on the quantum-related features, restricting ourselves to the strong version of the bisimulations. A first difference with lqCCS is that they are mostly based on labelled bisimilarities. Table 1 summarizes distinctive prototypical processes (in the lqCCS syntax) deemed bisimilar or not according to different approaches.

One of the discrepancies is the visibility of qubits that are neither sent nor discarded. The first three lines contain processes whose bisimilarity depends on the assumption about the visibility of these unsent qubits. Our linear type system makes the former assumptions irrelevant. In the fourth line, the processes send pairs of qubits with the same partial trace if taken separately, even if a pair is entangled and the other is not. The fifth line compares processes where the state of the sent qubits is represented by the same density operator, whose bisimilarity is implied by Theorem 4.8. Finally, the sixth line compares two processes where a qubit is sent non-deterministically over two channels: for each channel, the state of the sent qubits is represented by the same density operator, but if the chosen channel depends on the outcome of the measurement the two processes can be distinguished. Bisimilarities that do not distinguish these two processes cannot satisfy Theorem 4.12.

6.1 QPAlg

The Quantum Process Algebra (QPAlg) is an extension of synchronous value-passing CCS with primitives for unitary transformations and measurements. As common, quantum operations are silent, and quantum communication updates quantum variables. They propose a probabilistic branching bisimilarity, adapted for stateful computations by requiring bisimilar processes to send the same quantum state, defined as the partial trace of the global quantum state. However, this bisimilarity is coarser than prescribed by the theory when states are entangled [Davidson 2012].

Example 6.1. The processes in the fourth line of Table 1 are bisimilar in QPAlg, as they send pairs of qubits with the same partial trace ($tr_{q_0}(\Phi^+) = tr_{q_1}(\Phi^+) = tr_{q_0}(\frac{1}{4}I) = tr_{q_1}(\frac{1}{4}I) = \frac{1}{2}I$). Such processes are not bisimilar according to $\sim_{cs}$, as the context of Example 3.10 discriminates the two.

Finally, behaviourally equivalent processes are not required to behave similarly on unsent qubits, e.g. $H(q).\mathbf{0}$ and $X(q).\mathbf{0}$ of the first line of Table 1. In lqCCS, the above processes are not legal, but a similar result holds for $H(q).\mathbf{0}_q$ and $X(q).\mathbf{0}_q$.

6.2 CQP

The calculus of Communicating Quantum Processes (CQP) is inspired by the π-calculus and it is enriched with qubits declarations (that extend the quantum state) and quantum transformations, but without guards or match operators, thus lacking the form of classical control used in lqCCS. They introduce an affine type system prescribing that every qubit is sent at most once. CQP comes with a reduction semantics [Gay and Nagarajan 2005, 2006] and a labelled one [Davidson 2012], both based on pure quantum states. Davidson proposes mixed configurations, i.e. configurations where a single process is paired with a probability distribution of classical and quantum states. Mixed configurations represent non-observable probabilities due to measurements whose result is not communicated yet, and they are treated as a single state by the semantics. Our proposal generalizes CQP mixed configurations to distributions of configurations with possibly different processes. This is necessary for extending the approach to processes with boolean guards.

A branching bisimilarity is defined for the labelled semantics of CQP. To avoid the problem of QPAlg with entangled states, bisimilarity requires that the reduced state obtained by collecting *all* the sent qubits coincide. Moreover, mixed configurations allow relating processes sending indistinguishable quantum states. The resulting bisimilarity is a congruence for parallel composition and is capable of equating interesting cases such as the one of the fifth line of Table 1.

Example 6.2. Consider $\langle |+\rangle\langle+| \, , M_{01}(q \rhd x)).c!q \rangle$ and $\langle |0\rangle\langle 0| \, , M_{\pm}(q \rhd x).c!q \rangle$. Even though they end up in different quantum states, the two configurations above are bisimilar according to CQP, because they send on channel c qubits with the same partial trace. Our proposed bisimilarity replicates this result by resorting to contexts with constrained non-determinism (see Example 4.6). Indeed, a context receiving the qubit cannot behave differently depending on its state if not through measurement, and when measured, the states of the two qubits coincide.

Our cs-bisimilarity extends the one of CQP in a context-based fashion over standard distributions. CQP behaves as QPAlg with respect to unsent qubits (see the first line of Table 1).

6.3 qCCS

Our process calculus takes its most direct inspiration from qCCS, a synchronous CCS-style calculus with superoperators and measurements where syntactic restrictions guarantee each qubit is sent at most once. A feature of qCCS is the support for recursive processes, which we postpone to future work. Two different labelled bisimilarities are proposed for qCCS: the first is based on standard probabilistic bisimulations; the second one relies on transition consistency and subdistributions.

The probabilistic bisimilarity [Feng et al. 2007, 2012] (denoted by $\sim_p$ in Table 1) requires bisimilar processes to send the same names on the same channels and to produce the same quantum state of qubits that are not owned any more. In addition, bisimulations must be closed under applications of trace-preserving superoperators on not-owned qubits. Therefore, the processes of the first line of Table 1 are distinguished. We recover this assumption by sending the qubits (see the third line).

Moreover, Proposition 4.14 shows that cd-bisimilarity replicates the $\sim_p$ requirements over superoperators and not owned qubits. The probabilistic bisimilarity of qCCS is proved to be a congruence with respect to parallel composition. Further extensions are the (weak) open bisimilarity proposed in Deng and Feng [2012], proven to be a weak barbed congruence, and a symbolic version of the bisimilarity in Feng et al. [2014], that relieves from considering all the (universally quantified) quantum states of a configuration when verifying bisimilarity.

Configurations like the ones of the fifth line of Table 1 are not bisimilar for $\sim_p$, even though they are indistinguishable according to quantum theory. This discrepancy was signalled in Kubota et al. [2012] and lead to a new proposal called distribution bisimilarity [Deng 2018; Feng and Ying 2015] (denoted by $\sim_d$ in Table 1), which is directly defined on distributions and is based on transition consistency. A distribution is called transition consistent if any configuration in its support has exactly the same set of enabled visible actions. In addition to closure with respect to superoperator application, bisimilar distributions are required to be such that: (i) the weighted sums of the state of not owned qubits in the support coincide; (ii) the possible transitions of one transition consistent distribution are matched by the other one, and; (iii) if the distributions are not transition consistent, then they must be decomposable in bisimilar transition consistent distributions. On the one hand, considering distributions as a whole when comparing the quantum states equates processes like the ones of the fifth line of Table 1. On the other hand, transition consistent decompositions recover a weakened version of decomposability, avoiding equating distributions that cannot evolve because the processes in the supports enable different actions only.

The use of transition consistency in $\sim_d$ implicitly constrains non-determinism. In the last line of Table 1, we compare such constraints with the ones we impose on lqCCS. While our $\sim_{cs}$ is capable of distinguishing the two processes, $\sim_d$ cannot. In fact, the lifting of the *labelled* semantics of qCCS forbids processes from replicating the moves of their refinements (as lqCCS does).

Example 6.3. Consider the pair of processes of the last line of Table 1. They reduce to

$$\Delta = \overline{\left\langle |0\rangle\langle 0|\,, c!q + d!q \right\rangle}\ {}_{1/2}{\oplus}\ \overline{\left\langle |1\rangle\langle 1|\,, c!q + d!q \right\rangle} \qquad \Theta = \overline{\left\langle |+\rangle\langle +|\,, c!q + d!q \right\rangle}\ {}_{1/2}{\oplus}\ \overline{\left\langle |-\rangle\langle -|\,, c!q + d!q \right\rangle}$$

We show in Example 4.13 that $\Delta \not\sim_{cs} \Theta$, as Δ can choose to send the qubit over c only when it is set to $|0\rangle$, while Θ cannot. In the distribution bisimulation of Feng and Ying [2015], instead, only the moves that choose the same channel in all the configurations of the support are considered, deeming the two distributions bisimilar. This means that $M_{01}(q \triangleright x).(c!q + d!q)$ cannot use the value of x to choose the channel over which to send, as it would be expected, and thus that the constraints over non-determinism are arguably too strong in Feng and Ying [2015].

Finally, Feng and Ying [2015] acknowledge that *weak* distribution bisimilarity is not a congruence. Its strong version is not a congruence either: take $\Delta \sim_d \Theta$ and $B[\,\cdot\,]$ of Example 4.1, it is easy to show that $B[\Delta] \not\sim_d B[\Theta]$. The same also holds for $\sim_{cs}$, which is a congruence with respect to observers but not to parallel composition. We believe that $\sim_d$ actually verifies the indistinguishability property over deterministic processes of Theorem 4.8, and $B[\Delta] \not\sim_d B[\Theta]$ shows that the result cannot be extended to general processes. On a similar note, $\sim_d$ does not preserve the expressiveness of non-deterministic choices based on classical information stated in Theorem 4.12.

7 CONCLUSIONS AND FUTURE WORK

We presented lqCCS, a quantum process calculus with asynchronous communication and a linear type system guaranteeing that each qubit is sent or discarded *exactly* once. The latter lifts the semantics from making arbitrary assumptions about the observability of unsent qubits, which was a discrepancy among related works.

The main result of this work is a novel stateful reduction semantics together with a saturated probabilistic bisimilarity that relies on contexts for distinguishing quantum processes. These choices allowed us to investigate and compare the discriminating capabilities of the bisimilarity against the principles of quantum theory. By employing standard contexts, we found that the problems highlighted by Davidson [2012] and Kubota et al. [2012] are caused by the interaction between non-determinism and quantum features. In particular the standard notion of non-determinism subverts a defining feature of quantum theory by allowing contexts to perform moves based on the possibly unknown quantum state, without performing a measurement and thus perturbing it. We enhanced the semantics of lqCCS and constrained non-determinism by requiring the contexts to perform the same move in all the configurations of a given distribution (when no classical branching is possible). The resulting bisimilarity relation is strictly coarser than the unconstrained one.

We prove two main properties: (i) indistinguishability of quantum states can be lifted to classes of bisimilar distributions of lqCCS configurations; and (ii) non-deterministic choices can perform moves according to known classical values, simulating the semantics of boolean guards. Intuitively, the first guarantees that constraints are indeed sufficient to prevent non-determinism from subverting quantum features, while the second ensures that constraints are not too restrictive. Moreover, we showed by counterexample in Table 1 that no bisimilarity in the literature satisfies both of them.

Furthermore, we proved that the novel bisimilarity is linear with respect to probabilistic composition, and closed for superoperator application on qubits not appearing in the processes, which are also required to be equal in bisimilar distributions. Moreover, discarded qubits can be "traced out" without affecting bisimilarity. An up-to technique is given to aid bisimilarity proofs. We tested our approach by modeling and analysing three real-world protocols. Finally, we compared our findings with previously proposed bisimilarities, using simple prototypical cases that highlights dinstinguishability features required by quantum theory.

Discussion. Our work starts with an example-based analysis of the proposed bisimilarities and their adherence to expected indistinguishability results prescribed by quantum theory. Through our analysis, we identify some desired properties that we later prove for our proposed bisimilarity (mainly, Theorem 4.8 and Theorem 4.12). Bisimilarities for quantum processes are difficult to justify and validate, as we have no touchstone but the prescriptions of quantum mechanics about what can be operationally distinguished. Our set of examples and the properties they suggest help with this problem, and they are sufficient to tell apart cs-bisimilarity and the previous proposals.

We opted to work with a well established and fairly standard calculus, limiting changes to the ones needed for addressing the problems at hand. Thus, we left unaltered the semantics of processes, only restricting the behaviour of observers, and we stick with a classical probabilistic approach.

Alternative approaches may be considered. One could characterise feasible non-deterministic choices in general, constraining them also in processes. Unfortunately, the expressivity of processes would be weaker than the ones considered in the related works, since this approach may result in overly constrained processes, thus making the comparison less direct. Otherwise, one could look for a more suitable notion of *quantum* distribution that naturally satisfy the desired properties of indistinguishability, similarly to what is done by Davidson [2012] and Feng et al. [2014].

Both these approaches seem promising follow-ups for our work, that can serve as a preliminary investigation on how process semantics should be changed to accommodate to quantum theory.

Future Work. One aim of our future work is to extend lqCCS, namely with qubit declaration primitives and recursive processes. We will also explore weak versions of the constrained bisimilarity, as done by Feng et al. [2007] and Davidson [2012], and enhanced proof methodologies, i.e. by investigating pruning techniques and by looking for an equivalent labelled bisimulation, following the approach of Bonchi et al. [2014]. The advantage would be two-fold: to avoid the universal quantification over contexts and to identify an adequate set of observable properties.

Moreover, we will further investigate some of the shortcomings of probabilistic bisimulation with respect to non-determinism. The solution presented in this work is only one of many possible approaches, where non-determinism is unconstrained in the processes and constrained in the contexts. An alternative approach is to characterize feasible choices in general, constraining non-determinism also in processes, by taking into account all the legit reasons for configurations of the same distribution to behave differently. We guess this will give a bisimilarity that is a congruence and that still satisfies our desired properties, something which is missing among current proposals.

Finally we will investigate how spurious non-deterministic moves impact on model checking when applied to quantum systems.

DATA AVAILABILITY STATEMENT

The extended version of this work, featuring the full proofs, is available at [Ceragioli et al. 2023].

ACKNOWLEDGMENTS

This study was carried out within the National Centre on HPC, Big Data and Quantum Computing - SPOKE 10 (Quantum Computing) and received funding from the European Union Next-GenerationEU - National Recovery and Resilience Plan (NRRP) – MISSION 4 COMPONENT 2, INVESTMENT N. 1.4 – CUP N. I53C22000690001.

REFERENCES

Charles H. Bennet and Gilles Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025 Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. 1993. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* 70 (1993), 1895–1899. Issue 13. https://doi.org/10.1103/PhysRevLett.70.1895

Charles H. Bennett and Stephen J. Wiesner. 1992. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* 69 (Nov 1992), 2881–2884. Issue 20. https://doi.org/10.1103/PhysRevLett.69.2881

Filippo Bonchi, Fabio Gadducci, and Giacoma Valentina Monreale. 2014. A General Theory of Barbs, Contexts, and Labels. *ACM Transactions on Computational Logic* 15, 4 (2014), 1–27. https://doi.org/10.1145/2631916

Filippo Bonchi, Alexandra Silva, and Ana Sokolova. 2017. The Power of Convex Algebras. In *28th International Conference on Concurrency Theory (CONCUR 2017) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 85)*, Roland Meyer, Uwe Nestmann, and Marc Herbstritt (Eds.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 23:1–23:18. https://doi.org/10.4230/LIPICS.CONCUR.2017.23

Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2023. Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-Deterministic Observers. https://doi.org/10.48550/arXiv.2311.06116

Timothy A. S. Davidson. 2012. *Formal Verification Techniques Using Quantum Process Calculus*. Ph. D. Dissertation. University of Warwick. http://wrap.warwick.ac.uk/51368/

Pierpaolo Degano and Corrado Priami. 2001. Enhanced operational semantics. *ACM Computing Survey* 33, 2 (2001), 135–176. https://doi.org/10.1145/384192.384194

Yuxin Deng. 2018. Bisimulations for Probabilistic and Quantum Processes (Invited Paper). In *29th International Conference on Concurrency Theory, CONCUR 2018, September 4-7, 2018, Beijing, China (LIPIcs, Vol. 118)*, Sven Schewe and Lijun Zhang (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2:1–2:14. https://doi.org/10.4230/LIPIcs.CONCUR.2018.2

Yuxin Deng and Yuan Feng. 2012. Open Bisimulation for Quantum Processes. In *Theoretical Computer Science - 7th IFIP TC 1/WG 2.2 International Conference, TCS 2012, Amsterdam, The Netherlands, September 26-28, 2012. Proceedings (Lecture Notes in Computer Science, Vol. 7604)*, Jos C. M. Baeten, Thomas Ball, and Frank S. de Boer (Eds.). Springer, 119–133. https://doi.org/10.1007/978-3-642-33475-7_9

Yuan Feng, Yuxin Deng, and Mingsheng Ying. 2014. Symbolic Bisimulation for Quantum Processes. *ACM Transactions on Computational Logic* 15, 2 (2014), 14:1–14:32. https://doi.org/10.1145/2579818

Yuan Feng, Runyao Duan, Zhengfeng Ji, and Mingsheng Ying. 2007. Probabilistic Bisimulations for Quantum Processes. *Information and Computation* 205, 11 (2007), 1608–1639. https://doi.org/10.1016/j.ic.2007.08.001

Yuan Feng, Runyao Duan, and Mingsheng Ying. 2012. Bisimulation for Quantum Processes. *ACM Transactions on Programming Languages and Systems* 34, 4 (2012), 17:1–17:43. https://doi.org/10.1145/2400676.2400680

Yuan Feng and Mingsheng Ying. 2015. Toward Automatic Verification of Quantum Cryptographic Protocols. In *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015 (LIPIcs, Vol. 42)*, Luca Aceto and David de Frutos-Escrig (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 441–455. https://doi.org/10.4230/LIPIcs.CONCUR.2015.441

Simon J. Gay and Rajagopal Nagarajan. 2005. Communicating quantum processes. In *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2005, Long Beach, California, USA, January 12-14, 2005*, Jens Palsberg and Martín Abadi (Eds.). ACM, 145–157. https://doi.org/10.1145/1040305.1040318

Simon J. Gay and Rajagopal Nagarajan. 2006. Types and Typechecking for Communicating Quantum Processes. *Mathematical Structures in Computer Science* 16, 3 (2006), 375–406. https://doi.org/10.1017/S0960129506005263

Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. 2009. Quantum Algorithm for Linear Systems of Equations. *Physical Review Letters* 103, 15 (2009). https://doi.org/10.1103/PhysRevLett.103.150502

Matthew Hennessy. 1991. A Proof System for Communicating Processes with Value-Passing. *Formal Aspects of Computing* 3, 4 (1991), 346–366. https://doi.org/10.1007/BF01642508

Matthew Hennessy. 2012. Exploring Probabilistic Bisimulations, Part I. *Formal Aspects of Computing* 24, 4-6 (2012), 749–768. https://doi.org/10.1007/s00165-012-0242-7

H. J. Kimble. 2008. The Quantum Internet. *Nature* 453, 7198 (2008), 1023–1030. https://doi.org/10.1038/nature07127

Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. 2012. Application of a Process Calculus to Security Proofs of Quantum Protocols. In *FCS'12*. 141–147.

Marie Lalire. 2006. Relations among quantum processes: bisimilarity and congruence. *Mathematical Structures in Computer Science* 16, 3 (2006), 407–428. https://doi.org/10.1017/S096012950600524X

Marie Lalire and Philippe Jorrand. 2004. A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics. *CoRR* quant-ph/0407005 (2004). https://doi.org/10.48550/arXiv.quant-ph/0407005

Robin Milner. 1992. Functions as Processes. *Mathematical Structures in Computer Science* 2, 2 (1992), 119–141. https://doi.org/10.1017/S0960129500001407

Michael A. Nielsen and Isaac L. Chuang. 2010. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press. https://doi.org/10.1017/CBO9780511976667

A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. 2004. Practical Quantum Key Distribution with Polarization-Entangled Photons. *Optics Express* 12, 16 (2004), 3865. https://doi.org/10.1364/OPEX.12.003865 arXiv:quant-ph/0404115

Damien Pous and Davide Sangiorgi. 2011. Enhancements of the Bisimulation Proof Method. In *Advanced Topics in Bisimulation and Coinduction*, Davide Sangiorgi and Jan Rutten (Eds.). Cambridge University Press, 233–289. https://doi.org/10.1017/CBO9780511792588.007

Roberto Segala. 1995. *Modeling and verification of randomized distributed real-time systems*. Ph. D. Dissertation. Massachusetts Institute of Technology, Cambridge, MA, USA. https://hdl.handle.net/1721.1/36560

Peter W. Shor. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. IEEE Computer Society, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Ana Sokolova. 2011. Probabilistic Systems Coalgebraically: A Survey. *Theoretical Computer Science* 412, 38 (2011), 5095–5110. https://doi.org/10.1016/j.tcs.2011.05.008

Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. 2012. Exact Quantum Algorithms for the Leader Election Problem. *ACM Transactions on Computation Theory* 4, 1 (2012), 1:1–1:24. https://doi.org/10.1145/2141938.2141939

Mingsheng Ying, Yuan Feng, Runyao Duan, and Zhengfeng Ji. 2009. An Algebra of Quantum Processes. *ACM Transactions on Computational Logic* 10, 3 (2009), 1–36. https://doi.org/10.1145/1507244.1507249

Received 2023-07-11; accepted 2023-11-07