

Verification of quantum protocols adopting physically admissible schedulers

Questa è la versione sottoposta a revisione paritaria (postprint) della seguente opera:

Original

Verification of quantum protocols adopting physically admissible schedulers / Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G.. - In: ACM TRANSACTIONS ON QUANTUM COMPUTING. - ISSN 2643-6817. - (In corso di stampa). [10.1145/3830909]

Availability:

This version is available at: 20.500.11771/44398

Publisher:

Association for Computing Machinery

Published

DOI:10.1145/3830909

Terms of use:

This publication is made accessible in accordance with the terms for deposit in the institutional repository, as defined by the IMT School for Advanced Studies Lucca's Open Access Policy.
(https://library.imtlucca.it/sites/default/files/regolamento-policy-open-access-imtlib_0.pdf).

Si prega di consultare le pagine informative dell'editore relative alle politiche di autoarchiviazione.

(Article begins on next page)

Verification of Quantum Protocols Adopting Physically Admissible Schedulers

LORENZO CERAGIOLI, IMT School for Advanced Studies Lucca, Lucca, Italy

FABIO GADDUCCI, Computer Science, University of Pisa, Pisa, Italy

GIUSEPPE LOMURNO, Computer Science, University of Pisa, Pisa, Italy

GABRIELE TEDESCHI, IRIF, CNRS – Université Paris Cité, Paris, France

Recent developments in the field of quantum communication demonstrate that secure communication protocols based on quantum features are already practical. Reliable verification techniques are of paramount importance for these technologies, given their high implementation cost and critical contexts of application. Extensions of process calculi such as CCS and π -calculus have been proposed in the literature, together with various notions of behavioural equivalence. However, their standard probabilistic models turn out to introduce some non-deterministic capabilities that are not aligned with the observational properties of physical quantum systems, leading to bisimilarity notions that distinguish processes that should be physically equivalent. Nonetheless, we argue that non-deterministic features are fundamental to account for inputs, environments and adversarial behaviour.

To address this issue, we propose lqCCS, a process calculus that integrates concurrency, non-determinism and quantum capabilities. The calculus is enriched with a linear type system that enforces the no-cloning principle and resolves ambiguities in the visibility of ancillary qubits. We introduce a novel semantics in terms of distributions, where explicit physically admissible schedulers constrain probabilistic composition and forbid ill-defined non-deterministic moves, while preserving the expressivity needed to model real-world protocols. We investigate a scheduled version of saturated bisimilarity, deeming two lqCCS processes behaviourally equivalent if no observer can tell them apart. The adequacy of the approach is verified by lifting a known result from quantum mechanics to lqCCS, i.e. that equivalent processes acting on indistinguishable mixtures of quantum states are correctly recognized as bisimilar.

Finally, we give an alternative semantics and a labelled bisimilarity based on a quantum generalization of probability distributions. This provides an equivalent characterization of our behavioural equivalence that is a congruence with respect to the parallel operator, enabling compositional reasoning without the need to explicitly check all possible contexts. We describe a rich class of lqCCS processes for which equivalence is decidable using standard techniques, and we analyse real-world quantum communication protocols.

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

Additional Key Words and Phrases: Quantum Communication, Quantum Distribution, Behavioural Equivalence, Quantum Bisimulation.

1 Introduction

The recent advances in *quantum computation* and *quantum communication* mark a shift in the capabilities of quantum technologies, representing what many consider the second quantum revolution [MacFarlane et al.

Authors' Contact Information: Lorenzo Ceragioli, IMT School for Advanced Studies Lucca, Lucca, Italy; e-mail: lorenzo.ceragioli@imtlucca.it; Fabio Gadducci, Computer Science, University of Pisa, Pisa, Italy; e-mail: fabio.gadducci@unipi.it; Giuseppe Lomurno, Computer Science, University of Pisa, Pisa, Italy; e-mail: giuseppe.lomurno@phd.unipi.it; Gabriele Tedeschi, IRIF, CNRS – Université Paris Cité, Paris, France; e-mail: gabriele.tedeschi@cnrs.fr.



This work is licensed under a Creative Commons Attribution 4.0 International License.

© 2026 Copyright held by the owner/author(s).

ACM 2643-6817/2026/7-ART

<https://doi.org/10.1145/3830909>

2003]. This wave of development promises to harness quantum phenomena, particularly superposition and entanglement, for achieving groundbreaking results in algorithmic complexity and efficient implementation of secure data transmission.

At the forefront of this technological transformation lies *quantum communication*, one of the four pillars of quantum technologies [Riedel et al. 2017]. The unique properties of quantum systems, where information cannot be observed without stochastically altering the system state, provide physical safeguards against eavesdropping and enable the development of protocols that require exponentially less communication resources with respect to their classical counterparts [Brassard 2003]. Protocols have been developed targeting several use cases, such as key distribution, cryptographic coin tossing, private information retrieval, byzantine agreement [Ben-Or and Hassidim 2005; Bennet and Brassard 2014; Gao et al. 2019]. The benefits of these developments also impact the field of quantum algorithms. By leveraging multiple local systems connected both with quantum and classical channels, distributed implementations of algorithms can alleviate some scalability and fidelity issues still present in state-of-the-art quantum computers. In a rapidly evolving landscape, quantum communication channels are already practical, with both academic and real-world deployments. The vision of a worldwide network of quantum-capable machines, the *Quantum Internet*, capable of performing both cryptographic protocols and distributed computing is no longer confined to theoretical speculation [Kimble 2008; Zhang et al. 2024].

This flourishing development calls for theoretically grounded modelling and verification techniques, especially due to the substantial implementation costs of quantum technologies and their expected deployment in security-critical contexts. However, while the research on quantum circuits is mature, the verification of interactive quantum protocols received less attention. Following the well-established pattern of investigation for classical distributed systems with probabilistic and cryptographic features [Abadi and Gordon 1999; Larsen and Skou 1991; Milner 1980], we aim to develop a verification framework made of three components: (i) a description language for concurrent or distributed quantum processes; (ii) an adequate semantics; and (iii) a behavioural equivalence for comparing processes and verify their expected properties. In line with our intention, this framework will serve as a minimal starting point, needed as a stable foundation for building more advanced tools and verification mechanisms. The adequacy of the framework requires two properties: the *correctness* with respect to the prescriptions of quantum mechanics, and the *expressivity* needed to model concrete real-world protocols. We thus prove the correctness of our proposal, in particular with respect to the no-cloning theorem and the uncertainty principle, so that the system state can be inspected only by performing measurements. To guarantee the needed expressivity, we allow combining quantum and classical features, since quantum protocols rely on standard control flow and interaction with the external environment, usually modelled as non-deterministic agents.

The algebraic formalisms of process calculi, like CCS [Milner 1980] and CSP [Hoare 1978], have proven successful as modelling languages for classical distributed and concurrent systems. This success has naturally led to proposals for quantum counterparts, with several quantum process calculi sharing common features to model quantum capable participants of protocols [Feng et al. 2007; Gay and Nagarajan 2005; Lalire and Jorrand 2004]. Despite these efforts, the community has not yet reached a consensus on the standard approach for quantum process calculi, and quantum protocols continue to be predominantly described in natural language, which is both error-prone and incompatible with automated verification techniques [Singh et al. 2023].

As a modelling formalism, we propose lqCCS, a process calculus that seamlessly integrates classical communication, parallelism, and non-determinism with quantum capabilities. We enrich our calculus with a linear type system to enforce the no-cloning principle, and to resolve ambiguities regarding the visibility of ancillary qubits [Ceragioli et al. 2024c]. We demonstrate the expressivity of lqCCS by modelling and analysing three real-world protocols.

As a critical aspect of our modelling, we stress the necessity in our language of purely non-deterministic features, which are used to encode choices that are not specified at modelling time. When no assumption can

be made about the system behaviour, we must consider each possible alternative as a separate branch, thus expressing our properties in terms of an implicit universal quantification. This is fundamentally different from stochastic behaviour, where we assume that the available options come from a known probability distribution, each with its own likelihood. Non-deterministic capabilities are useful in modelling protocols where the user input is arbitrary, and in which implementation details are not made explicit. In addition, most proposed quantum protocols are cryptographic in nature. Therefore, we must account for attackers that are capable of tricking the system into following an adversarial execution path, even if it is unlikely when considering random probabilities. Lastly, non-determinism helps in modelling the behaviour of parallel processes, especially in dealing with race condition, i.e. when the sequence or timing of uncontrollable events may lead to unexpected or inconsistent results. The latter is even more critical in the quantum setting, where concurrent transformation of entangled states can influence the behaviour of other agents even without any explicit interaction or synchronization.

Regarding semantics and behavioural equivalences, the ones of existing quantum processes calculi are based on probabilistic labelled transition systems (pLTSs) and probabilistic bisimilarity. The choice seems natural, given the stochastic nature of quantum measurements; however, their use proves inadequate for quantum systems due to their failure to respect the observational limitations inherent in quantum theory. The core issues lie in the interplay between non-determinism, quantum features, and probabilistic behaviour. Previous proposals implicitly allow resolving non-determinism according to the unknown state of qubits, thus permitting a form of errorless quantum state inspection that causes no measurement-induced disturbance. The violation of this fundamental principle of quantum information manifests in practical terms as the presence of spurious moves in the semantics of processes, and causes behavioural equivalence to distinguish between quantum states that are indistinguishable according to quantum mechanics [Davidson 2012; Kubota et al. 2012]. To ensure that our framework strictly adheres to the prescriptions of quantum mechanics, we propose a new semantics of processes that makes explicit the scheduling choices performed by protocol participants, as done in the classical setting [Chatzikokolakis et al. 2009]. Then, we substitute the traditional pLTS-based semantics for one based on a labelled transition system where states hold distributions of processes. In doing so, we employ a constrained version of probabilistic composition, which only allows composing moves characterized by the same non-deterministic choices. These well-behaved schedulers strictly prohibit the unfeasible state inspections found in previous models, ensuring that the system state can only be accessed via proper measurement operators.

To give a natural notion of indistinguishability, we resort to saturated bisimilarity, a form of contextual equivalence that deems processes equivalent if there is no observer capable of distinguishing between the two [Bonchi et al. 2014]. More in detail, termination is the only property of lqCCS processes that is immediately observable, while other properties are inspected indirectly by putting the processes in parallel with other lqCCS processes called observers. This approach favours correctness and intuitiveness over decidability, reducing equivalence to an immediate notion of operational comparison on one hand, while at the same time requiring a universal quantification over all possible observers on the other hand. In this context, we discuss the adequacy of our approach, and we prove that using our physically feasible schedulers is sufficient to lift a known indistinguishability result from quantum states to lqCCS processes, namely that probabilistic mixtures of quantum states are indistinguishable if they can be represented as the same density operator. The same lifted property does not hold for the traditional approach from probabilistic systems that is often employed in quantum process calculi [Deng 2018; Deng and Feng 2012; Feng and Ying 2015; Wu et al. 2024].

Whereas contextual equivalences, like our saturated bisimilarity, have a clear operational interpretation which simplify reasoning on their correctness with respect to the real-world discriminating power, traditional labelled bisimilarities in terms of atomic observables offer an elegant mathematical formalization, and are easier to compute [Bonchi et al. 2014]. Therefore, we give an alternative succinct semantics that relies on a quantum generalization of probability distributions, and we characterize behavioural equivalence in terms of labelled bisimilarity. Finally, we prove the two characterizations equivalent, relieving the prover from the burden of

manually considering each possible distinguishing context. Noticeably, our labelled bisimilarity is closed under parallel composition, a feature often missing in literature that permits compositional reasoning on protocols by possibly verifying the behaviour of each agent in isolation.

To demonstrate the expressivity and practical utility of our framework, we apply lqCCS to the formalization and verification of real-world cryptographic systems. Using the Quantum Coin Flip (QCF) protocol as a primary example, we illustrate how our proposed bisimilarity can be utilized to rigorously model both the implementation and the specification of the system, successfully proving essential properties such as protocol fairness, data confidentiality, and the reliable detection of malicious cheating strategies.

Synopsis. In section 2 we introduce our process calculi and exemplify our approach by analysing the quantum coin flip protocol. In section 3 we give some background about probability distributions and quantum computing. We formally define lqCCS with schedulers in section 4, and discuss the adequacy of saturated bisimilarity in section 5. In section 6 we give an alternative semantics and equivalent labelled bisimilarity. In section 7 we apply our approach to three real-world protocols. Finally, we compare related works with ours in section 8, and we wrap-up the paper in section 9. Appendices contain the full proofs of our results.

Remark. This is an extended version of [Ceragioli et al. 2024b]; this paragraph discusses the novel contributions. In section 4, we relax our assumption about deterministic schedulers by allowing external non-determinism when receiving values on a channel. In section 5, we show that the problems caused by non-determinism also affect the modelling of isolated parallel processes that do not communicate (see Example 5.7). In a nutshell, the measurement-induced collapse is detected by a non-deterministic observer as if a message was sent faster than light. As a main novel contribution, section 6 describes a new semantics for lqCCS based on a quantum generalization of probability distributions, which internalize the equivalence stated in Theorem 5.10, and proves it fully abstract with respect to the probabilistic one (see Theorem 6.10). Our labelled bisimilarity requires relations to be closed for the application of arbitrary quantum superoperators, which hinder its decidability. Here, we prove that it cannot be omitted in general (Example 6.11), but also that it is not needed for a rich class of processes, for which our bisimilarity is decidable (Theorem 6.14). Finally, in section 7 we apply our approach beyond the standard verification of equivalence between specification and implementation: we model and verify the quantum coin flip protocol, showing how we can resort to our formal verification technique to characterize the desired security properties of a cryptographic protocol.

2 Preview of Our Verification Framework

In this section, we provide an overview of our formal approach to the verification of quantum protocols by presenting our modelling language and its intended usage on a concrete real-world example, the quantum coin flip protocol.

2.1 The lqCCS Process Calculus

As a modelling language, we propose lqCCS, a process calculus inspired by qCCS [Feng et al. 2012] where the primitive features of communication, parallelism and non-determinism of (value passing) CCS [Hennessy 1991] are extended with quantum capabilities.

Definition 2.1 (lqCCS Syntax). Let $\mathbb{B}$ be the set of boolean values ranged over by variable b , $\mathbb{N}$ natural numbers ranged over by n , Q qubit names ranged over by q , Chan communication channels ranged over by c , and Var

variables ranged over by x . The syntax of lqCCS processes is defined by the productions

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

where $\tilde{e}$ denotes a (possibly empty) tuple $e_1, \dots, e_n$ of expressions.

Processes can perform atomic operations, written as prefixes and followed by processes representing their continuation. As it is common in CCS, we assume that a process can perform an invisible internal action with τ ; receive over a channel c a value to bind to a variable x with $c?x$; send a value obtained by evaluating an expression e over a channel c with $c!e$. Note that channels abstractly model concrete communication means for classical and quantum values: the latter allow propagating qubit values (in some physical representation like light polarization) and are guaranteed to preserve their quantum features like superposition. In addition, a process can exploit its quantum capabilities to manipulate the state of some qubits via trace-preserving superoperators and measurement. We allow processes to modify the state of qubits denoted by $\tilde{e}$ (where each expression is either a qubit q or a variable x) by applying any trace-preserving superoperator $\mathcal{E}$ with $\mathcal{E}(\tilde{e})$. For example, the process can update the state of qubits by performing unitary transformations like $CNOT(q_0, q_1)$, the controlled not over q_0 , and $H(q_0)$, the Hadamard transformation over q_0 . We write $\mathcal{M}(\tilde{e} \triangleright x)$ for the operation that performs the measurement $\mathcal{M}$ to the qubits of $\tilde{e}$: the classical outcome is stored in the number variable x , and the state of the qubits is updated accordingly. For example, the process can apply $\mathcal{M}_{01}$, $\mathcal{M}_{\pm}$ or $\mathcal{M}_{\pm i}$, i.e. the projective measurements in the bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ and $\{|i\rangle, |-i\rangle\}$. Finally, the process $\mathbf{0}_{\tilde{e}}$ is an idle deadlock process that maintains ownership of the qubits in $\tilde{e}$. When $\tilde{e}$ is the empty sequence, we write $\mathbf{0}$ to stress the equivalence with the nil process of standard CCS.

Processes can be composed with parallel, non-deterministic, and boolean operators. With the parallel composition operator ($P \parallel Q$) each component can act independently or synchronize through communication over the same channel. The non-deterministic choice operator ($P + Q$) allows the process to select a specific component behaviour according to a yet unspecified policy. When a choice is performed according to a boolean expression the processes are composed with the conditional operator (**if** e **then** P **else** Q). Finally, the communication between two or more channels can be isolated from other processes with the restriction operator ($P \setminus c$), meaning that the channel c is private and can be used only inside P . For brevity, we sometimes write **if** e **then** $\alpha_1. R$ **else** $\alpha_2. R$ as (**if** e **then** α_1 **else** α_2). R , and we often omit the trailing $\mathbf{0}$, writing, e.g. $a!1$ for $a!1. \mathbf{0}$.

To comply with the no-cloning theorem, we enforce a single ownership principle, forbidding parallel processes from sharing qubit names. Because of that, $\mathbf{0}_{\tilde{e}}$ make the qubits in $\tilde{e}$ inaccessible to other processes: we say that it *discards* them. Explicitly writing the discarded qubits allows distinguishing those qubits that are hidden to the environment from the ones that can be accessed by external observers, solving an ambiguity in related works, see section 8.

2.2 Modelling and Analysing the Quantum Coin Flip Protocol

To exemplify our approach, we use a non-trivial concrete case, the Quantum Coin Flip protocol [Bennet and Brassard 2014], which is also a basis for implementing the more involved Quantum Byzantine Agreement [Ben-Or and Hassidim 2005]. The objective of the protocol is to randomly select a winner between two participants, named Alice and Bob, which do not trust each other. In a nutshell, Alice chooses a secret value between 0 and 1, and Bob tries to guess it: if he is right, he wins the game, otherwise he loses. As we will detail later, the underlying idea is to exploit the quantum features to guarantee different properties, e.g. that the game is fair (if both players follow the rules then each of them has equal winning probability), and that the players cannot cheat without risking getting caught.

Alice ::= $\mathcal{M}_{\text{bit}}(\triangleright s).$ if $s = 0$ then $H(q). \mathcal{M}_{01}(q \triangleright w).$ else $I(q). \mathcal{M}_{\pm}(q \triangleright w).$ $\text{AtoB!}q.$ $\text{guess?}g.$ $\text{witness!}w.$ $\text{secret!}s.$ $a!(g = s)$	Bob ::= $\text{AtoB?}x.$ $\mathcal{M}_{\text{bit}}(\triangleright g).$ if $g = 0$ then $\mathcal{M}_{\pm}(x \triangleright p).$ else $\mathcal{M}_{01}(x \triangleright p).$ $\text{guess!}g.$ $\text{witness?}w.$ $\text{secret?s}.$ $(b!(g = s) \parallel \text{cheat!}(g \neq s \wedge p \neq w) \parallel 0_x)$
--	--

QCF ::= $(\text{Alice} \parallel \text{Bob}) \setminus \{\text{AtoB}, \text{guess}, \text{secret}, \text{witness}\}$

Fig. 1. The Quantum Coin Flip protocol **QCF**, modelled using lqCCS.

Notably, lqCCS is expressive enough to model such kinds of real-world protocols.

Example 2.2. The formalization of the Quantum Coin Flip protocol in lqCCS is in Figure 1, where we assume the qubit q is prepared as $|0\rangle$. Alice starts with a simple probabilistic coin toss, formally represented as a measurement on no qubits $\mathcal{M}_{\text{bit}}(\triangleright s)$: the *secret basis* s will be instantiated as 0 or 1 with equal probability. If s is 0 then Alice will use the standard basis, otherwise, the Hadamard basis is used. The unitary transformation before measurement guarantees that each measurement result has the same probability of being observed. Depending on s , the qubit q is thus in either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, each with equal probability, and the classical *witness* w is a bit that corresponds to the quantum state (by convention, the first element of the basis corresponds to 0, while the second to 1). Alice, next, sends the prepared qubit to Bob, and keeps both s and w private. Bob, who is waiting on the main communication channel, receives the qubit and randomly selects a basis g : he will win if the guessed basis g coincides with Alice’s secret one s . If Bob selects the standard basis, he measures the received qubit on the Hadamard one, and vice versa. The classical result of the measurement is stored in the variable p , serving as a *fingerprint* of the original bit randomly generated by Alice, which will be used for checking if she is cheating. The guess of Bob is communicated to Alice via the guess channel. At this point, Alice reveals the secret s and the witness w , and she computes the winner: she sends 1 over her channel a if Bob is right, 0 otherwise. Bob receives the secret, he also computes and advertises the winner on his channel b , with the same encoding as Alice. Finally, he checks the received witness w : if the secret basis is not g , then it must be the one used by Bob for measuring the received qubit, and w must coincide with p . If this is not the case, a 1 bit is sent over the cheat channel, signalling that a misbehaviour has been detected.

A distinctive feature of process calculi is that they can be used to model both the implementation of a protocol and its specification: the intended behaviour of the system as seen from an external observer, in a black-box manner. In this setting, verification coincides with proving that no observer can tell the difference between implementation and specification, which is indeed the primary goal of our proposal. To this end, we introduce a notion of contextual equivalence known as *saturated bisimilarity*: namely, two processes are deemed bisimilar if no process in parallel can distinguish one from the other. As we will see, the standard probabilistic bisimilarity used in the literature does not coincide with the observational capability permitted by the inherent limitations of quantum theory. To address this problem, we propose a relation $\simeq$, based on physically admissible observers, characterized by a constrained probabilistic composition of non-deterministic choices, and we prove its adequacy to the prescriptions of quantum theory.

Example 2.3. The lqCCS modelling of the specification for the protocol is below, where τ^n is shorthand for a sequence of τ actions of length n . The specification represents a fair coin that selects Alice or Bob as the winner with equal probability. In addition, only the bit 0 is sent over the cheat channel, because Alice in Figure 1 is not

cheating.

$$\mathbf{FairCoin} ::= \mathcal{M}_{\text{bit}}(\triangleright x). \tau^8. (a!x \parallel b!x \parallel \text{cheat!}0)$$

In section 7, we will show that **QCF** and **FairCoin** are observationally equivalent: the protocol works as desired.

For some protocols, provably behaving as expected, when all participants act as desired, is not enough. In security contexts, like in coin flip and key exchange protocols, there are other important properties which can be investigated by resorting to our proposed bisimilarity. Ideally, we want to guarantee that in **QCF** cheating is either impossible, or at least that malicious attempts have a reasonable probability of being detected. Checking that Bob cannot cheat to increase his winning chances amounts to verifying confidentiality of Alice's secret value s . We can prove confidentiality by considering two versions of the same process that differ only in their private variables: confidentiality is violated when the two are not bisimilar, i.e. if and only if a distinguishing context is found.

Example 2.4. To guarantee that the protocol does not favour Bob, we show that he is not able to infer Alice's secret bit s from the received qubit q , even though it corresponds to the state of her chosen basis. To prove this it is sufficient to take the two versions of **Alice** when s is 0 or is 1, and to consider the part of the process that happens before the secret is revealed. We name them **Alice**₀ and **Alice**₁, defined below:

$$\mathbf{Alice}_0 = H(q). \mathcal{M}_{01}(q \triangleright w). \text{AtoB!}q \quad \mathbf{Alice}_1 = I(q). \mathcal{M}_{\pm}(q \triangleright w). \text{AtoB!}q$$

We will show that, when starting with q in the $|0\rangle$ state, the two processes above are bisimilar, thus there exists no observer process that distinguishes the two versions so as, e.g., to execute `guess!0` when Alice is observed to behave as **Alice**₀ and `guess!1` when she behaves as **Alice**₁. Indeed, there is no clever way of inferring the choice of Alice by inspecting the received qubits: Bob cannot do better than choosing his basis at random.

The confidentiality result heavily depends on the constraints that we impose on non-determinism in our behavioural equivalence. In particular, quantum theory prescribes indistinguishability classes of quantum states, thus a reasonable behavioural equivalence must reflect these classes. Previous results [Ceragioli et al. 2024c] have shown that this requires constraining non-determinism, which is also the solution that we apply in this work. Indeed, the traditional probabilistic bisimilarity incorrectly distinguishes the two versions of Alice in the previous example. As a result of this limitation, one would mistakenly conclude that **QCF** favours Bob over Alice, which is provably not the case.

The security of a protocol can also be investigated by substituting an honest participant with a specific attacker, as we show below by substituting Alice with two malicious versions of her: Alison and Alix, both modelled in Figure 2.

Example 2.5. Assume that Alice wants to cheat. A possible strategy is to consider the guess of Bob and reveal the opposite basis, independently of the secret s . This variant is named **Alison**, modelled by the left process in Figure 2.

$$\mathbf{QCF}' ::= (\mathbf{Alison} \parallel \mathbf{Bob}) \setminus \{\text{AtoB}, \text{guess}, \text{secret}, \text{witness}\}$$

The attack of Alison is not dangerous: she is the legitimate winner half of the time, whereas in the other cases Bob is capable of detecting the attack with half probability due to the witness (the overall probability of seeing 1 over the cheat channel is thus 1/4). Indeed, if the basis chosen by Bob does not coincide with the secret one of Alison, then the witness w is not correlated to the fingerprint p computed by Bob, and the two coincide only by chance if Alison is lucky. To show the success probability of Alison's attack, we will prove that **QCF'** is bisimilar to:

$$\mathcal{M}_{\frac{3}{4}}(\triangleright x). \tau^8. (a!0 \parallel b!0 \parallel \text{cheat!}x)$$

Alison ::= $\mathcal{M}_{\text{bit}}(\triangleright s).$ if $s = 0$ then $H(q). \mathcal{M}_{01}(q \triangleright w).$ else $I(q). \mathcal{M}_{\pm}(q \triangleright w).$ AtoB! $q.$ guess? $g.$ witness! $w.$ (secret!($1 - g$) $a!0$)	Alix ::= $H(q).$ CNOT(q, q'). AtoB! $q.$ guess? $g.$ if $g = 0$ then $\mathcal{M}_{\pm}(q' \triangleright w).$ else $\mathcal{M}_{01}(q' \triangleright w).$ witness! $w.$ (secret!($1 - g$) $a!0$)
--	--

Fig. 2. Two malicious versions of Alice, modelled using lqCCS.

where $\mathcal{M}_{\frac{3}{4}}(\triangleright x)$ is the measurement on no qubits that instantiates x to 0 with probability 3/4 and to 1 with probability 1/4. While we stick with the simplest case favouring simplicity, it is easy to show that increasing the number of qubits used for the witnesses leads to an exponential increase in the probability of Bob to detect the cheating attempt, since the witnesses she sends must exactly match *each* of Bob's measurement results.

However, Alice can adopt a better strategy, which always guarantees winning the toss with no risk of being discovered. For this attack, Alice must have access to an additional qubit q' . We name this variant **Alix**, modelled by the right process in Figure 2.

$$\mathbf{QCF}'' ::= (\mathbf{Alix} \parallel \mathbf{Bob}) \setminus \{\text{AtoB}, \text{guess}, \text{secret}, \text{witness}\}$$

The idea behind this attack is that of preparing a state that collapses in two equivalent states when Bob performs his measurement (for any basis that Bob can choose). This allows Alix to forge a valid witness for the basis chosen by Bob, even if it is unknown. To show that this attack always succeeds, we will prove that $\mathbf{QCF}''$ is bisimilar to:

$$\tau^9. (a!0 \parallel b!0 \parallel \text{cheat!}0)$$

Intuitively, Alix exploits entanglement to correlate two qubits such that when measured they result in the same state.

Note the critical difference of the result of our analysis with respect to one resorting to standard probabilistic bisimilarity. Whereas the standard approach deems that Bob can distinguish the state of the qubit sent by Alice, thus implicitly inferring the secret and winning the game, our proposal correctly predicts that Alice (and only Alice) has a winning strategy.

3 Background

We recall some background on probability distributions and quantum computing, referring to [Nielsen and Chuang 2010] for further reading.

3.1 Probability Distributions

Given a function $\Delta : S \rightarrow [0, 1]$ from a set S to the interval of real numbers $[0, 1]$, we let its *support* be the set $[\Delta] = \{s \in S \mid \Delta(s) > 0\}$. When the support is finite, we define the *mass* of Δ as $|\Delta| = \sum_{s \in S} \Delta(s)$. A *probability distribution* $\Delta \in \mathcal{D}^{\leq}(S)$ over a set S is a function $\Delta : S \rightarrow [0, 1]$ with finite support such that $|\Delta| \leq 1$. A *full probability distribution* $\Delta \in \mathcal{D}(S) \subseteq \mathcal{D}^{\leq}(S)$ is a probability distribution with mass equal to 1.

We let ϵ be the empty distribution with mass equal zero, i.e. such that $\epsilon(s) = 0$ for all $s \in S$. For each $s \in S$, we let $p \cdot s$ be the *point distribution* such that $(p \cdot s)(s) = p$. Finally, we define the following two operations over probability distributions: the scaling of Δ with $p \in [0, 1]$ is defined as the distribution $p\Delta$ with $(p\Delta)(s) = p(\Delta(s))$; the sum of Δ and Θ is a partial operation defined when $|\Delta| + |\Theta| \leq 1$ as the distribution $\Delta \oplus \Theta$ with $(\Delta \oplus \Theta)(s) = \Delta(s) + \Theta(s)$.

In general, we write $\sum_{i \in I} p_i \cdot \Delta_i$ for $p_1 \Delta_1 \oplus p_2 \Delta_2 \cdots \oplus p_n \Delta_n$ when $i = \{1, 2, \dots, n\}$. When writing $\Delta \oplus \Theta$, it is assumed that the operation is defined on the operands.

A relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(S) \times \mathcal{D}^{\leq}(S)$ is *left-linear* if $\Delta_i \mathcal{R} \Theta_i$ for $i \in I$ and $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ implies $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ is defined and $\Delta \mathcal{R} \Theta$, for any finitely indexed set of probabilities $p_i \in [0, 1]$ and distributions Δ_i and Θ_i . A relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(S) \times \mathcal{D}^{\leq}(S)$ is *right-linear* if $\Delta_i \mathcal{R} \Theta_i$ for $i \in I$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ implies $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ is defined and $\Delta \mathcal{R} \Theta$, for any finitely indexed set of probabilities $p_i \in [0, 1]$ and distributions Δ_i and Θ_i . A relation is *linear* if it is both left- and right-linear. Notice that linearity implies convexity in the sense of [Bonchi et al. 2017], because both Δ and Θ are always defined if $\sum_{i \in I} p_i = 1$. A relation $\mathcal{R}$ is *left-decomposable* if for any p, Δ_1, Δ_2 and Θ , $(p \cdot \Delta_1 \oplus (1-p) \cdot \Delta_2) \mathcal{R} \Theta$ implies $\Theta = p \cdot \Theta_1 \oplus (1-p) \cdot \Theta_2$ for some Θ_1, Θ_2 with $\Delta_i \mathcal{R} \Theta_i$ for $i = 1, 2$. Right-decomposability is defined symmetrically, and a relation is *decomposable* when it is both left- and right-decomposable.

Given $\mathcal{R} \subseteq A \times \mathcal{D}^{\leq}(B)$, its *left-linear lifting* $\text{lft}(\mathcal{R}) \subseteq \mathcal{D}^{\leq}(A) \times \mathcal{D}^{\leq}(B)$ is the smallest left-linear relation such that $1 \cdot s \text{ lft}(\mathcal{R}) \Theta$ if $s \mathcal{R} \Theta$. Regarding this lifting, we can prove the following lemma

LEMMA 3.1. *For any relation $\mathcal{R} \subseteq S \times \mathcal{D}(S)$, $\text{lft}(\mathcal{R})$ is left-decomposable.*

3.2 Quantum Computing

An isolated physical system is associated with a *Hilbert space* $\mathcal{H}$, i.e. a complex vector space equipped with an inner product $\langle \cdot | \cdot \rangle$. We indicate column vectors as $|\psi\rangle$ and their conjugate transpose as $\langle \psi| = |\psi\rangle^\dagger$. The states of a system are *unit vectors* in $\mathcal{H}$, i.e. vectors $|\psi\rangle$ such that $\langle \psi | \psi \rangle = 1$. A two-dimensional physical system is known as a *qubit*, and we denote its Hilbert space as $\hat{\mathcal{H}} = \mathbb{C}^2$. The vectors $|0\rangle = (1, 0)^T$ and $|1\rangle = (0, 1)^T$ form the *computational basis* of $\hat{\mathcal{H}}$. Other important states are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which form the *Hadamard basis*. In quantum terminology, the states in the Hadamard basis are *superpositions* with respect to the computational basis, as they are a linear combination of $|0\rangle$ and $|1\rangle$. A third basis of $\hat{\mathcal{H}}$ contains $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. All $|+\rangle, |-\rangle, |i\rangle$ and $|-i\rangle$ are superpositions of $|0\rangle, |1\rangle$.

We represent the state space of a composite physical system as the *tensor product* of the state spaces of its components. Consider the Hilbert spaces $\mathcal{H}_A$ with $\{|\psi_i\rangle\}_{i \in I}$ one of its bases, and $\mathcal{H}_B$ with $\{|\phi_j\rangle\}_{j \in J}$ one of its bases. We let their tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ be the Hilbert space with bases $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{(i,j) \in I \times J}$, where $|\psi\rangle \otimes |\phi\rangle$ is the Kronecker product. We often omit the tensor product and write $|\psi\phi\rangle$ for $|\psi\rangle \otimes |\phi\rangle$. We write $\hat{\mathcal{H}}^{\otimes n}$ for the 2^n -dimensional Hilbert space defined as the tensor product of n copies of $\hat{\mathcal{H}}$ (i.e. the possible states of n qubits). 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 $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

In quantum physics, the evolution of an isolated system is described by a unitary transformation. For each linear operator A on $\mathcal{H}$, its *adjoint* $A^\dagger$ is the unique linear operator such that $\langle \psi | A | \phi \rangle = \langle A^\dagger \psi | \phi \rangle$. A linear operator U is *unitary* when $UU^\dagger = U^\dagger U = \mathbb{I}$, with $\mathbb{I}$ the identity matrix. Quantum computers allow the programmer to manipulate registers via unitaries like H, X, Z and $CNOT$, which are defined by the following equalities and by linearity in all the other cases:

$$\begin{aligned} H|0\rangle &= |+\rangle & H|1\rangle &= |-\rangle & X|0\rangle &= |1\rangle & X|1\rangle &= |0\rangle & Z|+\rangle &= |-\rangle & Z|-\rangle &= |+\rangle \\ CNOT|10\rangle &= |11\rangle & CNOT|11\rangle &= |10\rangle & CNOT|0\psi\rangle &= |0\psi\rangle \end{aligned}$$

3.3 Density operator formalism

The density operator formalism puts together quantum systems and probability distributions by considering mixed states, i.e. *probability distributions of quantum states*. A point distribution $1 \cdot |\psi\rangle$ (called a pure state) is represented by the matrix $|\psi\rangle\langle\psi|$. In general, a mixed state $\Delta \in \mathcal{D}^{\leq}(\hat{\mathcal{H}}^{\otimes n})$ for n qubits is represented by the

matrix $\rho_\Delta \in \mathbb{C}^{2^n \times 2^n}$, known as its *density operator*, with $\rho_\Delta = \sum_{|\psi\rangle \in [\Delta]} \Delta(|\psi\rangle) |\psi\rangle\langle\psi|$. The trace of a square matrix A , denoted $\text{tr}(A)$, is defined as the sum of the elements on the main diagonal. For a density operator ρ , the trace $\text{tr}(\rho)$ is the mass of the probability distribution of quantum states represented by ρ . We write $\mathcal{DO}^\leq(\mathcal{H})$ for the set of density operators of $\mathcal{H}$ and $\mathcal{DO}(\mathcal{H})$ for the set $\{\rho \in \mathcal{DO}^\leq(\mathcal{H}) \mid \text{tr}(\rho) = 1\}$, corresponding to full probability distributions of quantum states. For example, the mixed state $\frac{1}{3} \cdot |0\rangle \oplus \frac{2}{3} \cdot |+\rangle$ is represented by the density operator $\frac{1}{3} |0\rangle\langle 0| + \frac{2}{3} |+\rangle\langle +|$. The empty distribution ϵ corresponds instead to the all-zero matrix $\mathbb{O}$.

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

Fact 1. Two distributions of pure quantum states $\Delta, \Theta \in \mathcal{D}(\mathcal{H})$ are indistinguishable for any physical observer whenever

$$\rho_\Delta = \sum_{|\psi\rangle \in [\Delta]} \Delta(|\psi\rangle) |\psi\rangle\langle\psi| = \sum_{|\psi\rangle \in [\Theta]} \Theta(|\psi\rangle) |\psi\rangle\langle\psi| = \rho_\Theta.$$

Since density operators encode distributions of pure states, the same result is easily extended to indistinguishable distributions of mixed states.

When modelling composite systems, density operators are composed with the Kronecker product as well. Unlike pure states, they can also describe local information about subsystems. Let $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ represent a composite system, with subsystems A and B . Given a (not necessarily separable) $\rho^{AB} \in \mathcal{H}_{AB}$, the state of the subsystem A is described as the *reduced density operator* $\rho^A = \text{tr}_B(\rho^{AB})$, with tr_B the *partial trace over B* , defined as the linear transformation such that $\text{tr}_B(|\psi\rangle\langle\psi'| \otimes |\phi\rangle\langle\phi'|) = |\psi\rangle\langle\psi'| \text{tr}(|\phi\rangle\langle\phi'|)$.

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 mixed state, because “forgetting” the information on the subsystem B leaves only partial information on subsystem A . For example, the partial trace over the first qubit of $|\Phi^+\rangle\langle\Phi^+|$ is the maximally mixed state.

The evolution of mixed states is given by *trace non-increasing superoperators*, i.e. functions on density operators. A superoperator $\mathcal{E} : \mathcal{DO}^\leq(\mathcal{H}) \rightarrow \mathcal{DO}^\leq(\mathcal{H})$ on a d -dimensional Hilbert space $\mathcal{H}$ is a function defined by its *Kraus operator sum decomposition* $\{E_i\}_{i=1,\dots,d^2}$, satisfying that $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ and $\sum_i E_i^\dagger E_i \subseteq \mathbb{I}$, where $A \subseteq B$ means that $B - A$ is a positive semidefinite matrix. We call $\mathcal{SO}^\leq(\mathcal{H})$ the set of trace non-increasing superoperators on $\mathcal{H}$, and $\mathcal{SO}(\mathcal{H}) \subseteq \mathcal{SO}^\leq(\mathcal{H})$ the set of all *trace-preserving* superoperators, i.e. such that $\sum_i E_i^\dagger E_i = \mathbb{I}$. Intuitively, trace-preserving superoperators are maps between distributions of quantum states that preserve the mass of the distributions, e.g. full-distributions to full-distributions, while trace non-increasing superoperators may map to distributions with less mass, e.g. full distributions to distributions.

Notably, the tensor product of superoperators is obtained by tensoring their Kraus decompositions, and any unitary transformation U can be seen as a superoperator, that we still denote as U , with $\{U\}$ as its Kraus decomposition.

Quantum measurements describe how to extract information from a physical system. Performing a measurement on a quantum state returns a probabilistic classical result and causes the quantum state to change (i.e. to *collapse*). A measurement with k different outcomes is a set $\mathcal{M} = \{M_m\}_{m=0}^{k-1}$ of k linear operators, satisfying the *completeness* equation $\sum_{m=0}^{k-1} M_m^\dagger M_m = \mathbb{I}$. If the state of the system is ρ before the measurement, then the probability of m -th outcome occurring is $p_m = \text{tr}(M_m \rho M_m^\dagger)$. If m is the outcome, then the state after the measurement will be $M_m \rho M_m^\dagger / p_m$. Note that each operator M_m defines a trace non-increasing superoperator $\mathcal{M}_m$, with $\mathcal{M}_m(\rho) = M_m \rho M_m^\dagger$, and the resulting state after the m -th outcome is the normalization of $\mathcal{M}_m(\rho)$.

$$\begin{array}{c}
\text{NIL} \quad \frac{\tilde{e} \in \tilde{\Sigma}}{\Sigma \vdash \mathbf{0}_{\tilde{e}}} \quad \text{TAU} \quad \frac{\Sigma \vdash P}{\Sigma \vdash t:\tau.P} \quad \text{TAUPAIR} \quad \frac{\Sigma \vdash P}{\Sigma \vdash (t,t'):\tau.P} \quad \text{QOP} \quad \frac{\mathcal{E} : \text{Op}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad \Sigma \vdash P}{\Sigma \vdash t:\mathcal{E}(\tilde{e}).P} \\
\\
\text{QMEAS} \quad \frac{\mathcal{M} : \text{Meas}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad x : \mathbb{N} \quad \Sigma \vdash P}{\Sigma \vdash t:\mathcal{M}(\tilde{e} \triangleright x).P} \quad \text{CRECV} \quad \frac{c : \hat{T} \quad x : T \in \{\mathbb{B}, \mathbb{N}\} \quad \Sigma \vdash P}{\Sigma \vdash t:c?x.P} \\
\\
\text{QRECV} \quad \frac{c : \hat{Q} \quad x : Q \quad \Sigma \cup \{x\} \vdash P}{\Sigma \vdash t:c?x.P} \quad \text{CSEND} \quad \frac{c : \hat{T} \quad e : T \in \{\mathbb{B}, \mathbb{N}\} \quad \Sigma \vdash P}{\Sigma \vdash t:c!e.P} \quad \text{QSEND} \quad \frac{c : \hat{Q} \quad e \in \Sigma \quad \Sigma \setminus \{e\} \vdash P}{\Sigma \vdash t:c!e.P} \\
\\
\text{ITE} \quad \frac{e : \mathbb{B} \quad \Sigma \vdash P \quad \Sigma \vdash Q}{\Sigma \vdash \text{if } e \text{ then } P \text{ else } Q} \quad \text{SUM} \quad \frac{\Sigma \vdash P \quad \Sigma \vdash Q}{\Sigma \vdash P + Q} \quad \text{PAR} \quad \frac{\Sigma_1 \cap \Sigma_2 = \emptyset \quad \Sigma_1 \vdash P \quad \Sigma_2 \vdash Q}{\Sigma_1 \cup \Sigma_2 \vdash P \parallel Q} \quad \text{RESTR} \quad \frac{\Sigma \vdash P}{\Sigma \vdash P \setminus c}
\end{array}$$

Fig. 3. Typing rules for lqCCS

The simplest measurements project a state into the elements of a basis, e.g. $\mathcal{M}_{01} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $\mathcal{M}_{\pm} = \{|+\rangle\langle +|, |-\rangle\langle -|\}$ for the computational and Hadamard basis of $\hat{\mathcal{H}}$. As expected, applying $\mathcal{M}_{01}$ to $|0\rangle$ always returns the classical outcome 0 and the state $|0\rangle$. When applying the same measurement on $|+\rangle$, instead, the outcome is 0 and the state is $|0\rangle$, or 1 and $|1\rangle$ with equal probability. Symmetrically, measuring $|0\rangle$ with $\mathcal{M}_{\pm}$ leads to either 0 and $|+\rangle$, or 1 and $|-\rangle$, with equal probability. Finally, applying the measurement $\mathcal{M}_{\pm i} = \{|i\rangle\langle i|, |-i\rangle\langle -i|\}$ to each of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ returns 0 and $|i\rangle$, or 1 and $|-i\rangle$ with equal probability.

4 Quantum Process Calculus and Probabilistic Semantics

In this section, we describe the internal syntax of lqCCS processes, i.e. one in which available actions are individually tagged. We also define a type system for enforcing single ownership of qubits, thus guaranteeing adherence to the no-cloning theorem. Our process calculus is enriched with a linear type system, reflecting the *no-cloning theorem* of quantum mechanics, which forbids quantum values to be copied or broadcasted. We define a formal semantics where transitions are decorated with schedulers. Tags in the syntax name all the possible non-deterministic choices, while schedulers in the semantics allow choosing among the available tags.

4.1 Internal Syntax and Type System

We assume a denumerable set Tag ranged over by t, t', t_0, t_1 , etc. The syntax of tagged lqCCS processes is obtained by augmenting the actions in Definition 2.1 with syntactic tags.

$$\alpha ::= t:\tau \mid (t,t'):\tau \mid t:c?x \mid t:c!e \mid t:\mathcal{E}(\tilde{e}) \mid t:\mathcal{M}(\tilde{e} \triangleright x)$$

A symbol $\mathcal{E}$ denotes a trace-preserving superoperator on $\hat{\mathcal{H}}^{\otimes n}$ for some $n > 0$, and we write $\mathcal{E} : \text{Op}(n)$ to indicate that $\mathcal{E}$ is a superoperator of arity n . A symbol $\mathcal{M}$ denotes a measurement $\{M_0, \dots, M_{k-1}\}$ with k different outcomes; we write $\mathcal{M} : \text{Meas}(n)$ to indicate that each M_i acts on n qubits, and denote $|\mathcal{M}|$ the cardinality k of $\mathcal{M}$. Concerning the tags, for the silent action τ we consider two possibilities. This distinction is useful for using τ actions to write an abstract specification of a concrete protocol: $t:\tau$ models an action with tag t , $(t,t'):\tau$ models a

synchronization. Tags are intended to explicitly name the non-deterministic choices that a scheduler can perform when running a process. In the following, we assume that processes come with their associated tags.

The visibility of qubits is enforced explicitly through the linear type system in Figure 3. The typing judgment $\Sigma \vdash P$ indicates that the process P is well-typed under the usage of the set of qubits $\Sigma \subseteq \mathcal{Q}$. Given a set of terms E , we write $\tilde{E}$ for the set of all tuples $\tilde{e}$ composed of all and only the elements in E (in any possible order without repetitions). Atomic values are typed by their domain set: $\mathbb{N}$ for natural numbers, $\mathbb{B}$ for boolean values, and $\mathcal{Q}$ for qubit names. Similarly, we assume that variables come associated with the type of their possible values. Channels $c \in \text{Chan}$ are typed as $\widehat{\mathbb{N}}$, $\widehat{\mathbb{B}}$ and $\widehat{\mathcal{Q}}$, according to the values that they can propagate. Note that processes composed in parallel must use two disjoint sets of qubits, thus enforcing single ownership.

Since the type of a process is unique, we will call Σ_P the only context which types P (when such a type exists).

THEOREM 4.1. *Whenever $\Sigma \vdash P$ and $\Sigma' \vdash P$ then $\Sigma = \Sigma'$*

Example 4.2. Consider a quantum lottery $\mathbf{QL} = \mathbf{Pr} \parallel \mathbf{An}$ formed by processes $\mathbf{Pr}$, which prepares a qubit used as a source of randomness, and $\mathbf{An}$, which receives it, measures it, and announces the winner between Alice and Bob.

$$\begin{aligned} \mathbf{Pr} &= (t_1: X(q). t_3: c!q. \mathbf{0}) + (t_2: H(q). t_3: c!q. \mathbf{0}) \\ \mathbf{An} &= t_4: c?x. t_4: \mathcal{M}_{01}(x \triangleright y). \text{if } y = 0 \text{ then } t_5: a!1. \mathbf{0}_x \text{ else } t_6: b!1. \mathbf{0}_x \end{aligned}$$

Intuitively, $\mathbf{Pr}$ can prepare and send a qubit by applying either X or H to its qubit q , and $\mathbf{An}$ announces that Alice wins with $a!1$ if the received qubit is found in state $|0\rangle$, or that Bob wins with $b!1$ if it is found in state $|1\rangle$. The unique typing of $\mathbf{QL}$ is $\{q\} \vdash \mathbf{QL}$, with $a, b : \widehat{\mathbb{N}}$, $c : \widehat{\mathcal{Q}}$, $y : \mathbb{N}$, and $q, x : \mathcal{Q}$. In more detail, we have $\{q\} \vdash \mathbf{Pr}$, as both branches manipulate the q qubit and then send it; we have $\emptyset \vdash \mathbf{An}$, as its only quantum variable x is bound by the reception. Note that $\mathbf{An}$ is forced to terminate with either a discard $\mathbf{0}_x$ or a send $c!x$, because our linear type system forbids weakening of quantum variables: we have $\{x\} \vdash \mathbf{0}_x$ and $\{x\} \vdash c!x$, but not $\{x\} \vdash \mathbf{0}$. Concretely, this means that each process must either send or discard the qubits it uses, preventing ambiguities of previous approaches [Feng et al. 2007; Gay and Nagarajan 2006; Lalire and Jorrand 2004], as explained in [Ceragioli et al. 2024c]. By choosing the discard $\mathbf{0}_q$, we state that the final value of the qubit q is not relevant for the lottery protocol.

4.2 Operational Semantics

We describe a labelled semantics for lqCCS in terms of *configurations* $\langle \rho, P \rangle \in \text{Conf}$, each composed by a global quantum state and a tagged lqCCS process. Given a set $\Sigma = \{q_1, \dots, q_n\} \subseteq \mathcal{Q}$ and its associated Hilbert space $\mathcal{H}_\Sigma = \widehat{\mathcal{H}}^{\otimes n}$, a global quantum state ρ is a density operator in $\mathcal{DO}(\mathcal{H}_\Sigma)$. The type system is extended to configurations and distributions by considering the qubits of the underlying quantum state. Let Σ_ρ be the set of qubits appearing in ρ .

Definition 4.3 (Configuration Typing). Let $\langle \rho, P \rangle \in \text{Conf}$, with P typed and $\Sigma_P \subseteq \Sigma_\rho$, then we let $(\Sigma_\rho, \Sigma_P) \vdash \langle \rho, P \rangle$.

Let $\Delta \in \mathcal{D}^\leq(\text{Conf})$, then we let $(\Sigma, \Sigma') \vdash \Delta$ if $(\Sigma, \Sigma') \vdash C$ for any $C \in [\Delta]$.

Hereafter, we restrict ourselves to well-typed distributions, and denote with $\Sigma_{\bar{P}}$ the set $\Sigma_\rho \setminus \Sigma_P$, i.e. the qubits in the quantum state that are not owned by the process and thus freely accessible by the environment.

Our semantics is decorated with *syntactic schedulers*, which resolve non-determinism by choosing a tag. The syntax of schedulers $s \in \text{Sched}$ for tagged lqCCS is defined as follows

$$s ::= t \mid (t, t)$$

$$\begin{array}{c}
\text{TAU} \quad \langle \rho, t: \tau. P \rangle \xrightarrow{\tau}_t 1 \cdot \langle \rho, P \rangle \qquad \text{TAUSYNCH} \quad \langle \rho, (t, t'): \tau. P \rangle \xrightarrow{\tau}_{(t, t')} 1 \cdot \langle \rho, P \rangle \qquad \text{SOP} \quad \langle \rho, t: \mathcal{E}(\tilde{q}). P \rangle \xrightarrow{\tau}_t 1 \cdot \langle \mathcal{E}^{\tilde{q}}(\rho), P \rangle \\
\\
\text{MEAS} \quad \langle \rho, t: \mathcal{M}(\tilde{q} \triangleright x). P \rangle \xrightarrow{\tau}_t \sum_{m=0}^{|\mathbb{M}|-1} \text{tr}(M_m^{\tilde{q}}(\rho)) \cdot \left\langle \frac{M_m^{\tilde{q}}(\rho)}{\text{tr}(M_m^{\tilde{q}}(\rho))}, P[m/x] \right\rangle \qquad \text{SEND} \quad \frac{e \Downarrow v}{\langle \rho, t: c!e. P \rangle \xrightarrow{c!v}_t 1 \cdot \langle \rho, P \rangle} \\
\\
\text{RECV} \quad \frac{c: \widehat{Q} \Rightarrow v \in \Sigma_\rho \setminus \Sigma_P}{\langle \rho, t: c?v. P \rangle \xrightarrow{c?v}_t 1 \cdot \langle \rho, P[v/x] \rangle} \qquad \text{ITET} \quad \frac{e \Downarrow tt \quad \langle \rho, P \rangle \xrightarrow{\mu}_s \Delta}{\langle \rho, \text{if } e \text{ then } P \text{ else } Q \rangle \xrightarrow{\mu}_s \Delta} \qquad \text{ITEF} \quad \frac{e \Downarrow ff \quad \langle \rho, Q \rangle \xrightarrow{\mu}_s \Delta}{\langle \rho, \text{if } e \text{ then } P \text{ else } Q \rangle \xrightarrow{\mu}_s \Delta} \\
\\
\text{SUML} \quad \frac{\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta}{\langle \rho, P + Q \rangle \xrightarrow{\mu}_s \Delta} \qquad \text{SUMR} \quad \frac{\langle \rho, Q \rangle \xrightarrow{\mu}_s \Delta}{\langle \rho, P + Q \rangle \xrightarrow{\mu}_s \Delta} \qquad \text{PARL} \quad \frac{\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta \quad \mu \notin \{c?v \mid v \in \Sigma_Q\}}{\langle \rho, P \parallel Q \rangle \xrightarrow{\mu}_s \Delta \parallel Q} \\
\\
\text{PARR} \quad \frac{\langle \rho, Q \rangle \xrightarrow{\mu}_s \Delta \quad \mu \notin \{c?v \mid v \in \Sigma_P\}}{\langle \rho, P \parallel Q \rangle \xrightarrow{\mu}_s P \parallel \Delta} \qquad \text{SYNCHL} \quad \frac{\langle \rho, P \rangle \xrightarrow{c!v}_t 1 \cdot \langle \rho, P' \rangle \quad \langle \rho, Q \rangle \xrightarrow{c?v}_{t'} 1 \cdot \langle \rho, Q' \rangle}{\langle \rho, P \parallel Q \rangle \xrightarrow{\tau}_{(t, t')} 1 \cdot \langle \rho, P' \parallel Q' \rangle} \\
\\
\text{SYNCHR} \quad \frac{\langle \rho, P \rangle \xrightarrow{c?v}_t 1 \cdot \langle \rho, P' \rangle \quad \langle \rho, Q \rangle \xrightarrow{c!v}_{t'} 1 \cdot \langle \rho, Q' \rangle}{\langle \rho, P \parallel Q \rangle \xrightarrow{\tau}_{(t, t')} 1 \cdot \langle \rho, P' \parallel Q' \rangle} \qquad \text{RESTR} \quad \frac{\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta \quad \mu \notin \{c!v, c?v \mid v\}}{\langle \rho, P \setminus c \rangle \xrightarrow{\mu}_s \Delta \setminus c}
\end{array}$$

Fig. 4. Rules of lqCCS semantics.

A scheduler can select an action with a tag t , or a synchronization with a pair (t_1, t_2) . Intuitively, tags represent available visible options, upon which the scheduler can choose (possibly using a pair of them for synchronization). We call $\text{Tag}(P)$ and $\text{Tag}(s)$ the sets of tags that syntactically appear in the process P and in the scheduler s , respectively; we let $\text{Tag}(\Delta) = \bigcup_{\langle \rho, P \rangle \in [\Delta]} \text{Tag}(P)$.

We assume a set Act of actions, containing τ , $c!v$ and $c?v$ for any channel c and value v , i.e. either $n \in \mathbb{N}$, $b \in \mathbb{B}$, or $q \in \mathbb{Q}$. Intuitively, τ represents internal actions of processes, indistinguishable from the outside, while $c!v$ and $c?v$ model their interactions with the external environment, namely sending or receiving of classical and quantum values. The semantics of lqCCS is a probabilistic LTS (pLTS), i.e. a triple $(\text{Conf}, \text{Act}, \longrightarrow)$, with $\longrightarrow \subseteq \text{Conf} \times \text{Act} \times \text{Sched} \times \mathcal{D}(\text{Conf})$. A transition $(\langle \rho, P \rangle, \mu, s, \Delta) \in \longrightarrow$ is also denoted as $\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta$, and denotes that a configuration $\langle \rho, P \rangle$ can evolve under scheduler s with an action μ in a distribution Δ .

The transition relation $\longrightarrow$ is the smallest relation over configurations with closed processes that satisfies the rules in Figure 4. As expected, tagged actions require a matching tag on the transition. Expressions e are evaluated through a big step semantics $e \Downarrow v$ with v a value. We restrict to arithmetic and logical operations, and therefore omit the rules and assume that free variables are not evaluated. Note that the values of the qubits can only be observed through measurements, which alter such values and have a probabilistic outcome. In particular, the expression $q = q'$ just compares two qubit names, and not their values. In rule TAU and TAUSYNCH, the process performs a silent action and continues as P . The only difference between the two is that the former is caused by a

scheduler t and models an internal action, the latter is caused by (t, t) and models an internal synchronization. In rule **SOP**, the superoperator $\mathcal{E}$ is applied to the qubits in $\tilde{q}$. Since $\tilde{q}$ can be smaller than the whole Σ_ρ , we define $\mathcal{E}^{\tilde{q}}$ as the superoperator that acts on the whole ρ but “ignores” the qubits outside $\tilde{q}$. More precisely, $\mathcal{E}^{\tilde{q}}$ is obtained by composing: (i) a suitable set of SWAP unitaries to bring the qubits $\tilde{q}$ in the first positions; (ii) the tensor product 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]. In rule **MEAS**, given a measurement $\mathcal{M} = \{M_m\}$, for each m , M_m stands for the trace non-increasing superoperator such that $M_m(\sigma) = M_m \sigma M_m^\dagger$, and M_m^q is defined as before. In rule **SEND**, the process $t: c!e. P$ evaluates an expression e and sends the resulting value v on channel c . In rule **RECV**, a value v is received from a channel c and syntactically substituted in place of the variable x , with one caveat: if c is a quantum channel, v must be one of the “available” qubits, i.e. the ones in ρ not owned by P . In the rules **ITET** and **ITEF**, the process **if** e **then** P **else** Q decides to behave as either P or Q depending on the value of e . In the rules **SUML** and **SUMR**, instead, the process $P + Q$ non-deterministically decides to behave as either P or Q . In the rules **PARL** and **PARR**, both parallel processes P and Q can evolve independently, and the “idle” process remains identical. In the conclusion, we use the parallel composition of a distribution $\Delta = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle$ and a process Q , defined as $\Delta \parallel Q = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \parallel Q \rangle$, and similarly for $Q \parallel \Delta$. Moreover, if μ is a quantum reception, we must ensure that P is not receiving a qubit owned by Q , and vice-versa: labelled actions represent communication with the environment and not with other processes. In the rules **SYNCHL** and **SYNCHR** two parallel processes synchronize, by sending and receiving on the same channel: the value gets captured by the receiver, and the transition is not visible to the environment, resulting in a τ label. Notice how a scheduler must specify two different tags, t and t' , in order to select both a transition of P and one of Q . Finally, in rule **RESTR**, we forbid a process $P \setminus c$ to perform visible actions (i.e. communications to and from the environment) on channel c . In the conclusion, we write $\Delta \setminus c$ for the restriction on c of all the processes in Δ , similarly to $\Delta \parallel P$ defined above. For example, notice that a process $\langle \rho, (t_0: c!0. P \parallel t_1: c?x. Q) \setminus c \rangle$ cannot communicate with the environment, but can still synchronize by sending 0 on the channel c , as synchronization causes a τ action, not a visible one.

Example 4.4. The pLTS semantics of the quantum lottery **QL** from Example 4.2 on quantum state $|0\rangle\langle 0|$ is in Figure 5, where **An'** stands for $t_4: M_{01}(x \triangleright y). \mathbf{An''}$, and **An''** is **if** $y = 0$ **then** $t_5: a!1. 0_x$ **else** $t_6: b!1. 0_x$. To simplify the presentation, we draw $\xrightarrow{s: \mu}$ instead of $\xrightarrow{\mu}_s$ and we represent probability distributions graphically: in place of a distribution $\sum p_i \cdot \langle \rho_i, P_i \rangle$, we draw a black dot connected with a probability-labelled squiggly arrow to each $\langle \rho_i, P_i \rangle$ in the support. For brevity, we drop the probabilistic label 1. A scheduler for **QL** must decide (i) which unitary **Pr** applies to the qubit q , either X (i.e. $s = t_1$) or H (i.e. $s = t_2$); and (ii) whether the qubit is sent to **An** or to the external environment since the channel is not restricted, i.e. the available moves are with label τ and scheduler (t_3, t_4) , or with label $c!q$ and $s = t_3$. Intuitively, if **Pr** chooses X , then Bob will win, otherwise either Alice or Bob will win with the same probability. Note that at the beginning, in configuration $\langle |0\rangle\langle 0|, \mathbf{QL} \rangle$, the choice t_4 cannot be taken because the quantum state has no qubit apart from those in $\Sigma_{\mathbf{QL}}$.

Our chosen semantics follows a labelled approach based on pLTSs, designed to be a minimal extension of value-passing CCS [Hennessy 1991] to the quantum setting. Other, more compact presentations are possible, for example using structural congruence rules and reduction systems as in [Ceragioli et al. 2024c], which recover the τ fragment of our pLTS. Whereas a reduction system models only internal actions and synchronizations between processes, a labelled semantics puts the emphasis on the interaction with the external environment, thus allowing for compositional reasoning. Indeed, when studying a composite system, we can address its components one by one, each time interpreting the others as the environment; we can then combine their semantics to distil the behaviour of the composite. Finally, as explored in section 6 a labelled semantics is key for deriving a decidable characterization of behavioural equivalence.

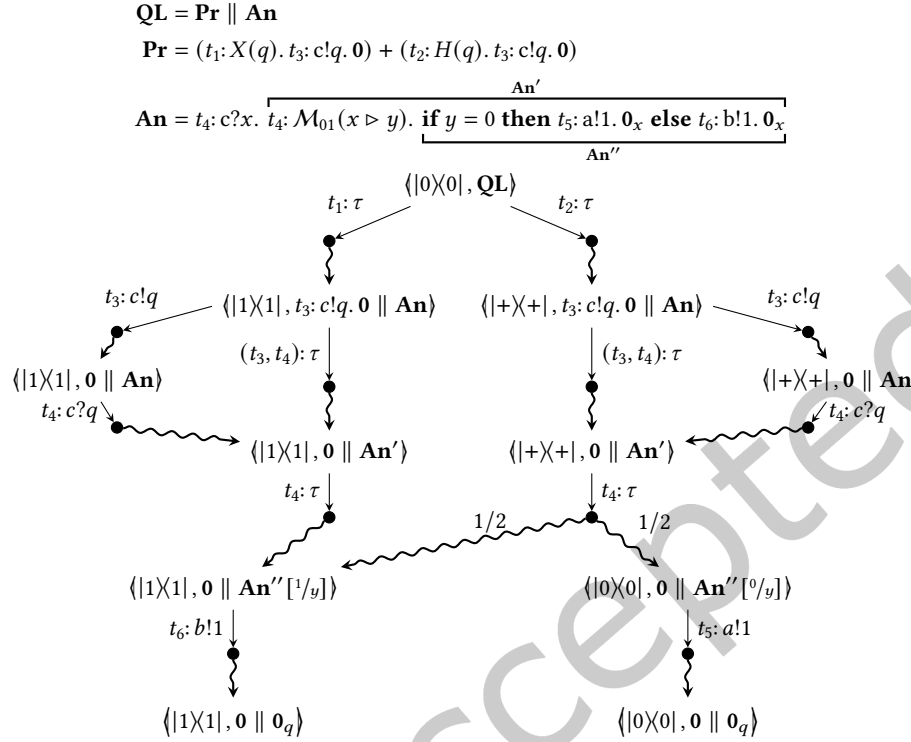


Fig. 5. Semantics of the quantum lottery process.

It is worth noting that the typing is preserved by τ -transitions.

THEOREM 4.5 (TYPING PRESERVATION). *If $(\Sigma_\rho, \Sigma_P) \vdash \langle \rho, P \rangle$ and $\langle \rho, P \rangle \xrightarrow{\tau}_s \Delta$ then $(\Sigma_\rho, \Sigma_P) \vdash \Delta$.*

As hinted by the previous theorem, type preservation does not hold in general. However, the updated typing context is uniquely determined by the transition label, and it is still a subset of the qubits available in the quantum state.

THEOREM 4.6 (TYPING QUASI-PRESERVATION). *Let $\Sigma \subseteq Q$ and $\mu \in Act$. Then there exists Σ' such that for all $(\Sigma'', \Sigma) \vdash C$ and $\Delta \in \mathcal{D}(Conf)$ with $C \xrightarrow{\mu}_s \Delta$ it holds $(\Sigma'', \Sigma') \vdash \Delta$.*

Following standard practice, we assume hereafter that processes are tagged in a deterministic way, meaning that the behaviour of configurations is determined by the choice of the scheduler. For this, we take the standard approach of [Chatzikokolakis et al. 2009; Chatzikokolakis and Palamidessi 2007], and we extend it to deal with the value-passing features of lqCCS. Intuitively, a deterministic process associates a different tag to all of its available non-deterministic choices, thus any given scheduler s forces a unique action μ and a unique transition $\xrightarrow{\mu}_s$. However, this is too restrictive for a labelled semantics where receptions are caused by the choices of other processes. Our schedulers, indeed, solve only the *internal* non-determinism (like $t: c!0. P + t': c!1. Q$), and do not address the *external* one, which comes from outside input (like $c?x. P$). Thus, only for input transitions, we allow

a deterministic process P to have multiple reductions for the same scheduler s , one for each value it can receive, like $\xrightarrow{s}^{c?0}$ and $\xrightarrow{s}^{c?1}$.

Definition 4.7 (Deterministic Process). A process P is *deterministic* if for all $\rho \in \mathcal{H}_\Sigma$ with $\Sigma \supseteq \Sigma_P$, $s \in \text{Tag}(P)$, $\mu, \mu' \in \text{Act}$ and $\Delta, \Delta' \in \mathcal{D}^\leq(\text{Conf})$, if $\langle \rho, P \rangle \xrightarrow{s}^\mu \Delta$ and $\langle \rho, P \rangle \xrightarrow{s}^{\mu'} \Delta'$, then either $\mu = \mu'$ and $\Delta = \Delta'$, or $\mu \neq \mu'$ and there exists c, v and v' such that $\mu = c?v$ and $\mu' = c?v'$.

Assumption 1. All processes considered in the following are deterministic.

In quantum process calculi, it is useful to consider a pLTS as a simple LTS between distributions [Ceragioli et al. 2024c; Deng 2018; Feng and Ying 2015]. Intuitively, we want to lift the probabilistic transition relation, that goes from configurations to distributions of configurations, to a transition relations from distributions to distributions, thanks to the $\text{llift}(\cdot)$ operation presented in section 3. We will detail two different way to lift our scheduled pLTSs semantics: one preserves the scheduler information and the other one ignores it. We will explore the difference of these two systems in the next section, showing how consistent scheduling policies are crucial in the quantum setting.

First, we define a semantics in which $\Delta \xrightarrow{s}^\mu \Delta'$ means that a system in state Δ can transition to Δ' if all the elements of the support of Δ perform the move chosen by the scheduler s with action μ . As an initial step, we add a “deadlock” rule, allowing configurations to evolve to the empty distribution if no legal move is available for the same label and scheduler: Formally, we let $\text{bot}(\xrightarrow{s}) \in \text{Conf} \times \text{Act} \times \text{Sched} \times \mathcal{D}^\leq(\text{Conf})$ as the least relation such that $\text{bot}(\xrightarrow{s}) \supseteq \xrightarrow{s}$ and $C \text{ bot}(\xrightarrow{s}) \in$ if there is no Δ such that $C \xrightarrow{s}^\mu \Delta$. Notice that, by definition, $(\Sigma, \Sigma') \vdash \epsilon$ for any (Σ, Σ') , since the support of ϵ is empty. Then, we lift the semantics to deal with distributions of configurations, defining $\xrightarrow{s}$ as the relation in $\mathcal{D}^\leq(\text{Conf}) \times \text{Act} \times \text{Sched} \times \mathcal{D}^\leq(\text{Conf})$ such that for all μ and s , it holds that $\xrightarrow{s}^\mu = \text{llift}(\text{bot}(\xrightarrow{s}^\mu))$. The obtained transition relation is linear and left-decomposable, by Lemma 3.1.

Due to Assumption 1, the evolution of distributions under a given action is uniquely determined by the scheduler.

PROPOSITION 4.8. *For any distribution $\Delta \in \mathcal{D}^\leq(\text{Conf})$ composed of deterministic processes, $\mu \in \text{Act}$, $s \in \text{Sched}$, and $\Theta, \Theta' \in \mathcal{D}^\leq(\text{Conf})$, if $\Delta \xrightarrow{s}^\mu \Theta$ and $\Delta \xrightarrow{s}^\mu \Theta'$ then $\Theta = \Theta'$.*

Finally, to discuss the impact of using schedulers, and their importance for correctly representing feasible choices of quantum-capable agents, we define an unscheduled lifted semantics for comparison. Let $\xrightarrow{\bullet}$ be the relation in $\mathcal{D}^\leq(\text{Conf}) \times \text{Act} \times \mathcal{D}^\leq(\text{Conf})$ such that for each μ it holds that $\xrightarrow{\bullet}^\mu = \text{llift}(\bigcup_s \text{bot}(\xrightarrow{s}^\mu))$. Intuitively, $\xrightarrow{\bullet}^\mu$ allows to probabilistic compose moves regardless of whether the schedulers coincide.

Example 4.9. Recall Example 4.4. The *scheduled* lifted semantics to distributions of configurations is in Figure 6. The application of the lifting operations is evident in the last step of the protocol of the right branch. After the measurement the semantics has reached the full distribution of configuration $\frac{1}{2} \cdot \langle |0\rangle\langle 0|, 0 \parallel \mathbf{An}''[0/y] \rangle \oplus \frac{1}{2} \cdot \langle |1\rangle\langle 1|, 0 \parallel \mathbf{An}''[1/y] \rangle$, where, as expected, both Alice and Bob have half of the probability of being selected. Each element of the distribution has a continuation with a distinct tag and action, therefore by definition of $\text{bot}(\cdot)$ the other pairing can only move to the empty distribution ϵ , e.g. $\frac{1}{2} \cdot \langle |0\rangle\langle 0|, 0 \parallel \mathbf{An}''[0/y] \rangle \xrightarrow{b!1}_{t_6} \epsilon$. Thus, by lifting, full distribution can evolve either in the distribution $\frac{1}{2} \cdot \langle |0\rangle\langle 0|, 0 \parallel 0_q \rangle$ with tag t_5 and action $a!1$ or to the distribution $\frac{1}{2} \cdot \langle |1\rangle\langle 1|, 0 \parallel 0_q \rangle$ with tag t_6 and action $b!1$.

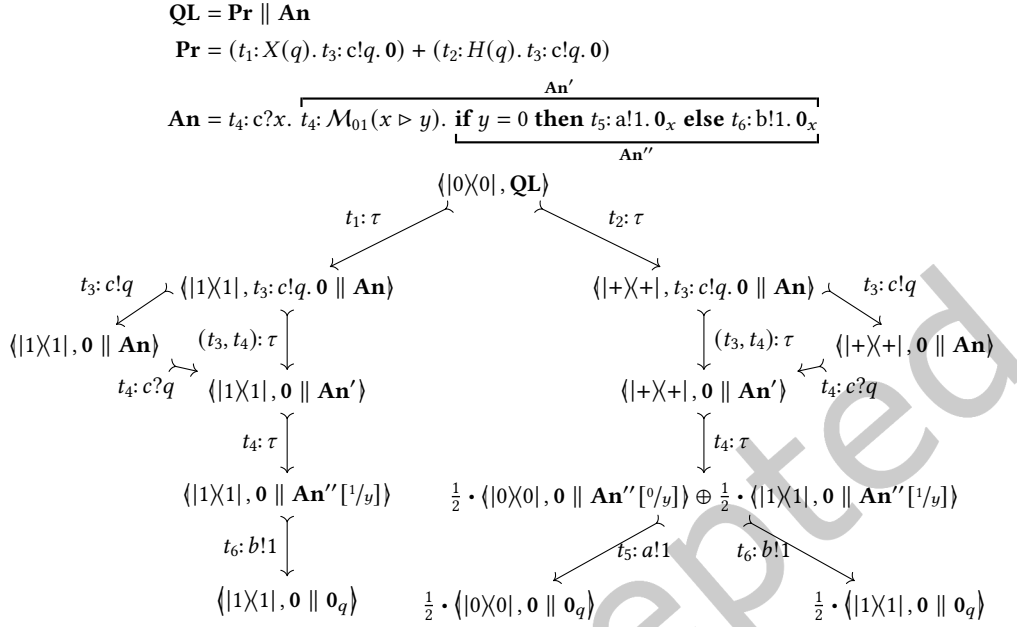


Fig. 6. Lifted semantics of the quantum lottery process.

5 Contextual Equivalences for Quantum Systems

We now pursue a suitable behavioural equivalence for concurrent quantum systems. We start by defining a saturated bisimilarity *à la* [Bonchi et al. 2014], a natural notion of contextual equivalence that relates systems when they are indistinguishable for any observer. We show that the naive definition of saturated probabilistic bisimilarity is not consistent with the prescriptions of quantum theory. Next, we show that schedulers guarantee adherence with the prescriptions of quantum theory, as contexts cannot choose their move based on the unknown states of unmeasured qubits, and we investigate some desired properties of the scheduled saturated bisimilarity. The main drawback of our saturated approach is that the quantification over all possible observers make the relation difficult to compute. Thus, in the next section, we will give an equivalent characterization in terms of labelled bisimulations.

5.1 Saturated Bisimilarity

Before presenting saturated bisimilarity, we need a couple of definitions. We start by introducing well-typed relations, i.e. those that only associate equally typed distributions of configurations. Recall that the empty distribution ϵ is typed by any pair of sets of qubits (Σ, Σ') with $\Sigma' \subseteq \Sigma$.

Definition 5.1 (Well-typed Relation). A relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$ is well-typed if $\Delta \mathcal{R} \Theta$ implies $(\Sigma, \Sigma') \vdash \Delta$ and $(\Sigma, \Sigma') \vdash \Theta$ for some Σ, Σ' .

In saturated bisimilarities, we call *contexts* processes with a typed hole; they play the role of process-discriminating observers.

Definition 5.2 (Context). A context $B[\cdot]_\Sigma$ is generated by the productions $B[\cdot]_\Sigma ::= [\cdot]_\Sigma \mid [\cdot]_\Sigma \parallel P$ typed according to the rules in Figure 3, extended as such:

$$\begin{array}{c} \text{ID} \\ \Sigma \vdash [\cdot]_\Sigma \end{array} \qquad \frac{\text{HOLE} \quad \Sigma' \setminus \Sigma \vdash P \quad \Sigma \subseteq \Sigma'}{\Sigma' \vdash [\cdot]_\Sigma \parallel P}.$$

A context is applied to a process P 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. We write $B[\langle \rho, P \rangle]$ for $\langle \rho, B[P] \rangle$, 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. In the following we let $\text{Tag}(B[\cdot])$ be $\text{Tag}(P)$ if $B[\cdot] = [\cdot] \parallel P$ and $\emptyset$ if $B[\cdot] = [\cdot]$.

We formalize compatible contexts that can be applied to distributions as follows.

Definition 5.3 (Compatible Context). A context $\Sigma' \vdash B[\cdot]_\Sigma$ is compatible with respect to a distribution $\Delta \in \mathcal{D}^\leq(\text{Conf})$ if $(\Sigma'', \Sigma) \vdash \Delta$ for some Σ'' such that $\Sigma' \subseteq \Sigma''$, and if $\text{Tag}(\Delta) \cap \text{Tag}(B[\cdot]) = \emptyset$.

The requirement for tags to be distinct between distributions and contexts ensures that distributions preserve their determinism when inserted into compatible contexts. Intuitively, this guarantees that we are not introducing non-deterministic behaviour besides the one regulated by schedulers and by the external choices.

LEMMA 5.4. *For all deterministic $P, R \in \text{Proc}$, if $\text{Tag}(P) \cap \text{Tag}(R) = \emptyset$ then $P \parallel R$ is deterministic.*

PROOF SKETCH. By case analysis on the scheduler. The interesting case is the synchronization between P and R . By Assumption 1 there cannot be both a valid SYNCHL and SYNCHR transition otherwise there would be two moves with distinct labels with the same scheduler in both P and R . Furthermore, reception and sending must have the same value in synchronizations, and since by Assumption 1 there can only be one specific sending value, then also the reception must be compatible. $\square$

We are now ready to introduce our first equivalence. A saturated bisimulation is a relation over distributions where related pairs must have the same type and mass, and must reduce in related distributions under every possible compatible context. We start with unscheduled saturated bisimilarity, which is the standard definition for probabilistic systems, used e.g. in [Feng et al. 2007].

Definition 5.5 (Unscheduled Saturated Bisimilarity). A well-typed relation $\mathcal{R} \subseteq \mathcal{D}^\leq(\text{Conf}) \times \mathcal{D}^\leq(\text{Conf})$ is a (unscheduled) *saturated bisimulation* if $\Delta \mathcal{R} \Theta$ implies $|\Delta| = |\Theta|$ and, for any context $B[\cdot]$ compatible with both Δ and Θ , it holds that

- whenever $B[\Delta] \xrightarrow{\tau} \Delta'$, there exists Θ' such that $B[\Theta] \xrightarrow{\tau} \Theta'$ and $\Delta' \mathcal{R} \Theta'$;
- whenever $B[\Theta] \xrightarrow{\tau} \Theta'$, there exists Δ' such that $B[\Delta] \xrightarrow{\tau} \Delta'$ and $\Delta' \mathcal{R} \Theta'$.

Let *unscheduled saturated bisimilarity*, denoted $\simeq_\bullet$, be the largest unscheduled saturated bisimulation.

We now compare the bisimilarity above with the prescriptions of quantum theory, showing that it is not consistent with Fact 1.

We consider a specific counterexample of processes that should be indistinguishable according to quantum theory: 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 in both

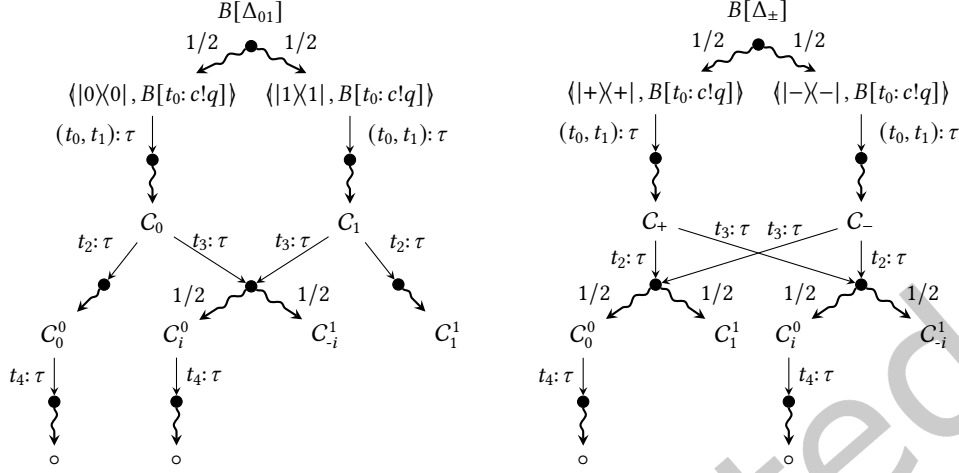


Fig. 7. Indistinguishable qubit sources Δ_{01} and $\Delta_{\pm}$ are distinguished by the context $B[\cdot]$.

cases the received qubit is in state $\frac{1}{2}I$, and therefore behaves the same (see [Nielsen and Chuang 2010]). One expects the lqCCS encoding of these sources to be bisimilar, however, this is not the case for $\simeq_{\bullet}$.

Example 5.6. The lqCCS encodings of these sources follows:

$$\Delta_{01} = \frac{1}{2} \cdot \langle |0\rangle\langle 0|, t_0: c!q \rangle \oplus \frac{1}{2} \cdot \langle |1\rangle\langle 1|, t_0: c!q \rangle \quad \text{and} \quad \Delta_{\pm} = \frac{1}{2} \cdot \langle |+\rangle\langle +|, t_0: c!q \rangle \oplus \frac{1}{2} \cdot \langle |-\rangle\langle -|, t_0: c!q \rangle$$

The unscheduled bisimilarity erroneously discriminates the two sources. To see that $\Delta_{01} \not\simeq_{\bullet} \Delta_{\pm}$, take $B[\cdot] \parallel t_1: c?x. (P + Q)$ where

$$P = t_2: \mathcal{M}_{01}(x \triangleright y). R \quad \text{and} \quad Q = t_3: \mathcal{M}_{\pm i}(x \triangleright y). R \quad \text{with} \quad R = (\text{if } y = 0 \text{ then } t_4: \tau \text{ else } 0) \parallel 0_x$$

Notice that P and Q perform different measurements and make the outcome observable by enabling a τ -transition only when $y = 0$. In a nutshell, we distinguish the sources since a series of reductions $B[\Delta_{01}] \xrightarrow{\tau} \Delta'_{01} \xrightarrow{\tau} \Delta''_{01} \xrightarrow{\tau} \Theta_{01}$ exists where $|\Theta_{01}| = 3/4$, while all reductions $B[\Delta_{\pm}] \xrightarrow{\tau} \Delta'_{\pm} \xrightarrow{\tau} \Delta''_{\pm} \xrightarrow{\tau} \Theta_{\pm}$ are such that $|\Theta_{\pm}| = 1/2$.

Formally, let C_{ψ} be $\langle |\psi\rangle\langle \psi|, P + Q \rangle [q/x]$ and C_{ψ}^n be $\langle |\psi\rangle\langle \psi|, R[n/y] \rangle$ for $n \in \{0, 1\}$, then Figure 7 shows the τ -transitions of the two systems: $B[\Delta_{01}]$ reduces to $\Delta'_{01} = \frac{1}{2} \cdot C_0 \oplus \frac{1}{2} \cdot C_1$, and $B[\Delta_{\pm}]$ can only reduce to $\Delta'_{\pm} = \frac{1}{2} \cdot C_+ \oplus \frac{1}{2} \cdot C_-$ to match this move. As seen in figure, each C_{ψ} has available reductions both with t_2 and t_3 . Consider the following ones:

$$\begin{aligned} C_0 &\xrightarrow{t_2} 1 \cdot \langle |0\rangle\langle 0|, R[0/y] \rangle = 1 \cdot C_0^0, \\ C_1 &\xrightarrow{t_3} \frac{1}{2} \cdot \langle |i\rangle\langle i|, R[0/y] \rangle \oplus \frac{1}{2} \cdot \langle |-i\rangle\langle -i|, R[1/y] \rangle = \frac{1}{2} \cdot C_i^0 \oplus \frac{1}{2} \cdot C_{-i}^1 \end{aligned}$$

In the unscheduled semantics, Δ'_{01} can mix the two choices and reduce C_0 with t_2 and C_1 with t_3 , formally, $\Delta'_{01} \xrightarrow{\tau} \frac{1}{2} \cdot C_0^0 \oplus \frac{1}{4} \cdot C_i^0 \oplus \frac{1}{4} \cdot C_{-i}^1 = \Delta''_{01}$. This move corresponds to taking the left reductions both probabilistic branches of the pLTS of Figure 7. However, choosing these tags requires knowing if we are in C_0 or C_1 , which should be only possible by measuring the received qubit, which is not the case. Finally, note that $\Delta''_{01} \xrightarrow{\tau} \Theta_{01}$ with $|\Theta_{01}| = 3/4$, because C_{ψ}^n can move (with t_4) only if $n = 0$.

Consider now $\Delta'_\pm$. The following moves are all those available for C_+ :

$$\begin{aligned} C_+ &\xrightarrow{t_2} \frac{1}{2} \cdot \langle |0\rangle\langle 0|, R[0/y] \rangle \oplus \frac{1}{2} \cdot \langle |1\rangle\langle 1|, R[1/y] \rangle = \frac{1}{2} \cdot C_0^0 \oplus \frac{1}{2} \cdot C_1^1 \\ C_+ &\xrightarrow{t_3} \frac{1}{2} \cdot \langle |i\rangle\langle i|, R[0/y] \rangle \oplus \frac{1}{2} \cdot \langle |-i\rangle\langle -i|, R[1/y] \rangle = \frac{1}{2} \cdot C_i^0 \oplus \frac{1}{2} \cdot C_{-i}^1, \end{aligned}$$

Noticeably, the available moves of C_- coincide.

It is easy to check that $\Delta'_\pm$ cannot replicate the behaviour of Δ'_{01} : for any choice of t_2 and t_3 it will reduce to a $\Delta''_\pm$ where only half of the configurations in the support can move, i.e. such that $\Delta''_\pm \xrightarrow{\tau} \bullet \Theta_\pm$ only if $|\Theta_\pm| = 1/2$.

Example 5.6 is paradigmatic, where different mixtures of quantum states are discriminated because the moves are chosen according to the value of some received qubit, which in theory should be unknown. Our schedulers do not allow processes to replicate this behaviour, forcing distributions to make a reasonable choice based on classically determined tags. On a practical account, this feature is relevant for real-world applications, as several quantum protocols rely on the indistinguishability of these sources (or similar ones).

The counterexample highlighted by the example above is not typical of our specific formulation. Indeed, the two sources are commonly discriminated by the earliest probabilistic bisimilarities proposed for quantum protocols, e.g., the ones of [Deng and Feng 2012; Feng et al. 2007]. This problem is solved by more recent proposals [Deng 2018; Feng and Ying 2015], which correctly identify the two processes. However, similar cases remain unsolved in literature, calling for a principled approach like the one we propose. As an example, we present a simple protocol that does not feature communication, yet it permits unscheduled bisimilarity to instantly distinguish which operation has been locally performed, achieving physically implausible faster-than-light communication. Furthermore, this example proves that schedulers are needed also when no quantum communication is involved.

Example 5.7. The protocol is set between two actors, Alice and Bob, who share an entangled pair of qubits (q_1, q_2) in the entangled state $|\Phi^+\rangle$. Before moving apart, they synchronize their clocks and agree that at some given time Alice will measure her qubit in one of two agreed bases, and Bob will immediately try to guess which measurement Alice performed. If the two succeed in finding a physically realizable procedure for Bob to correctly guess the measurement, then Alice can instantly communicate a bit to Bob, regardless of the distance separating them. Such a procedure should be impossible according to the commonly understood laws of physics.

Assume Alice and Bob agree that Alice will measure her qubit in either the computational or diagonal basis, thus implicitly sending respectively 0 or 1. We will model the actors in lqCCS as follows

$$\begin{aligned} A_{01} &:= t_0: \mathcal{M}_{01}(q_1 \triangleright x). 0_{q_1} \\ A_\pm &:= t_0: \mathcal{M}_\pm(q_1 \triangleright x). 0_{q_1} \\ B &:= (t_1: \mathcal{M}_{01}(q_2 \triangleright y). t_1: c!y. 0_{q_2}) + (t_2: \mathcal{M}_{\pm i}(q_2 \triangleright y). t_2: c!y. 0_{q_2}) \end{aligned}$$

Superluminal communication is possible if Bob is capable of distinguishing the two Alice processes, that is, if we have that $\langle |\Phi^+\rangle\langle \Phi^+|, A_{01} \parallel B \rangle \neq_\bullet \langle |\Phi^+\rangle\langle \Phi^+|, A_\pm \parallel B \rangle$.

Assume Alice performs her measure, as expected

$$\begin{aligned} 1 \cdot \langle |\Phi^+\rangle\langle \Phi^+|, A_{01} \parallel B \rangle &\xrightarrow{\tau} \bullet \Delta = \frac{1}{2} \cdot \langle |00\rangle\langle 00|, 0_{q_1} \parallel B \rangle \oplus \frac{1}{2} \cdot \langle |11\rangle\langle 11|, 0_{q_1} \parallel B \rangle \\ 1 \cdot \langle |\Phi^+\rangle\langle \Phi^+|, A_\pm \parallel B \rangle &\xrightarrow{\tau} \bullet \Theta = \frac{1}{2} \cdot \langle |++\rangle\langle ++|, 0_{q_1} \parallel B \rangle \oplus \frac{1}{2} \cdot \langle |--\rangle\langle --|, 0_{q_1} \parallel B \rangle \end{aligned}$$

In the unscheduled semantics, the distribution Δ can evolve by selecting distinct tags for each element of its distribution, for example by performing the measurement on the standard basis for the distribution with state

$|00\rangle\langle 00|$ and the measurement in the imaginary basis for the distribution with state $|11\rangle\langle 11|$.

$$\frac{1}{2} \cdot \langle |00\rangle\langle 00|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \oplus \frac{1}{2} \cdot \langle |11\rangle\langle 11|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \xrightarrow{\tau} \Delta' = \frac{1}{2} \cdot C_{|00\rangle}^0 \oplus \frac{1}{4} \cdot C_{|1i\rangle\langle 1i|}^0 \oplus \frac{1}{4} \cdot C_{|11\rangle\langle 11|}^1$$

where $C_{|\psi\rangle}^i$ is the configuration $\langle |\psi\rangle\langle\psi|, \mathbf{0}_{q_1} \parallel c!i. \mathbf{0}_{q_2} \rangle$. Take the context $B[\cdot] = [\cdot] \parallel c?x. \text{if } x = 0 \text{ then } \tau. \mathbf{0} \text{ else } \mathbf{0}$, that immediately goes in deadlock only if the output on the channel c is 1. After performing the synchronization, only the distribution starting from C^0 can perform another move, therefore the total mass of the distribution is $3/4$.

This particular execution cannot be replicated by Θ for any possible combination of tags.

$$\begin{aligned} & \frac{1}{2} \cdot \langle |++\rangle\langle ++|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \oplus \frac{1}{2} \cdot \langle |--\rangle\langle --|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \xrightarrow{\tau} \frac{1}{4} \cdot C_{|+0\rangle}^0 \oplus \frac{1}{4} \cdot C_{|+1\rangle}^1 \oplus \frac{1}{4} \cdot C_{|-0\rangle\langle -0|}^0 \oplus \frac{1}{4} \cdot C_{|-1\rangle\langle -1|}^1 \\ & \frac{1}{2} \cdot \langle |++\rangle\langle ++|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \oplus \frac{1}{2} \cdot \langle |--\rangle\langle --|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \xrightarrow{\tau} \frac{1}{4} \cdot C_{|+0\rangle}^0 \oplus \frac{1}{4} \cdot C_{|+1\rangle}^1 \oplus \frac{1}{4} \cdot C_{|-i\rangle\langle -i|}^0 \oplus \frac{1}{4} \cdot C_{|-1\rangle\langle -1|}^1 \\ & \frac{1}{2} \cdot \langle |++\rangle\langle ++|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \oplus \frac{1}{2} \cdot \langle |--\rangle\langle --|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \xrightarrow{\tau} \frac{1}{4} \cdot C_{|+i\rangle}^0 \oplus \frac{1}{4} \cdot C_{|+1\rangle}^1 \oplus \frac{1}{4} \cdot C_{|-0\rangle\langle -0|}^0 \oplus \frac{1}{4} \cdot C_{|-1\rangle\langle -1|}^1 \\ & \frac{1}{2} \cdot \langle |++\rangle\langle ++|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \oplus \frac{1}{2} \cdot \langle |--\rangle\langle --|, \mathbf{0}_{q_1} \parallel \mathbf{B} \rangle \xrightarrow{\tau} \frac{1}{4} \cdot C_{|+i\rangle}^0 \oplus \frac{1}{4} \cdot C_{|+1\rangle}^1 \oplus \frac{1}{4} \cdot C_{|-i\rangle\langle -i|}^0 \oplus \frac{1}{4} \cdot C_{|-1\rangle\langle -1|}^1 \end{aligned}$$

It is evident that applying the same context $B[\cdot]$ as for Δ , after the synchronization the mass of the resulting distribution is always $1/2$. Therefore, we showed that $\langle |\Phi^+\rangle\langle\Phi^+|, \mathbf{A}_{01} \parallel \mathbf{B} \rangle \neq \langle |\Phi^+\rangle\langle\Phi^+|, \mathbf{A}_{\pm} \parallel \mathbf{B} \rangle$, and proved that an unscheduled semantics allows superluminal communication.

5.2 Scheduled Bisimilarity

The two examples on qubit sources show that classical probabilistic approaches fail to correctly model quantum observability, due to processes capable to act differently in each element of a distribution. In the following we define a scheduled bisimilarity, where distributions are required to evolve according to the same scheduler.

Definition 5.8 (Scheduled Saturated Bisimilarity). A well-typed relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$ is a *scheduled saturated bisimulation* if $\Delta \mathcal{R} \Theta$ implies $|\Delta| = |\Theta|$ and for any context $B[\cdot]$ compatible with both Δ and Θ , and for any scheduler s , it holds that

- whenever $B[\Delta] \xrightarrow{\tau}_s \Delta'$, there exists Θ' such that $B[\Theta] \xrightarrow{\tau}_s \Theta'$ and $\Delta' \mathcal{R} \Theta'$;
- whenever $B[\Theta] \xrightarrow{\tau}_s \Theta'$, there exists Δ' such that $B[\Delta] \xrightarrow{\tau}_s \Delta'$ and $\Delta' \mathcal{R} \Theta'$.

Let *scheduled saturated bisimilarity*, denoted $\simeq$, be the largest scheduled saturated bisimulation.

Schedulers suffice for guaranteeing indistinguishability of qubit sources sending $|0\rangle$ and $|1\rangle$ or $|+\rangle$ and $|-\rangle$ with equal probability.

Example 5.9. Consider a pair of non-biased random qubit sources as those of Example 5.6. Fittingly, the lqCCS encodings of these sources are scheduled saturated bisimilar: $\Delta_{01} \simeq \Delta_{\pm}$. Intuitively, this holds because scheduler consistency in the definition of $\xrightarrow{\tau}$ forbids to combine moves labelled by different choices: Δ'_{01} cannot mix the two choices to obtain an outcome that $\Delta'_{\pm}$ cannot replicate as it does in Example 5.6. In a nutshell, this allows to prove that both Δ_{01} and $\Delta_{\pm}$ are bisimilar to the point distribution with quantum state $\frac{1}{2}\mathbb{I}$, as one may expect from Fact 1.

$$\begin{aligned} \Delta_{01} &= \frac{1}{2} \cdot \langle |0\rangle\langle 0|, t_0: c!q \rangle \oplus \frac{1}{2} \cdot \langle |1\rangle\langle 1|, t_0: c!q \rangle \simeq 1 \cdot \left\langle \frac{1}{2}\mathbb{I}, t_0: c!q \right\rangle \\ \Delta_{\pm} &= \frac{1}{2} \cdot \langle |+\rangle\langle +|, t_0: c!q \rangle \oplus \frac{1}{2} \cdot \langle |-\rangle\langle -|, t_0: c!q \rangle \simeq 1 \cdot \left\langle \frac{1}{2}\mathbb{I}, t_0: c!q \right\rangle \end{aligned}$$

The following theorem generalizes the equality of the example above, and lifts to lqCCS the indistinguishability relations between quantum states of Fact 1. This property states that the same process, acting on two different but indistinguishable mixed quantum states, exhibits behaviour that cannot be distinguished by any observer, therefore yielding bisimilar distributions.

THEOREM 5.10. *If $\sum_i p_i \cdot \rho_i = \sum_j q_j \cdot \rho_j$ then $\sum_i p_i \cdot \langle \rho_i, P \rangle \simeq \sum_j q_j \cdot \langle \rho_j, P \rangle$.*

PROOF SKETCH. We prove that $\Delta = p \cdot \langle \rho, P \rangle \oplus (1-p) \cdot \langle \sigma, P \rangle \simeq 1 \cdot \langle p \cdot \rho + (1-p) \cdot \sigma, P \rangle = \Theta$, and the theorem follows by transitivity. First, we show that Δ replicates the moves of Θ by the linearity of superoperators, i.e. $p \cdot \mathcal{E}(\rho) + (1-p) \cdot \mathcal{E}(\sigma) = \mathcal{E}(p \cdot \rho + (1-p) \cdot \sigma)$, and similarly for measurements. Then, we show that Θ simulates Δ . Here, the presence of schedulers is key: it forbids Δ from combining different non-deterministic choices to perform a move that would not be available to Θ (see Example 5.6). $\square$

This result directly derives from the use of schedulers, and it is not common in quantum versions of CCS: it holds only for specific distributions in [Ceragioli et al. 2024c] and in [Deng 2018].

Finally, we notice that $\simeq$ is a linear relation, meaning that probabilistic combinations of bisimilar distributions yield bisimilar distributions. In symbols, whenever $\Delta_i \simeq \Theta_i$ for all $i \in I$, then we have $\sum_{i \in I} p_i \cdot \Delta_i \simeq \sum_{i \in I} p_i \cdot \Theta_i$.

THEOREM 5.11. *The bisimilarity $\simeq$ is linear.*

PROOF SKETCH. We first define the *linear closure operator* $\text{lc}(\cdot)$ on relations between distributions

$$\frac{\forall i \in I. \Delta_i \mathcal{R} \Theta_i \quad |\sum_{i \in I} p_i \cdot \Delta_i| \leq 1 \quad |\sum_{i \in I} p_i \cdot \Theta_i| \leq 1}{(\sum_{i \in I} p_i \cdot \Delta_i) \text{ lc}(\mathcal{R}) (\sum_{i \in I} p_i \cdot \Theta_i)}$$

Then we prove that $\text{lc}(\cdot)$ is *compatible with bisimilarity*, in the sense of [Pous and Sangiorgi 2011]. From this it follows that bisimilarity is linearly closed, i.e. $\text{lc}(\simeq) \subseteq \simeq$. This essentially derives from the fact that $\succ^{\tau}_s$ is linear and decomposable, thus all the moves of $\sum_{i \in I} p_i \cdot \Delta_i$ descend from the ones of the Δ_i components. $\square$

Example 5.12. The scheduled semantics of the processes $\mathbf{A}_{01} \parallel \mathbf{B}$ and $\mathbf{A}_{\pm} \parallel \mathbf{B}$ are shown in Figure 8, where C^i denotes the process $0_{q_1} \parallel c!i. 0_{q_2}$, and $C^i_{|\psi\rangle}$ is the configuration $(|\psi\rangle\langle\psi|, 0_{q_1} \parallel c!i. 0_{q_2})$. From the figures it is evident that the branching structure of the two semantics is identical, therefore we will focus on the mass of the distribution. As for the unscheduled semantics, the only information that context can use to distinguish the two processes is the result communicated on the channel c . However, all final distributions of configurations have the same uniform distribution of 0 and 1 outcomes, therefore cannot be discriminated.

6 Deciding Behavioural Equivalence Through Labelled Bisimilarities

Having chosen $\simeq$ as our preferred behavioural equivalence, we search a computable alternative characterization. We present a novel semantics that is based on a quantum extension of probability distributions; subsequently, we give a labelled bisimilarity, and we discuss its adherence with respect to the scheduled bisimilarity. Finally, we prove its decidability for a rich class of lqCCS processes.

6.1 Density Operator Semantics

The indistinguishability relation of Fact 1 suggests a new operational semantics. Instead of dealing with multiple indistinguishable distributions of lqCCS configurations, we represent them with the same mathematical object, just as a single density operators represents multiple indistinguishable distributions of quantum values. This leads to a semantics based on a quantum generalization of probability distributions, one that satisfies Theorem 5.10 by construction.

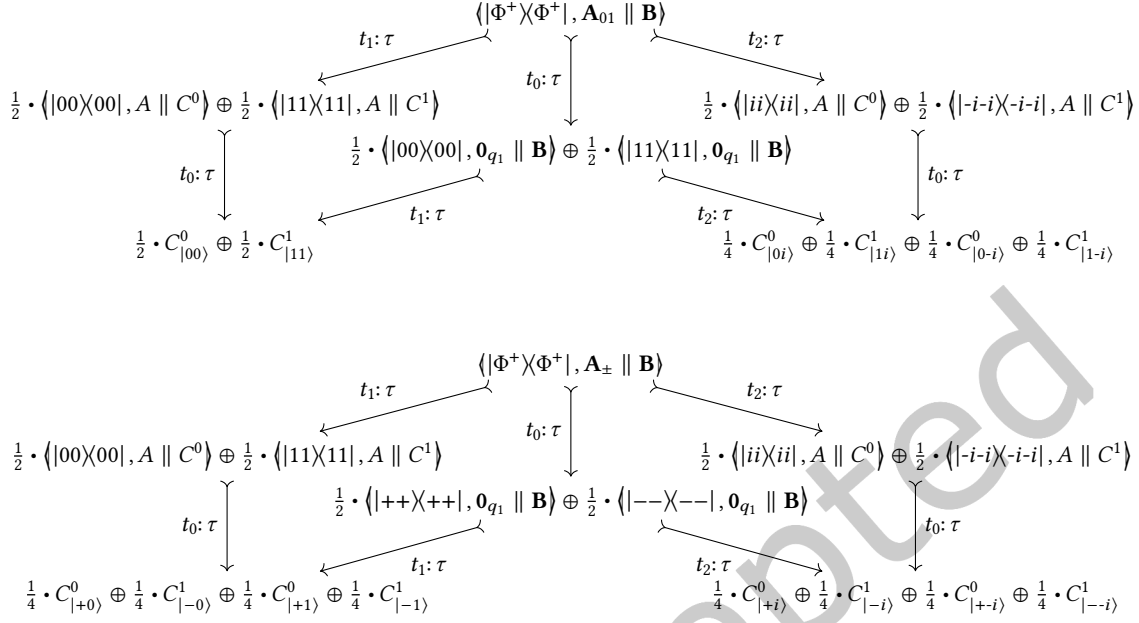


Fig. 8. Scheduled semantics of the protocol described in Example 5.7

We introduce *quantum distributions*, which have density operators as weights, instead of real numbers in $[0, 1]$. More in detail, density operators exhibit a *Partial Commutative Monoid* (PCM) structure: they can be summed with matrix addition, but only if the result is still in $\mathcal{DO}^\leq(\mathcal{H})$. This generalizes the case of probabilities, i.e. the PCM of real numbers with sum in the interval $[0, 1]$. Building upon this similarity, we can define quantum distributions as follows.

Definition 6.1 (Quantum Distribution). Given a Hilbert space $\mathcal{H}_\Sigma$, the set of *quantum distributions* over S is

$$\mathcal{Q}_\Sigma(S) = \left\{ \mathfrak{D} \in \mathcal{DO}^\leq(\mathcal{H}_\Sigma)^S \mid [\mathfrak{D}] \text{ is finite and } \sum_{s \in S} \text{tr}(\mathfrak{D}(s)) \leq 1 \right\}$$

where $[\mathfrak{D}]$ is the support of $\mathfrak{D}$, i.e. the set $\{s \in S \mid \mathfrak{D}(s) \neq \mathbb{O}\}$.

We maintain the same notation: we write ϵ for the empty distribution associating each element of S with the matrix $\mathbb{O}$; we let $\rho \cdot s$ be a distribution such that $(\rho \cdot s)(s) = \rho$ and $(\rho \cdot s)(s') = \mathbb{O}$ if $s \neq s'$; finally, we write $\sum_{i \in I} p_i \cdot \mathfrak{D}_i$ for the distribution such that $(\sum_{i \in I} p_i \cdot \mathfrak{D}_i)(s) = \sum_{i \in I} p_i \mathfrak{D}_i(s)$, with $\{p_i\}_{i \in I}$ a finite set of non-negative reals and $\sum_{i \in I} p_i = 1$. Note that $\mathcal{Q}_\emptyset(S)$ is isomorphic to $\mathcal{D}(S)$ since 1-dimensional density operators are just real numbers in $[0, 1]$.

Our new semantics is given directly on quantum distributions of lqCCS processes $\mathcal{Q}_\Sigma(\text{Proc})$, where both the qubits' state and the classical probability is encoded in the weights of the distribution. The type system is extended to quantum distributions: distributions defined on a Hilbert space $\mathcal{H}_\Sigma$ must contain only processes manipulating qubits in Σ .

Definition 6.2 (Quantum Distribution Typing). We say that a quantum distribution of lqCCS processes $\mathfrak{D} \in \mathcal{Q}_\Sigma(\text{Proc})$ has type (Σ, Σ') (written $(\Sigma, \Sigma') \vdash \mathfrak{D}$) if $\Sigma' \vdash P$ for all processes $P \in [\mathfrak{D}]$, and if $\Sigma' \subseteq \Sigma$.

$$\begin{array}{c}
\text{TAU} \quad \rho \cdot t : \tau. P \xrightarrow{\tau} \rho \cdot P \quad \text{TAUSYNCH} \quad \rho \cdot (t, t') : \tau. P \xrightarrow{\tau}_{(t, t')} \rho \cdot P \quad \text{SOP} \quad \rho \cdot t : \mathcal{E}(\tilde{q}). P \xrightarrow{\tau} \mathcal{E}^{\tilde{q}}(\rho) \cdot P \\
\\
\text{MEAS} \quad \rho \cdot t : \mathcal{M}(\tilde{q} \triangleright x). P \xrightarrow{\tau}_t \sum_{m=0}^{|\mathcal{M}|-1} \mathcal{M}_m^{\tilde{q}}(\rho) \cdot P[m/x] \quad \text{SEND} \quad \frac{e \Downarrow v}{\rho \cdot t : c!e. P \xrightarrow{c!v}_t \rho \cdot P} \quad \text{RECV} \quad \frac{c : \widehat{Q} \Rightarrow v \in \Sigma_\rho \setminus \Sigma_P}{\rho \cdot t : c?x. P \xrightarrow{c?v}_t \rho \cdot P[v/x]} \\
\\
\text{ITET} \quad \frac{e \Downarrow tt \quad \rho \cdot P \xrightarrow{\mu}_s \mathcal{D}}{\rho \cdot \text{if } e \text{ then } P \text{ else } Q \xrightarrow{\mu}_s \mathcal{D}} \quad \text{ITEF} \quad \frac{e \Downarrow ff \quad \rho \cdot Q \xrightarrow{\mu}_s \mathcal{D}}{\rho \cdot \text{if } e \text{ then } P \text{ else } Q \xrightarrow{\mu}_s \mathcal{D}} \quad \text{SUML} \quad \frac{\rho \cdot P \xrightarrow{\mu}_s \mathcal{D}}{\rho \cdot P + Q \xrightarrow{\mu}_s \mathcal{D}} \\
\\
\text{SUMR} \quad \frac{\rho \cdot Q \xrightarrow{\mu}_s \mathcal{D}}{\rho \cdot P + Q \xrightarrow{\mu}_s \mathcal{D}} \quad \text{PARL} \quad \frac{\rho \cdot P \xrightarrow{\mu}_s \mathcal{D} \quad \mu \notin \{c?v \mid v \in \Sigma_Q\}}{\rho \cdot P \parallel Q \xrightarrow{\mu}_s \mathcal{D} \parallel Q} \quad \text{PARR} \quad \frac{\rho \cdot Q \xrightarrow{\mu}_s \mathcal{D} \quad \mu \notin \{c?v \mid v \in \Sigma_P\}}{\rho \cdot P \parallel Q \xrightarrow{\mu}_s P \parallel \mathcal{D}} \\
\\
\text{SYNCHL} \quad \frac{\rho \cdot P \xrightarrow{c!v}_{t'} \rho \cdot P' \quad \rho \cdot Q \xrightarrow{c?v}_{t'} \rho \cdot Q'}{\rho \cdot P \parallel Q \xrightarrow{\tau}_{(t, t')}} \quad \text{SYNCHR} \quad \frac{\rho \cdot P \xrightarrow{c?v}_{t'} \rho \cdot P' \quad \rho \cdot Q \xrightarrow{c!v}_{t'} \rho \cdot Q'}{\rho \cdot P \parallel Q \xrightarrow{\tau}_{(t, t')}} \\
\\
\text{RESTR} \quad \frac{\rho \cdot P \xrightarrow{\mu}_s \mathcal{D} \quad \mu \notin \{c!v, c?v \mid v\}}{\rho \cdot P \setminus c \xrightarrow{\mu}_s \mathcal{D} \setminus c} \quad \text{ID} \quad \frac{\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}'}{\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}'} \quad \text{NOT} \quad \frac{\mathcal{D} \not\xrightarrow{\mu}_s}{\mathcal{D} \xrightarrow{\mu}_s \epsilon} \quad \text{CONV} \quad \frac{\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}' \quad \mathcal{I} \xrightarrow{\mu}_s \mathcal{I}'}{\mathcal{D} \oplus \mathcal{I} \xrightarrow{\mu}_s \mathcal{D}' \oplus \mathcal{I}'}
\end{array}$$

Fig. 9. Rules of Density Operator Semantics.

Hereafter, we assume a fixed set of qubits, and drop the Σ from $\mathcal{Q}_\Sigma(\text{Proc})$. Moreover, we restrict ourselves to well-typed distributions. The new labelled semantics for lqCCS is given in terms of LTS of quantum distributions of processes, i.e. a triple $(\mathcal{Q}(\text{Proc}), \text{Act}, \xrightarrow{\cdot})$, with $\xrightarrow{\cdot} \subseteq \mathcal{Q}(\text{Proc}) \times \text{Act} \times \text{Sched} \times \mathcal{Q}(\text{Proc})$.

To define the transition relation $\xrightarrow{\cdot}$, we first consider the smallest transition relation $\xrightarrow{\cdot}$ over quantum distributions of closed processes that satisfies the related rules in Figure 9. Note that these rules are almost in one-to-one correspondence with the ones in Figure 4, and that they define the behaviour of distributions with a single element in the support. The main difference with the configuration semantics is made clear by the MEAS rule, where both the resulting quantum state and the probability of observing it are encoded as a single partial density operator. The transition relation $\xrightarrow{\cdot}$ is finally obtained by applying the last three rules in Figure 9, which includes a “deadlock” rule for distributions that cannot evolve otherwise, and recovers convexity by stating that the components of a quantum distribution can evolve altogether with the same scheduler and label.

Example 6.3. Take the following process which measures and outputs a qubit, ignoring the classical outcome x of the measurement.

$$\mathbf{P} ::= t_0 : \mathcal{M}_{01}(q \triangleright x). t_0 : c!q$$

Consider its evolution with the starting state $|+\rangle\langle+|$, essentially modelling the first source of Example 5.6.:

$$|+\rangle\langle+| \cdot \mathbf{P} \xrightarrow{\tau}_{t_0} \frac{1}{2} |0\rangle\langle 0| \cdot t_0: c!q \oplus \frac{1}{2} |1\rangle\langle 1| \cdot t_0: c!q \xrightarrow{c!q}_{t_0} \frac{1}{2} \mathbb{I} \cdot \mathbf{0}$$

The first step follows the MEAS rule. Note that, in the second distribution, the processes of the two branches coincide, since the measurement outcome x is ignored. This means that we can rewrite $\frac{1}{2} |0\rangle\langle 0| \cdot t_0: c!q \oplus \frac{1}{2} |1\rangle\langle 1| \cdot t_0: c!q$ as $\frac{1}{2} \mathbb{I} \cdot t_0: c!q$, as they denote the same quantum distribution. In other words, our new semantics naturally embodies the equivalence between indistinguishable probability distributions of Theorem 5.10.

6.2 Labelled Bisimilarity

We now move to define a suitable labelled bisimilarity relation based on the quantum distribution semantics. As a first ingredient of our bisimilarity, we extend well-typed relations to quantum distributions.

Definition 6.4 (Well-typed Relation). A relation $\mathcal{R} \subseteq \mathcal{Q}(\text{Conf}) \times \mathcal{Q}(\text{Conf})$ is well-typed if $\mathcal{D} \mathcal{R} \mathcal{I}$ implies $(\Sigma, \Sigma') \vdash \mathcal{D}$ and $(\Sigma, \Sigma') \vdash \mathcal{I}$ for some Σ, Σ' .

As it is common, bisimilarity should be closed over transitions, meaning that each bisimilar processes must be capable of matching the moves of the others.

Definition 6.5 (Transition-Closed Relation). A relation $\mathcal{R} \subseteq \mathcal{Q}(\text{Proc}) \times \mathcal{Q}(\text{Proc})$ is *transition-closed* if $\mathcal{D} \mathcal{R} \mathcal{I}$ implies that for each s and μ :

- whenever $\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}'$, there exists $\mathcal{I}'$ such that $\mathcal{I} \xrightarrow{\mu}_s \mathcal{I}'$ and $\mathcal{D}' \mathcal{R} \mathcal{I}'$;
- whenever $\mathcal{I} \xrightarrow{\mu}_s \mathcal{I}'$, there exists $\mathcal{D}'$ such that $\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}'$ and $\mathcal{D}' \mathcal{R} \mathcal{I}'$.

Before defining labelled bisimulation, we introduce some notation and discuss some which properties of quantum distributions can be immediately distinguished by contexts. Our goal is finding atomic observable properties that match the discriminating power of a context-closed relation like $\simeq$.

Given a quantum distribution $\mathcal{D}$ of lqCCS processes, we let its mass $|\mathcal{D}|$ be defined as the sum of its weights $\sum_{P \in \text{Proc}} \mathcal{D}(P)$, as it is for probability distributions. Note that, if (Σ, Σ') is the type of $\mathcal{D}$, then $|\mathcal{D}|$ is a (partial) density operator in $\mathcal{DO}^\leq(\mathcal{H}_\Sigma)$. We are particularly interested in a fragment of $|\mathcal{D}|$, namely in $\text{tr}_{\Sigma'}(|\mathcal{D}|)$, which we call the *environment* of $\mathcal{D}$, i.e. the state of the qubits that are unused by the processes of $\mathcal{D}$ and that the contexts can observe immediately. The environment of bisimilar quantum distributions must coincide, otherwise a context performing a simple measurement would distinguish them.

Definition 6.6 (Environment-preserving Relation). The *environment* of an quantum distribution $\mathcal{D} \in \mathcal{Q}_\Sigma(\text{Proc})$ is $\text{env}(\mathcal{D}) = 0$ if $\mathcal{D} = \epsilon$, otherwise it is $\text{env}(\mathcal{D}) = \text{tr}_{\Sigma'}(|\mathcal{D}|)$ with Σ' the only set of qubit names such that $(\Sigma, \Sigma') \vdash \mathcal{D}$.

A relation $\mathcal{R} \subseteq \mathcal{Q}(\text{Proc}) \times \mathcal{Q}(\text{Proc})$ is a *environment-preserving* if $\mathcal{D} \mathcal{R} \mathcal{I}$ implies $\text{env}(\mathcal{D}) = \text{env}(\mathcal{I})$.

We allow applying superoperators to configurations and distributions. Given $(\Sigma, \Sigma') \vdash \mathcal{D} = \sum_{i \in I} \rho_i \cdot P_i$ and $\mathcal{E} \in \mathcal{SO}^\leq(\mathcal{H}_\Sigma)$, we let $\mathcal{E}(\mathcal{D})$ be the quantum distribution $\sum_{i \in I} \mathcal{E}(\rho_i) \cdot P_i$ where all the weights are updated by the superoperator. In the following, we allow updating $\mathcal{D}$ also with superoperators that are defined on a subset of the qubits, i.e. with $\mathcal{E} \in \mathcal{SO}^\leq(\mathcal{H}_{\Sigma''})$ with $\Sigma'' \subseteq \Sigma$. In this case, we assume $\mathcal{E}$ to be padded as needed by tensoring its Kraus representation with the identity matrix. We are interested in relations that are closed over the application of superoperators defined on the environment. Intuitively, this is needed for matching contexts that modify qubits through trace preserving superoperators and measurements before sending them to processes.

Definition 6.7 (Superoperator-closed Relation). A superoperator $\mathcal{E}$ is *compatible* with respect to a distribution $\mathcal{D}$ if $\mathcal{E} \in \mathcal{SO}^\leq(\mathcal{H}_{\Sigma \setminus \Sigma'})$ with $(\Sigma, \Sigma') \vdash \mathcal{D}$.

A relation $\mathcal{R} \subseteq \mathcal{Q}(\text{Proc}) \times \mathcal{Q}(\text{Proc})$ is *closed for compatible superoperators* if $\mathcal{D} \mathcal{R} \mathcal{I}$ implies $\mathcal{E}(\mathcal{D}) \mathcal{R} \mathcal{E}(\mathcal{I})$ for any superoperator compatible with both $\mathcal{D}$ and $\mathcal{I}$.

We can now define *labelled scheduled bisimulations*. In addition to the usual transition closure, labelled bisimulations are required to satisfy two additional conditions: paired distributions must share the same environment; and the relation must be closed for the application of superoperators over the qubits of the environment. Intuitively, this is needed for proving that labelled bisimilarity has the same observing power of saturated bisimilarity, as a context $B[\cdot] = [\cdot] \parallel R$ can read and modify the qubits of the environment.

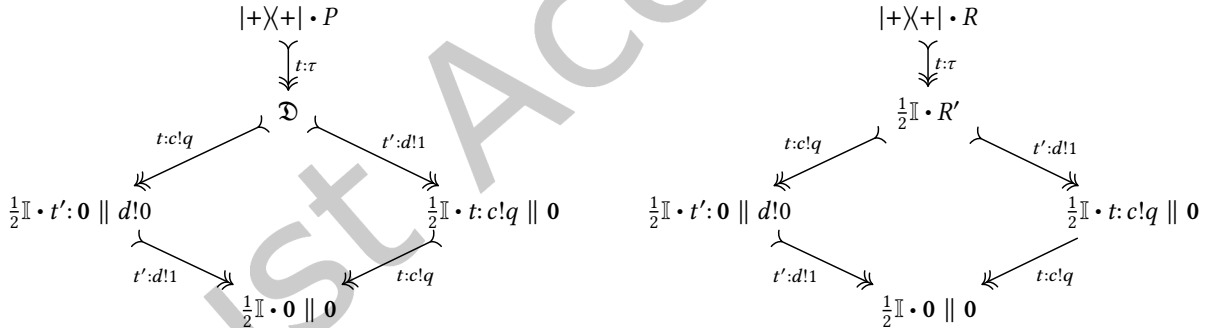
Definition 6.8 (Labelled Scheduled Bisimilarity). A relation $\mathcal{R} \subseteq Q(\text{Proc}) \times Q(\text{Proc})$ is a *labelled scheduled bisimulation* if it is well-typed, transition-closed, environment-preserving and closed for compatible superoperators. Let *labelled scheduled bisimilarity*, denoted $\sim$, be the largest labelled scheduled bisimulation.

We now provide an example of bisimulation between two simple distributions, highlighting how $\sim$ encompasses both quantum indistinguishability (as it respects Theorem 5.10 by construction) and classical equivalences (like the commutativity of the parallel operator).

Example 6.9. Assume a process $\mathbf{P} := t: \mathcal{M}_{01}(q \triangleright x). \text{if } x = 0 \text{ then } (t: c!q \parallel t': d!1) \text{ else } (t': d!1 \parallel t: c!q)$, which takes a qubit q and collapses it in the computational basis, then sends it on a quantum channel c and signals termination on a classical channel d (for "done"). This process does inspect the classical outcome x of the measurement, but it does nothing meaningful with it: the difference between the "then" branch and the "else" branch is only syntactical, as both branches communicate the same messages. For these reasons, if we execute P on the input $|+\rangle\langle+|$ it is functionally the same as setting the qubit to $\frac{1}{2}\mathbb{I}$.

More in detail, we can define another process $\mathbf{R} := t: \mathcal{S}(q). (t: c!q \parallel t': d!1)$, which uses the constant "Set" superoperator $\mathcal{S}$ such that $\mathcal{S}(\rho) = \frac{1}{2}\mathbb{I}$ for any ρ . We can then prove that $|+\rangle\langle+| \cdot \mathbf{P} \sim |+\rangle\langle+| \cdot \mathbf{R}$, highlighting that $\mathbf{P}$ does not leak the measurement outcome to the environment.

The transition systems of the two distributions are as follows



where $\mathfrak{D} = \frac{1}{2} |0\rangle\langle 0| \cdot P'[0/x] \oplus \frac{1}{2} |1\rangle\langle 1| \cdot P'[1/x]$, $P' = \text{if } x = 0 \text{ then } (t: c!q \parallel t': d!1) \text{ else } (t': d!1 \parallel t: c!q)$ and $R' = (t: c!q \parallel t': d!1)$.

We can build a bisimulation $\mathcal{R}$ that relates all the states above, and includes also the identity relation. We define $\mathcal{R}$ the smallest relation such that $|+\rangle\langle+| \cdot \mathbf{P} \mathcal{R} |+\rangle\langle+| \cdot \mathbf{R}$, $\mathfrak{D} \mathcal{R} \frac{1}{2}\mathbb{I} \cdot \mathbf{R}'$, and $\rho \cdot \mathbf{Q} \mathcal{R} \rho \cdot \mathbf{Q}$ for any well-typed $\rho \cdot \mathbf{Q}$.

To prove that $\mathcal{R}$ is a bisimulation, we must show that it is well-typed, transition-closed, environment-preserving, and closed for compatible superoperators. It is easy to check that it is well-typed, and it is transition-closed as well, simply by inspecting the above transition systems. It is environment-preserving: for the first two couples, we have $\text{env}(|+\rangle\langle+| \cdot \mathbf{P}) = 1 = \text{env}(|+\rangle\langle+| \cdot \mathbf{R}) = \text{env}(\mathfrak{D}) = \text{env}(\frac{1}{2}\mathbb{I} \cdot \mathbf{R}')$; for the identity couples, they have trivially the same environment. Finally, the relation $\mathcal{R}$ is closed for compatible superoperators: for the first two couples, there are no compatible superoperators, as there are no environment qubits; for the identity couples, we have $\mathcal{E}(\rho) \cdot \mathbf{Q} \mathcal{R} \mathcal{E}(\rho) \cdot \mathbf{Q}$ for any superoperator $\mathcal{E}$.

Thus, we can conclude that $|+\rangle\langle+| \cdot \mathbf{P} \sim |+\rangle\langle+| \cdot \mathbf{R}$. Notice how we had to resort to a bisimulation containing infinite couples, due to the requirement of superoperator-closedness. Defining a finite $\mathcal{R}$ relating only the states in the transition system, for example, would have not been sufficient: if we relate $\frac{1}{2}\mathbb{I} \cdot \mathbf{0} \mathcal{R} \frac{1}{2}\mathbb{I} \cdot \mathbf{0}$, we need to do the same for all possible compatible superoperators $\mathcal{E}$.

We prove that saturated bisimilarity in the probabilistic semantics coincides with labelled bisimilarity in the quantum distribution semantics.

THEOREM 6.10 (FULL ABSTRACTION). *For any ρ, σ, P, Q it holds that*

$$1 \cdot \langle \rho, P \rangle \simeq 1 \cdot \langle \sigma, Q \rangle \text{ if and only if } \rho \cdot P \sim \sigma \cdot Q$$

PROOF SKETCH. To simplify the proof, we introduce a probabilistic labelled bisimilarity $\sim_p$ as a bridge between the probabilistic saturated bisimilarity $\simeq$ and the quantum labelled one $\sim$. We prove the equivalence between $\simeq$ and $\sim_p$ using standard methods for probabilistic systems, like up-to techniques. We then show a fully-abstract translation between the probabilistic and quantum distributions that preserves and reflects their defined equivalences ($\sim_p$ and $\sim$ respectively). $\square$

6.3 Deciding Equivalence of Protocols

None of the conditions of Definition 6.8 can be omitted. As shown by the following counterexample, the closure over the environments superoperators is needed to recover the distinguishing capability of the saturated approach, making our labelled bisimilarity not adequate for verification.

Example 6.11. Take the following processes which measure a qubit received from the environment in two orthogonal basis

$$\mathbf{P} ::= t: c?x. t: \mathcal{M}_{01}(x \triangleright y). t: c!y. \mathbf{0}_x \quad \text{and} \quad \mathbf{Q} ::= t: c?x. t: \mathcal{M}_{\pm}(x \triangleright y). t: c!y. \mathbf{0}_x$$

Consider their evolution with starting state $|i\rangle\langle i|$:

$$\begin{aligned} |i\rangle\langle i| \cdot \mathbf{P} &\xrightarrow{c?q}_t |i\rangle\langle i| \cdot t: \mathcal{M}_{01}(q \triangleright y). t: c!y. \mathbf{0}_q \xrightarrow{\tau}_t \frac{1}{2} |0\rangle\langle 0| \cdot t: c!0. \mathbf{0}_q \oplus \frac{1}{2} |1\rangle\langle 1| \cdot t: c!1. \mathbf{0}_q \\ |i\rangle\langle i| \cdot \mathbf{Q} &\xrightarrow{c?q}_t |i\rangle\langle i| \cdot t: \mathcal{M}_{\pm}(q \triangleright y). t: c!y. \mathbf{0}_q \xrightarrow{\tau}_t \frac{1}{2} |+\rangle\langle+| \cdot t: c!0. \mathbf{0}_q \oplus \frac{1}{2} |-\rangle\langle-| \cdot t: c!1. \mathbf{0}_q \end{aligned}$$

It is evident that the two configurations are equated if in place of $\sim$ we consider the largest environment-preserving relation that is closed with respect to $\xrightarrow{\mu}_s$ for all μ and s (note that the different resulting quantum state is invisible due to the discard at the end).

However, since the sent qubit q is received from the environment, it can be transformed by the context before communication. Thus, $|i\rangle\langle i| \cdot \mathbf{P}$ is bisimilar to $|i\rangle\langle i| \cdot \mathbf{Q}$ only if $\mathcal{E}(|i\rangle\langle i| \cdot \mathbf{P}) \sim \mathcal{E}(|i\rangle\langle i| \cdot \mathbf{Q})$ for any compatible $\mathcal{E}$. To see that indeed this is not the case, consider the superoperator $\mathcal{E}$ that applies the unitary SH to q (recall that $SH|i\rangle = |0\rangle$ and $SH|-i\rangle = |1\rangle$); then the semantics become:

$$\begin{aligned} \mathcal{E}(|i\rangle\langle i| \cdot \mathbf{P}) &= |0\rangle\langle 0| \cdot \mathbf{P} \xrightarrow{c?q}_t |i\rangle\langle i| \cdot t: \mathcal{M}_{01}(q \triangleright y). t: c!y. \mathbf{0}_q \xrightarrow{\tau}_t |0\rangle\langle 0| \cdot t: c!0. \mathbf{0}_q \\ \mathcal{E}(|i\rangle\langle i| \cdot \mathbf{Q}) &= |0\rangle\langle 0| \cdot \mathbf{Q} \xrightarrow{c?q}_t |i\rangle\langle i| \cdot t: \mathcal{M}_{\pm}(q \triangleright y). t: c!y. \mathbf{0}_q \xrightarrow{\tau}_t \frac{1}{2} |+\rangle\langle+| \cdot t: c!0. \mathbf{0}_q \oplus \frac{1}{2} |-\rangle\langle-| \cdot t: c!1. \mathbf{0}_q \end{aligned}$$

It is evident that the two configurations are not bisimilar: the former can only send 0 over c while the latter can send 1 with probability $1/2$.

The capability of modifying the qubits in the environment is evident with saturated bisimilarity, where the two configurations are distinguished by $B[\cdot] = [\cdot] \parallel SH(q). c!q$.

There is a practical limitation in using the scheduled bisimilarity of Definition 6.8 to verify distributed quantum systems and protocols: the universal quantification over all possible environment superoperators make the relation difficult to prove. In addition, the Example 6.11 shows that the closure must be considered, otherwise there is the risk of equating systems that can be distinguished by some context. Luckily, this closure is only needed because of processes that can receive qubits from the environment, such as those of Example 6.11. Indeed, lots of concrete cases do not need this feature, and if we remove it we can give an equivalent decidable relation, as we show below.

Definition 6.12 (Input-Restricted Processes). Let $Proc_g \subset Proc$ be the set of lqCCS *input-restricted processes*, i.e. with no unrestricted input channels of type $\widehat{Q}$. Formally, P is in $Proc_g$ if $uic(P) = \emptyset$ where $uic(\cdot)$ is defined as:

$$\begin{aligned} uic(0_{\bar{e}}) &= \emptyset & uic(P \setminus c) &= uic(P) \setminus \{c\} & uic(t:c?x.P) &= \begin{cases} \{c\} \cup uic(P) & \text{if } c : \widehat{Q} \\ uic(P) & \text{otherwise} \end{cases} \\ uic(t:\tau.P) &= uic((t,t):\tau.P) = uic(t:\mathcal{E}(\bar{e}).P) = uic(t:\mathcal{M}(\bar{e} \triangleright x).P) = uic(t:cle.P) = uic(P) \\ uic(\text{if } e \text{ then } P \text{ else } P') &= uic(P + P') = uic(P \parallel P') = uic(P) \cup uic(P') \end{aligned}$$

Definition 6.13 (Labelled Ground Scheduled Bisimilarity). A relation $\mathcal{R} \subseteq Q(Proc) \times Q(Proc)$ is a *labelled ground scheduled bisimulation* if it is well-typed, transition-closed and environment-preserving. Let *labelled ground scheduled bisimilarity*, denoted $\sim_g$, be the largest labelled ground scheduled bisimulation.

We extend Theorem 6.10 to the case of $Proc_g$, showing that labelled ground bisimilarity matches saturated bisimilarity if processes do not receive values from the environment.

THEOREM 6.14. *For any $P, Q \in Proc_g$, ρ, σ it holds that $1 \cdot \langle \rho, P \rangle \approx 1 \cdot \langle \sigma, Q \rangle$ if and only if $\rho \cdot P \sim_g \sigma \cdot Q$*

PROOF SKETCH. When limited to processes in $Proc_g$, we can prove that ground bisimilarity is superoperator closed, thus $\sim_g$ and $\sim$ coincide. Then the result follows from Theorem 6.10. $\square$

As a final remark, note that the problem with unconstrained non-determinism and unscheduled bisimilarity is critical also for processes that cannot freely receive input from the environment. Indeed, both Example 5.6 and Example 5.7 are in $Proc_g$, as well as the quantum coin flip introduced in section 2.

7 Tackling Real-World Protocols

We conclude with three real-world examples, showing the expressivity of lqCCS and what kind of properties can be verified thanks to labelled bisimilarity. We will focus on Superdense Coding [Bennett and Wiesner 1992], Quantum Teleportation [Bennett et al. 1993], and the already cited quantum Coin Flipping [Bennet and Brassard 2014].

Example 7.1 (Superdense Coding). The superdense coding protocol allows Alice to communicate a two-bit integer to Bob by sending him a single qubit, exploiting an entangled pair $|\Phi^+\rangle$. The protocol is as follows: Alice chooses an integer in $[0, 3]$ and encodes it by applying suitable transformations to her entangled qubit, which is then sent to Bob; Bob receives the qubit and decodes it by performing $CNOT$ and $H \otimes I$ on the pair of qubits (the received qubit and his original one). Finally, he measures the qubits in the standard basis, recovering the integer chosen by Alice.

The actions of Alice (as well as the final result) are dependent on the integer input of the protocol, and are modelled as a non-deterministic choice. We can encode the different possible inputs directly in the tags: Alice starts by choosing either t_0, t_1, t_2 or t_3 , which correspond to encoding 0, 1, 2 or 3 in the qubit sent by Alice. Bob's moves are all tagged with the same tag t .

We consider the following encoding of the protocol $\mathbf{SDC} = (\mathbf{A} \parallel \mathbf{B}) \setminus c$, where we assume that Alice ($\mathbf{A}$) and Bob ($\mathbf{B}$) already share an entangled pair (q_1, q_2) , and we write $t: \tau^n$ for the repetition of n consecutive t -tagged silent moves.

$$\begin{array}{lll}
 \mathbf{A} ::= (t_0: I(q_0). t: c!q_0. \mathbf{0}) + & \mathbf{B} ::= t: c?x. & \mathbf{Spec} ::= t_0: \tau. (t, t): \tau. t: \tau^3. t: out!0. \mathbf{0}_{q_0, q_1} + \\
 (t_1: X(q_0). t: c!q_0. \mathbf{0}) + & t: CNOT(x, q_1). & t_1: \tau. (t, t): \tau. t: \tau^3. t: out!1. \mathbf{0}_{q_0, q_1} + \\
 (t_2: Z(q_0). t: c!q_0. \mathbf{0}) + & t: H(x). & t_2: \tau. (t, t): \tau. t: \tau^3. t: out!2. \mathbf{0}_{q_0, q_1} + \\
 (t_3: ZX(q_0). t: c!q_0. \mathbf{0}) & t: \mathcal{M}_{01}^2(x, q_1 \triangleright y). & t_3: \tau. (t, t): \tau. t: \tau^3. t: out!3. \mathbf{0}_{q_0, q_1} \\
 & t: out!y. \mathbf{0}_{x, q_1} &
 \end{array}$$

We let $\mathfrak{D} = |\Phi^+ \rangle \langle \Phi^+| \cdot \mathbf{SDC}$, with $\mathfrak{T} = |\Phi^+ \rangle \langle \Phi^+| \cdot \mathbf{Spec}$ its specification. Note that $\mathbf{Spec}$ states that the choice of the initial unitary determines the final value to be communicated. Since the process has no unrestricted input, we can resort to the ground version of our bisimilarity to prove the adequacy of the protocol. We now sketch the proof for $\Delta \sim_g \Theta$.

The evolutions of $\mathfrak{D}$ and $\mathfrak{T}$ are as follows, for $n = 0, 1, 2, 3$

$$\begin{aligned}
 \mathfrak{D} &\xrightarrow{\tau} \mathfrak{D}_{t_n} \xrightarrow{\tau} \mathfrak{D}_{(t,t)} \xrightarrow{\tau} \mathfrak{D}_t^3 \quad \mathfrak{D}_n = |n\rangle \langle n| \cdot t: out!n. \mathbf{0}_{q_0, q_1} \setminus c \\
 \mathfrak{T} &\xrightarrow{\tau} \mathfrak{T}_{t_n} \xrightarrow{\tau} \mathfrak{T}_{(t,t)} \xrightarrow{\tau} \mathfrak{T}_t^3 \quad \mathfrak{T}_n = |\Phi^+ \rangle \langle \Phi^+| \cdot t: out!n. \mathbf{0}_{q_0, q_1} \setminus c
 \end{aligned}$$

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.

The two qubits are always owned by the processes, so the environment of all the distributions is trivially the same. Note that $\mathfrak{D}_n \sim_g \mathfrak{T}_n$ for any n , because both distributions $\mathfrak{D}_n$ and $\mathfrak{T}_n$ sends the number n on the channel out , and reduce to deadlock distributions. These conditions are enough to construct a ground bisimulation between $\mathfrak{D}$ and $\mathfrak{T}$.

Example 7.2 (Quantum Teleportation). The objective of the teleportation protocol is to allow Alice to send quantum information to Bob without a quantum channel. Alice and Bob must have each one of the qubits 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 her part of the entangled pair; then, she measures the qubits and sends the classical outcome to Bob, which applies different unitaries to his 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.

This protocol does not involve any non-deterministic choice, thus we have great freedom in the choice of tags. We follow a simple policy, where all Alice's and Bob's actions are tagged by t .

Consider the following encoding of the protocol $\mathbf{Tel} = (\mathbf{A} \parallel \mathbf{B}) \setminus c$, where we assume that Alice ($\mathbf{A}$) and Bob ($\mathbf{B}$) already share an entangled pair (q_1, q_2) .

$$\begin{array}{lll}
 \mathbf{A} ::= t: CNOT(q_0, q_1). & \mathbf{B} ::= t: c?y. & \mathbf{Spec} ::= t: \tau^3. \\
 t: H(q_0). & \text{if } y = 0 \text{ then } t: I(q_2). & (t, t): \tau. \\
 t: \mathcal{M}_{01}^2(q_0, q_1 \triangleright x). & \text{else if } y = 1 \text{ then } t: X(q_2). & t: SWAP(q_0, q_2). \\
 t: c!x. \mathbf{0}_{q_0, q_1} & \text{else if } y = 2 \text{ then } t: Z(q_2). & t: out!q_2. \mathbf{0}_{q_0, q_1} \\
 & \text{else } t: ZX(q_2). & \\
 & t: out!q_2 &
 \end{array}$$

We write $\mathcal{M}_{01}^2$ to denote the two-qubit measurement in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Note that $\mathbf{Spec}$ simply states that, after the tagged operations, the state of qubits is swapped and the correct state is communicated over the expected channel. We let $\mathfrak{D} = |\psi \Phi^+ \rangle \langle \psi \Phi^+| \cdot \mathbf{Tel}$, with $\mathfrak{T} = |\psi \Phi^+ \rangle \langle \psi \Phi^+| \cdot \mathbf{Spec}$ its specification for any $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and sketch the proof for $\Delta \sim_g \Theta$ below.

The relevant steps of the evolution of $\mathfrak{D}$ and $\mathfrak{I}$ are

$$\begin{aligned}
\mathfrak{D} &\xrightarrow{\tau} \mathfrak{D}' = \sum_{n=0}^3 \frac{1}{4} |n\rangle\langle n| \otimes |\psi_n\rangle\langle\psi_n| \cdot t: c!n. \mathbf{0}_{q_0, q_1} \parallel \mathbf{B} \setminus c \\
&\xrightarrow{\tau}_{(t, t)} \mathfrak{D}'' = \mathbb{I}/4 \otimes |\psi\rangle\langle\psi| \cdot \mathbf{0}_{q_0, q_1} \parallel t: out!q_2 \setminus c \\
&\xrightarrow{out!q_2}_{(t, t)} \mathfrak{D}''' = \mathbb{I}/4 \otimes |\psi\rangle\langle\psi| \cdot \mathbf{0}_{q_0, q_1} \setminus c \\
\mathfrak{I} &\xrightarrow{\tau} \mathfrak{I}' = |\Phi^+\rangle\langle\Phi^+| \otimes |\psi\rangle\langle\psi| \cdot t: out!q_2. \mathbf{0}_{q_0, q_1} \setminus c \\
&\xrightarrow{out!q_2}_{(t, t)} \mathfrak{I}'' = |\Phi^+\rangle\langle\Phi^+| \otimes |\psi\rangle\langle\psi| \cdot \mathbf{0}_{q_0, q_1} \setminus c
\end{aligned}$$

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. Until the last move, all the qubits are owned by the processes, and so the environments coincide. The last move is then a send on the channel *out* for both distributions. The bisimilarity then is easily checked as $\mathfrak{D}'''$ and $\mathfrak{I}''$ are in deadlock, and $\text{tr}_{q_0, q_1} |\mathfrak{D}''| = |\psi\rangle\langle\psi| = \text{tr}_{q_0, q_1} |\mathfrak{I}''|$. These conditions are enough to construct a ground bisimulation between $\mathfrak{D}$ and $\mathfrak{I}$. Notice how there are no inputs in our processes, and so we do not have to consider a universal quantification over all possible compatible superoperators.

Example 7.3 (Quantum Coin Flip). We restate here the Quantum Coin Flip protocol described in section 2. Similarly to the previous example, we employ the trivial policy of tagging almost everything with t , whereas the last operations are tagged by t_a , t_b and t_c to guarantee determinism.

Alice ::= $t: \mathcal{M}_{\text{bit}}(\triangleright s).$ if $s = 0$ then $t: H(q). t: \mathcal{M}_{01}(q \triangleright w).$ else $t: I(q). t: \mathcal{M}_{\pm}(q \triangleright w).$ $t: \text{AtoB!}q.$ $t: \text{guess?}g.$ $t: \text{witness!}w.$ $t: \text{secret!}s.$ $t_a: a!(g = s)$	Bob ::= $t: \text{AtoB?}x.$ $t: \mathcal{M}_{\text{bit}}(\triangleright g).$ if $g = 0$ then $t: \mathcal{M}_{\pm}(x \triangleright p).$ else $t: \mathcal{M}_{01}(x \triangleright p).$ $t: \text{guess!}g.$ $t: \text{witness?}w.$ $t: \text{secret?s}.$ $(t_b: b!(g = s) \parallel t_c: \text{cheat!}(g \neq s \wedge p \neq w) \parallel \mathbf{0}_x)$
--	--

Thanks to lqCCS and to ground labelled bisimilarity, we can investigate both correctness and security of this protocol, proving the properties presented in section 2.

Correctness. A correct execution of the protocol should correspond to tossing a fair coin to select the winner, and having both Alice and Bob agreeing on the winner. Since tags do not carry any semantics in this example, we consider a protocol equivalent to its specification when there exists a tagging making them bisimilar. Formally, the intended behaviour can be written down as

$$\mathbf{FairCoin} ::= t: \mathcal{M}_{\text{bit}}(\triangleright x). t: \tau^2. (t, t): \tau. t: \tau^2. (t, t): \tau^3. (t_a: a!x \parallel t_b: b!x \parallel t_c: \text{cheat!}0).$$

This tagging of the specification is obtained simply by specifying which steps are synchronization and which are internal action. In the general case, there is a finite set of "reasonable" tagging policies to check.

Since $\mathbf{QCF} ::= (\mathbf{Alice} \parallel \mathbf{Bob}) \setminus \{\text{AtoB}, \text{guess}, \text{secret}, \text{witness}\}$ is in Proc_g , we do not need to consider super-operator closedness, and we can prove correctness by showing the bisimilarity below via tedious but simple calculations.

$$|0\rangle\langle 0| \cdot \mathbf{QCF} \sim_g |0\rangle\langle 0| \cdot \mathbf{FairCoin}.$$

Bob's Attacks. To guarantee that the protocol does not favour Bob, we show that he is not able to infer Alice's secret bit s from the received qubit q . It is sufficient to take the two versions of **Alice** when s is 0 or is 1, and to consider the part of the process that happens before the secret is revealed, **Alice**₀ and **Alice**₁:

$$\mathbf{Alice}_0 = t: H(q). t: \mathcal{M}_{01}(q \triangleright w). t: \text{AtoB!}q \quad \mathbf{Alice}_1 = t: I(q). t: \mathcal{M}_{\pm}(q \triangleright w). t: \text{AtoB!}q$$

We have that $|0\rangle\langle 0| \cdot \mathbf{Alice}_0 \sim_g |0\rangle\langle 0| \cdot \mathbf{Alice}_1$, as both of them evolve into $\frac{1}{2}\mathbb{I} \cdot t: \text{AtoB!}q$ after two τ transitions. Note that the unscheduled saturated bisimilarity tells the two processes apart, as their evolution coincide with the two qubit sources of Example 5.6. Thus, analyses that do not constraint unfeasible non-determinism implicitly deem that Bob can distinguish the secret value of Alice and always win the toss.

Alice's Attacks. To examine the protocol resistance to a dishonest Alice, we can write down two known attacks from [Bennet and Brassard 2014], and study the resulting transition system. As detailed in section 2, we will consider two attackers, namely **Alison** and **Alix**.

$$\begin{aligned} \mathbf{Alison} &::= t: \mathcal{M}_{\text{bit}}(\triangleright s). \\ &\quad \text{if } s = 0 \text{ then } t: H(q). t: \mathcal{M}_{01}(q \triangleright w). \\ &\quad \quad \text{else } t: I(q). t: \mathcal{M}_{\pm}(q \triangleright w). \\ &\quad t: \text{AtoB!}q. \\ &\quad t: \text{guess?}g. \\ &\quad t: \text{witness!}w. \\ &\quad (t: \text{secret!}(1 - g) \parallel t_a: a!0) \\ \mathbf{Alix} &::= t: H(q). \\ &\quad t: \text{CNOT}(q, q'). \\ &\quad t: \text{AtoB!}q. \\ &\quad t: \text{guess?}g. \\ &\quad \text{if } g = 0 \text{ then } t: \mathcal{M}_{\pm}(q' \triangleright w). \\ &\quad \quad \text{else } t: \mathcal{M}_{01}(q' \triangleright w). \\ &\quad t: \text{witness!}w. \\ &\quad (t: \text{secret!}(1 - g) \parallel t_a: a!0) \end{aligned}$$

Alison's attack is not particularly dangerous, as we can prove that

$$|0\rangle\langle 0| \cdot (\mathbf{Alison} \parallel \mathbf{Bob}) \setminus C \sim_g |0\rangle\langle 0| \cdot \mathbf{LeakyUnfairCoin},$$

where we write C for the set of channels $\{\text{AtoB}, \text{guess}, \text{secret}, \text{witness}\}$, and **LeakyUnfairCoin** for the process that always select 0 (i.e. Alison) as winner and goes undetected (cheat!0) three fourths of the time.

$$\mathbf{LeakyUnfairCoin} ::= t: \mathcal{M}_{\frac{3}{4}}(\triangleright x). t: \tau^2. (t, t): \tau. t: \tau^2. (t, t): \tau^3. (t_a: a!0 \parallel t_b: b!0 \parallel t_c: \text{cheat!}x).$$

When executing the protocol with multiple qubits, the chances of Alison going undetected increases multiplicatively for each qubit, making it exponentially unlikely.

On the contrary, Alix's attack goes undetected with probability 1, and we can prove that

$$|0\rangle\langle 0| \cdot (\mathbf{Alix} \parallel \mathbf{Bob}) \setminus C \sim_g |0\rangle\langle 0| \cdot \mathbf{UnfairCoin},$$

where we write **UnfairCoin** for the process

$$\mathbf{UnfairCoin} ::= t: \tau^3. (t, t): \tau. t: \tau^2. (t, t): \tau^3. (t_a: a!0 \parallel t_b: b!0 \parallel t_c: \text{cheat!}0).$$

8 Related Works

We consider approaches that share our objectives: (i) a description language for concurrent or distributed quantum processes; (ii) an adequate operational semantics; and (iii) an approach to verify the expected properties of processes.

8.1 Description Languages

Proposed process calculi for quantum systems may have different syntax, but share mostly the same feature set. The Quantum Process Algebra (QPA) [Lalire 2006; Lalire and Jorrand 2004] extends value-passing CCS with syntactic operators for unitary transformations and measurements. As in lqCCS, quantum operations are silent τ -moves. Qubit names are treated according to an affine policy, in place of the linearity of lqCCS: a process

can simply ignore a qubit that it owns, as e.g. in $H(q).0$. In this case, QPAlg assumes that qubits are implicitly discarded, i.e. they cannot be observed by the environment ($H(q).0$ is the same as $H(q).0_q$).

The Communicating Quantum Processes (CQP) calculus [Gay and Nagarajan 2005, 2006] is inspired by the π -calculus with primitives for qubit transformations, measurements and creation. It features an affine type system with the objective of enforcing single ownership for qubits, and it assumes qubits to be implicitly discarded, similarly to QPAlg. Although name passing is technically possible, it is hardly considered in examples, and it is also explicitly ruled out in a version of the calculus [Davidson 2012]. For technical reasons, the same version also rules out the classical if-then-else conditional composition, which greatly reduce the expressive power of CQP as a modelling language.

The Quantum Calculus of Communicating Systems qCCS [Feng et al. 2007, 2012] shares the core syntax with lqCCS, but also features recursive processes. The adherence to the no-cloning theorem is obtained with syntactic requirements in place of a type system. Like for CQP, qubit names are treated according to an affine policy in place of the linearity of lqCCS; however, on the contrary of CQP, qCCS assumes that processes make their qubits implicitly visible ($H(q).0$ makes the qubit q visible, roughly as if it was sent on some unrestricted channel $H(q).e!q$).

We first developed our description language, lqCCS, in [Ceragioli et al. 2024c], where we give an asynchronous version of the calculus, equipped with a reduction semantics. The linear type system is introduced both to comply with the no-cloning theorem and to precisely characterize the set of visible qubits, solving the discrepancy discussed above between the other proposed formalisms: lqCCS can recover the visibility implicitly assumed by QPAlg, CQP and qCCS by applying an adequate discarding discipline. In the present paper, we focus on a minimal set of features, which still suffice to express real-world protocols like the ones of section 7. For the moment, we postpone to extend lqCCS with primitives for recursively defined processes à la qCCS and for qubit creation à la CQP.

8.2 Operational Semantics

All the proposed process calculi discussed above have an operational semantics in terms of pLTSs, with transitions mapping configurations to distributions of configurations. Communicating quantum values by sending qubits' name is nowadays the prevalent approach, since labelling send instructions with the sent qubits' reduced density operator, as in [Lalire 2006; Lalire and Jorrand 2004], misrepresents the effects of entanglement (see [Ceragioli et al. 2024c] for a counterexample). The pLTS semantics is used *as it is* in most related works [Feng et al. 2007; Gay and Nagarajan 2005; Lalire and Jorrand 2004]; however, this state-based approach has been ruled out in the most recent developments of qCCS and CQP, because of the problem of Example 5.6.

The author of [Davidson 2012] proposed a novel semantics for CQP based upon *mixed configurations*, i.e. single processes associated with distributions of classical and quantum values. Mixed configurations encode private invisible information, like measurement outcomes; they are resolved to classical, visible probabilistic distributions when the measurement outcome is revealed by sending it on some visible channel. Indeed, this solves the problem of Example 5.6. However, the calculus does not include any form of classical control primitive, and an extension of the semantic model in this sense seems challenging because of the formal constraints of mixed-configurations, making the semantics not fully adequate for modelling the behaviour of real-world protocols.

For qCCS, the authors of [Feng and Ying 2015] have proposed an LTS of *full* probability distributions of configurations, obtained by lifting the semantics in a standard manner [Hennessy 2012]. This approach simplifies working with quantum values, since the environment is made explicit by combining the visible values in a weighted sum of density operators. In addition, lifted semantics forbid composing moves that choose different visible actions (or that choose not to move), with the objective of preventing a form of leakage of quantum data similar to the one we discuss in Example 5.6. A known drawback of lifting a pLTS to a LTS of full distributions

is that actions available only in some processes of the support are in deadlock. This requires ad-hoc solutions when defining behavioural equivalences, like imposing some form of decomposability [Hennessy 2012]. The most recent proposal for qCCS solves this problem by lifting to (not necessarily full) distributions (often named subdistributions in related works) [Deng 2018]. However, this works well only for visible actions and in action-deterministic transition systems: the proposal still permits invisible τ -moves to access quantum data without performing measurements, and in general different choices that exhibit the same visible label are unconstrained. As we will discuss later, the proposed labelled bisimilarity based on this semantics still suffers from some observational problems linked to unconstrained non-determinism.

None of the previous approaches considers schedulers, hence allowing the composition of moves obtained through different choices. Instead, in our lifting, we obtain a constrained version of decomposability by removing from the support the configurations that cannot evolve with the given scheduler choice.

The original presentation of lqCCS [Ceragioli et al. 2024c] comes only with a reduction-based semantics, while here we present a labelled one. In addition, the syntactic locus of the process is used in place of explicit tags, and only the moves of distinguishing contexts are constrained. Here, we use syntactic tags and schedulers, which is a standard and more versatile approach, and we consistently constrain non-determinism in both processes and contexts with the same technique. A limitation of the current proposal is that we focus on minimal schedulers, whereas the more expressive ones of [Ceragioli et al. 2024c] permit mixing moves that are chosen according to some classical value, i.e. they allow the non-deterministic composition $P + Q$ to replicate the behaviour of any process of the form **if** e **then** P **else** Q for some boolean e (see Theorem 4.12 of [Ceragioli et al. 2024c]). Instead, the present paper adopts a different perspective: we prefer a minimalist approach, favouring well-behaved, simple schedulers, and we prove stronger results, namely, the equivalence between labelled and reduction characterizations of indistinguishability. An extension to more sophisticated scheduling policies is left for future work.

Regarding our quantum-distribution based semantics, other works have proposed similar generalization of probability distributions in the setting of quantum protocols and process algebras. A symbolic version of the pLTS semantics of qCCS is proposed in [Feng et al. 2014], which uses boolean guards as additional labels and superoperators as weights. Similarly, in [Ceragioli et al. 2025, 2024a], we give a semantic model for a minimal process calculus by moving from pLTSs to ELTSs with weights from an effect algebra $\mathbb{E}$, discussing different notions of bisimilarity in the case of quantum effects [Heinosaari and Ziman 2011]. The objective of these works is to model several instantiations of the same process with different quantum data in a symbolic way, therefore simplifying verification. Although these promising contributions address the important problem of verifying protocols without assuming a specific initial quantum state, their proposed semantics are not lifted, and they do not consider schedulers nor other solutions to the problem of non-determinism. As a result, they suffer from the same adequacy problems of the standard probabilistic approach, currently impeding their concrete applications to real-world protocols.

8.3 Equivalence Relations and Other Verification Approaches

The first proposed behavioural equivalences for QPAI and qCCS were based on the standard probabilistic labelled bisimilarity, adapted to the quantum setting by requiring bisimilar configurations to agree on visible qubits, including the ones sent on open channels. Different works follow this approach; we focus hereafter on the most recent and well discussed, being the weak bisimilarity for qCCS of [Feng et al. 2012]. An equivalence between this labelled bisimilarity and a contextual equivalence is proved in [Deng and Feng 2012], where the authors also characterize them in terms of a modal logic. In addition, a symbolic bisimilarity is used to prove equivalence of processes for any possible initial state [Feng et al. 2014]. Finally, a probabilistic branching bisimulation [Wu et al. 2024] based on ϵ -trees is given, that is a congruence for parallel composition.

This kind of bisimilarity was found too strict to adhere to the prescriptions of quantum theory [Feng and Ying 2015; Kubota et al. 2016]. The proposed counterexample is similar to Example 5.6, where two mixtures of qubits that should be equated are distinguished because each element is considered in isolation. To solve this problem, the most recent labelled bisimilarities for qCCS are based on a (possibly not full) distribution semantics [Deng 2018] (or, equivalently, on full distributions with transition-consistent decompositions [Feng and Ying 2015]). An approximate version of this bisimulation is also discussed, which equates processes if they behave the same with high enough probability, and it is applied to several real-world protocols [Vitale 2022]. As previously stated, lifted semantics work well for labelled bisimilarity, because they allow comparing the visible qubits of sub-distributions as a whole, instead of comparing the states of single configurations independently. The bisimilarity proposed in [Deng 2018] correctly handles the identified counterexample (as well as Example 5.6), but falls short with similar cases, like Example 5.7. As discussed in section 5, the reason is actually the semantic model, which does not forbid ill-defined moves. No general property is proved about the adherence with quantum theory, nor a characterization in terms of distinguishing observers is made explicit. Finally, the proposed bisimilarity is not a congruence with respect to the parallel operator, even when reduced to its strong version, as shown in [Ceragioli et al. 2024c].

Based on the mixed distribution semantics, [Davidson 2012] proposed a branching bisimilarity for CQP that is a congruence for the parallel operator. The proposed bisimilarity correctly solves the problems of Example 5.6 and Example 5.7. However, the language does not feature any classical control primitive, impeding its application to the cases considered here.

We employ the same sub-distribution approach of [Deng 2018] for our strong labelled bisimilarity, but we also discuss the saturated approach, showing consistency and thus congruence with respect to the parallel operator (Theorem 6.10). Moreover, we prove that our version correctly relates processes acting on indistinguishable quantum states in general (Theorem 5.10). We restrict our focus to strong bisimilarity for simplicity and postpone to future work the investigation on weak and branching versions.

The choice of saturated bisimilarity as the touchstone behavioural equivalence is introduced in [Ceragioli et al. 2024c], where it is shown that unconstrained non-deterministic contexts do not comply with the observational limitations of quantum theory. The paper presents a different semantics for processes and contexts, constraining non-determinism only in the latter. Here we treat them uniformly by adding tags and constraining non-determinism in both of them, obtaining a congruence with respect to parallel composition. Moreover, we additionally propose an equivalent labelled bisimilarity in terms of a quantum-distributions based semantics, explicitly representing the observable properties of concurrent systems.

Tagged processes have been introduced in [Chatzikokolakis and Palamidessi 2007], and are vastly used in probabilistic systems for characterizing which choices are “admissible” or “realistic” [Andrés et al. 2011; Canetti et al. 2006; Song et al. 2015]. Our tags are reminiscent of the ones used by [Chatzikokolakis et al. 2009; Chatzikokolakis and Palamidessi 2007] to prevent schedulers from choosing a move based on private data. In the same works, the authors show that different tagging policies correspond to different classes of schedulers. Our usage of tags is somewhat similar, as we use them to impose limitations on what can affect the choice of schedulers, but our constraints are motivated by the physical limitations prescribed by quantum theory instead of secrecy assumptions. However, our schedulers lack conditionals, which are present in [Chatzikokolakis and Palamidessi 2007]. This is intended as we focus on simple, constrained schedulers and not general ones.

Some works address the verification of quantum protocols with techniques different from bisimilarities. Session types for quantum systems are proposed in [Lanese et al. 2024]. Their objective is to guarantee communication safety properties, such as deadlock-freedom, as well as conformance with the no-cloning theorem. Probabilistic model checkers have been applied to verify quantum cryptographic protocols [Gay et al. 2005]. A model checker designed specifically for quantum systems (QMC) is proposed in [Gay et al. 2008], and a translation from CQP processes to the QMC description language is given in [Davidson et al. 2012], allowing for the automatic

verification of properties expressed in a quantum version of the Computational Tree Logic. Both model checker approaches study the execution of protocols on their own, or in the presence of a known attacker. In contrast, we consider simpler properties, but allow protocols to interact with an unspecified external environment. Indeed, accounting for environments simplifies compositional verification, and provides rigorous guarantees for the verified properties, ensuring they hold against all possible attackers and deployment conditions. The verification techniques for checking equivalence between concurrent processes proposed by [Ardeshtir-Larijani et al. 2018] allow comparing protocols that are functional, in the sense of computing a deterministic input-output relation. By computing the superoperator describing the semantics of each possible interleaving arising from concurrency in the system, the authors reduce equivalence checking for a process calculus similar to qCCS to the comparison of a set of sequential programs. The equivalence is implemented in a tool called QEC (Quantum Equivalence Checker), which is also applied to several real-world quantum protocols. The proposed approach does not consider open systems that can receive any value from the environment, and the only non-determinism that is modelled is the pure interleaving of sequential programs. In contrast, non-determinism and unrestricted communication is central in our investigation, as we consider it essential when reasoning about the properties of protocols. In some exploratory works, we proposed both a trace semantics and a testing equivalence for lqCCS [Ceragioli et al. 2024d,e]. Although preliminary, these relations demonstrate that ill-defined non-deterministic moves have severe impact on the correctness of behavioural equivalences along all the linear-time–branching-time spectrum [van Glabbeek 1990], and that the definition of an operational semantics grounded in quantum theory is a main concern for verifying quantum systems.

9 Conclusion

To address the problem of verifying quantum protocols, we introduced a novel, rigorous framework designed specifically for concurrent and distributed quantum processes. This framework is built upon three core components: an expressive description language in terms of the lqCCS process calculus, an adequate semantics based on feasible schedulers, and a behavioural equivalence capable of verifying expected protocol properties. Our process calculus seamlessly integrates classical communication, parallelism, and non-determinism with quantum capabilities, making it capable of expressing real-world protocols.

Previous approaches are shown to spuriously discriminate indistinguishable processes, in contrast with the prescriptions of quantum mechanics. To address this problem, we introduced a labelled version of lqCCS, enriched by tag-based schedulers. Resorting to simple schedulers allowed us to constrain processes so that they only perform physically admissible choices, i.e. those independent of the quantum states. This suffices for making our operational semantics compliant with the limited observational power prescribed by quantum theory, ensuring that quantum values can only be inspected by causing measurement-induced disturbance. As a result of that, we were capable of lifting a known result linked to the uncertainty principle, from equivalent qubit values to bisimilar lqCCS processes that cannot be distinguished by any observer (Theorem 5.10).

Finally, we characterized the atomic observable properties of lqCCS by deriving a labelled bisimilarity, provably discriminating all and only those processes that can be operationally distinguished by some feasible observer (Theorem 6.10). This makes our behavioural equivalence also a congruence for the parallel operator. Moreover, we identified a rich class of lqCCS processes where labelled bisimilarity is checkable, without requiring any universal quantification (Theorem 6.14). To showcase our approach, we analysed three real-world protocols: superdense coding, quantum teleportation and quantum coin flip.

Future Work. A clear desideratum of a behavioural equivalence is decidability. Our labelled bisimilarity goes in this direction, thereby avoiding the need to compare processes under every possible context. However, to compare two protocols, it is still required to consider an infinite number of initial quantum states. In line with [Ceragioli et al. 2025, 2024a], we will investigate symbolic versions of our semantics. The goal is comparing lqCCS processes

in a state-independent fashion, to verify if they are bisimilar when instantiating the quantum input with any value. Moreover, given that qubits received from the environment may be essentially in any possible state, we expect that this will also help us to characterize the superoperators closure in a decidable fashion.

Our schedulers are admittedly simple: all configurations in the support of a distribution must choose the same tag. A simple extension would allow processes to resolve non-deterministic choices based on classical information, making our system comparable with the one in [Ceragioli et al. 2024c]. Scheduled bisimilarities like ours, where processes must behave the same when choosing the same tag, are sometimes called *demonic*; in contrast, an *angelic* bisimilarity uses tags only to compute feasible moves. We will investigate this different flavour of behavioural equivalence, which relieves the user from guessing the correct annotation of processes when tag names do not carry relevant information on the intended behaviour.

Acknowledgments

Supported by the European Union through the MSCA-SE project QCOMICAL (Grant Agreement ID: 101182520). Partially funded by the Plan France 2030 through the PEPR project EPiQ (ANR-22-PETQ0007).

References

- Martin Abadi and Andrew D. Gordon. 1999. A Calculus for Cryptographic Protocols: The Spi Calculus. *Information and Computation* 148, 1 (1999), 1–70. doi:10.1006/inco.1998.2740
- Miguel E. Andrés, Catuscia Palamidessi, Peter van Rossum, and Ana Sokolova. 2011. Information Hiding in Probabilistic Concurrent Systems. *Theoretical Computer Science* 412, 28 (2011), 3072–3089.
- Ebrahim Ardeshtir-Larijani, Simon J. Gay, and Rajagopal Nagarajan. 2018. Automated Equivalence Checking of Concurrent Quantum Systems. *ACM Trans. Comput. Logic* 19, 4, Article 28 (Nov. 2018), 32 pages. doi:10.1145/3231597
- Michael Ben-Or and Avinatan Hassidim. 2005. Fast quantum byzantine agreement. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing* (Baltimore, MD, USA) (STOC '05). Association for Computing Machinery, New York, NY, USA, 481–485. doi:10.1145/1060590.1060662
- Charles H. Bennet and Gilles Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (2014), 7–11. doi:10.1016/j.tcs.2014.05.025
- 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 E instein-Podolsky-Rosen channels. *Physical Review Letters* 70 (1993), 1895–1899. Issue 13.
- Charles H. Bennett and Stephen J. Wiesner. 1992. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters* 69 (1992), 2881–2884. Issue 20.
- Filippo Bonchi, Fabio Gadducci, and Giacomina Valentina Monreale. 2014. A General Theory of Barbs, Contexts, and Labels. *ACM Transactions on Computational Logic* 15, 4 (2014), 1–27.
- Filippo Bonchi, Alexandra Silva, and Ana Sokolova. 2017. The Power of Convex Algebras. In *CONCUR 2017 (LIPIcs, Vol. 85)*, Roland Meyer, Uwe Nestmann, and Marc Herbst (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 23:1–23:18.
- Gilles Brassard. 2003. Quantum communication complexity. *Foundations of Physics* 33, 11 (2003), 1593–1616. doi:10.1023/A:1026009100467
- Ran Canetti, Ling Cheung, Dilsun Kirli Kaynar, Moses D. Liskov, Nancy A. Lynch, Olivier Pereira, and Roberto Segala. 2006. Time-Bounded Task-PIOAs: A Framework for Analyzing Security Protocols. In *DISC 2006 (LNCS, Vol. 4167)*, Shlomi Dolev (Ed.). Springer, 238–253.
- Lorenzo Ceragioli, Elena Di Lavore, Giuseppe Lomurno, and Gabriele Tedeschi. 2025. A Coalgebraic Model of Quantum Bisimulation. *Electronic Proceedings in Theoretical Computer Science* 429 (Sept. 2025), 249–269. doi:10.4204/eptcs.429.14
- Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024a. Effect Semantics for Quantum Process Calculi. In *CONCUR 2024 (LIPIcs, Vol. 311)*, Rupak Majumdar and Alexandra Silva (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 16:1–16:22.
- Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024b. Quantum Bisimilarity Is a Congruence Under Physically Admissible Schedulers. In *Programming Languages and Systems - 22nd Asian Symposium, APLAS 2024, Kyoto, Japan, October 22–24, 2024, Proceedings (Lecture Notes in Computer Science, Vol. 15194)*, Oleg Kiselyov (Ed.). Springer, 176–195. doi:10.1007/978-981-97-8943-6_9
- Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024c. Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers. *Proceedings of the ACM on Programming Languages* 8, POPL (2024), 43:1269–43:1297.
- Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024d. Testing Quantum Processes. In *Leveraging Applications of Formal Methods, Verification and Validation. REoCAS Colloquium in Honor of Rocco De Nicola - 12th International Symposium, ISoLA 2024, Crete, Greece, October 27–31, 2024, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 15219)*, Tiziana Margaria and Bernhard Steffen (Eds.). Springer, 10:1–10:22.

- (Eds.). Springer, 132–151. doi:10.1007/978-3-031-73709-1_9
- Lorenzo Ceragioli, Giuseppe Lomurno, and Gabriele Tedeschi. 2024e. Reconciling Quantum Theory and Process Equivalence via Physically Admissible Schedulers. In *Recent Trends in Algebraic Development Techniques - 27th IFIP WG 1.3 International Workshop, WADT 2024, Enschede, The Netherlands, July 8, 2024, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 15587)*, Ionut Tutu (Ed.). Springer, 111–133. doi:10.1007/978-3-031-88930-1_6
- Konstantinos Chatzikokolakis, Gethin Norman, and David Parker. 2009. Bisimulation for Demonic Schedulers. In *FOSSACS 2009 (LNCS, Vol. 5504)*, Luca de Alfaro (Ed.). Springer, 318–332.
- Konstantinos Chatzikokolakis and Catuscia Palamidessi. 2007. Making Random Choices Invisible to the Scheduler. In *CONCUR 2007 (LNCS, Vol. 4703)*, Luís Caires and Vasco Thudichum Vasconcelos (Eds.). Springer, 42–58.
- Timothy A. S. Davidson. 2012. *Formal Verification Techniques Using Quantum Process Calculus*. Ph. D. Dissertation. University of Warwick.
- Timothy A. S. Davidson, Simon J. Gay, Hynek Mlnarik, Rajagopal Nagarajan, and Nick Papanikolaou. 2012. Model Checking for Communicating Quantum Processes. *Int. J. Unconv. Comput.* 8, 1 (2012), 73–98. <http://www.oldcitypublishing.com/journals/ijuc-home/ijuc-issue-contents/ijuc-volume-8-number-1-2012/ijuc-8-1-p-73-98/>
- Yuxin Deng. 2018. Bisimulations for Probabilistic and Quantum Processes. In *CONCUR 2018 (LIPIcs, Vol. 118)*, Sven Schewe and Lijun Zhang (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2:1–2:14.
- Yuxin Deng and Yuan Feng. 2012. Open Bisimulation for Quantum Processes. In *TCS 2012 (LNCS, Vol. 7604)*, Jos C. M. Baeten, Thomas Ball, and Frank S. de Boer (Eds.). Springer, 119–133.
- 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. doi: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. doi: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.
- Yuan Feng and Mingsheng Ying. 2015. Toward Automatic Verification of Quantum Cryptographic Protocols. In *CONCUR 2015 (LIPIcs, Vol. 42)*, Luca Aceto and David de Frutos-Escrig (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 441–455.
- Fei Gao, SuJuan Qin, Wei Huang, and QiaoYan Wen. 2019. Quantum Private Query: A New Kind of Practical Quantum Cryptographic Protocol. *Science China Physics, Mechanics & Astronomy* 62, 7 (2019), 70301.
- Simon J. Gay and Rajagopal Nagarajan. 2005. Communicating quantum processes. In *POPL 2005*, Jens Palsberg and Martin Abadi (Eds.). ACM, 145–157.
- Simon J. Gay and Rajagopal Nagarajan. 2006. Types and Typechecking for Communicating Quantum Processes. *Mathematical Structures in Computer Science* 16, 3 (2006), 375–406. doi:10.1017/S0960129506005263
- Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. 2005. Probabilistic Model-Checking of Quantum Protocols. *ArXiv abs/quant-ph/0504007* (2005). <https://api.semanticscholar.org/CorpusID:6622187>
- Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. 2008. QMC: A Model Checker for Quantum Systems. In *Computer Aided Verification*, Aarti Gupta and Sharad Malik (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 543–547.
- Teiko Heinosaari and Mário Ziman. 2011. *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*. Cambridge University Press.
- Matthew Hennessy. 1991. A Proof System for Communicating Processes with Value-Passing. *Formal Aspects of Computing* 3, 4 (1991), 346–366. doi:10.1007/BF01642508
- Matthew Hennessy. 2012. Exploring Probabilistic Bisimulations, Part I. *Formal Aspects of Computing* 24, 4–6 (2012), 749–768.
- C. A. R. Hoare. 1978. Communicating sequential processes. *Commun. ACM* 21, 8 (Aug. 1978), 666–677. doi:10.1145/359576.359585
- H. J. Kimble. 2008. The Quantum Internet. *Nature* 453, 7198 (2008), 1023–1030. doi: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 2012*, Hamid R. Arabnia, George A. Gravvanis, and Ashu M. G. Solo (Eds.). CSREA Press, 141–147.
- Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. 2016. Semi-Automated Verification of Security Proofs of Quantum Cryptographic Protocols. *Journal of Symbolic Computation* 73 (2016), 192–220.
- Marie Lalire. 2006. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science* 16, 3 (2006), 407–428.
- Marie Lalire and Philippe Jorrand. 2004. A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics. *CoRR quant-ph/0407005* (2004).
- Ivan Lanese, Ugo Dal Lago, and Vikraman Choudhury. 2024. Towards Quantum Multiparty Session Types. In *Software Engineering and Formal Methods - 22nd International Conference, SEFM 2024, Aveiro, Portugal, November 6–8, 2024, Proceedings (Lecture Notes in Computer Science, Vol. 15280)*, Alexandre Madeira and Alexander Knapp (Eds.). Springer, 385–403. doi:10.1007/978-3-031-77382-2_22
- Kim G. Larsen and Arne Skou. 1991. Bisimulation through Probabilistic Testing. *Information and Computation* 94, 1 (1991), 1–28. doi:10.1016/0890-5401(91)90030-6

- A. G. J. MacFarlane, Jonathan P. Dowling, and Gerard J. Milburn. 2003. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 361, 1809 (06 2003), 1655–1674. arXiv:<https://royalsocietypublishing.org/rsta/article-pdf/361/1809/1655/323777/rsta.2003.1227.pdf> doi:10.1098/rsta.2003.1227
- Robin Milner. 1980. *A Calculus of Communicating Systems*. Lecture Notes in Computer Science, Vol. 92. Springer. doi:10.1007/3-540-10235-3
- Michael A. Nielsen and Isaac L. Chuang. 2010. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.
- 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.
- Max F Riedel, Daniele Binosi, Rob Thew, and Tommaso Calarco. 2017. The European quantum technologies flagship programme. *Quantum Science and Technology* 2, 3 (jun 2017), 030501. doi:10.1088/2058-9565/aa6aca
- Shraddha Singh, Mina Doosti, Natansh Mathur, Mahshid Delavar, Atul Mantri, Harold Ollivier, and Elham Kashefi. 2023. Towards a Unified Quantum Protocol Framework: Classification, Implementation, and Use Cases. arXiv:2310.12780
- Lei Song, Yuan Feng, and Lijun Zhang. 2015. Decentralized Bisimulation for Multiagent Systems. In *AAMAS 2015*, Gerhard Weiss, Pinar Yolum, Rafael H. Bordini, and Edith Elkind (Eds.). ACM, 209–217.
- R. J. van Glabbeek. 1990. The linear time - branching time spectrum. In *CONCUR '90 Theories of Concurrency: Unification and Extension*, J. C. M. Baeten and J. W. Klop (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 278–297.
- Marco Vitale. 2022. *Verification of Quantum Bit Commitment Protocols using Bisimulation Techniques*. Ph.D. Dissertation. <https://amslaurea.unibo.it/id/eprint/25306/>
- Hao Wu, Qizhe Yang, and Huan Long. 2024. Branching bisimulation semantics for quantum processes. *Inform. Process. Lett.* 186 (2024), 106492. doi:10.1016/j.ipl.2024.106492
- Peiying Zhang, Ning Chen, Shigen Shen, Shui Yu, Sheng Wu, and Neeraj Kumar. 2024. Future Quantum Communications and Networking: A Review and Vision. *IEEE Wireless Communications* 31, 1 (2024), 141–148.

A Proofs Probability Distributions

LEMMA A.1. For any $\Delta, \Theta \in \mathcal{D}(S)$ and relation $\mathcal{R} \subseteq S \times \mathcal{D}(S)$, $\Delta \text{ lift}(\mathcal{R}) \Theta$ if and only if there is a finite index set I such that $\Delta = \sum_{i \in I} p_i \cdot s_i$, $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ and $s_i \mathcal{R} \Theta_i$.

PROOF. ($\Leftarrow$) By definition of lift , $1 \cdot s_i \text{ lift}(\mathcal{R}) \Theta_i$. Then, by definition of left linear relation it holds that $\sum_{i \in I} p_i \cdot s_i \text{ lift}(\mathcal{R}) \sum_{i \in I} p_i \cdot \Theta_i$.

($\Rightarrow$) By rule induction.

If $\Delta = 1 \cdot s$, then it follows trivially.

If $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ then by hypothesis $\Delta_i \text{ lift}(\mathcal{R}) \Theta_i$ for any $i \in I$ and $\sum_{i \in I} p_i \cdot \Delta_i$ is defined. By inductive hypothesis $\Delta_i = \sum_{j \in J_i} p_{ij} \cdot s_{ij}$ and $\Theta_i = \sum_{j \in J_i} p_{ij} \cdot \Theta_{ij}$ with $s_{ij} \mathcal{R} \Theta_{ij}$. Then $\Delta = \sum_{i \in I} \sum_{j \in J_i} p_i p_{ij} \cdot s_{ij}$ and $\Theta = \sum_{i \in I} \sum_{j \in J_i} p_i p_{ij} \cdot \Theta_{ij}$, therefore it suffices to take the set $IJ = \{ij | i \in I, j \in J_i\}$ as indices with $\{p_i p_{ij} | i \in I, j \in J_i\}$ as probabilities. We still need to check definiteness. By hypothesis Δ defined means that $\sum_{i,j \in IJ} p_i p_{ij} \leq 1$. We prove that $|\Theta| \leq 1$. $|\Theta| = \sum_{i,j \in IJ} p_i p_{ij} |\Theta_{ij}| \leq \sum_{i,j \in IJ} p_i p_{ij} \alpha \leq 1$, where $\alpha = \max_{i,j \in IJ} |\Theta_{ij}|$ that by inductive hypothesis are all less than 1 and thus $\alpha \leq 1$. $\square$

LEMMA 3.1. For any relation $\mathcal{R} \subseteq S \times \mathcal{D}(S)$, $\text{lift}(\mathcal{R})$ is left-decomposable.

PROOF. Assume $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ and $\Delta \text{ lift}(\mathcal{R}) \Theta$. By Lemma A.1 there is a family J such that $\Delta = \sum_{j \in J} q_j \cdot s_j$, $\Theta = \sum_{j \in J} q_j \cdot \Theta_j$ with $s_j \mathcal{R} \Theta_j$. Note that $\Delta_i = \sum_{s \in [\Delta_i]} \Delta_i(s) \cdot \sum_{j \in J | s=s_j} \frac{q_j}{\Delta(s)} \cdot s_j$. Thus, take Θ_i defined as $\Theta_i = \sum_{s \in [\Delta_i]} \Delta_i(s) \cdot \sum_{j \in J | s=s_j} \frac{q_j}{\Delta(s)} \cdot \Theta_j$. Since $s_j \mathcal{R} \Theta_j$, by left linearity it follows that $\Delta_i \text{ lift}(\mathcal{R}) \Theta_i$ for any $i \in I$.

We can simply compute that $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$

$$\begin{aligned} \sum_{i \in I} p_i \cdot \Theta_i &= \sum_{s \in [\Delta]} \sum_{i \in I} p_i \Delta_i(s) \cdot \sum_{j \in J | s=s_j} \frac{q_j}{\Delta(s)} \cdot \Theta_j \\ &= \sum_{s \in [\Delta]} \Delta(s) \cdot \sum_{j \in J | s=s_j} \frac{q_j}{\Delta(s)} \cdot \Theta_j \\ &= \sum_{s \in [\Delta]} \sum_{j \in J | s=s_j} q_j \cdot \Theta_j \\ &= \sum_{j \in J} q_j \cdot \Theta_j \\ &= \Theta \end{aligned}$$

$\square$

B Proofs about Type and Semantics

THEOREM 4.1. Whenever $\Sigma \vdash P$ and $\Sigma' \vdash P$ then $\Sigma = \Sigma'$

PROOF. By induction on the derivation $\Sigma \vdash P$ and $\Sigma' \vdash P$.

Nil It must be that $P = 0_{\tilde{e}}$ for some sequence of qubits $\tilde{e}$, therefore $\tilde{e} \in \tilde{\Sigma}$ and $\tilde{e} \in \tilde{\Sigma}'$. Since $\tilde{e}$ must contain all elements in both Σ and Σ' it must be that $\Sigma = \Sigma'$.

QRecv By inductive hypothesis $\Sigma \cup \{e\} = \Sigma' \cup \{e\}$. However, by $e \notin \Sigma$ and $e \notin \Sigma'$ it must be that $\Sigma = \Sigma'$.

QSend It must be that $P = c!q.R$ for a qubit q , therefore both $q \in \Sigma$ and $q \in \Sigma'$. By inductive hypothesis $\Sigma \setminus \{q\} = \Sigma' \setminus \{q\}$.

Par By hypothesis of the rule $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\Sigma' = \Sigma'_1 \cup \Sigma'_2$ with $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $\Sigma'_1 \cap \Sigma'_2 = \emptyset$. Since it must be that $P = Q \parallel R$, by inductive hypothesis $\Sigma_1 = \Sigma'_1$ and $\Sigma_2 = \Sigma'_2$, therefore $\Sigma = \Sigma'$.

Otherwise By application of the inductive hypothesis.

$\square$

LEMMA B.1. *If $\Sigma \cup \{x\} \vdash P$ and $q \notin \Sigma$ then $\Sigma \cup \{q\} \vdash P[q/x]$.*

PROOF. By structural induction on the typing derivation of $\Sigma \cup \{x\} \vdash P$.

Nil It must be that $P = 0_{\tilde{e}}$ with $x \in \tilde{e}$. By NIL, trivially $\Sigma \cup \{q\} \vdash 0_{\tilde{e}}[q/x]$.

Sop It must be that $P = \mathcal{E}(\tilde{e}).R$ for some process R .

If $x \notin \tilde{e}$ then $P[q/x] = \mathcal{E}(\tilde{e}).R[q/x]$, which is typed by SOP and the inductive hypothesis.

If $x \in \tilde{e}$ and $\tilde{e} \in \tilde{\Sigma}'$, then by substitution in the SOP rule, $\tilde{e}[q/x] \in \Sigma' \setminus \{x\} \cup \{q\}$. Trivially $\Sigma' \setminus \{x\} \cup \{q\} \subseteq \Sigma \cup \{q\}$, and by inductive hypothesis $\Sigma \cup \{q\} \vdash R[q/x]$.

Meas It must be that $P = \mathcal{M}(\tilde{e} \triangleright y).R$ for some process R . The result follows by the same reasoning of the SOP case, noting that the new variable y cannot be the same as the to-be-substituted variable x due to mismatching types.

QSend It must be that $P = c!e.R$ for some process R .

If $e = x$ then by typing the substitution has no effect on R , thus the result follows trivially by QSEND, since $(c!x.R)[q/x] = c!q.R$.

If $e \neq x$ then the result follows from the inductive hypothesis.

Par It must be that $P = R \parallel Q$ for some processes R and Q , with $\Sigma \cup \{x\} = \Sigma_1 \cup \Sigma_2$, $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $\Sigma_1 \vdash R$, $\Sigma_2 \vdash Q$. Without loss of generality assume that $x \in \Sigma_1$. By inductive hypothesis $\Sigma_1 \setminus \{x\} \cup \{q\} \vdash R[q/x]$ and $\Sigma_2 \vdash Q[q/x]$ since the substitution has no effect on Q because the variable x is not in Σ_2 and thus does not appear in Q . The result follows by the PAR rule.

Otherwise By application of the inductive hypothesis. $\square$

THEOREM 4.6 (TYPING QUASI-PRESERVATION). *Let $\Sigma \subseteq Q$ and $\mu \in \text{Act}$. Then there exists Σ' such that for all $(\Sigma'', \Sigma) \vdash C$ and $\Delta \in \mathcal{D}(\text{Conf})$ with $C \xrightarrow{\mu}_s \Delta$ it holds $(\Sigma'', \Sigma') \vdash \Delta$.*

PROOF. Consider the function f which takes as input a typing context and an action

$$f(\Sigma, \mu) = \begin{cases} \Sigma \cup \{q\} & \text{if } \mu = c?q \text{ with } c : \hat{Q} \\ \Sigma \setminus \{q\} & \text{if } \mu = c!q \text{ with } c : \hat{Q} \\ \Sigma & \text{otherwise} \end{cases}$$

Let $(\Sigma'', \Sigma) \vdash C$ and $C \xrightarrow{\mu}_s \Delta$. We will prove that $(\Sigma'', f(\Sigma, \mu)) \vdash \Delta$.

By induction on the derivation of $\xrightarrow{\mu}_s$.

ParL It must be that $C = \langle \rho, P_1 \parallel P_2 \rangle$, for some processes P_1 and P_2 such that $\Sigma = \Sigma_1 \cup \Sigma_2$, $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $(\Sigma'', \Sigma_1) \vdash P_1$. By induction $(\Sigma'', f(\Sigma_1, \mu)) \vdash \Delta$, with $\langle \rho, P_1 \rangle \xrightarrow{\mu}_s \Delta$. We must verify that $(\Sigma'', f(\Sigma_1, \mu) \cup \Sigma_2) \vdash \Delta \parallel P_2$ with $f(\Sigma_1, \mu) \cap \Sigma_2 = \emptyset$. If $\mu = \tau$ or $\mu = c!v, c?v$ with c a classical channel, then $f(\Sigma_1, \mu) = \Sigma_1$, which trivially satisfies the requirements. If $\mu = c!v$ with $c : \hat{Q}$ then $f(\Sigma_1, c!v) = \Sigma_1 \setminus \{v\}$, but by the QSEND rule $v \in \Sigma_1$ and by PAR $v \notin \Sigma_2$, thus the requirements hold.

ParR Symmetrically to the PARL case.

SynchL It must be that $C = \langle \rho, P \parallel Q \rangle$, for some processes P and Q such that $\langle \rho, P \rangle \xrightarrow{c!v}_t 1 \cdot \langle \rho, P' \rangle$, $\langle \rho, Q \rangle \xrightarrow{c?v}_{t'} 1 \cdot \langle \rho, Q' \rangle$, and $\Delta = 1 \cdot \langle \rho, P' \parallel Q' \rangle$. If c is a classical channel then as for the parallel cases, there exists Σ_1 and Σ_2 such that $\Sigma = \Sigma_1 \cup \Sigma_2$, $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $(\Sigma'', \Sigma_1) \vdash P$, $(\Sigma'', \Sigma_2) \vdash Q$. By induction and application of f , $(\Sigma'', \Sigma_1 \setminus \{v\}) \vdash P'$ and $(\Sigma'', \Sigma_2 \cup \{v\}) \vdash Q'$. As for the previous case, $v \in \Sigma_1$, thus $v \in \Sigma''$, and by PAR $v \notin \Sigma_2$. Thus, $f(\Sigma_1, c!v) \cup f(\Sigma_2, c?v) = (\Sigma_1 \setminus \{v\}) \cup (\Sigma_2 \cup \{v\}) = \Sigma = f(\Sigma, \tau)$.

Otherwise By induction hypothesis and trivial correspondence with their respective typing rules. $\square$

THEOREM 4.5 (TYPING PRESERVATION). *If $(\Sigma_\rho, \Sigma_P) \vdash \langle \rho, P \rangle$ and $\langle \rho, P \rangle \xrightarrow{\tau}_s \Delta$ then $(\Sigma_\rho, \Sigma_P) \vdash \Delta$.*

PROOF. It follows from the proof Theorem 4.6, by noticing that for $C \xrightarrow{\tau}_s \Delta$, the unique Σ_τ is exactly Σ_P . $\square$

LEMMA B.2. *Let $\Sigma \subseteq \mathcal{Q}$ and $\mu \in \text{Act}$. Then there exists Σ' such that for all $(\Sigma'', \Sigma) \vdash \Delta$ and $\Theta \in \mathcal{D}(\text{Conf})$ with $\Delta \succ^{\mu}_s \Theta$ it holds $(\Sigma'', \Sigma') \vdash \Theta$.*

PROOF. Let $\Delta = \sum_{i \in I} p_i \cdot C_i$, where every C_i is unique with $(\Sigma'', \Sigma) \vdash \Delta$ and $(\Sigma'', \Sigma) \vdash C_i$ for all $i \in I$. If I is empty then $\Delta = \epsilon$ and by definition of $\succ^{\mu}_s$, $\Delta' = \epsilon$, which is always well-typed. Otherwise, since $\succ^{\mu}_s$ is left decomposable then for any $i \in I$ there exist a Θ_i such that $C \succ^{\mu}_s \Theta_i$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$. By Theorem 4.6, there exists a Σ' such that for any $C_i \xrightarrow{\mu}_s \Theta_i$ it holds $(\Sigma'', \Sigma') \vdash \Theta_i$, and thus also $(\Sigma'', \Sigma') \vdash \Theta$. $\square$

We now prove some basic properties on our probabilistic semantics.

LEMMA B.3. *For any configuration $C \in \text{Conf}$, $s \in \text{Sched}$, if $C \xrightarrow{\mu}_s \Delta$ and $C \xrightarrow{\mu}_s \Delta'$ then $\Delta = \Delta'$.*

PROOF. By Assumption 1 since the two labels are equals it must be that $\Delta = \Delta'$. $\square$

LEMMA B.4. *For any configuration $C \in \text{Conf}$, $s \in \text{Sched}$, if $C \text{ bot}(\xrightarrow{\mu}_s) \Delta$ and $C \text{ bot}(\xrightarrow{\mu}_s) \Delta'$ then $\Delta = \Delta'$.*

PROOF. Assume $C \text{ bot}(\xrightarrow{\mu}_s) \Delta$ and $C \text{ bot}(\xrightarrow{\mu}_s) \Delta'$ and proceed by cases: if $\Delta = \epsilon$ then, by definition of $\text{bot}(\cdot)$ there is no other Δ' such that $C \text{ bot}(\xrightarrow{\mu}_s) \Delta$, thus $\Delta = \Delta' = \epsilon$. Otherwise, it holds by Lemma B.3. $\square$

PROPOSITION 4.8. *For any distribution $\Delta \in \mathcal{D}^{\leq}(\text{Conf})$ composed of deterministic processes, $\mu \in \text{Act}$, $s \in \text{Sched}$, and $\Theta, \Theta' \in \mathcal{D}^{\leq}(\text{Conf})$, if $\Delta \succ^{\mu}_s \Theta$ and $\Delta \succ^{\mu}_s \Theta'$ then $\Theta = \Theta'$.*

PROOF. Let $\Delta = \sum_{i \in I} p_i \cdot C_i$ where every C_i is unique, and assume $\Delta \succ^{\mu}_s \Theta$ and $\Delta \succ^{\mu}_s \Theta'$. Since $\succ^{\mu}_s$ and $\succ^{\mu'}_s$ are left decomposable there exists families $\{\Theta_i\}_{i \in I}$ and $\{\Theta'_i\}_{i \in I}$ such that $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ with $1 \cdot C_i \succ^{\mu}_s \Theta_i$, and $\Theta' = \sum_{i \in I} p_i \cdot \Theta'_i$ with $1 \cdot C_i \succ^{\mu}_s \Theta'_i$. By Lemma B.4 for any $i \in I$ it holds $\Theta_i = \Theta'_i$ and thus $\Theta = \Theta'$. $\square$

LEMMA B.5. *For any process $\Sigma \vdash P$, and scheduler s , there is a (possibly empty) family I of trace non-increasing superoperators $\mathcal{E}_i \in \mathcal{SO}^{\leq}(\mathcal{H}_{\Sigma})$ and processes P_i such that for all density operator ρ , $\langle \rho, P \rangle \xrightarrow{\tau}_s \Delta$ if and only if*

$$\Delta = \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\rho)) \neq 0} \text{tr}(\mathcal{E}_i(\rho)) \cdot \left\langle \frac{\mathcal{E}_i(\rho)}{\text{tr}(\mathcal{E}_i(\rho))}, P_i \right\rangle.$$

PROOF. We proceed by induction on the rules of the semantics.

Sop It must be that $P = s: \mathcal{E}(x).R$ for some process R and superoperator $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\Sigma})$. Then $\Delta = 1 \cdot \langle \mathcal{E}(\rho), R \rangle$.

Note that since $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\Sigma})$, and $\text{tr}(\rho) = 1$, then $\text{tr}(\mathcal{E}(\rho)) = 1$. Take the singleton family with $\mathcal{E}$ and R .

Meas It must be that $P = s: \mathcal{M}(\tilde{q} \triangleright x).R$ for some process R and measurement $\mathcal{M} = \{M_m\}_m$. Then $\Delta = \sum_m \text{tr}(M_m(\rho)) \cdot \left\langle \frac{M_m(\rho)}{\text{tr}(M_m(\rho))}, R[m/x] \right\rangle$. Take the operators M_m such that $\text{tr}(M_m(\rho)) \neq 0$ and their respective processes $R[m/x]$.

Other non-inductive The rules TAU, TAUSYNCH, SEND and RECV do not modify the quantum state and require Δ to be of the form $1 \cdot \langle \rho, P' \rangle$. Thus, take the singleton family with the identity superoperator $\mathbb{I}$ and process P' .

Otherwise The other cases follow trivially from the inductive hypothesis. $\square$

We define the following notation for the family of superoperators and processes that represents the evolution in a parametric way with respect to density operators.

Definition B.6. For any process $P \in Proc$, scheduler $s \in Sched$ and action $\mu \in Act$, we say $\{\mathcal{E}_i, P_i\}_{i \in I} \in \text{next}(P, s, \mu)$ if $\{\mathcal{E}_i, P_i\}_{i \in I}$ is an I -indexed family of pairs of superoperators $\mathcal{E}_i \in SO^\leq(\mathcal{H}_{\Sigma_P})$ with $\sum_{i \in I} \mathcal{E}_i \in SO(\mathcal{H}_{\Sigma_P})$, and processes $P_i \in Proc$ such that either:

- if $I = \emptyset$ then $\langle \rho, P \rangle \xrightarrow{\mu}_s$ for any state ρ ; otherwise
- if $I \neq \emptyset$ then $\langle \rho, P \rangle \xrightarrow{\mu}_s \sum_{i \in I} \text{tr}(\mathcal{E}_i(\rho)) \cdot \left\langle \frac{\mathcal{E}_i(\rho)}{\text{tr}(\mathcal{E}_i(\rho))}, P_i \right\rangle$ for any state ρ .

Note that under Assumption 1 there is only one family I in $\text{next}(P, s, \mu)$ for all P, s and μ , and we will write $\text{next}(P, s, \mu) = \{\mathcal{E}_i, P_i\}_{i \in I}$ to denote such family.

Moreover, we allow applying superoperators to configurations and distributions. Given $\mathcal{E} \in SO^\leq(\mathcal{H})$, we define $\mathcal{E} : \mathcal{D}(Conf) \rightarrow \mathcal{D}(Conf)$ as

$$\mathcal{E} \left(\sum_i p_i \cdot \langle \rho_i, P_i \rangle \right) = \sum_i p_i \cdot \text{tr}(\mathcal{E}(\rho_i)) \cdot \left\langle \frac{\mathcal{E}(\rho_i)}{\text{tr}(\mathcal{E}(\rho_i))}, P_i \right\rangle.$$

Roughly, if $\mathcal{E}$ is trace-preserving it is just applied to configurations. If $\mathcal{E}$ is trace non-increasing, then after its application each ρ_i is normalized and the weight of the i -th configuration is updated accordingly.

Finally, given $\Sigma, \Sigma' \vdash \Delta$, if $\mathcal{E}$ is defined on $\tilde{q}$, which are only some of the qubits in Σ , we write $\mathcal{E}(\Delta)$ for $\mathcal{E}^{\tilde{q}}(\Delta)$ (recall that $\mathcal{E}^{\tilde{q}}$ extends $\mathcal{E}$ by tensoring it with the identity).

LEMMA B.7. *For any processes $P, R \in Proc$ with $\text{Tag}(P) \cap \text{Tag}(R) = \emptyset$, we have $\langle \rho, P \parallel R \rangle \xrightarrow{\mu}_s \Delta$ if and only if one of the following holds:*

- (1) $\Delta = \Delta' \parallel R$ with $\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta'$ and $\text{Tag}(s) \subseteq \text{Tag}(P)$;
- (2) $\Delta = P \parallel \Delta'$ with $\langle \rho, R \rangle \xrightarrow{\mu}_s \Delta'$ and $\text{Tag}(s) \subseteq \text{Tag}(R)$;
- (3) $\Delta = 1 \cdot \langle \rho, P' \parallel R \rangle$ where there exists a channel c and value v such that $\langle \rho, P \rangle \xrightarrow{c?v}_{t_1} 1 \cdot \rho, P'$, $\langle \rho, R \rangle \xrightarrow{c!v}_{t_2} 1 \cdot \rho, R'$ with $s = (t_1, t_2)$, $t_1 \in \text{Tag}(P)$ and $t_2 \in \text{Tag}(R)$;
- (4) $\Delta = 1 \cdot \langle \rho, P' \parallel R \rangle$ where there exists a channel c and value v such that $\langle \rho, P \rangle \xrightarrow{c!v}_{t_1} 1 \cdot \rho, P'$, $\langle \rho, R \rangle \xrightarrow{c?v}_{t_2} 1 \cdot \rho, R'$ with $s = (t_1, t_2)$, $t_1 \in \text{Tag}(P)$ and $t_2 \in \text{Tag}(R)$.

PROOF. A transition of the form $\langle \rho, P \parallel R \rangle \xrightarrow{\mu}_s \Delta$ can happen only through one of the rules **PARL**, **PARR**, **SYNCHL** and **SYNCHR**. Each of the four cases is a sufficient and necessary condition to apply one of the rules above. $\square$

LEMMA B.8. *For any processes P and R with $\text{Tag}(P) \cap \text{Tag}(R) = \emptyset$, we have $\langle \rho, P \parallel R \rangle \text{ bot}(\xrightarrow{\mu}_s) \in$ if and only if all of the following hold:*

- P cannot move, i.e. $\langle \rho, P \rangle \not\xrightarrow{\mu}_s$;
- R cannot move, i.e. $\langle \rho, R \rangle \not\xrightarrow{\mu}_s$;
- P and R cannot synchronize, i.e. for all c and v , if $\mu = \tau$ and $s = (t_1, t_2)$ we have $\text{next}(R, t_2, c!v) \neq \emptyset \implies \langle \rho, P \rangle \xrightarrow{c?v}_{t_1}$ and $\text{next}(R, t_2, c?v) \neq \emptyset \implies \langle \rho, P \rangle \xrightarrow{c!v}_{t_1}$.

PROOF. For the only if direction, we know that $\langle \rho, P \parallel R \rangle \xrightarrow{\mu}_s$, and this implies that $\langle \rho, P \parallel R \rangle$ can not move with any of the rules **PARL** (first case), **PARR** (second case), **SYNCHL** and **SYNCHR** (third case). For the if direction, since all three cases hold, we know that none of the above rule can be applied, and thus $\langle \rho, P \parallel R \rangle \not\xrightarrow{\mu}_s$ and $\langle \rho, P \parallel R \rangle \text{ bot}(\xrightarrow{\mu}_s) \in$. $\square$

LEMMA B.9. For any non-empty distribution $\Delta \in \mathcal{D}^{\leq}(\text{Conf})$ and process $R \in \text{Proc}$ with $\text{Tag}(\Delta) \cap \text{Tag}(R) = \emptyset$, we have $\Delta \parallel R \xrightarrow{\mu}_s \Theta \neq \epsilon$ if and only if one of the following holds:

- (1) $\text{Tag}(s) \subseteq \text{Tag}(\Delta)$ and there exists Θ' such that $\Theta = \Theta' \parallel R$ and $\Delta \xrightarrow{\mu}_s \Theta'$;
- (2) $\text{Tag}(s) \subseteq \text{Tag}(R)$ and $\Theta = \sum_{i \in I} \mathcal{E}_i(\Delta \parallel R_i)$ with $\text{next}(R, s, \mu) = \{\mathcal{E}_i, R_i\}_{i \in I}$;
- (3) $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$, and $\Theta = \Theta' \parallel R'$, $\exists c, v. \Delta \xrightarrow{c?v}_{t_1} \Theta'$ with $\text{next}(R, t_2, c!v) = \{\mathbb{I}, R'\}$;
- (4) $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$, and $\Theta = \sum_{v \in V} \Theta_v \parallel R_v$, $\exists c, V. \forall v \in V. \Delta \xrightarrow{c!v}_{t_1} \Theta_v$ with $\text{next}(R, t_2, c?v) = \{\mathbb{I}, R_v\}$.

PROOF. We start with the “only if” direction. Let $\Delta \parallel R \xrightarrow{\mu}_r \Theta$ and let $\Delta = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle$ where every $\langle \rho_i, P_i \rangle$. By left-decomposability, $1 \cdot \langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s \Theta_i$ for all $i \in I$ with $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$. Since $\Theta \neq \epsilon$, there is a subset $J \subseteq I$ such that $1 \cdot \langle \rho_j, P_j \parallel R \rangle \xrightarrow{\mu}_s \Theta_j$ with $\Theta_j \neq \epsilon$, i.e. $\langle \rho_j, P_j \parallel R \rangle \xrightarrow{\mu}_s \Theta_j$ for all $j \in J$. Consider a single $j \in J$. By Lemma B.7 we have to consider four cases:

- (1) If $\text{Tag}(s) \subseteq \text{Tag}(P_j)$, $\langle \rho_j, P_j \rangle \xrightarrow{\mu}_s \Theta'_j$ and $\Theta_j = \Theta'_j \parallel R$, then $\text{Tag}(s) \cap \text{Tag}(R) = \emptyset$. Thus, for all $i \in I$ either $\langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s$ so $\Theta_i = \epsilon$ and by Lemma B.8 $\langle \rho_i, P_i \rangle \xrightarrow{\mu}_s$, or $\langle \rho_i, P_i \rangle \xrightarrow{\mu}_s \Theta'_i$ so $\langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s \Theta'_i \parallel R = \Theta_i$ by Lemma B.7. Note that the latter are exactly all the configuration in J . Therefore, $\Delta = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle \xrightarrow{\mu}_s \sum_{j \in J} p_j \cdot \Theta'_j = \Theta'$ and $\Theta = \Theta' \parallel R = \sum_{i \in I} p_i \cdot \Theta_i = \sum_{j \in J} p_j \cdot \Theta'_j \parallel R$.
- (2) If $\text{Tag}(s) \subseteq \text{Tag}(R)$, by Lemma B.5, $\text{next}(R, s, \mu) = \{\mathcal{E}_k, R_k\}_{k \in K}$. Since $\text{Tag}(s) \cap \text{Tag}(\Delta) = \emptyset$, by Lemma B.7, $\langle \rho_i, R \rangle \xrightarrow{\mu}_s \sum_{k \in K} \text{tr}(\mathcal{E}_k(\rho_i)) \cdot \left\langle \frac{\mathcal{E}_k(\rho_i)}{\text{tr}(\mathcal{E}_k(\rho_i))}, R_k \right\rangle$ for all i , and thus $\langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s \sum_{k \in K} \text{tr}(\mathcal{E}_k(\rho_i)) \cdot \left\langle \frac{\mathcal{E}_k(\rho_i)}{\text{tr}(\mathcal{E}_k(\rho_i))}, P_i \parallel R_k \right\rangle$. Therefore, $\Delta \parallel R = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s \sum_{i \in I} p_i \cdot \sum_{k \in K} \text{tr}(\mathcal{E}_k(\rho_i)) \cdot \left\langle \frac{\mathcal{E}_k(\rho_i)}{\text{tr}(\mathcal{E}_k(\rho_i))}, P_i \parallel R_k \right\rangle = \sum_{k \in K} \mathcal{E}_k(\Delta \parallel R_k)$.
- (3) If $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$ and there are c and v such that $\text{next}(R, t_2, c!v) = \{\mathbb{I}, R'\}$ then by Lemma B.7 $\langle \rho_j, P_j \parallel R \rangle \xrightarrow{\tau}_s 1 \cdot \langle \rho_j, P'_j \parallel R' \rangle$ with $\text{next}(P_j, t_1, c?v) = \{\mathbb{I}, P'_j\}$. Note that c and v are unique due to the assumption of determinism, and by Lemma B.7, the same holds for all $j \in J$. By left-linearity $\Delta \parallel R \xrightarrow{\tau}_s \Theta' \parallel R'$ where $\Theta' = \sum_{j \in J} p_j \cdot P'_j$.
- (4) If $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$ and there are c and v such that $\text{next}(R, t_2, c?v) = \{\mathbb{I}, R_v\}$. Let J_v be the subset of J such that $\langle \rho_j, P_j \rangle \xrightarrow{c!v}_{t_1} 1 \cdot \langle \rho_j, P'_j \rangle$, and let $\Theta_v = \sum_{j \in J_v} p_j \cdot \langle \rho_j, P'_j \rangle$. By Lemma B.7 and linearity we have $\sum_{j \in J_v} p_j \cdot \langle \rho_j, P_j \rangle \xrightarrow{c!v}_{t_1} \Theta_v$ and $\sum_{j \in J_v} p_j \cdot \langle \rho_j, P_j \parallel R \rangle \xrightarrow{\tau}_s \Theta_v \parallel R_v$. Let J^x be the subset of processes in deadlock. Therefore, $\Delta \parallel R = \sum_{v \in V} \sum_{j \in J_v} p_j \cdot \langle \rho_j, P_j \parallel R \rangle \oplus \sum_{j \in J^x} p_j \cdot \langle \rho_j, P_j \parallel R \rangle \xrightarrow{\tau}_s \sum_{v \in V} \Theta_v \parallel R_v \oplus \epsilon$.

The “if” direction is similar: any of the four cases implies $\Delta \parallel R \xrightarrow{\mu}_s \Theta$. $\square$

LEMMA B.10. For any non-empty distribution $\Delta \in \mathcal{D}^{\leq}(\text{Conf})$ and process $R \in \text{Proc}$ with $\text{Tag}(\Delta) \cap \text{Tag}(R) = \emptyset$, we have $\Delta \parallel R \xrightarrow{\mu}_s \epsilon$ if and only if all of the following hold:

- Δ cannot move, i.e. $\Delta \xrightarrow{\mu}_s \epsilon$;
- R cannot move, i.e. $\text{next}(R, s, \mu) = \emptyset$;
- Δ and R cannot synchronize, i.e. for all c and v , if $\mu = \tau$ and $s = (t_1, t_2)$ we have $\text{next}(R, t_2, c!v) \neq \emptyset \implies \Delta \xrightarrow{c?v}_{t_1} \epsilon$ and $\text{next}(R, t_2, c?v) \neq \emptyset \implies \Delta \xrightarrow{c!v}_{t_1} \epsilon$.

PROOF. Let $\Delta = \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle$ where every $\langle \rho_i, P_i \rangle$ is unique. By left-decomposability $1 \cdot \langle \rho_i, P_i \parallel R \rangle \xrightarrow{\mu}_s \epsilon$ for all $i \in I$. For all $i \in I$ we can apply Lemma B.8, and thus we know that

- For all $i \in I$, $\langle \rho_i, P_i \rangle \not\xrightarrow{\mu}_s$;
- For all $i \in I$, $\langle \rho_i, R_i \rangle \not\xrightarrow{\mu}_s$;
- For all i, c and v , if $\mu = \tau$ and $s = (t_1, t_2)$ we have $next(R, t_2, c!v) \neq \emptyset \implies \langle \rho_i, P_i \rangle \xrightarrow{c?v}_{t_1}$ and $next(R, t_2, c?v) \neq \emptyset \implies \langle \rho_i, P_i \rangle \xrightarrow{c!v}_{t_1}$.

The first point is equivalent to saying that $\Delta \xrightarrow{\mu}_s \epsilon$. The second point holds if and only if $next(R, s, \mu) = \emptyset$, thanks to Lemma B.5. If we move the quantification on all the i s into the implication, the third point is equivalent to $next(R, t_2, c!v) \neq \emptyset \implies \Delta \xrightarrow{c?v}_{t_1} \epsilon$ and $next(R, t_2, c?v) \neq \emptyset \implies \Delta \xrightarrow{c!v}_{t_1} \epsilon$. $\square$

LEMMA 5.4. For all deterministic $P, R \in Proc$, if $Tag(P) \cap Tag(R) = \emptyset$ then $P \parallel R$ is deterministic.

PROOF. Let ρ be a quantum state and assume $\langle \rho, P \parallel R \rangle \xrightarrow{\mu}_s \Delta$ and $\langle \rho, P \parallel R \rangle \xrightarrow{\mu'}_s \Delta'$. By cases on s .

If $Tag(s) \subseteq Tag(P)$, by Lemma B.5 there exists Δ_P and Δ'_P such that $\Delta = \Delta_P \parallel R$ with $\langle \rho, P \rangle \xrightarrow{\mu}_s \Delta_P$ and $\Delta' = \Delta'_P \parallel R$ with $\langle \rho, P \rangle \xrightarrow{\mu'}_s \Delta'_P$. By Assumption 1 either $\mu = \mu'$ and $\Delta_P = \Delta'_P$ or $\mu = c?v$ and $\mu' = c?v'$. In either case the requirements of Assumption 1 are trivially satisfied by $P \parallel R$.

The case for $Tag(s) \subseteq Tag(R)$ follows the same line of reasoning.

If $Tag(s) \not\subseteq Tag(P \parallel R)$ then the process must be in deadlock.

If $Tag(s) \subseteq Tag(P \parallel R)$ but $Tag(s) \not\subseteq Tag(P)$ and $Tag(s) \not\subseteq Tag(R)$, then $s = (t_1, t_2)$ with $t_1 \in Tag(P)$ and $t_2 \in Tag(R)$. By the form of the process and the form of the scheduler the only applicable semantic rules are either SYNCHL or SYNCHR. Without loss of generality assume $\langle \rho, P \parallel R \rangle \xrightarrow{\mu}_s \Delta$ by SYNCHL. Therefore, it must be that $\mu = \tau$, $\langle \rho, P \rangle \xrightarrow{c!v}_{t_1} \langle \rho, P_{cont} \rangle$, $\langle \rho, R \rangle \xrightarrow{c?v}_{t_2} \langle \rho, R_{cont} \rangle$ and $\Delta = \langle \rho, P_{cont} \parallel R_{cont} \rangle$ for some channel c , value v and processes P_{cont}, R_{cont} . Then it must be that also $\langle \rho, P \parallel R \rangle \xrightarrow{\mu'}_s \Delta'$ by SYNCHL, because if it moves by SYNCHR then $\langle \rho, P \rangle \xrightarrow{d?v}_{t_1} \Delta''$, meaning that with the process P can perform two moves with distinct labels with the same scheduler t_1 , violating Assumption 1. Thus, $\mu' = \tau$, $\langle \rho, P \rangle \xrightarrow{c'!v'}_{t_1} \langle \rho, P'_{cont} \rangle$, $\langle \rho, P \rangle \xrightarrow{c'?v'}_{t_2} \langle \rho, R'_{cont} \rangle$ and $\Delta' = \langle \rho, P'_{cont} \parallel R'_{cont} \rangle$ for some channel c' , value v' and processes P'_{cont}, R'_{cont} . By Assumption 1 and since $c!v$ and $c'!v'$ are both not receptions, $P_{cont} = P'_{cont}$ and $c!v = c'!v'$, thus it must be that $c?v = c'?v'$ and $R_{cont} = R'_{cont}$. $\square$

C Proofs about Saturated Bisimulations

Definition C.1. Let $\mathcal{R} \subseteq \mathcal{D}^\leq(Conf) \times \mathcal{D}^\leq(Conf)$. The weak linear closure $lc(\mathcal{R})$ of $\mathcal{R}$ is the least relation satisfying the following rule

$$\frac{\forall i \in I. \Delta_i \mathcal{R} \Theta_i \quad |\sum_{i \in I} p_i \cdot \Delta_i| \leq 1 \quad |\sum_{i \in I} p_i \cdot \Theta_i| \leq 1}{(\sum_{i \in I} p_i \cdot \Delta_i) \text{ } lc(\mathcal{R}) \text{ } (\sum_{i \in I} p_i \cdot \Theta_i)}$$

Notice how this definition is based on "weak linearity", meaning that the composite distributions must be related only if they are both defined. Instead, in a left-linear relation, $|\sum_{i \in I} p_i \cdot \Theta_i| \leq 1$ is a consequence and not a requirement. Nonetheless, if $\mathcal{R}$ is mass-preserving, the weak linear closure is indeed linear.

PROPOSITION C.2. Let $\mathcal{R} \subseteq \mathcal{D}^\leq(Conf) \times \mathcal{D}^\leq(Conf)$, where $|\Delta| \geq |\Theta|$ whenever $\Delta \mathcal{R} \Theta$. The weak linear closure $lc(\mathcal{R})$ is left-linear.

PROOF. Let I be the index of families $\{\Delta_i\}$ and $\{\Theta_i\}$ such that $\Delta_i \text{ lc}(\mathcal{R}) \Theta_i$ for all $i \in I$. By hypothesis for any $i \in I$ it also holds that $|\Delta_i| \geq |\Theta_i|$. Take $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ with $|\Delta| \leq 1$. By definition of mass:

$$1 \geq |\Delta| = \left| \sum_{i \in I} p_i \cdot \Delta_i \right| = \sum_{i \in I} p_i |\Delta_i| \geq \sum_{i \in I} p_i |\Theta_i| = \left| \sum_{i \in I} p_i \cdot \Theta_i \right| = |\Theta|$$

Since Θ is defined, we have that $\Delta \text{ lc}(\mathcal{R}) \Theta$. $\square$

PROPOSITION C.3. Let $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$, where $|\Delta| = |\Theta|$ whenever $\Delta \mathcal{R} \Theta$. The linear closure $\text{lc}(\mathcal{R})$ is linear.

PROOF. Let I be the index of families $\{\Delta_i\}$ and $\{\Theta_i\}$ such that $\Delta_i \text{ lc}(\mathcal{R}) \Theta_i$ for all $i \in I$. By hypothesis for any $i \in I$ it also holds that $|\Delta_i| = |\Theta_i|$. Take $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ with $|\Delta| \leq 1$. By definition of mass:

$$1 \geq |\Delta| = \left| \sum_{i \in I} p_i \cdot \Delta_i \right| = \sum_{i \in I} p_i |\Delta_i| = \sum_{i \in I} p_i |\Theta_i| = \left| \sum_{i \in I} p_i \cdot \Theta_i \right| = |\Theta|$$

Since Θ is defined, we have that $\Delta \text{ lc}(\mathcal{R}) \Theta$. The same reasoning also holds if we assume that $|\Theta| \leq 1$, meaning that $\text{lc}(\mathcal{R})$ is also right-linear and thus linear. $\square$

Definition C.4. Let $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$. The context closure $\mathbf{B}(\mathcal{R})$ of $\mathcal{R}$ is the least relation satisfying the following rule

$$\frac{\Delta \mathcal{R} \Theta}{B[\Delta] \mathbf{B}(\mathcal{R}) B[\Theta]}$$

where $\Sigma \vdash \Delta, \Theta$ and $B[\cdot]$ has a hole of type Σ .

Definition C.5. A relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$ is a *saturated bisimulation up-to $\text{lc} \circ \mathbf{B}$* if $\Delta \mathcal{R} \Theta$ implies $(\Sigma, \Sigma') \vdash \Delta, \Theta$ for some Σ, Σ' , $|\Delta| = |\Theta|$ and for any context $B[\cdot]$ it holds

- whenever $B[\Delta] \xrightarrow{\tau}_s \Delta'$, there exists Θ' such that $B[\Theta] \xrightarrow{\tau}_s \Theta'$ and $\Delta' \text{ lc}(\mathbf{B}(\mathcal{R})) \Theta'$;
- whenever $B[\Theta] \xrightarrow{\tau}_s \Theta'$, there exists Δ' such that $B[\Delta] \xrightarrow{\tau}_s \Delta'$ and $\Delta' \text{ lc}(\mathbf{B}(\mathcal{R})) \Theta'$.

We now prove that bisimulation up-to $\text{lc} \circ \mathbf{B}$ is *valid*, i.e. that we can use it to prove bisimilarity. We define the function b over relations, of which saturated bisimilarity is the greatest fixpoint.

$$b(\mathcal{R}) := \left\{ (\Delta, \Theta) \left| \begin{array}{l} |\Delta| = |\Theta| \\ B[\Delta] \xrightarrow{\tau}_s \Delta' \Rightarrow \exists \Theta'. B[\Theta] \xrightarrow{\tau}_s \Theta' \wedge \Delta' \mathcal{R} \Theta' \\ B[\Theta] \xrightarrow{\tau}_s \Theta' \Rightarrow \exists \Delta'. B[\Delta] \xrightarrow{\tau}_s \Delta' \wedge \Delta' \mathcal{R} \Theta' \end{array} \right. \right\}$$

Observe that b , lc and $\mathbf{B}$ are monotone functions on the lattice of relations.

LEMMA C.6 (**lc** IS b -COMPATIBLE). Let $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$. $\text{lc}(b(\mathcal{R})) \subseteq b(\text{lc}(\mathcal{R}))$.

PROOF. Assume $(\Delta, \Theta) \in \text{lc}(b(\mathcal{R}))$. By definition of lc and b , $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$, $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$ with $\Delta_i b(\mathcal{R}) \Theta_i$ and $|\Delta_i| = |\Theta_i|$ for any $i \in I$ and $|\Delta| \leq 1$. Then $|\Delta| = |\Theta|$. Take any context $B[\cdot]$, $B[\Delta] = \sum_{i \in I} p_i \cdot B[\Delta_i] \xrightarrow{\tau}_s \Delta'$. By decomposability of $\xrightarrow{\tau}_s$, for any $i \in I$, $B[\Delta_i] \xrightarrow{\tau}_s \Delta'_i$, and $\sum_{i \in I} p_i \cdot \Delta'_i = \Delta'$ with $|\Delta'| \leq 1$. Since $\Delta_i \mathcal{R} \Theta_i$, for all $i \in I$ there exists Θ'_i such that $B[\Theta_i] \xrightarrow{\tau}_s \Theta'_i$. By linearity of $\xrightarrow{\tau}_s$ and by definition of lc , $B[\Theta] \xrightarrow{\tau}_s \sum_{i \in I} p_i \cdot \Theta'_i = \Theta'$ where $|\Theta'|$ must be less than one and $\Delta' \text{ lc}(\mathcal{R}) \Theta'$. The argument is symmetric for the last condition. $\square$

LEMMA C.7 (**B** IS b -COMPATIBLE). Let $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$. $\mathbf{B}(b(\mathcal{R})) \subseteq b(\mathbf{B}(\mathcal{R}))$.

PROOF. Assume $(B[\Delta], B[\Theta]) \in \mathbf{B}(b(\mathcal{R}))$. If $B[\cdot] = [\cdot]$ then the proof is trivial ($(\Delta, \Theta) \in b(\mathcal{R}) \subset b(\mathbf{B}(\mathcal{R}))$ and $b(\mathcal{R}) \subseteq b(\mathbf{B}(\mathcal{R}))$ as b is monotone and $\mathcal{R} \subseteq \mathbf{B}(\mathcal{R})$). Let $B[\cdot] = [\cdot] \parallel P$. Since the contexts is applied linearly, for any Δ , $|B[\Delta]| = |\Delta|$, therefore $|B[\Delta]| = |\Delta| = |\Theta| = |B[\Theta]|$. For the other requirements of b , let $B'[\cdot]$ be any context. If $B'[\cdot] = [\cdot]$ then the proof is again trivial. Thus, let $B'[\cdot] = [\cdot] \parallel R$. We have that $B'[B[\Delta]] = \Delta \parallel P \parallel R$ and that $B'[B[\Theta]] = \Theta \parallel P \parallel R$. By assumption, we have that $\Delta b(\mathcal{R}) \Theta$. Therefore with the context $B''[\cdot] = [\cdot] \parallel P \parallel R$, if $B''[\Delta] \succ^{\tau}_s \Delta'$ then there exists a Θ' such that $B''[\Theta] \succ^{\tau}_s \Theta'$ and $\Delta' \mathcal{R} \Theta'$. However, by definition of $\mathbf{B}$, $\Delta' \mathcal{R} \Theta'$ implies that $\Delta' \mathbf{B}(\mathcal{R}) \Theta'$. $\square$

THEOREM C.8. *Bisimulation up-to $\mathbf{lc} \circ \mathbf{B}$ is a valid proof technique for $\simeq$, meaning that if $\Delta \mathcal{R} \Theta$ for a saturated bisimulation up-to $\mathbf{lc} \circ \mathbf{B}$, then $\Delta \simeq \Theta$.*

PROOF. From [Pous and Sangiorgi 2011], we know that if two functions f_1 and f_2 are b -compatible, then also $f_1 \circ f_2$ is b -compatible. Furthermore, bisimulations up-to f are a sound proof technique whenever f is b -compatible. $\square$

THEOREM 5.11. *The bisimilarity $\simeq$ is linear.*

PROOF. By requirement of saturated bisimulations, the bisimilarity $\simeq$ must associate only distributions with equal mass, therefore by Proposition C.3 $\mathbf{lc}(\simeq)$ is linear. However, as a corollary of Theorem C.8 $\mathbf{lc}(\simeq) = \simeq$ therefore $\simeq$ is linear. $\square$

THEOREM 5.10. *If $\sum_i p_i \cdot \rho_i = \sum_j q_j \cdot \rho_j$ then $\sum_i p_i \cdot \langle \rho_i, P \rangle \simeq \sum_j q_j \cdot \langle \rho_j, P \rangle$.*

PROOF. We will prove that $1 \cdot \langle p \cdot \rho + (1-p) \cdot \sigma, P \rangle \simeq p \cdot \langle \rho, P \rangle \oplus 1 - p \cdot \langle \sigma, P \rangle$ for any operators ρ, σ , process P and $p \in [0, 1]$. By linearity of $\simeq$ we have that

$$\sum_i p_i \cdot \langle \rho_i, P \rangle \simeq 1 \cdot \left\langle \sum_i p_i \rho_i, P \right\rangle \simeq 1 \cdot \left\langle \sum_j q_j \sigma_j, P \right\rangle \simeq \sum_i q_i \cdot \langle \sigma_i, P \rangle$$

We define the relation $\mathcal{R}$ and prove that is a bisimulation up-to $\mathbf{lc}$.

$$\mathcal{R} = \{(1 \cdot \langle p \cdot \rho + (1-p) \cdot \sigma, P \rangle, p \cdot \langle \rho, P \rangle \oplus 1 - p \cdot \langle \sigma, P \rangle) \mid \rho, \sigma, p, P\}$$

Take $(\Delta, \Theta) \in \mathcal{R}$ and a compatible context $B[\cdot]$. Let $\Delta = 1 \cdot \langle \nu, P \rangle$, $\Theta = p \cdot \langle \rho, P \rangle \oplus 1 - p \cdot \langle \sigma, P \rangle$, with $\nu = p\rho + (1-p)\sigma$. Note that $1 \cdot \langle \nu, B[P] \rangle \simeq^{\tau}_s \Xi$ iff $\langle \nu, B[P] \rangle \text{ bot } (\xrightarrow{\tau}_s) \Xi$ (and similarly for ρ and σ). Thus, by Lemma B.5, there exists a family $\text{next}(B[P], s)$ of trace non-increasing superoperators $\mathcal{E}_i$ and processes P_i such that $B[\Delta] \succ^{\tau}_s \Delta'$ if and only if

$$\Delta' = \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\nu)) \neq 0} \text{tr}(\mathcal{E}_i(\nu)) \cdot \left\langle \frac{\mathcal{E}_i(\nu)}{\text{tr}(\mathcal{E}_i(\nu))}, P_i \right\rangle = \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\nu)) \neq 0} \text{tr}(\mathcal{E}_i(\rho) \cdot p + \mathcal{E}_i(\sigma)) \cdot \left\langle \frac{\mathcal{E}_i(\rho) \cdot p + \mathcal{E}_i(\sigma)}{\text{tr}(\mathcal{E}_i(\rho) \cdot p + \mathcal{E}_i(\sigma))}, P_i \right\rangle$$

Where $_p \oplus _ = p \oplus (1-p)_$ and $_p + _ = p + (1-p)_$.

Moreover, by Lemma B.5, left decomposability and left linearity of $\succ^{\tau}_s$, $B[\Theta] \succ^{\tau}_s \Theta'$ if and only if

$$\Theta' = \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\rho)) \neq 0} \text{tr}(\mathcal{E}_i(\rho)) \cdot \left\langle \frac{\mathcal{E}_i(\rho)}{\text{tr}(\mathcal{E}_i(\rho))}, P_i \right\rangle \oplus \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\sigma)) \neq 0} \text{tr}(\mathcal{E}_i(\sigma)) \cdot \left\langle \frac{\mathcal{E}_i(\sigma)}{\text{tr}(\mathcal{E}_i(\sigma))}, P_i \right\rangle$$

Recall that both superoperators and the trace are linear operators. Also by linearity, $\text{tr}(\mathcal{E}_i(\rho_p + \sigma)) \neq 0$ iff $\text{tr}(\mathcal{E}_i(\rho))_p + \text{tr}(\mathcal{E}_i(\sigma)) \neq 0$, and Θ' can be rewritten in the following form

$$\Theta' = \sum_{i \in I \text{ s.t. } \text{tr}(\mathcal{E}_i(\nu)) \neq 0} \text{tr}(\mathcal{E}_i(\rho))_p + \text{tr}(\mathcal{E}_i(\sigma)) \cdot \left(\left\langle \frac{\mathcal{E}_i(\rho)}{\text{tr}(\mathcal{E}_i(\rho))}, P_i \right\rangle \frac{p \text{tr}(\mathcal{E}_i(\rho))}{\text{tr}(\mathcal{E}_i(\rho))_p + \text{tr}(\mathcal{E}_i(\sigma))} \oplus \left\langle \frac{\mathcal{E}_i(\sigma)}{\text{tr}(\mathcal{E}_i(\sigma))}, P_i \right\rangle \right)$$

By performing some simple calculations, one can prove that Δ' and Θ' have the same weights, and thus $\Delta' \text{lc}(\mathcal{R}) \Theta'$. $\square$

D Proofs about Probabilistic Labelled Bisimulations

As an intermediate step for proving the full abstraction of Theorem 6.10, we introduce a probabilistic version of the labelled bisimilarity, and prove its complete adherence with respect to the saturated equivalence.

We need some auxiliary definitions. First, given a distribution Δ of lqCCS processes, we let $\text{env}(\Delta)$ be its visible quantum state $\sum_{(\rho, P) \in [\Delta]} \Delta((\rho, P)) \cdot \text{tr}_{\Sigma'}(\rho)$, where $\Sigma, \Sigma' \vdash \Delta$. Notice that $\text{env}(\Delta)$ is a partial density operator in $\mathcal{D}^\leq(\mathcal{H}_{\Sigma \setminus \Sigma'})$, with $\text{tr}(\text{env}(\Delta)) = |\Delta|$.

We can now define our labelled bisimilarity.

Definition D.1 (Labelled Bisimilarity). A relation $\mathcal{R} \subseteq \mathcal{D}^\leq(\text{Conf}) \times \mathcal{D}^\leq(\text{Conf})$ is a *labelled bisimulation* if $\Delta \mathcal{R} \Theta$ implies $(\Sigma, \Sigma') \vdash \Delta$ and $(\Sigma, \Sigma') \vdash \Theta$ for some Σ, Σ' , and it holds that

- $\text{env}(\Delta) = \text{env}(\Theta)$;
- $\mathcal{E}(\Delta) \mathcal{R} \mathcal{E}(\Theta)$ for any superoperator $\mathcal{E} \in \mathcal{SO}^\leq(\mathcal{H}_{\Sigma \setminus \Sigma'})$;
- whenever $\Delta \xrightarrow{\mu}_s \Delta'$, there exists Θ' such that $\Theta \xrightarrow{\mu}_s \Theta'$ and $\Delta' \mathcal{R} \Theta'$;
- whenever $\Theta \xrightarrow{\mu}_s \Theta'$, there exists Δ' such that $\Delta \xrightarrow{\mu}_s \Delta'$ and $\Delta' \mathcal{R} \Theta'$.

Let *labelled bisimilarity*, denoted $\sim_p$, be the largest labelled bisimulation.

We will now introduce some lemmas, useful to prove that $\simeq$ and $\sim_p$ coincide.

LEMMA D.2. *For any Δ and t , and for any tag t' fresh in Δ ,*

$$\Delta \xrightarrow{\tau}_s \Delta' \quad \text{if and only if} \quad \Delta[t'/t] \xrightarrow{\tau}_{s[t'/t]} \Delta'[t'/t]$$

PROOF. By induction on the operational semantics. $\square$

LEMMA D.3. *For any Δ, Θ and t , and for any tag t' fresh in Δ and Θ ,*

$$\Delta \simeq \Theta \quad \text{if and only if} \quad \Delta[t'/t] \simeq \Theta[t'/t]$$

PROOF. Let $\mathcal{R}$ be the smallest relation such that $\simeq \subseteq \mathcal{R}$ and $\mathcal{R} \subseteq \{(\Delta[t'/t], \Theta[t'/t]) \mid \Delta \mathcal{R} \Theta \text{ and } t' \text{ is fresh in } \Delta, \Theta\}$. We will show that $\mathcal{R}$ is a bisimulation.

In the following, we write $[t'_i/t_i]_{i \in I}$ for the substitution $[t'_{x_0}/t_{x_0}][t'_{x_1}/t_{x_1}] \dots [t'_{x_n}/t_{x_n}]$, with $I = \{x_0, x_1, \dots, x_n\}$.

Take $\Delta[t'_i/t_i]_{i \in I}$ and $\Theta[t'_i/t_i]_{i \in I}$ in $\mathcal{R}$, with $\Delta \simeq \Theta$, and take a generic context $B[\cdot] = [\cdot] \parallel R$. Assume that

$$\Delta[t'_i/t_i]_{i \in I} \parallel R \xrightarrow{\tau}_s \Delta'.$$

Take then a collection of distinct fresh tags t''_i . By Lemma D.2,

$$\begin{aligned} (\Delta[t'_i/t_i]_{i \in I} \parallel R)[t''_i/t_i, t'_i/t'_i]_{i \in I} &= \Delta[t'_i/t_i, t''_i/t'_i]_{i \in I} \parallel R[t'_i/t_i, t'_i/t'_i]_{i \in I} = \\ &= \Delta \parallel R[t'_i/t_i, t'_i/t'_i]_{i \in I} \xrightarrow{\tau}_{s[t'_i/t_i, t'_i/t'_i]_{i \in I}} \Delta'[t'_i/t_i, t'_i/t'_i]_{i \in I}. \end{aligned}$$

Since $\Delta \simeq \Theta$, then it must be that $\Theta \parallel R[t_i''/t_i, t_i/t_i']_{i \in I} \xrightarrow{\tau}_s \Theta'$, with $\Delta'[t_i''/t_i, t_i/t_i']_{i \in I} \simeq \Theta'$. By Lemma D.2, $(\Theta \parallel R[t_i''/t_i, t_i/t_i']_{i \in I})[t_i'/t_i, t_i/t_i']_{i \in I} = \Theta[t_i'/t_i]_{i \in I} \parallel R \xrightarrow{\tau}_s \Theta'[t_i'/t_i, t_i/t_i']_{i \in I}$. We conclude by noting that $\Delta' \mathcal{R} \Theta'[t_i'/t_i, t_i/t_i']_{i \in I}$ because $\Delta' = \Delta'[t_i''/t_i, t_i/t_i']_{i \in I}[t_i'/t_i, t_i/t_i']_{i \in I}$. $\square$

LEMMA D.4. For any Δ, Δ' , and $B[\cdot]$, and for any s with only tags that are fresh in $B[\cdot]$,

$$B[\Delta] \xrightarrow{\tau}_s \Delta' \quad \text{if and only if} \quad \Delta \xrightarrow{\tau}_s \Delta'' \text{ and } \Delta' = B[\Delta'']$$

PROOF. By the rules for the parallel composition. $\square$

LEMMA D.5. For any $\Sigma, \Sigma' \vdash \Delta, \Theta$, for any q in $\Sigma \setminus \Sigma'$, we have that $\Delta \simeq \Theta$ if and only if $\Delta \parallel t:c!q \simeq \Theta \parallel t:c!q$ for some t fresh both in Δ and Θ .

PROOF. $\Delta \simeq \Theta$ implies $\Delta \parallel t:c!q \simeq \Theta \parallel t:c!q$ because saturated bisimilarity is a congruence by definition. For the other side, it suffices showing that $\mathcal{R} = \{(\Delta, \Theta) \mid \Delta \parallel t:c!q \simeq \Theta \parallel t:c!q\}$ is a bisimulation.

Take $(\Delta, \Theta) \in \mathcal{R}$ and $\Sigma' \vdash B[\cdot]_{\Sigma'} = [\cdot] \parallel R$. We consider two cases depending on q being in Σ'' or not.

If $q \in \Sigma''$, then let $\Sigma'' \vdash B'[\cdot]_{\Sigma' \cup \{q\}} = [\cdot] \parallel t':c?x.R[x/q][t''/t]$, with t' and t'' fresh tags in Δ, Θ and R . We have then that $B'[\Delta \parallel t:c!q] \xrightarrow{\tau}_{(t,t')} \Delta \parallel R[t''/t]$, and $B'[\Theta \parallel t:c!q] \xrightarrow{\tau}_{(t,t')} \Theta \parallel R[t''/t]$. Since $\Delta \parallel t:c!q \simeq \Theta \parallel t:c!q$ by assumption, we know that $\Delta \parallel R[t''/t] \simeq \Theta \parallel R[t''/t]$, and the property follows by Lemma D.3 since t'' is chosen free in Δ, Θ and R .

If $q \notin \Sigma''$, then let $\Sigma'' \vdash B'[\cdot]_{\Sigma'} = [\cdot] \parallel R[t'/t]$, with $t' \neq t$ fresh in Δ, Θ and R . Then, assume $B[\Delta] \xrightarrow{\tau}_s \Delta'$. Notice that $B[\Delta][t'/t] = B'[\Delta]$ since t is fresh in Δ . Hence, $B'[\Delta] \xrightarrow{\tau}_{s'} \Delta'[t'/t]$, with $s' = s[t'/t]$, by Lemma D.2. Clearly, t does not appear in s , hence, by Lemma D.4, $B'[\Delta \parallel t:c!q] \xrightarrow{\tau}_{s'} \Delta'[t'/t] \parallel t:c!q$ (where we exploit the associativity of the parallel operator). Since $\Delta \parallel t:c!q \simeq \Theta \parallel t:c!q$, we know that $B'[\Theta \parallel t:c!q] \xrightarrow{\tau}_{s'} \Theta'$, with $\Delta'[t'/t] \parallel t:c!q \simeq \Theta'$. Moreover, by Lemma D.4, Θ' is of the form $\Theta'' \parallel t:c!q$, and $B'[\Theta] \xrightarrow{\tau}_{s'} \Theta''$. By Lemma D.2, we then know that $\Theta'' = \Theta'''[t'/t]$ for some Θ such that $B[\Theta] \xrightarrow{\tau}_s \Theta'''$. We know that $\Delta'[t'/t] \parallel t:c!q \simeq \Theta'''[t'/t] \parallel t:c!q$, hence, by Lemma D.2,

$$(\Delta'[t'/t] \parallel t:c!q)[t'/t', t'/t] = \Delta' \parallel t':c!q \simeq \Theta''' \parallel t:c!q = (\Theta'''[t'/t] \parallel t:c!q)[t'/t', t'/t].$$

Therefore, $(\Delta', \Theta''') \in \mathcal{R}$. $\square$

In the following we will write $\tilde{t}:c!\tilde{q}$ for the process

$$t_0:c!q_0 \parallel t_1:c!q_1 \parallel \dots \parallel t_n:c!q_n,$$

with c any channel, and $\tilde{t} = t_0, t_1, \dots, t_n$ and $\tilde{q} = q_0, q_1, \dots, q_n$ any sequences of (distinct) tags and qubit names.

LEMMA D.6. Let $\Delta \simeq \Theta$. Then

- $env(\Delta) = env(\Theta)$;
- $\mathcal{E}(\Delta) \simeq \mathcal{E}(\Theta)$ for any trace non-increasing superoperator over the environment.

PROOF. For the first point, suppose that $env(\Delta) \neq env(\Theta)$, we will show that $\Delta \neq \Theta$. Since $env(\Delta) \neq env(\Theta)$, then there exists a positive linear operator E such that $\text{tr}(E \cdot env(\Delta)) \neq \text{tr}(E \cdot env(\Theta))$ [Heinosaari and Ziman 2011]. We can construct the measurement $\mathcal{M}_E$ with measurement operators $\{\sqrt{E}, \sqrt{\mathbb{I} - E}\}$ and the context $B[\cdot] = [\cdot] \parallel t_0:\mathcal{M}_E(\tilde{q} \triangleright x).R$, where $R = \text{if } x = 0 \text{ then } t_1:\tau.\mathbf{0}_{\tilde{q}} \text{ else } \mathbf{0}_{\tilde{q}}$, t_0, t_1 are fresh tags and $\tilde{q}$ is the tuple of

all the qubits outside of Δ . For $\Delta = \sum_i p_i \cdot \langle \rho_i, P_i \rangle$ and $\Theta = \sum_j p_j \cdot \langle \rho_j, P_j \rangle$ we have

$$\begin{aligned} B[\Delta] &\xrightarrow{\tau}_{t_0} \sum_i p_i \cdot \left(q_i \cdot \langle \rho_i^E, P_i \parallel R[0/x] \rangle \oplus (1 - q_i) \cdot \langle \rho_i^{\mathcal{E}}, P_i \parallel R[1/x] \rangle \right) \\ &\xrightarrow{\tau}_{t_1} \sum_i p_i q_i \cdot \langle \rho_i^E, P_i \parallel \mathbf{0}_{\tilde{q}} \rangle = \Delta' \end{aligned}$$

and

$$\begin{aligned} B[\Theta] &\xrightarrow{\tau}_{t_0} \sum_j p_j \cdot \left(q_j \cdot \langle \rho_j^E, P_j \parallel R[0/x] \rangle \oplus (1 - q_j) \cdot \langle \rho_j^{\mathcal{E}}, P_j \parallel R[0/x] \rangle \right) \\ &\xrightarrow{\tau}_{t_1} \sum_j p_j q_j \cdot \langle \rho_j^E, P_j \parallel \mathbf{0}_{\tilde{q}} \rangle = \Theta' \end{aligned}$$

where ρ_n^E (respectively $\rho_n^{\mathcal{E}}$) is the state resulting from the successful (failed) measurement of E on ρ_n , q_n is the probability $\text{tr}(E \otimes \mathbb{I} \cdot \rho_n)$. We have that $\text{tr}(E \cdot \text{env}(\Delta)) = \text{tr}(E \otimes \mathbb{I} \cdot \sum_i p_i \rho_i) = |\Delta'|$, and thus $|\Delta'| \neq |\Theta'|$ and Δ, Θ are not bisimilar.

For the second point, we consider separately the case of a trace-preserving superoperator $\mathcal{E}$. In this case, we take the distinct fresh tags t and $\tilde{t}$, and we build a context $B[\cdot] = [\cdot] \parallel t: \mathcal{E}(\tilde{q}).\tilde{t}: c!\tilde{q}$. After a $\xrightarrow{\tau}_t$ transition, Δ goes in $\mathcal{E}(\Delta) \parallel \tilde{t}: c!\tilde{q}$ and Θ goes in $\mathcal{E}(\Theta) \parallel \tilde{t}: c!\tilde{q}$, from which we know $\mathcal{E}(\Delta) \simeq \mathcal{E}(\Theta)$ thank to Lemma D.5.

Finally, Suppose $\mathcal{E} = \{K_0, \dots, K_{n-1}\}$ is a trace non-increasing superoperator with n Kraus operators, we define n superoperators $\mathcal{M}_i = \{K_i\}$ for $i = 0, \dots, n-1$. We have that, for any ρ , $\mathcal{E}(\rho) = \sum_{i=0}^{n-1} \mathcal{M}_i(\rho)$ and $\text{tr}(\mathcal{E}(\rho)) = \sum_{i=0}^{n-1} \text{tr}(\mathcal{M}_i(\rho))$. Since $\mathcal{E}$ is trace non-increasing, we know by definition that $\mathbb{I} - \sum_{i=0}^{n-1} K_i^\dagger K_i$ is a positive matrix, and we call this difference M . We build a measurement $\mathcal{M}$ with measurement operators $\{K_0, \dots, K_{n-1}, \sqrt{M}\}$. This is an $n+1$ -outcome measurement, one for each Kraus operator of $\mathcal{E}$ and an additional one signifying that $\mathcal{E}$ does not happen. Take then the context $B[\cdot] = [\cdot] \parallel t: \mathcal{M}(\tilde{q} \triangleright x).R$ where $R = \text{if } x \neq n \text{ then } t': \tau.\tilde{t}: c!\tilde{q} \text{ else } \tilde{t}: c!\tilde{q}$ and $t, t', \tilde{t}$ are distinct fresh tags. Suppose that $\Delta = \sum_j p_j \cdot \langle \rho_j, P_j \rangle$, then a possible sequence of transition of $B[\Delta]$ is

$$\begin{aligned} B[\Delta] &\xrightarrow{\tau}_{t_0} \sum_j p_j \cdot \left(\sum_{i=0}^n \text{tr}(\mathcal{M}_i(\rho_j)) \cdot \left\langle \frac{\mathcal{M}_i(\rho_j)}{\text{tr}(\mathcal{M}_i(\rho_j))}, P_j \parallel R[i/x] \right\rangle \right) \\ &\xrightarrow{\tau}_{t'} \sum_j p_j \cdot \left[\text{tr}(\mathcal{E}(\rho_j)) \cdot \left(\sum_{i=0}^{n-1} \frac{\text{tr}(\mathcal{M}_i(\rho_j))}{\text{tr}(\mathcal{E}(\rho_j))} \cdot \left\langle \frac{\mathcal{M}_i(\rho_j)}{\text{tr}(\mathcal{M}_i(\rho_j))}, P_j \parallel \tilde{t}: c!\tilde{q} \right\rangle \right) \right] = \Delta' \end{aligned}$$

Applying Theorem 5.10 to such Δ' , we get by linearity

$$\begin{aligned} \Delta' &\sim \sum_j p_j \cdot \left[\text{tr}(\mathcal{E}(\rho_j)) \cdot \left\langle \frac{\sum_{i=0}^{n-1} \mathcal{M}_i(\rho_j)}{\text{tr}(\mathcal{E}(\rho_j))}, P_j \parallel \tilde{t}: c!\tilde{q} \right\rangle \right] \\ &= \sum_j p_j \text{tr}(\mathcal{E}(\rho_j)) \cdot \left\langle \frac{\mathcal{E}(\rho_j)}{\text{tr}(\mathcal{E}(\rho_j))}, P_j \parallel \tilde{t}: c!\tilde{q} \right\rangle \\ &= \mathcal{E}(\Delta) \parallel \tilde{t}: c!\tilde{q}. \end{aligned}$$

This sequence of transition must be replicated also by $B[\Theta]$, and so we know that

$$\begin{aligned} B[\Delta] &\xrightarrow{\tau}_t \xrightarrow{\tau}_{t'} \Delta' \simeq \mathcal{E}(\Delta) \parallel \tilde{t}:c!\tilde{q} \\ &\Downarrow \\ B[\Theta] &\xrightarrow{\tau}_t \xrightarrow{\tau}_{t'} \Theta' \simeq \mathcal{E}(\Theta) \parallel \tilde{t}:c!\tilde{q} \end{aligned}$$

We thus know that $\mathcal{E}(\Delta) \simeq \mathcal{E}(\Theta)$ thanks to Lemma D.5. Notice how all the contexts we used in this proof use fresh tags, and thus can be legally applied to Δ and Θ due to Lemma 5.4. $\square$

THEOREM D.7. $\simeq \subseteq \sim_p$.

PROOF. We have to prove that $\simeq$ is a labelled bisimulation. The first two conditions are already proven in Lemma D.6, we must check the last two. Suppose $\Delta \simeq \Theta$ and $\Delta \xrightarrow{\mu}_s \Delta'$. We proceed by cases on μ , and build contexts capable of bringing Δ to Δ' . All the contexts we will build use fresh tags, and thus can be legally applied to Δ and Θ due to Lemma 5.4.

If $\mu = \tau$, then $B[\Delta] \xrightarrow{\tau}_s \Delta'$ for the empty context $B[\cdot] = \cdot$, thus there exists a Θ' such that $B[\Theta] = \Theta \xrightarrow{\tau}_s \Theta'$ and $\Delta' \simeq \Theta'$.

If $\mu = c?v$, then $\Delta \parallel t:c!v \xrightarrow{\tau}_{(s,t)} \Delta' \parallel \mathbf{0}$. By $\Delta \simeq \Theta$, there exists Θ' such that $\Theta \parallel t:c!v \xrightarrow{\tau}_{(s,t)} \Theta' \parallel \mathbf{0}$. From the semantics of synchronization we also know that $\Theta \xrightarrow{c?v}_s \Theta'$ and $\Delta' \parallel \mathbf{0} \simeq \Theta' \parallel \mathbf{0}$. It is possible to show that $\Delta \parallel \mathbf{0} \simeq \Delta'$ for any Δ , and thus we get $\Delta' \simeq \Theta'$.

If $\mu = c!v$, when v is a quantum name, we build the context $B[\cdot] = [\cdot] \parallel t:c?x.R$ with $R = \mathbf{if} \ x = v \ \mathbf{then} \ t':\tau.t'':c!x \ \mathbf{else} \ t'':c!x$. Then we have that $B[\Delta] \xrightarrow{\tau}_{(s,t)} \Delta' \parallel R[v/x]$, and thus $B[\Theta] \xrightarrow{\tau}_{(s,t)} \Theta' \parallel R[u/x]$ and $\Theta \xrightarrow{c!u}_s \Theta'$ for some quantum name u possibly different from v . Thanks to the bisimilarity between $\Delta' \parallel R[v/x]$ and $\Theta' \parallel R[u/x]$, we can prove $u = v$: $\Delta' \parallel R[v/x] \xrightarrow{\tau}_{t'} \Delta' \parallel t'':c!v$, and also $\Theta' \parallel R[u/x]$ must have the same action available, so it must be $u = v$. To sum up, we know that $\Theta \xrightarrow{c?v}_s \Theta'$ and that $\Delta' \parallel t'':c!v \simeq \Theta' \parallel t'':c!v$. This implies $\Delta' \simeq \Theta'$ thanks to Lemma D.5.

The case for $\mu = c!v$ for a classical value v is the same, using the context $B[\cdot] = \cdot \parallel t:c?x.\mathbf{if} \ x = v \ \mathbf{then} \ t':\tau.\mathbf{0} \ \mathbf{else} \ \mathbf{0}$. $\square$

THEOREM D.8. $\sim_p \subseteq \simeq$.

PROOF. It is sufficient to show that $\sim_p$ is a saturated bisimulation up-to $\mathbf{lc} \circ \mathbf{B}$. Assume $\Delta \sim_p \Theta$. To see that $|\Delta| = |\Theta|$ it is sufficient to notice that $\text{env}(\Delta) = \text{env}(\Theta)$, by definition of $\sim_p$, and that $|\Delta| = \text{tr}(\text{env}(\Delta))$ for any Δ .

We now show that for all $B[\cdot], \Delta, \Theta, \Delta'$, if $\Delta \sim_p \Theta$ and $B[\Delta] \xrightarrow{\tau}_s \Delta'$ then Θ' exists such that $B[\Theta] \xrightarrow{\tau}_s \Theta'$ and $\Delta' \mathbf{lc}(\mathbf{B}(\sim_p)) \Theta'$. If $B[\cdot] = \cdot$, then from $\Delta \sim_p \Theta$ we have $\Delta' \sim_p \Theta'$ for some Θ' such that $\Delta' \sim_p \Theta'$, and $\sim_p \subseteq \mathbf{lc}(\mathbf{B}(\sim_p))$.

When $\Delta = \Theta = \epsilon$, we have that $B[\Delta] = B[\Theta] = \epsilon \xrightarrow{\mu}_s \epsilon$ for any B, μ and s , and it is possible to prove that $\epsilon \simeq \epsilon$.

Otherwise, we know that $\Delta \neq \epsilon \neq \Theta$, and that $B[\cdot] = \cdot \parallel R$ for some R . If $\Delta \parallel R \xrightarrow{\tau}_s \epsilon$, then we know from Lemma B.10 that:

- (1) $\Delta \xrightarrow{\tau}_s \epsilon$, which implies that $\Theta \xrightarrow{\tau}_s \epsilon$, since $\Delta \sim_p \Theta$;
- (2) $\text{next}(R, s, \tau) = \emptyset$;

(3) For all c and v , if $s = (t_1, t_2)$ we have

$$\text{next}(R, t_2, c!v) \neq \emptyset \implies \Delta \xrightarrow{c?v}_{t_1} \epsilon \implies \Theta \xrightarrow{c?v}_{t_1} \epsilon$$

and

$$\text{next}(R, t_2, c?v) \neq \emptyset \implies \Delta \xrightarrow{c!v}_{t_1} \epsilon \implies \Theta \xrightarrow{c!v}_{t_1} \epsilon.$$

In other words, we know all the three points necessary to apply Lemma B.10 on Θ in the reverse direction, obtaining that $\Theta \parallel R \xrightarrow{\tau}_s \epsilon$.

Suppose instead that $\Delta \parallel R \xrightarrow{\tau}_s \Delta' \neq \epsilon$, then we know from Lemma B.9 that one of the following is true:

- (1) $\text{Tag}(s) \subseteq \text{Tag}(\Delta)$ and there exists Δ'' such that $\Delta' = \Delta'' \parallel R$ and $\Delta \xrightarrow{\tau}_s \Delta''$. The latter implies $\Theta \xrightarrow{\tau}_s \Theta'$ for some $\Theta' \sim_p \Delta''$, since $\Delta \sim_p \Theta$. But then, it must be $\text{Tag}(s) \subseteq \text{Tag}(\Theta)$, and from Lemma B.9 we know $\Theta \parallel R \xrightarrow{\tau}_s \Theta' \parallel R$, and $\Delta'' \parallel R \mathbf{B}(\sim_p) \Theta' \parallel R$.
- (2) $\text{Tag}(s) \subseteq \text{Tag}(R)$ and $\Delta' = \sum_{i \in I} \mathcal{E}_i(\Delta \parallel R_i)$ with $\text{next}(R, s, \mu) = \{\mathcal{E}_i, R_i\}_{i \in I}$. But then we know from Lemma B.9 that $\Theta \parallel R \xrightarrow{\tau}_s \sum_{i \in I} \mathcal{E}_i(\Theta \parallel R_i)$. Thanks to superoperator closure, we know for all the i that $\mathcal{E}_i(\Delta) \sim_p \mathcal{E}_i(\Theta)$, and thus $\mathcal{E}_i(\Delta \parallel R_i \mathbf{B}(\sim_p) \Theta \parallel R_i)$ (notice how $\mathcal{E}_i(\Delta) \parallel R = \mathcal{E}_i(\Delta \parallel R)$). This proves that $\sum_{i \in I} \mathcal{E}_i(\Delta \parallel R_i) \mathbf{lc}(\mathbf{B}(\sim_p)) \sum_{i \in I} \mathcal{E}_i(\Theta \parallel R_i)$.
- (3) $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$, and $\Delta' = \Delta'' \parallel R'$, $\exists c, v, \Delta \xrightarrow{c?v}_{t_1} \Delta''$ with $\text{next}(R, t_2, c!v) = \{\mathbb{I}, R'\}$. This implies $\Theta \xrightarrow{c?v}_{t_1} \Theta'$ for some $\Theta' \sim_p \Delta''$, since $\Delta \sim_p \Theta$, and thus $\Theta \parallel R \xrightarrow{\tau}_s \Theta' \parallel R'$ thanks to Lemma B.9, where we have $\Delta'' \parallel R \mathbf{B}(\sim_p) \Theta' \parallel R$.
- (4) $s = (t_1, t_2)$, $t_1 \in \text{Tag}(\Delta)$, $t_2 \in \text{Tag}(R)$, and $\exists c, V, \Delta' = \sum_{v \in V} \Delta_v \parallel R_v$, and $\forall v \in V, \Delta \xrightarrow{c!v}_{t_1} \Delta_v$ with $\text{next}(R, t_2, c?v) = \{\mathbb{I}, R_v\}$. This implies $\Theta \xrightarrow{c!v}_{t_1} \Theta_v$ for some $\Theta_v \sim_p \Delta_v$ for any $v \in V$, and thus $\Theta \parallel R \xrightarrow{\tau}_s \sum_{v \in V} \Theta_v \parallel R_v = \Theta'$ thanks to Lemma B.9, where we have $\Delta' \mathbf{B}(\sim_p) \Theta'$.

□

THEOREM D.9. For any Δ and Θ , $\Delta \sim_p \Theta$ if and only if $\Delta \simeq \Theta$.

PROOF. By Theorem D.7 and D.8. □

E Proofs about Quantum Labelled Bisimulations

Definition E.1. We define the following:

- The function $\alpha : \mathcal{D}^{\leq}(\text{Conf}) \rightarrow \mathcal{Q}(\text{Proc})$ is given by

$$\alpha \left(\sum_{i \in I} \sum_{j \in J_i} p_j \cdot \langle \rho_j, P_i \rangle \right) = \sum_{i \in I} \left(\sum_{j \in J_i} p_j \rho_j \right) \cdot P_i$$

where processes are indexed by $i \in I$, and the states and probabilities associated to a process P_i are indexed by $j \in J_i$.

- The function $\gamma : \mathcal{Q}(\text{Proc}) \rightarrow \mathcal{D}^{\leq}(\text{Conf})$ is given by

$$\gamma \left(\sum_{i \in I} \rho_i \cdot P_i \right) = \sum_{i \in I} \text{tr}(\rho_i) \cdot \left\langle \frac{\rho_i}{\text{tr}(\rho_i)}, P_i \right\rangle$$

where processes are indexed by $i \in I$.

LEMMA E.2. α is the left inverse of γ , and γ is the left inverse of α up-to bisimilarity.

$$\mathfrak{D} = \alpha(\gamma(\mathfrak{D})) \quad \Delta \simeq \gamma(\alpha(\Delta))$$

PROOF. The first point follows from definition, the second from Theorem 5.10 and Theorem D.9. $\square$

LEMMA E.3. The function α and γ respect transitions, i.e.:

- For any $\Delta, \Delta' \in \mathcal{D}^\leq(\text{Conf})$, if $\Delta \xrightarrow{\mu}_s \Delta'$ then $\alpha(\Delta) \xrightarrow{\mu}_s \alpha(\Delta')$.
- For any $\mathfrak{D}, \mathfrak{D}' \in \mathcal{Q}(\text{Proc})$, if $\mathfrak{D} \xrightarrow{\mu}_s \mathfrak{D}'$ then $\gamma(\mathfrak{D}) \xrightarrow{\mu}_s \Delta'$ for some $\Delta' \in \mathcal{D}^\leq(\text{Conf})$ such that $\mathfrak{D}' = \alpha(\Delta')$.

PROOF. By definition of α and since the rules for $\xrightarrow{\mu}_s$ and $\xrightarrow{\mu}_s$ match one-to-one, it is trivial to show that $\Delta \xrightarrow{\mu}_s \Delta'$ if and only if $\alpha(\Delta) \xrightarrow{\mu}_s \alpha(\Delta')$.

Regarding the first point, if $\Delta' = \epsilon$ then every configuration in Δ is in deadlock, and thus also the corresponding quantum distribution mapped by α are in deadlock. If $\Delta' \neq \epsilon$, then Δ' is obtained via linear combinations of Δ'_j with weights p_j where $\langle \rho_j, P_i \rangle \xrightarrow{\mu}_s \Delta'_j$. But then $\alpha(p_j \cdot \langle \rho_j, P_i \rangle) \xrightarrow{\mu}_s \alpha(p_j \cdot \Delta'_j)$ and the result follows from applications of ID and CONV.

Regarding the second point, let $\mathfrak{D} = \sum_{i \in I} \rho_i \cdot P_i$. If $\rho_i \cdot P_i \xrightarrow{\mu}_s \epsilon$ and thus $\rho_i \cdot P_i \not\xrightarrow{\mu}_s$ then also $\left\langle \frac{\rho_i}{\text{tr}(\rho_i)}, P_i \right\rangle \not\xrightarrow{\mu}_s$ and $\alpha(\epsilon) = \epsilon$. If $\rho_i \cdot P_i \xrightarrow{\mu}_s \mathfrak{D}'_i$, by Lemma E.2 and the equivalence noted earlier, $\alpha(1 \cdot \langle \rho_i, P_i \rangle) \xrightarrow{\mu}_s \alpha(\gamma(\mathfrak{D}'_i))$ if and only if $\langle \rho_i, P_i \rangle \xrightarrow{\mu}_s \gamma(\mathfrak{D}'_i)$. Take $\Delta' = \sum_{i \in I} \gamma(\mathfrak{D}'_i)$, thus trivially $\mathfrak{D}' = \alpha(\Delta')$. $\square$

LEMMA E.4. The function α preserves environment, i.e. $\text{env}(\Delta) = \text{env}(\alpha(\Delta))$

PROOF.

$$\begin{aligned} \text{env}(\Delta) &= \text{env}\left(\sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle\right) = \text{tr}_\Sigma \left| \sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle \right| \\ &= \text{tr}_\Sigma \left(\sum_{i \in I} p_i \cdot \rho_i \right) \\ &= \text{tr}_\Sigma \left| \sum_{i \in I} (p_i \cdot \rho_i) \cdot P_i \right| = \text{tr}_\Sigma \left| \alpha \left(\sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle \right) \right| = \text{env}(\alpha(\Delta)) \end{aligned}$$

$\square$

LEMMA E.5. The function α commutes with superoperator application, i.e. $\alpha(\mathcal{E}(\Delta)) = \mathcal{E}(\alpha(\Delta))$

PROOF.

$$\begin{aligned}
\alpha(\mathcal{E}(\Delta)) &= \alpha(\mathcal{E}(\sum_{i \in I} p_i \cdot \langle \rho_i, P_i \rangle)) \\
&= \alpha\left(\sum_{i \in I} (p_i \cdot \text{tr}(\mathcal{E}(\rho_i))) \cdot \left\langle \frac{\mathcal{E}(\rho_i)}{\text{tr}\{\mathcal{E}(\rho_i)\}}, P_i \right\rangle\right) \\
&= \sum_{i \in I} (p_i \cdot \mathcal{E}(\rho_i)) \cdot P_i \\
&= \mathcal{E}\left(\sum_{i \in I} (p_i \cdot \rho_i) \cdot P_i\right) \\
&= \mathcal{E}(\alpha(\Delta))
\end{aligned}$$

□

LEMMA E.6. *The function γ commutes with superoperator application up to bisimilarity, i.e. $\gamma(\mathcal{E}(\mathfrak{D})) \simeq \mathcal{E}(\gamma(\mathfrak{D}))$*

PROOF. Follows by Lemma E.5 and Lemma E.2:

$$\gamma(\mathcal{E}(\Delta)) = \gamma \circ \mathcal{E} \circ \alpha \circ \gamma(\Delta) = \gamma \circ \alpha \circ \mathcal{E} \circ \gamma(\Delta) \simeq \mathcal{E}(\gamma(\Delta)).$$

□

We can now prove full-abstraction.

LEMMA E.7. *For any two probability distributions $\Delta, \Theta \in \mathcal{D}^{\leq}(\text{Conf})$, if $\Delta \sim_p \Theta$, then $\alpha(\Delta) \sim \alpha(\Theta)$*

PROOF. We define the relation $\mathcal{R} \subseteq \mathcal{Q}(\text{Proc}) \times \mathcal{Q}(\text{Proc})$ as

$$\mathcal{R} = \{(\alpha(\Delta), \alpha(\Theta)) \mid \Delta \sim_p \Theta\}$$

and prove it to be a labelled quantum bisimilarity. It is environment preserving thanks to Lemma E.4, as

$$\text{env}(\alpha(\Delta)) = \text{env}(\Delta) = \text{env}(\Theta) = \text{env}(\alpha(\Theta)).$$

It is superoperator closed thanks to Lemma E.5, as

$$\begin{aligned}
\alpha(\Delta) \mathcal{R} \alpha(\Theta) &\Rightarrow \Delta \sim_p \Theta \Rightarrow \mathcal{E}(\Delta) \sim_p \mathcal{E}(\Theta) \\
&\Rightarrow \alpha(\mathcal{E}(\Delta)) \mathcal{R} \alpha(\mathcal{E}(\Theta)) \Rightarrow \mathcal{E}(\alpha(\Delta)) \mathcal{R} \mathcal{E}(\alpha(\Theta)).
\end{aligned}$$

All is left to prove is that it is transition closed. Suppose that $\alpha(\Delta) \xrightarrow{\mu}_s \mathfrak{D}'$, we will prove that $\alpha(\Theta) \xrightarrow{\mu}_s \mathfrak{I}'$ and $\mathfrak{D}' \mathcal{R} \mathfrak{I}'$. The other direction is symmetrical.

$$\begin{array}{ccccccc}
\alpha(\Delta) & & \gamma(\alpha(\Delta)) & \sim_p & \Delta & \sim_p & \Theta & & \alpha(\Theta) \\
\downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Rightarrow & \downarrow s:\mu \\
\mathfrak{D}' & \xleftarrow{\alpha} & \Delta' & \sim_p & \Delta'' & \sim_p & \Theta' & \xrightarrow{\alpha} & \alpha(\Theta')
\end{array}$$

From left to right, we have used Lemma E.3, Lemma E.2, definition of $\mathcal{R}$, Lemma E.3, and we use the dashed alpha arrow to indicate when a probability distribution gets transformed in a density distribution. □

LEMMA E.8. *For any two density distributions $\mathfrak{D}, \mathfrak{I} \in \mathcal{Q}(\text{Proc})$, if $\mathfrak{D} \sim \mathfrak{I}$, then $\gamma(\mathfrak{D}) \sim_p \gamma(\mathfrak{I})$*

PROOF. We define the relation $\mathcal{R} \subseteq \mathcal{D}^{\leq}(\text{Conf}) \times \mathcal{D}^{\leq}(\text{Conf})$ as

$$\mathcal{R} = \{(\Delta, \Theta) \mid \mathfrak{D} \sim \mathfrak{I}, \Delta \sim_p \gamma(\mathfrak{D}), \Theta \sim_p \gamma(\mathfrak{I})\}$$

and prove it to be a labelled bisimilarity. It is environment preserving thanks to Lemma E.4, as

$$\text{env}(\Delta) = \text{env}(\gamma(\mathfrak{D})) = \text{env}(\gamma(\mathfrak{I})) = \text{env}(\Theta).$$

It is superoperator closed thanks to Lemma E.6 and the fact that $\sim_p$ is superoperator closed, as

$$\begin{aligned} \Delta \mathcal{R} \Theta &\Rightarrow \Delta \sim_p \gamma(\mathfrak{D}) \wedge \Theta \sim_p \gamma(\mathfrak{I}) \\ &\Rightarrow \mathcal{E}(\Delta) \sim_p \mathcal{E}(\gamma(\mathfrak{D})) \sim_p \gamma(\mathcal{E}(\mathfrak{D})) \wedge \mathcal{E}(\Theta) \sim_p \mathcal{E}(\gamma(\mathfrak{I})) \sim_p \gamma(\mathcal{E}(\mathfrak{I})) \\ &\Rightarrow \mathcal{E}(\Delta) \mathcal{R} \mathcal{E}(\Theta) \end{aligned}$$

where in the last row we have used the fact that $\mathfrak{D} \sim \mathfrak{I}$ implies $\mathcal{E}(\mathfrak{D}) \sim \mathcal{E}(\mathfrak{I})$. All is left to prove is that it is transition closed. Suppose that $\Delta \xrightarrow{\mu}_s \Delta'$, we will prove that $\Theta \xrightarrow{\mu}_s \Theta''$ and $\Delta' \mathcal{R} \Theta''$. The other direction is symmetrical.

$$\begin{array}{ccccccc} \Delta & \sim_p & \gamma(\mathfrak{D}) & & \alpha(\gamma(\mathfrak{D})) & = & \mathfrak{D} \sim \mathfrak{I} & & \gamma(\mathfrak{I}) \sim_p & \Theta \\ \downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Leftrightarrow & \downarrow s:\mu & \Rightarrow & \downarrow s:\mu & \Rightarrow \\ \Delta' & \sim_p & \Delta'' & \xrightarrow{\alpha} & \alpha(\Delta'') & = & \alpha(\Delta'') & \sim & \mathfrak{I}' & \xrightarrow{\alpha} & \Theta' \sim_p & \Theta'' \end{array}$$

From left to right, we have used the definition of $\mathcal{R}$, Lemma E.3, Lemma E.2, definition of $\mathcal{R}$, Lemma E.3, definition of $\mathcal{R}$, and we use the dashed alpha arrow to indicate when a probability distribution gets transformed in a density distribution. To show that $\Delta' \mathcal{R} \Theta''$, it is sufficient to notice that $\alpha(\Delta'') \sim \mathfrak{I}$, and if we apply γ to both we get by Lemma E.2 $\gamma(\alpha(\Delta'')) \sim_p \Delta'' \sim_p \Delta'$ and $\gamma(\mathfrak{I}) = \gamma(\alpha(\Theta')) \sim_p \Theta' \sim_p \Theta''$. $\square$

LEMMA E.9. For any $\Delta, \Theta \in \mathcal{D}^{\leq}(\text{Conf})$, $\Delta \simeq \Theta$ if and only if $\alpha(\Delta) \sim \alpha(\Theta)$.

PROOF. Let $\Delta \simeq \Theta$, by Theorem D.9 it holds if and only if $\Delta \sim_p \Theta$. It consequently holds if and only if $\alpha(\Delta) \sim \alpha(\Theta)$ from Lemma E.7 and Lemma E.8. $\square$

THEOREM 6.10 (FULL ABSTRACTION). For any ρ, σ, P, Q it holds that

$$1 \cdot \langle \rho, P \rangle \simeq 1 \cdot \langle \sigma, Q \rangle \text{ if and only if } \rho \cdot P \sim \sigma \cdot Q$$

PROOF. By Lemma E.9 $1 \cdot \langle \rho, P \rangle \simeq 1 \cdot \langle \sigma, Q \rangle$ if and only if $\alpha(1 \cdot \langle \rho, P \rangle) \sim \alpha(1 \cdot \langle \sigma, Q \rangle)$ and by definition of α , $\rho \cdot P \sim \sigma \cdot Q$. $\square$

LEMMA E.10. For any $\mathfrak{D}, \mathfrak{D}' \in \mathcal{Q}(\text{Proc})$ with $(\Sigma, \Sigma') \vdash \mathfrak{D}$, if $\mathfrak{D} \xrightarrow{\mu}_s \mathfrak{D}'$ then for all $\mathcal{E} \in \mathcal{SO}^{\leq}(\Sigma \setminus \Sigma')$ $\mathcal{E}(\mathfrak{D}) \xrightarrow{\mu}_s \mathcal{E}(\mathfrak{D}')$.

PROOF. First, note that transitions are uniquely determined by the process syntax and thus, all the transitions available for $\mathfrak{D}$ are also available for $\mathcal{E}(\mathfrak{D})$, although possibly with a different resulting distribution for the application of either a superoperator or a measurement. However, it is sufficient to note that, the operator $\mathcal{E}$ and the applications of superoperators and measurements are on distinct qubits and thus they commute. $\square$

LEMMA E.11. For all $\mathfrak{D}, \mathfrak{D}' \in \mathcal{Q}(\text{Proc})$ with $(\Sigma, \Sigma') \vdash \mathfrak{D}$, and $\mathcal{E} \in \mathcal{SO}^{\leq}(\Sigma \setminus \Sigma')$, if $\mathcal{E}(\mathfrak{D}) \xrightarrow{\mu}_s \mathfrak{D}'$ then there exists $\mathfrak{D}'' \in \mathcal{Q}(\text{Proc})$ such that $\mathfrak{D} \xrightarrow{\mu}_s \mathfrak{D}''$ and $\mathfrak{D}' = \mathcal{E}(\mathfrak{D}'')$.

PROOF. By induction on the transition $\mathcal{E}(\mathcal{D}) \xrightarrow{\mu}_s \mathcal{D}'$. $\square$

LEMMA E.12. For all $\mathcal{D}, \mathcal{I} \in Q(Proc_g)$, if $\mathcal{D} \sim_g \mathcal{I}$ with $(\Sigma, \Sigma') \vdash \mathcal{D}$ and $(\Sigma, \Sigma') \vdash \mathcal{I}$, then $\mathcal{E}(\mathcal{D}) \sim_g \mathcal{E}(\mathcal{I})$ for all $\mathcal{E} \in SO^{\leq}(\Sigma \setminus \Sigma')$.

PROOF. We will prove that the relation

$$SO^{\leq}(\sim_g) = \{(\mathcal{E}(\mathcal{D}), \mathcal{E}(\mathcal{I})) \mid (\Sigma, \Sigma') \vdash \mathcal{D}, (\Sigma, \Sigma') \vdash \mathcal{I}, \mathcal{D} \sim_g \mathcal{I}, \mathcal{E} \in SO^{\leq}(\Sigma \setminus \Sigma')\}$$

is a ground bisimulation.

The relation $SO^{\leq}(\sim_g)$ is trivially well-typed because superoperator application does not affect the support of distributions. Moreover, it is environment preserving, since the superoperator $\mathcal{E}$ only affects the qubits in the environment and thus commutes with the partial trace, i.e. $\text{tr}_{\Sigma'}(\text{qs}(\mathcal{E}(\mathcal{D}))) = \mathcal{E}(\text{tr}_{\Sigma'}(\text{qs}(\mathcal{D}))) = \mathcal{E}(\text{tr}_{\Sigma'}(\text{qs}(\mathcal{I}))) = \text{tr}_{\Sigma'}(\text{qs}(\mathcal{E}(\mathcal{I})))$.

We show transition closure by considering the case of reception separately. Assume a transition $\mathcal{E}(\mathcal{D}) \xrightarrow{\mu}_s \mathcal{D}'$ exists with $\mu \neq c?e$. By Lemma E.11 there exists a $\mathcal{D}''$ such that $\mathcal{D} \xrightarrow{\mu}_s \mathcal{D}''$ and $\mathcal{D}' = \mathcal{E}(\mathcal{D}'')$. However, $\mathcal{D} \sim_g \mathcal{I}$, therefore, there exists a $\mathcal{I}''$ such that $\mathcal{I} \xrightarrow{\mu}_s \mathcal{I}''$ and $\mathcal{D}'' \sim_g \mathcal{I}''$. Since the move is not a reception, the environment of $\mathcal{D}''$ and $\mathcal{I}''$ contains the same qubit or one more, thus by Lemma E.10 $\mathcal{E}(\mathcal{I}) \xrightarrow{\mu}_s \mathcal{E}(\mathcal{I}'')$, and by definition of $SO^{\leq}(\sim_g)$ we have $\mathcal{E}(\mathcal{D}'') SO^{\leq}(\sim_g) \mathcal{E}(\mathcal{I}'')$.

Assume a transition $\mathcal{E}(\mathcal{D}) \xrightarrow{c?e}_s \mathcal{D}'$ exists. As in the previous case, $\mathcal{D} \sim_g \mathcal{I}$ together with Lemma E.11 and Lemma E.10 imply that there exists a $\mathcal{I}'$ such that $\mathcal{E}(\mathcal{I}) \xrightarrow{c?e}_s \mathcal{I}'$ with $\mathcal{D}' \sim_g \mathcal{I}'$. Note that c cannot be a quantum channel because of the syntactic constraints of $Proc_g$, and the type of $\mathcal{D}$ is the same of the one of qd' . Then, since $\mathbb{I}(\mathcal{D}') = \mathcal{D}'$ and $\mathbb{I}(\mathcal{I}') = \mathcal{I}'$ we also have $\mathcal{D}' SO^{\leq}(\sim_g) \mathcal{I}'$. $\square$

COROLLARY E.13. Let $\mathcal{D}, \mathcal{I} \in Q(Proc)$. If $\mathcal{D} \sim_g \mathcal{I}$ then $\mathcal{D} \sim \mathcal{I}$.

LEMMA E.14. For any $\Delta, \Theta \in \mathcal{D}^{\leq}(Proc_g)$, $\Delta \simeq \Theta$ if and only if $\alpha(\Delta) \sim_g \alpha(\Theta)$.

PROOF. Follows immediately from Lemma E.12. $\square$

THEOREM 6.14. For any $P, Q \in Proc_g$, ρ, σ it holds that $1 \cdot \langle \rho, P \rangle \simeq 1 \cdot \langle \sigma, Q \rangle$ if and only if $\rho \cdot P \sim_g \sigma \cdot Q$

PROOF. Follows immediately from Lemma E.14. $\square$

Received 26 March 2026; revised 26 March 2026; accepted 7 July 2026