Logical Methods in Computer Science
Volume 20, Issue 2, 2024, pp. 5:1–5:45
https://lmcs.episciences.org/

Submitted Dec. 05, 2022
Published Apr. 30, 2024

ENCODABILITY CRITERIA FOR QUANTUM BASED SYSTEMS

ANNA SCHMITT [a], KIRSTIN PETERS [b], AND YUXIN DENG [c]

[a] TU Darmstadt, Germany
e-mail address: Anna.Schmitt@tu-darmstadt.de

[b] Augsburg University, Germany
e-mail address: kirstin.peters@uni-a.de

[c] East China Normal University, Shanghai
e-mail address: yxdeng@sei.ecnu.edu.cn

Abstract. Quantum based systems are a relatively new research area for that different modelling languages including process calculi are currently under development. Encodings are often used to compare process calculi. Quality criteria are used then to rule out trivial or meaningless encodings. In this new context of quantum based systems, it is necessary to analyse the applicability of these quality criteria and to potentially extend or adapt them. As a first step, we test the suitability of classical criteria for encodings between quantum based languages and discuss new criteria.

Concretely, we present an encoding, from a language inspired by CQP into a language inspired by qCCS. We show that this encoding satisfies compositionality, name invariance (for channel and qubit names), operational correspondence, divergence reflection, success sensitiveness, and that it preserves the size of quantum registers. Then we show that there is no encoding from qCCS into CQP that is compositional, operationally corresponding, and success sensitive.

1. Introduction

The technological progress turns quantum based systems from theoretical models to hopefully soon practicable realisations. This progress inspired research on quantum algorithms and protocols. They allow for a significant increase in efficiency in many cases and provide new approaches to secure systems. These algorithms and protocols in turn call for verification methods that can deal with the new quantum based setting.

Among the various tools for such verifications, also several process calculi for quantum based systems are developed [JL04, GN05, Gay06, YFDJ09]. To compare the expressive power and suitability for different application areas, encodings have been widely used for classical, i.e., not quantum based, systems. To rule out trivial or meaningless encodings, they are required to satisfy quality criteria. In this new context of quantum based systems,

Key words and phrases: Process calculi and Quantum Based Systems and Encodings.
We thank the anonymous reviewers for their constructive feedback and help to improve this paper.

DOI:10.46298/LMCS-20(2:5)2024

we have to analyse the applicability of these quality criteria and potentially extend or adapt them.

Therefore, we start by considering a well-known framework of quality criteria introduced by Gorla in [Gor10] for the classical setting. As a case study we want to compare *Communicating Quantum Processes* (CQP) introduced in [GN05] and the *Algebra of Quantum Processes* (qCCS) introduced in [FDJY07, YFDJ09]. These two process calculi are particularly interesting, because they model quantum registers and the behaviour of quantum based systems in fundamentally different ways. CQP considers closed systems, where qubits are manipulated by unitary transformations and the behaviour is expressed by a probabilistic transition system. In contrast, qCCS focuses on open systems and super-operators. Moreover, the transition system of qCCS as presented at [YFDJ09] is non-probabilistic. (Unitary transformations and super-operators are discussed in the next section.)

Unfortunately, the languages also differ in classical aspects: CQP has π-calculus-like name passing but the CCS based qCCS does not allow to transfer names; qCCS has operators for choice and recursion but CQP in [GN05] has not. Therefore, comparing the languages directly would yield negative results in both directions, that do not depend on their treatment of qubits. To avoid these obvious negative results and to concentrate on the treatment of qubits, we consider CQS, a strictly less expressive sublanguage of CQP that removes name passing and simplifies the syntax/semantics, but as we claim does treat qubits in the same way as CQP. As second language we consider OQS that is similar to qCCS as presented in [YFDJ09] extended by an operator for a conditional, but as we claim again does treat qubits in the same way as qCCS. Accordingly, our focus is not exactly on the languages CQP and qCCS but on how they treat qubits. The language CQS, for *closed quantum systems*, inherits from CQP the closed systems with only unitary transformations and has a semantics that is no longer probabilistic, but explicitly deals with probability distributions. In contrast OQS, for *open quantum systems*, inherits from qCCS the open systems and super-operators and a non-probabilistic semantics without explicitly considering probability distributions. We further discuss the differences between CQP and CQS as well as qCCS and OQS when we introduce these languages.

We then show that there exists an encoding from CQS into OQS that satisfies the quality criteria of Gorla and thereby that the treatment of qubits in OQS/qCCS is strong enough to emulate the treatment of qubits in CQS/CQP. We also show that the opposite direction is more difficult, even if we restrict the classical operators in qCCS. In fact, the counterexample that we use to prove the non-existence of an encoding considers the treatment of qubits only, i.e., relies on the application of a specific super-operator that has no unitary equivalent.

These two results show that the quality criteria can still be applied in the context of quantum based systems and are still meaningful in this setting. They may, however, not be exhaustive. Therefore, we discuss directions of additional quality criteria that might be relevant for quantum based systems.

Our encoding satisfies compositionality, name invariance w.r.t. channel names and qubit names, strong operational correspondence, divergence reflection, success sensitiveness, and that the encoding preserves the size of quantum registers. We also show that there is no encoding from OQS/qCCS into CQS/CQP that satisfies compositionality, operational correspondence, and success sensitiveness, where we consider a variant qCCS with a measurement operator as given in [FDJY07, FDY12].

Summary. We need a number of preliminaries: Quantum based systems are briefly discussed in §2, the considered process calculi are introduced in §3, and §4 presents the quality criteria of Gorla. §5 introduces the encoding from CQS into OQS and comments on its correctness. The negative result from OQS/qCCS with a measurement operator into CQS/CQP is presented in §6. In §7 we discuss directions for criteria specific to quantum based systems. We conclude in §8. The present work extends and revises [SPD22a, SPD22b]. In particular, we restore the negative result in §6, since unfortunately the counterexample used in [SPD22a] was an invalid super-operator. Moreover, we revise both of the considered languages to get closer to the original versions of qCCS and CQP and more clearly describe the differences to their respective prototypes. We present detailed proofs of the mentioned results and provide more explanations.

2. Quantum Based Systems

We briefly introduce the aspects of quantum based systems, which are needed for the rest of this paper. For more details, we refer to the books by Nielsen and Chuang [NC10], Gruska [Gru09], and Rieffel and Polak [RP00].

A *quantum bit* or *qubit* is a physical system which has the two base states: $|0\rangle$ and $|1\rangle$. These states correspond to one-bit classical values. The general state of a quantum system is a *superposition* or linear combination of base states, concretely $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Thereby, α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$, e.g. $|0\rangle = 1|0\rangle + 0|1\rangle$. Further, a state can be represented by column vectors $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$, which sometimes for readability will be written in the format $(\alpha, \beta)^\mathsf{T}$, where $^\mathsf{T}$ stands for transpose. The vector space of these vectors is a *Hilbert space*, denoted by $\mathfrak{H}$. It forms the state space of a quantum based system. In [YFDJ09] finite-dimensional and countably infinite-dimensional Hilbert spaces are considered, where the latter are treated as tensor products of countably infinitely many finite-dimensional Hilbert spaces. For this work finite-dimensional Hilbert spaces are sufficient.

The basis $\{|0\rangle, |1\rangle\}$ is called *standard basis* or *computational basis*, but sometimes there are other orthonormal bases of interest, especially the *diagonal* or *Hadamard* basis consisting of the vectors $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We assume the standard basis in the following.

The evolution of a closed quantum system can be described by *unitary transformations* [NC10]. A unitary transformation U is represented by a complex-valued matrix such that the effect of U onto a state of a qubit is calculated by matrix multiplication. It holds that $U^\dagger U = \mathcal{I}$, where $U^\dagger$ is the adjoint of U and $\mathcal{I}$ is the *identity matrix*. Thereby, $\mathcal{I}$ is one of the *Pauli matrices* together with $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. Another important unitary transformation is the *Hadamard* transformation $\mathcal{H}$, as it creates the superpositions $\mathcal{H}|0\rangle = |+\rangle$ and $\mathcal{H}|1\rangle = |-\rangle$.

$$\mathcal{I} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \mathcal{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad \mathcal{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \quad \mathcal{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \quad \mathcal{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

All of these five unitary transformations are applied to a single qubit. As mentioned above, $\mathcal{I}$ is identity. $\mathcal{X}$ performs the quantum version of a bit-flip. It interchanges the amplitudes, i.e., $\mathcal{X}(\alpha, \beta)^\mathsf{T} = (\beta, \alpha)^\mathsf{T}$. Intuitively, $\mathcal{Y}$ moves a qubit by the imaginary i, i.e., $\mathcal{Y}(\alpha, \beta)^\mathsf{T} = (-i\beta, i\alpha)^\mathsf{T}$. The transformation $\mathcal{Z}$, that is sometimes called phase flip, leaves the upper component of the vector unchanged but flips the sign of the second component,

i.e., $\mathcal{Z}(\alpha,\beta)^\mathsf{T} = (\alpha,-\beta)^\mathsf{T}$. Hadamard $\mathcal{H}$ intuitively moves a qubit halfway between the base states $|0\rangle$ and $|1\rangle$, e.g. $\mathcal{H}|0\rangle = \mathcal{H}(1,0)^\mathsf{T} = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\mathcal{H}|+\rangle = |0\rangle$.

Another key feature of quantum computing is the *measurement*. Measuring a qubit q in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ results in 0 (leaving it in $|0\rangle$) with probability $|\alpha|^2$ and in 1 (leaving it in $|1\rangle$) with probability $|\beta|^2$.

By combining qubits, we create *multi-qubit systems*. Therefore the spaces U and V with bases $\{u_0,\ldots,u_i,\ldots\}$ and $\{v_0,\ldots,v_j,\ldots\}$ are joined using the *tensor product* into one space $U\otimes V$ with basis $\{u_0\otimes v_0,\ldots,u_i\otimes v_j,\ldots\}$. So a system consisting of n qubits has a 2^n-dimensional space with standard bases $|00\ldots0\rangle\ldots|11\ldots1\rangle$. Within these systems we can measure a single or multiple qubits. As an example for measurement, consider the 2-qubit system with the basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ and the general state $\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle$ with $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2 = 1$. A measurement of the first qubit gives result 0 with probability $|\alpha|^2+|\beta|^2$ and leaves the system in state $\dfrac{1}{\sqrt{|\alpha|^2+|\beta|^2}}(\alpha|00\rangle+\beta|01\rangle)$. The result 1 is given with probability $|\gamma|^2+|\delta|^2$. In this case the system has state $\dfrac{1}{\sqrt{|\gamma|^2+|\delta|^2}}(\gamma|10\rangle+\delta|11\rangle)$. Further, the measurement of both qubits simultaneously gives result 0 for both qubits with probability $|\alpha|^2$ (leaving the system in state $|00\rangle$), result 0 for the first and 1 for the second qubit with probability $|\beta|^2$ (leaving the system in state $|01\rangle$) and so on. We use binary numbers to refer to measurement results, i.e., for two qubits the measurement results are 00, 01, 10, or 11.

In multi-qubit systems unitary transformations can be performed on single or several qubits. As an example for an unitary transformation, consider the transformation $\mathcal{X}$ on both qubits of a 2-qubit system in state $|00\rangle$ simultaneously, we use the unitary transformation $\mathcal{X}\otimes\mathcal{X}$. The result of $(\mathcal{X}\otimes\mathcal{X})|00\rangle$ is the state $|11\rangle$. To apply $\mathcal{X}$ only to the second qubit, we use $\mathcal{I}\otimes\mathcal{X}$ and $(\mathcal{I}\otimes\mathcal{X})|00\rangle = |01\rangle$. The Pauli matrix $\mathcal{I}$ denotes the identity matrix in 2^1 dimensional space. By slightly abusing notation we also use $\mathcal{I}_{\{q_1,\ldots,q_n\}}$ or simply $\mathcal{I}$ to denote identity in 2^n dimensional space for all natural numbers n.

The multi-qubit systems can exhibit *entanglement*, meaning that states of qubits are correlated, e.g. in $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ which is one of the so-called *Bell pairs*. Here, a measurement of the first qubit in the computational basis results in 0 (leaving the state $|00\rangle$) with probability $\frac{1}{2}$ and in 1 (leaving the state $|11\rangle$) with probability $\frac{1}{2}$. In both cases a subsequent measurement of the second qubit in the same basis gives the same result as the first measurement with probability 1. The effect also occurs if the entangled qubits are physically separated. Because of this, states with entangled qubits cannot be written as a tensor product of single-qubit states.

States of quantum systems can also be described by *density matrices* or *density operators*. In contrast to the vector description of states, density matrices allow to describe the states of open systems. A density operator in a Hilbert space $\mathfrak{H}$ is a linear operator ρ on it, such that $|\psi\rangle^\dagger\rho|\psi\rangle \geq 0$ for all $|\psi\rangle$ and $\mathsf{tr}(\rho) = 1$, where the trace $\mathsf{tr}(\rho)$ is the sum of elements on the main diagonal of the matrix ρ. A positive operator ρ is called a partial density operator if $\mathsf{tr}(\rho)\leq 1$. We write $\mathfrak{D}(\mathfrak{H})$ for the set of (partial) density operators on $\mathfrak{H}$. For every state $|\psi\rangle$ in the above described vector representation, we obtain the corresponding density matrix by the outer product $|\psi\rangle\langle\psi| = |\psi\rangle|\psi\rangle^\dagger$. For example, consider again the 2-qubit system in general state $|\psi\rangle = \alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle$ which corresponds to the vector $(\alpha,\beta,\gamma,\delta)^\mathsf{T}$.

The corresponding density matrix is given as:

$$|\psi\rangle\langle\psi| = |\psi\rangle|\psi\rangle^\dagger = \begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix}\left(\overline{\alpha},\overline{\beta},\overline{\gamma},\overline{\delta}\right) = \begin{pmatrix}\alpha\overline{\alpha} & \alpha\overline{\beta} & \alpha\overline{\gamma} & \alpha\overline{\delta}\\ \beta\overline{\alpha} & \beta\overline{\beta} & \beta\overline{\gamma} & \beta\overline{\delta}\\ \gamma\overline{\alpha} & \gamma\overline{\beta} & \gamma\overline{\gamma} & \gamma\overline{\delta}\\ \delta\overline{\alpha} & \delta\overline{\beta} & \delta\overline{\gamma} & \delta\overline{\delta}\end{pmatrix}$$

where the adjoint $|\psi\rangle^\dagger = \left(\overline{\alpha},\overline{\beta},\overline{\gamma},\overline{\delta}\right)$ is the conjugate transpose of $|\psi\rangle$. Here, $\overline{x}$ denotes the complex conjugate of x. For real numbers a and b, the complex conjugate of $a+ib$ is $a-ib$. Such states, i.e., states that result from the outer product of a vector with itself, are called *pure states*. Additionally, density matrices can represent *mixed states*, that arise either when the system is not fully known or when one wants to describe a system which is entangled with another. Every density matrix can be represented as $\sum_i p_i|\psi_i\rangle\langle\psi_i|$, called *sum representation*, i.e., by an ensemble of pure states $|\psi_i\rangle$ with their probabilities $p_i \geq 0$ and $\sum_i p_i = 1$.

We often use density matrix to refer to a state of a potentially open system and call the transformations on these states *super-operators*. Note that unitary transformations can only describe transitions in closed systems. Super-operators are strictly more expressive, since they can also express interaction with an (unknown) environment. Example 6.1 in Section 6 presents a super-operator that does not resemble any unitary transformation. This super-operator can be used to model a specific kind of noise in quantum communication. Intuitively, noise is a form of partial entanglement with an unkown environment. Note that the channels that are used to transfer qubit-systems in CQP, CQS, qCCS, and OQS, are modelled as noise-free channels, i.e., noise has to be added explicitly by respective super-operators as discussed in [YFDJ09]. There are different ways to define super-operators, e.g. via the sum representation.

Definition 2.1 (Super-Operator, Operator-Sum Representation, [NC10])**.** Let ρ be the initial state of a system, $|e_1\rangle,\ldots,|e_n\rangle$ be an orthonormal basis for the (finite dimensional) state space of the environment, and $\rho_{\mathsf{env}} = |e_0\rangle\langle e_0|$ be the initial state of the environment. A *super-operator* $\mathcal{E}(\rho)$ on the system ρ is an operator $\mathcal{E}$ which is defined as $\mathcal{E}(\rho) = \sum_i E_i\rho E_i^\dagger$, where $E_i = \langle e_i|U|e_0\rangle$ is an operator on the state space of the system. Thereby, the operators $\{E_i\}$ are known as *operation elements* for the quantum operation $\mathcal{E}$, which have to satisfy $\sum_i E_i^\dagger E_i \leq \mathcal{I}$. The super-operator $\mathcal{E}$ is *trace-preserving* if $\sum_i E_i^\dagger E_i = \mathcal{I}$.

For every unitary transformation U, $U(\rho) = U\rho U^\dagger$ is a trace-preserving super-operator. Let $\{M_m\}$ such that $\sum_m M_m^\dagger M_m = \mathcal{I}$. Then, by [YFDJ09], $\{M_m\}$ is a collection of measurement operators. We usually let m refer to the measurement outcome. For each m, let $\mathcal{E}_m(\rho) = M_m\rho M_m^\dagger$ for any state $\rho \in \mathfrak{D}(\mathfrak{H})$. Moreover, let $\mathcal{E}(\rho) = \sum_m M_m\rho M_m^\dagger$ for any state $\rho \in \mathfrak{D}(\mathfrak{H})$. Then $\mathcal{E}_m$ is a super-operator, which is not necessarily trace-preserving, whereas $\mathcal{E}$ is a trace-preserving super-operator (see Example 2.5 in [YFDJ09]).

According to [NC10] the equation $\mathcal{E}(\rho) = \sum_i E_i\rho E_i^\dagger$ from Definition 2.1, is a re-statement of $\mathcal{E}(\rho) = \mathsf{tr}_{\mathsf{env}}\left(U\left(\rho\otimes\rho_{\mathsf{env}}\right)U^\dagger\right)$, where $\mathsf{tr}_{\mathsf{env}}()$ is a partial trace over the environment to obtain the reduced state of the system. Within this equation it is assumed, that the environment starts in a pure state. This assumption can be made without loss of generality, since we are free to introduce an extra system purifying the environment, if it starts in a mixed state. Another assumption made within this equation is that the system and the environment start in a product state. This is not true in general, as quantum systems

constantly interact with their environment by which correlations are created. Nonetheless, in many cases of practical interest it is reasonable to make this assumption, as by bringing a quantum system to a specific state these correlations are destroyed, leaving the system in a pure state. We refer to [NC10] for further informations on super-operators.

3. Process Calculi

A *process calculus* is a language $\mathfrak{L} = \langle \mathfrak{C}, \longmapsto \rangle$ that consists of a set of *configurations* $\mathfrak{C}$ (its syntax) and a relation $\longmapsto : \mathfrak{C} \times \mathfrak{C}$ on configurations (its reduction semantics). To range over the configurations we use the upper case letters $C, C', \ldots$. Further, a configuration C contains a *term* out of the set of (process) terms $\mathfrak{P}$ on which we range over using the upper case letters $P, Q, P', \ldots$.

Assume three pairwise distinct countably-infinite sets $\mathcal{N}$ of *names*, $\mathcal{V}$ of *qubit variables*, and $\mathcal{B}$ of *variables for binary numbers*. We use lower case letters to range over names $a, c, \ldots$, qubits names $q, q', x, y, \ldots$, binary numbers $b, b', \ldots$, and variables for binary numbers $v, v', \ldots$. We write $bv, bv', \ldots$ for objects that are either a binary number or a variable for binary numbers. Let $\tau \notin \mathcal{V} \cup \mathcal{N} \cup \mathcal{B}$. The *scope* of a name defines the area in which this name is known and can be used. It can be useful to restrict this scope, for example to forbid interactions between two processes or with an unknown and, hence, potentially untrusted environment. While names with a restricted scope are called *bound names*, the remaining ones are called *free names*.

The *syntax* of a process calculus is usually defined by a context-free grammar defining operators, i.e., functions $\mathrm{op} : \mathfrak{P}^n \to \mathfrak{P}$ with $n \geq 0$. An operator of arity 0 is a *constant*. The *semantics* of a process calculus is given as a *structural operational semantics* consisting of inference rules defined on the operators of the language [Plo04]. The semantics is provided often in two forms, as *reduction semantics* and as *labelled transition semantics*. We assume that at least the reduction semantics is given, because its treatment is easier in the context of encodings. As we naturally extend the definition of the syntax to configurations, a *(reduction) step*, written as $C \longmapsto C'$, is a single application of the reduction semantics where C' is called *derivative*. Let $C \longmapsto$ denote the existence of a step from C. We write $C \longmapsto^{\omega}$ if C has an *infinite sequence* of steps and $\Longmapsto$ to denote the *reflexive and transitive closure* of $\longmapsto$.

To reason about environments of terms, we use functions on process terms called contexts. More precisely, a *context* $\mathcal{C}([\cdot]_1, \ldots, [\cdot]_n) : \mathfrak{P}^n \to \mathfrak{P}$ with n holes is a function from n terms into one term, i.e., given $P_1, \ldots, P_n \in \mathfrak{P}$, the term $\mathcal{C}(P_1, \ldots, P_n)$ is the result of inserting $P_1, \ldots, P_n$ in the corresponding order into the n holes of $\mathcal{C}$. We naturally extend the definition of contexts to configurations, i.e., consider also contexts $\mathcal{C}([\cdot]_1, \ldots, [\cdot]_n) : \mathfrak{P}^n \to \mathfrak{C}$.

A substitution is a finite mapping on either names or qubits or variables for binary numbers defined by a non-empty set $\{h_1/g_1, \ldots, h_n/g_n\} = \{h_1, \ldots, h_n/g_1, \ldots, g_n\}$ of renamings, where the $g_1, \ldots, g_n$ are pairwise distinct. The application $P\{h_1/g_1, \ldots, h_n/g_n\}$ of a substitution on a term is defined as the result of simultaneously replacing all free occurrences of g_i by h_i for $i \in \{1, \ldots, n\}$, possibly applying α-conversion to avoid capture or name clashes. For all names in $\mathcal{N} \setminus \{g_1, \ldots, g_n\}$ or qubits in $\mathcal{V} \setminus \{g_1, \ldots, g_n\}$ or variables in $\mathcal{B} \setminus \{g_1, \ldots, g_n\}$ the substitution behaves as the identity mapping. Substitutions on qubits additionally cannot translate different qubits to the same qubit, since this might violate the no-cloning principle. More on substitutions of qubits can be found, e.g. , in [YFDJ09]. We naturally extend substitutions to mappings that instantiate variables for binary numbers by

binary numbers. We equate terms and configurations modulo alpha conversion on (qubit) names.

For the last criterion of [Gor10] in Section 4, we need a special constant ✓, called *success(ful termination)*, in both considered languages. Therefore, we add ✓ to the grammars of both languages without explicitly mentioning them. Success is used as a barb, where $C{\downarrow_{\checkmark}}$ if the term contained in the configuration C has an unguarded occurrence of ✓ and $C{\Downarrow_{\checkmark}} = \exists C'.\, C \Longmapsto C' \wedge C'{\downarrow_{\checkmark}}$, to implement some form of (fair) testing.

3.1. **A Calculus for Closed Quantum Systems.** Communicating Quantum Processes (CQP) is introduced in [GN05]. CQP is further studied e.g. in [DGNP12] to study quantum error correction, in [FGP13, FGP14] to describe and analyse linear optical quantum computing, or in [GP12], where it is extended to be able to describe d-dimensional quantum systems.

As indicated in Section 1, we build CQS by inheriting some ideas of CQP. However, the resulting language CQS is strictly less expressive than CQP. We simplify the definition of CQP by removing name passing and contexts, the additional layer on expressions in the syntax and semantics, do not allow to construct channel names from expressions, and by using a monadic version of communication in that only qubits can be transmitted. Then we add a standard conditional operator, that allows to compare two binary numbers. CQP in [GN05] does not have such a conditional, but as stated in footnote 3 in [GN05] the language can easily be extended by an operator to test the result of measurement—just as the conditional we add here. We claim, however that the treatment of qubits, in particular the manipulations of the quantum register as well as the communication of qubits, is the same as in CQP. Let $\mathsf{b}(i)$ return the binary number representing the natural number i.

Definition 3.1 (CQS)**.** The CQS *terms*, denoted by $\mathfrak{P}_{\mathsf{C}}$, are given by:

$$P ::= \mathbf{0} \mid P \mid P \mid c?[x].P \mid c![x].P \mid \{\tilde{x} *= U\}.P$$
$$\mid (v := \mathsf{measure}\ \tilde{x}).P \mid (\mathsf{new}\ c)P \mid (\mathsf{qubit}\ x)P \mid \mathsf{if}\ bv = bv'\ \mathsf{then}\ P$$

CQS *configurations* $\mathfrak{C}_{\mathsf{C}}$ are given by $(\sigma; \phi; P)$ or $\boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi; P\{\mathsf{b}(i)/v\})$, where σ, σ_i have the form $q_0, \ldots, q_{n-1} = |\psi\rangle$ with $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |\psi_i\rangle$, $r \le n$, ϕ is the list of channels in the system, and $P \in \mathfrak{P}_{\mathsf{C}}$.

The syntax of CQS is π-calculus like. The inactive process is denoted by $\mathbf{0}$ and $P \mid P$ defines parallel composition. A term $c?[x].P$ receives a qubit $q \in \mathcal{V}$ over channel $c \in \mathcal{N}$ and proceeds as $P\{q/x\}$. Similarly, $c![x].P$ first sends a qubit $x \in \mathcal{V}$ over channel $c \in \mathcal{N}$ before proceeding as P. The term $\{\tilde{x} *= U\}.P$ applies the unitary transformation U to the qubits in sequence $\tilde{x}$ and then proceeds as P. The process $(v := \mathsf{measure}\ \tilde{x}).P$ measures the qubits in $\tilde{x}$ with $|\tilde{x}| > 0$ and saves the result in the variable v for binary numbers. The terms $(\mathsf{new}\ c)P$ and $(\mathsf{qubit}\ x)P$ create a fresh, global channel $a \in \mathcal{N}$ and a fresh qubit $q_n \in \mathcal{V}$ (for a quantum register $\sigma = q_0, \ldots, q_{n-1}$) and then proceed as $P\{a/c\}$ and $P\{q_n/x\}$, respectively.

The configuration $\boxplus_{0\le i<2^r} p_i \bullet C_i$ denotes a probability distribution over configurations $C_i = (\sigma_i; \phi; P\{\mathsf{b}(i)/v\})$, where $\sum_i p_i = 1$ and where the terms within the configurations C_i may differ only by instantiating a variable v by the binary number $\mathsf{b}(i)$. It results from measuring the first r qubits, where p_i is the probability of obtaining result $\mathsf{b}(i)$ from measuring the qubits $q_0, \ldots, q_{r-1}$ and C_i is the configuration of case i after the measurement. Indeed we restrict our attention to probability distributions of configurations that may be the result of measuring a state of a single configuration. In particular, this means that the states

$$
\begin{array}{rl}
\text{(R-MEASURE}_{\mathsf{CQS}}\text{)} & (\sigma;\phi;(v := \mathsf{measure}\ q_0,\dots q_{r-1}).P) \\
& \quad \longmapsto \boxplus_{0\le m<2^r} p_m \bullet (\sigma'_m;\phi;P\{\mathsf{b}(m)/v\}) \\
\text{(R-TRANS}_{\mathsf{CQS}}\text{)} & (q_0,\dots,q_{n-1}=|\psi\rangle;\phi;\{q_0,\dots,q_{r-1} *= U\}.P) \\
& \quad \longmapsto \big(q_0,\dots,q_{n-1}=\big(U\otimes \mathcal{I}_{\{q_r,\dots,q_{n-1}\}}\big)|\psi\rangle;\phi;P\big) \\
\text{(R-PERM}_{\mathsf{CQS}}\text{)} & (q_0,\dots,q_{n-1}=|\psi\rangle;\phi;P) \longmapsto \big(q_{\pi(0)},\dots,q_{\pi(n-1)}=\textstyle\prod|\psi\rangle;\phi;P\pi\big) \\
\text{(R-PROB}_{\mathsf{CQS}}\text{)} & \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i;\phi;P\{\mathsf{b}(i)/v\}) \\
& \quad \longmapsto (\sigma_j;\phi;P\{\mathsf{b}(j)/v\}) \quad \text{where } p_j\neq 0 \text{ and } r>0 \\
\text{(R-NEW}_{\mathsf{CQS}}\text{)} & (\sigma;\phi;(\mathsf{new}\ c)P) \longmapsto (\sigma;\phi,a;P\{a/c\}) \quad \text{where } a \text{ is fresh} \\
\text{(R-QBIT}_{\mathsf{CQS}}\text{)} & (q_0,\dots,q_{n-1}=|\psi\rangle;\phi;(\mathsf{qubit}\ x)P) \\
& \quad \longmapsto (q_0,\dots,q_{n-1},q_n=|\psi\rangle\otimes|0\rangle;\phi;P\{q_n/x\}) \\
\text{(R-COMM}_{\mathsf{CQS}}\text{)} & (\sigma;\phi;c![q].P \mid c?[x].Q) \longmapsto (\sigma;\phi;P\mid Q\{q/x\}) \\
\text{(R-PAR}_{\mathsf{CQS}}\text{)} & \dfrac{(\sigma;\phi;P)\longmapsto \boxplus_{0\le i<2^r} p_i\bullet(\sigma'_i;\phi';P'\{\mathsf{b}(i)/v\})}{(\sigma;\phi;P\mid Q)\longmapsto \boxplus_{0\le i<2^r} p_i\bullet(\sigma'_i;\phi';P'\{\mathsf{b}(i)/v\}\mid Q)} \\
\text{(R-CONG}_{\mathsf{CQS}}\text{)} & \dfrac{Q\equiv P \quad (\sigma;\phi;P)\longmapsto \boxplus_{0\le i<2^r} p_i\bullet(\sigma'_i;\phi';P'\{\mathsf{b}(i)/v\}) \quad P'\equiv Q'}{(\sigma;\phi;Q)\longmapsto \boxplus_{0\le i<2^r} p_i\bullet(\sigma'_i;\phi';Q'\{\mathsf{b}(i)/v\})} \\
\text{(R-COND}_{\mathsf{CQS}}\text{)} & \dfrac{b=b'}{(\sigma;\phi;\mathsf{if}\ b=b'\ \mathsf{then}\ P)\longmapsto(\sigma;\phi;P)}
\end{array}
$$

Figure 1: Semantics of CQS

σ_i of a probability distribution have to reflect the possible outcomes of the measurement, i.e., for a single qubit $\sigma_0 = q = |0\rangle$ and $\sigma_1 = q = |1\rangle$. We may also write a distribution as $p_1 \bullet C_1 \boxplus \dots \boxplus p_j \bullet C_j$ with $j = 2^r - 1$. We equate $(\sigma_0;\phi;P)$ and $\boxplus_{0\le i<2^0} 1 \bullet (\sigma_i;\phi;P\{\mathsf{b}(i)/v\})$, i.e., if $r = 0$ then we assume that v is not free in P.

The variable $x \in \mathcal{V}$ is bound in P by $c?[x].P$ and $(\mathsf{qubit}\ x)P$. Similarly, the variable $v \in \mathcal{B}$ is bound in P by $(v := \mathsf{measure}\ \tilde{x}).P$ and the variable $c \in \mathcal{N}$ is bound in P by $(\mathsf{new}\ c)P$. A variable is free if it is not bound. Let $\mathsf{fq}(P)$, $\mathsf{fc}(P)$, and $\mathsf{fv}(P)$ denote the sets of free qubits, free channels, and free variables for binary numbers in P, respectively.

The state σ is represented by a list of qubits $q_0,\dots,q_{n-1}$ as well as a linear combination $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|\psi_i\rangle$ which can also be rewritten by a vector $(\alpha_0,\dots,\alpha_{2^n-1})^{\mathsf{T}}$, where $^{\mathsf{T}}$ stands for transpose. As done in [GN05], we sometimes write as an abbreviated form $\sigma = q_0,\dots,q_{n-1}$ or $\sigma = |\psi\rangle$.

The semantics of CQS is defined by the reduction rules in Figure 1. These rules are inspired by the semantics of CQP in [GN05] but do not require a second layer for expressions, since we simplified the syntax, and drop the label of Rule (R-PROB$_{\mathsf{CQS}}$). Accordingly, CQS in contrast to CQP does not have a probabilistic transition system, but replaces probabilistic steps by non-deterministic steps. We do that, because the encodability criteria that we study here (see Section 4) do not consider probabilistic transitions systems. We discuss this issue in Section 7. Moreover, we add the Rule (R-COND$_{\mathsf{CQS}}$) to reduce conditionals. Rule (R-MEASURE$_{\mathsf{CQS}}$) measures the first r qubits of σ, where $\sigma = \alpha_0|\psi_0\rangle + \dots + \alpha_{2^n-1}|\psi_{2^n-1}\rangle$, $\sigma'_m = \frac{\alpha_{l_m}}{\sqrt{p_m}}|\psi_{l_m}\rangle + \dots + \frac{\alpha_{u_m}}{\sqrt{p_m}}|\psi_{u_m}\rangle$, $l_m = 2^{n-r}m$, $u_m = 2^{n-r}(m+1)-1$, and $p_m = |\alpha_{l_m}|^2 + \dots + |\alpha_{u_m}|^2$. As a result a probability distribution over the possible base vectors is generated, where σ'_m is the accordingly updated qubit vector and $\mathsf{b}(m)$ is the respective measurement outcome. Rule (R-TRANS$_{\mathsf{CQS}}$) applies the unitary transformation U on the

first r qubits. In contrast to [GN05], we explicitly list in the subscript of $\mathcal{I}$ the qubits it is applied to. As the rules (R-Measure$_{\mathsf{CQS}}$) and (R-Trans$_{\mathsf{CQS}}$) operate on the first r qubits within σ, Rule (R-Perm$_{\mathsf{CQS}}$) allows to permute the qubits in σ. Thereby, π is a permutation and $\prod$ is the corresponding unitary operator.

The Rule (R-Prob$_{\mathsf{CQS}}$) reduces a probability distribution with $r > 0$ to a single of its configurations $(\sigma_j; \phi; P\{\mathsf{b}(j)/v\})$ with non-zero probability p_j. In contrast to [GN05] we drop the label indicating the probability p_j of the chosen case. The rules (R-New$_{\mathsf{CQS}}$) and (R-Qbit$_{\mathsf{CQS}}$) create new channels and qubits and update the list of channel names or the qubit vector. Thereby, a new qubit is initialised to $|0\rangle$ and $|\psi\rangle \otimes |0\rangle$ is reshaped into a $\left(2^{n+1}\right)$-vector. The Rule (R-Comm$_{\mathsf{CQS}}$) defines communication in the style of the π-calculus. Rule (R-Par$_{\mathsf{CQS}}$) allows reduction to take place under parallel contexts and Rule (R-Cong$_{\mathsf{CQS}}$) enables the use of structural congruence as in the π-calculus. The structural congruence of CQS is defined, similarly to [GN05], as the smallest congruence containing α-equivalence that is closed under the following rules:

$$P \mid 0 \equiv P \qquad P \mid Q \equiv Q \mid P \qquad P \mid (Q \mid R) \equiv (P \mid Q) \mid R$$

Moreover, $(\sigma; \phi; P) \equiv (\sigma'; \phi; Q)$ if $P \equiv Q$ and $\sigma = \sigma'$ or if $(\sigma'; \phi; Q)$ is obtained from $(\sigma; \phi; P)$ by alpha conversion on the qubit names in σ. Finally, Rule (R-Cond$_{\mathsf{CQS}}$) unguards the continuation P of a conditional if its condition is satisfied, which checks equality of two binary numbers b and b'.

As CQP also CQS is augmented with a type system to ensure that two parallel components cannot share access to the same qubits, which is the realisation of the no-cloning principle of qubits in CQP. We use a very simple type system compared to [GN05], which is possible since we significantly simplified CQS in comparison to CQP and since we require the sets $\mathcal{N}$, $\mathcal{V}$, and $\mathcal{B}$ to be pairwise distinct. Remember that we equate configurations and terms modulo alpha conversion. We use this in the type system to ensure that there are no name clashes, i.e., that no two bound variables have the same name and no bound variable has the same name as a free variable. We extend this convention to also require that no variable of a qubit has the name q_i for any natural number i such that (R-Qbit$_{\mathsf{CQS}}$) does not cause name clashes. The CQS *types*, denoted by $\mathfrak{T}_{\mathsf{C}}$, are given by:

$$T ::= \mathsf{Bin} \quad | \quad \mathsf{Op}(n)$$

The data type Bin is used for binary numbers. The type $\mathsf{Op}(n)$ is used for unitary transformations that are applied to n qubits.

Type *judgements* for processes are of the form $\Sigma \vdash P$, where Σ is a set of qubit names and $P \in \mathfrak{P}_{\mathsf{C}}$. The set Σ is supposed to contain all free qubit names in the process as we show in Lemma 3.2. A type judgement $\Sigma \vdash P$ holds if it can be derived from the rules in Figure 2. These rules are inspired by [GN05]. By Rule (T-Par) parallel processes do not use the same qubits, since they can be typed w.r.t. to distinct sets Σ_1 and Σ_2. Rule (T-In) checks that the variable used in inputs is from $\mathcal{V}$ but not yet known to the continuation P, i.e., not in Σ. Conversely, (T-Out) ensures that the transmitted qubit x in outputs was known before, i.e., in $x \in \mathcal{V} \cup \Sigma$, but is no longer available to the continuation P after sending it away. To ensure the latter, P is checked against $\Sigma \setminus \{x\}$. Rule (T-Qbit) checks whether the new qubit x was not known before by $x \in \mathcal{V} \setminus \Sigma$ and then adds x to Σ for the analyse of the remaining process. The remaining rules are self-explanatory.

We show three properties of the type system. Since the focus of this paper is on encodability criteria and not type systems of process calculi, the proofs of these properties

$$\text{(T-Bin)}\ \frac{b \text{ is a binary number}}{\vdash b{:}\mathsf{Bin}} \qquad \text{(T-Op)}\ \frac{U \text{ is a unitary transformation on } n \text{ qubits}}{\vdash U{:}\mathsf{Op}(n)}$$

$$\text{(T-Nil)}\ \Sigma \vdash \mathbf{0} \qquad \text{(T-Suc)}\ \Sigma \vdash \checkmark \qquad \text{(T-Par)}\ \frac{\Sigma_1 \vdash P \quad \Sigma_2 \vdash Q \quad \Sigma_1 \cap \Sigma_2 = \emptyset}{\Sigma_1 \cup \Sigma_2 \vdash P \mid Q}$$

$$\text{(T-In)}\ \frac{c \in \mathcal{N} \quad x \in \mathcal{V} \setminus \Sigma \quad \Sigma \cup \{x\} \vdash P}{\Sigma \vdash c?[x].P} \qquad \text{(T-Out)}\ \frac{c \in \mathcal{N} \quad x \in \mathcal{V} \cap \Sigma \quad \Sigma \setminus \{x\} \vdash P}{\Sigma \vdash c![x].P}$$

$$\text{(T-Trans)}\ \frac{x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma \quad \vdash U{:}\mathsf{Op}(n) \quad \Sigma \vdash P}{\Sigma \vdash \{x_1, \ldots, x_n \mathrel{*}= U\}.P} \qquad \text{(T-New)}\ \frac{c \in \mathcal{N} \quad \Sigma \vdash P}{\Sigma \vdash (\mathsf{new}\ c)P}$$

$$\text{(T-Msure)}\ \frac{v \in \mathcal{B} \quad x_1, \ldots x_n \in \mathcal{V} \cap \Sigma \quad \Sigma \vdash P}{\Sigma \vdash (v := \mathsf{measure}\ x_1, \ldots, x_n).P} \qquad \text{(T-Qbit)}\ \frac{x \in \mathcal{V} \setminus \Sigma \quad \Sigma \cup \{x\} \vdash P}{\Sigma \vdash (\mathsf{qubit}\ x)P}$$

$$\text{(T-Cond)}\ \frac{(bv \in \mathcal{B} \vee \vdash bv{:}\mathsf{Bin}) \quad (bv' \in \mathcal{B} \vee \vdash bv'{:}\mathsf{Bin}) \quad \Sigma \vdash P}{\Sigma \vdash \mathsf{if}\ bv = bv'\ \mathsf{then}\ P}$$

Figure 2: Typing Rules for CQS

can be found in the Appendix A. First we capture the intuition behind Σ, as capturing at least all free qubit names of a process.

Lemma 3.2 (Free Qubits)**.** *If* $\Sigma \vdash P$ *then* $\mathsf{fq}(P) \subseteq \Sigma$.

Then we have the standard preservation property.

Lemma 3.3 (Preservation)**.** *If* $\Sigma \vdash P$ *and* $(\sigma; \phi; P) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; P_i)$ *or if* $\Sigma \vdash P'_k$ *for all* $0 \leq k < 2^t$ *and* $\boxplus_{0 \leq k < 2^t} p'_k \bullet (\sigma; \phi; P'_k) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; P_i)$ *then there is some* $\Sigma' \in \{\Sigma, \Sigma \cup \{q_n\}\}$ *for some fresh* q_n *such that* $\Sigma' \vdash P_i$ *for all* $0 \leq i < 2^r$.

Finally, Lemma 3.2 ensures the no-cloning principle for well-typed CQS-terms, since their parallel components cannot have access to the same qubit. With Lemma 3.3 the principle is then also preserved in all derivatives.

Lemma 3.4 (Unique Ownership of Qubits)**.** *If* $\Sigma \vdash P \mid Q$ *then* $\mathsf{fq}(P) \cap \mathsf{fq}(Q) = \emptyset$.

Note that Lemma 3.4 is an adaptation of the Theorem 2 in [GN05]—that there ensures the no cloning principle—to the present simpler type system.

As an example in CQS we consider an implementation of the quantum teleportation protocol [BBC$^+$93]. The quantum teleportation protocol is a procedure for transmitting a quantum state via a non-quantum medium. This protocol is particularly important: not only it is a fundamental component of several more complex protocols, but it is likely to be a key enabling technology for the development of the quantum repeaters [DRMT$^+$04] which will be necessary in large-scale quantum communication networks. The following example is an adaptation of the quantum teleportation example in Figure 3 of [GN05] adapted to CQS. Note that the original quantum teleportation protocol in [BBC$^+$93, GN05] does not require to transmit qubits but only two bits of classical information obtained from measuring qubits. Since we stripped CQS from the ability to transmit classical information, we have to cheat in the following example. After measuring the relevant qubits, the qubits themselves and not the result of their measurement is transmitted. However, since measurement transfers the respective qubits into base states, the respective communication does not carry any additional information than the result of measurement. Of course the relevance of quantum teleportation steams from the fact that the original protocol does not need to transfer qubits.

Example 3.5 (Quantum Teleportation)**.** Consider the CQS-configuration S

$$S = \left(q_0, q_1, q_2 = \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{\sqrt{2}}|111\rangle; \emptyset; \mathit{System}(q_0, q_1, q_2) \right)$$

where

$$\begin{aligned}
\mathit{System}(q_0, q_1, q_2) &= (\mathsf{new}\ c)\,(\mathit{Alice}(q_0, q_1) \mid \mathit{Bob}(q_2)) \\
\mathit{Alice}(q_0, q_1) &= \{q_0, q_1 *= \mathsf{CNOT}\}.\{q_0 *= \mathcal{H}\}.(v_0 := \mathsf{measure}\ q_0, q_1).c![q_0].c![q_1].\mathbf{0} \\
\mathit{Bob}(q_2) &= c?[x_0].c?[x_1].(v := \mathsf{measure}\ x_0, x_1).\big(\mathsf{if}\ v = 00\ \mathsf{then}\ \checkmark \\
&\quad \mid \mathsf{if}\ v = 01\ \mathsf{then}\ \{q_2 *= \mathcal{X}\}.\checkmark \mid \mathsf{if}\ v = 10\ \mathsf{then}\ \{q_2 *= \mathcal{Z}\}.\checkmark \\
&\quad \mid \mathsf{if}\ v = 11\ \mathsf{then}\ \{q_2 *= \mathcal{Y}\}.\checkmark\big)
\end{aligned}$$

Alice and Bob each possess one qubit (q_1 for Alice and q_2 for Bob) of an entangled pair in state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. q_0 is the second qubit owned by Alice. Within this example it is in state $|1\rangle$, but in general it can be in an arbitrary state. It is the qubit whose state will be teleported to q_2 and therefore to Bob.

By Figure 1, S can do the following steps

$$\begin{aligned}
S &\longmapsto (|\psi_0\rangle; c; \mathit{Alice}(q_0, q_1) \mid \mathit{Bob}(q_2)) \\
&\longmapsto (|\psi_1\rangle; c; \{q_1 *= \mathcal{H}\}.(v_0 := \mathsf{measure}\ q_0, q_1).c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \\
&\longmapsto (|\psi_2\rangle; c; (v_0 := \mathsf{measure}\ q_0, q_1).c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \\
&\longmapsto \frac{1}{4} \bullet (q_0, q_1, q_2, = |001\rangle; c; c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \boxplus \\
&\qquad \frac{1}{4} \bullet (q_0, q_1, q_2, = |010\rangle; c; c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \boxplus \\
&\qquad \frac{1}{4} \bullet (q_0, q_1, q_2, = |101\rangle; c; c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \boxplus \\
&\qquad \frac{1}{4} \bullet (q_0, q_1, q_2, = |110\rangle; c; c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) = S^*
\end{aligned}$$

with $|\psi_0\rangle = q_0, q_1, q_2 = \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{\sqrt{2}}|111\rangle$, $|\psi_1\rangle = q_0, q_1, q_2 = \frac{1}{\sqrt{2}}|110\rangle + \frac{1}{\sqrt{2}}|101\rangle$, and $|\psi_2\rangle = q_0, q_1, q_2 = \frac{1}{2}|001\rangle + \frac{1}{2}|010\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle$.

All configurations within the probability distribution in S^* have the same probability. We can e.g. choose the first one by using Rule (R-PROB$_{\mathsf{CQS}}$) with $|\psi_3\rangle = q_0, q_1, q_2 = |001\rangle$.

$$\begin{aligned}
S^* &\longmapsto (|\psi_3\rangle; c; c![q_0].c![q_1].\mathbf{0} \mid \mathit{Bob}(q_2)) \\
&\longmapsto \left(|\psi_3\rangle; c; \begin{array}{l} c![q_1].\mathbf{0} \mid c?[x_1].(v := \mathsf{measure}\ q_0, x_1).\big(\mathsf{if}\ v = 00\ \mathsf{then}\ \checkmark \\ \mid \mathsf{if}\ v = 01\ \mathsf{then}\ \{q_2 *= \mathcal{X}\}.\checkmark \mid \mathsf{if}\ v = 10\ \mathsf{then}\ \{q_2 *= \mathcal{Z}\}.\checkmark \\ \mid \mathsf{if}\ v = 11\ \mathsf{then}\ \{q_2 *= \mathcal{Y}\}.\checkmark\big) \end{array} \right) \\
&\longmapsto \left(|\psi_3\rangle; c; \begin{array}{l} (v := \mathsf{measure}\ q_0, q_1).\big(\mathsf{if}\ v = 00\ \mathsf{then}\ \checkmark \mid \mathsf{if}\ v = 01\ \mathsf{then}\ \{q_2 *= \mathcal{X}\}.\checkmark \\ \mid \mathsf{if}\ v = 10\ \mathsf{then}\ \{q_2 *= \mathcal{Z}\}.\checkmark \mid \mathsf{if}\ v = 11\ \mathsf{then}\ \{q_2 *= \mathcal{Y}\}.\checkmark\big) \end{array} \right) \\
&\longmapsto \left(|\psi_3\rangle; c; \begin{array}{l} \mathsf{if}\ 00 = 00\ \mathsf{then}\ \checkmark \mid \mathsf{if}\ 00 = 01\ \mathsf{then}\ \{q_2 *= \mathcal{X}\}.\checkmark \\ \mid \mathsf{if}\ 00 = 10\ \mathsf{then}\ \{q_2 *= \mathcal{Z}\}.\checkmark \mid \mathsf{if}\ 00 = 11\ \mathsf{then}\ \{q_2 *= \mathcal{Y}\}.\checkmark \end{array} \right) \\
&\longmapsto \left(|\psi_3\rangle; c; \begin{array}{l} \checkmark \mid \mathsf{if}\ 00 = 01\ \mathsf{then}\ \{q_2 *= \mathcal{X}\}.\checkmark \\ \mid \mathsf{if}\ 00 = 10\ \mathsf{then}\ \{q_2 *= \mathcal{Z}\}.\checkmark \mid \mathsf{if}\ 00 = 11\ \mathsf{then}\ \{q_2 *= \mathcal{Y}\}.\checkmark \end{array} \right)
\end{aligned}$$

□

3.2. **A Calculus for Open Quantum Systems.** The algebra of quantum processes (qCCS) is first introduced in [FDJY07] and further investigated e.g. in [YFDJ09, FDY12, YKK14] as a process calculus for quantum based systems and to study observational equivalences in the quantum setting or in [KKK$^+$12, KKK$^+$13] to study quantum crypto protocols. As qCCS is designed to model open systems, its states are described by density matrices or operators. We are mainly interested in the variant of qCCS presented in [YFDJ09], because it has the rare feature of introducing a quantum based calculus without a probabilistic transition system. Indeed earlier as well as later variants of qCCS e.g. in [FDJY07, FDY12] use probabilistic transition systems. The main reason for probabilistic transition systems in most quantum based systems is measurement, since its outcome is often a probability distribution. In [YFDJ09] measurement can be performed by a super-operator and the resulting probability distribution on potentially different measurement results is captured in the density matrix that represents the state after measurement. Since they refrain from providing a measurement-operator, they can introduce a non-probabilistic transition system. Unfortunately, without a separate operator for measurement there is no way in [YFDJ09] to directly get the results of measurement; although the resulting alteration of the state does of course influence the further behaviour. Remember that the state of a qubit cannot be read but only measured, so it is not possible to extract this information directly from the state after measurement. Because of that, we add for OQS an additional operator, a conditional to compare binary numbers and the outcome of measurement, to the syntax of qCCS as presented in [FDJY07].

Definition 3.6 (OQS)**.** The OQS *terms*, denoted by $\mathfrak{P}_{\mathsf{O}}$, are given by:

$$\begin{aligned} P \;::=\; & A(\tilde{x}) \;\mid\; \mathsf{nil} \;\mid\; \tau.P \;\mid\; \mathcal{E}[X].P \;\mid\; c?x.P \;\mid\; c!x.P \\ & \mid\; P+P \;\mid\; P \parallel P \;\mid\; P \setminus L \;\mid\; \mathsf{if}\ bv = e\ \mathsf{then}\ P \end{aligned}$$

where

$$e \;::=\; bv \;\mid\; \mathcal{M}[X]$$

The OQS *configurations* $\mathfrak{C}_{\mathsf{O}}$ are given by $\langle P, \rho\rangle$, where $P \in \mathfrak{P}_{\mathsf{O}}$ and $\rho \in \mathfrak{D}(\mathfrak{H})$.

Process constants $A(\tilde{x})$, where $\tilde{x} = x_1, \ldots, x_n$ is a sequence of pairwise distinct quantum variables, allow recursive definitions of terms. An inactive process is denoted by nil and the term $\tau.P$ executes the silent action and proceeds as P. The application of a super-operator $\mathcal{E}$ on the qubits in the finite set $X \subseteq \mathcal{V}$ is performed by the term $\mathcal{E}[X].P$. The terms $c?x.P$ and $c!x.P$ model input and output on channel $c \in \mathcal{N}$ to transfer a single qubit $x \in \mathcal{V}$. Choice and parallel composition are obtained from CCS and given by $P + P$ and $P \parallel P$. The term $P \setminus L$ restricts the scope of all channels within $L \subseteq \mathcal{N}$ to P. Finally, the conditional $\mathsf{if}\ bv = e\ \mathsf{then}\ P$ continues as P if either bv and e are the same binary number or bv is the binary number that results from measuring w.r.t. the standard basis the finite set of qubits $X \subseteq \mathcal{V}$. We use $\mathcal{M}$ to denote the super-operator for measurement in the standard base.

By slightly abusing notation, we use $\mathcal{V}$ to also denote the current set of qubit names of a given density matrix ρ. The variable x is bound in P by $c?x.P$ and the channels in L are bound in P by $P \setminus L$. A variable/channel is free if it is not bound. Let $\mathsf{fc}(P)$ and $\mathsf{fq}(P)$ denote the sets of free channels and free qubits in P, respectively. For each process constant scheme A, a defining equation $A(\tilde{x}) \stackrel{def}{=} P$ with $P \in \mathfrak{P}_{\mathsf{O}}$ and $\mathsf{fq}(P) \subseteq \tilde{x}$ is assumed. As done

$$(\textsc{Tau}_{\mathsf{OQS}})\ \langle \tau.P, \rho\rangle \xrightarrow{\tau} \langle P, \rho\rangle \qquad (\textsc{Input}_{\mathsf{OQS}})\ \langle c?x.P, \rho\rangle \xrightarrow{c?y} \langle P\{y/x\}, \rho\rangle \quad y \notin \mathsf{fq}(c?x.P)$$

$$(\textsc{Output}_{\mathsf{OQS}})\ \langle c!x.P, \rho\rangle \xrightarrow{c!x} \langle P, \rho\rangle \qquad (\textsc{Oper}_{\mathsf{OQS}})\ \langle \mathcal{E}[X].P, \rho\rangle \xrightarrow{\tau} \langle P, \mathcal{E}_X(\rho)\rangle$$

$$(\textsc{Choice}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle P + Q, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle} \qquad (\textsc{Def}_{\mathsf{OQS}})\ \frac{\langle P\{\tilde{y}/\tilde{x}\}, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle A(\tilde{y}), \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle} \quad A(\tilde{x}) \stackrel{def}{=} P$$

$$(\textsc{Res}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle P \setminus L, \rho\rangle \xrightarrow{\alpha} \langle P' \setminus L, \rho'\rangle} \quad \mathsf{cn}(\alpha) \cap L = \emptyset$$

$$(\textsc{Intl}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle P \parallel Q, \rho\rangle \xrightarrow{\alpha} \langle P' \parallel Q, \rho'\rangle} \quad \text{if } \alpha = c?x \text{ then } x \notin \mathsf{fq}(Q)$$

$$(\textsc{Comm}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{c?x} \langle P', \rho\rangle \quad \langle Q, \rho\rangle \xrightarrow{c!x} \langle Q', \rho\rangle}{\langle P \parallel Q, \rho\rangle \xrightarrow{\tau} \langle P' \parallel Q', \rho\rangle} \qquad (\textsc{Red}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\tau} \langle P', \rho'\rangle}{\langle P, \rho\rangle \longmapsto \langle P', \rho'\rangle}$$

$$(\textsc{Cond}_{\mathsf{OQS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle \quad (e = b' \wedge b = b' \wedge \rho' = \rho) \vee (e = \mathcal{M}[X] \wedge b \in \mathcal{M}[X](\rho) \wedge \rho' = \mathcal{M}[X](\rho))}{\langle \mathsf{if}\ b = e\ \mathsf{then}\ P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}$$

Figure 3: Semantics of OQS

in [YFDJ09], we require the following two conditions:

$$c!x.P \in \mathfrak{P}_{\mathsf{O}} \text{ implies } x \notin \mathsf{fq}(P) \tag{Cond1}$$

$$P \parallel Q \in \mathfrak{P}_{\mathsf{O}} \text{ implies } \mathsf{fq}(P) \cap \mathsf{fq}(Q) = \emptyset \tag{Cond2}$$

These conditions ensure the no-cloning principle of qubits within qCCS and OQS.

The semantics of OQS is defined by the inference rules in Figure 3. We start with a labelled variant of the semantics from [YFDJ09] for qCCS, add the Rule ($\textsc{Cond}_{\mathsf{OQS}}$) for the new conditional, and then add the Rule ($\textsc{Red}_{\mathsf{OQS}}$) to obtain a reduction semantics. We omit the symmetric forms of the rules ($\textsc{Choice}_{\mathsf{OQS}}$), ($\textsc{Intl}_{\mathsf{OQS}}$), and ($\textsc{Comm}_{\mathsf{OQS}}$). Let $\mathsf{cn}(\alpha)$ return the possibly empty set of channels in the label α.

Rule ($\textsc{Oper}_{\mathsf{OQS}}$) implements the application of a super-operator $\mathcal{E}$. It updates the state of the configuration by applying $\mathcal{E}$. To simplify the definition of a reduction semantics, we use (in contrast to [YFDJ09]) the label τ.

Rule ($\textsc{Input}_{\mathsf{OQS}}$) ensures that the received qubits are fresh in the continuation of the input. The rules ($\textsc{Intl}_{\mathsf{OQS}}$) and its symmetric rule ($\textsc{Intr}_{\mathsf{OQS}}$) forbid to receive qubits within parallel contexts that do posses this qubit. Rule ($\textsc{Res}_{\mathsf{OQS}}$) allows to do a step under a restriction. Rule ($\textsc{Cond}_{\mathsf{OQS}}$) allows a step of the continuation of a conditional if its condition is satisfied. Therefore either b and e need to be the same binary number and then the state ρ is not updated or $e = \mathcal{M}[X]$ and b is one of the binary numbers that results from measuring in the standard basis the qubits in X in the state ρ with non-zero probability. In the latter case the state ρ has to be updated according to the measurement operation. For instance if ρ is a 2-qubit system with the qubits q_0, q_1 in state $|0\rangle\langle 0| \otimes |1\rangle\langle 1|$ then $\mathsf{if}\ 01 = \mathcal{M}[q_0, q_1]\ \mathsf{then}\ \tau.\mathsf{nil} \longmapsto \mathsf{nil}$ but $\mathsf{if}\ b = \mathcal{M}[q_0, q_1]\ \mathsf{then}\ P$ cannot reduce for any $b \neq 01$. Note that to decide whether $b \in \mathcal{M}[X]\{\rho\}$ the system indeed has to measure the qubits; it is not sufficient to apply any super-operator on ρ even if it has the same effect on

ρ as measurement. Since we cannot read the qubit we have to measure it, to learn anything about its state. The other rules are self-explanatory.

Similar to CQS, structural congruence for OQS is the smallest congruence containing α-equivalence that is closed under the following rules:

$$P \parallel \mathsf{nil} \equiv P \qquad P \parallel Q \equiv Q \parallel P \qquad P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R$$

Moreover, $\langle P, \rho\rangle \equiv \langle Q, \rho\rangle$ if $P \equiv Q$ or if $\langle Q, \rho\rangle$ is obtained from $\langle P, \rho\rangle$ by alpha conversion on the qubit names in $\mathcal{V}$.

4. Encodings and Quality Criteria

Let $\mathfrak{L}_\mathsf{S} = \langle \mathfrak{C}_\mathsf{S}, \longmapsto_\mathsf{S}\rangle$ and $\mathfrak{L}_\mathsf{T} = \langle \mathfrak{C}_\mathsf{T}, \longmapsto_\mathsf{T}\rangle$ be two process calculi, denoted as *source* and *target* language. An *encoding* from $\mathfrak{L}_\mathsf{S}$ into $\mathfrak{L}_\mathsf{T}$ is a function $[\![\cdot]\!] : \mathfrak{C}_\mathsf{S} \to \mathfrak{C}_\mathsf{T}$. We often use $S, S', \ldots$ and $T, T', \ldots$ to range over $\mathfrak{C}_\mathsf{S}$ and $\mathfrak{C}_\mathsf{T}$, respectively.

To analyse the quality of encodings and to rule out trivial or meaningless encodings, they are augmented with a set of quality criteria. In order to provide a general framework, Gorla in [Gor10] suggests five criteria well suited for language comparison. They are divided into two structural and three semantic criteria. The structural criteria include (1) *compositionality* and (2) *name invariance*. The semantic criteria are (3) *operational correspondence*, (4) *divergence reflection*, and (5) *success sensitiveness*. We start with these criteria for classical systems.

Note that a behavioural relation $\preceq$ on the target is assumed for operational correspondence. Moreover, $\preceq$ needs to be success sensitive, i.e., $T_1 \preceq T_2$ implies $T_1 \Downarrow_\checkmark$ iff $T_2 \Downarrow_\checkmark$. As discussed in [PvG15], we pair operational correspondence as of [Gor10] with correspondence simulation.

Definition 4.1 (Correspondence Simulation, [PvG15])**.** A relation $\mathcal{R}$ is a *(weak) labelled correspondence simulation* if for each $(T_1, T_2) \in \mathcal{R}$:

- For all $T_1 \xrightarrow{\alpha} T_1'$, there exists T_2' such that $T_2 \xrightarrow{\alpha} T_2'$ and $(T_1', T_2') \in \mathcal{R}$.
- For all $T_2 \xrightarrow{\alpha} T_2'$, there exists T_1'', T_2'' such that $T_1 \Longmapsto\!\!\xrightarrow{\alpha} T_1''$, $T_2' \Longmapsto T_2''$, and $(T_1'', T_2'') \in \mathcal{R}$.
- $T_1 \Downarrow_\checkmark$ iff $T_2 \Downarrow_\checkmark$.

T_1 and T_2 are *correspondence similar*, denoted as $T_1 \preceq T_2$, if a correspondence simulation relates them.

Intuitively, an encoding is compositional if the translation of an operator is the same for all occurrences of that operator in a term. Hence, the translation of that operator can be captured by a context that is allowed in [Gor10] to be parametrised on the free names of the respective source configuration.

Definition 4.2 (Compositionality, [Gor10])**.** The encoding $[\![\cdot]\!]$ is *compositional* if, for every operator **op** with arity n of $\mathfrak{L}_\mathsf{S}$ and for every subset of names N, there exists a context $\mathcal{C}^N_{\mathbf{op}}([\cdot]_1, \ldots, [\cdot]_n)$ such that, for all $S_1, \ldots, S_n$ with $\mathsf{fc}(S_1) \cup \ldots \cup \mathsf{fc}(S_n) = N$, it holds that $[\![\mathbf{op}\,(S_1, \ldots, S_n)]\!] = \mathcal{C}^N_{\mathbf{op}}([\![S_1]\!], \ldots, [\![S_n]\!])$.

Name invariance ensures that encodings are independent of specific variables in the source. In [Gor10] name invariance is defined modulo a so-called renaming policy. Since our encoding in Section 5 translates variables to themselves and name invariance is not relevant for the separation result in Section 6, we do not need a renaming policy. This simplifies the

definition of name invariance such that an encoding is name invariant if it preserves and reflects substitutions.

Definition 4.3 (Name Invariance)**.** The encoding $[\![\cdot]\!]$ is *name invariant* if, for every $S \in \mathfrak{C}_{\mathsf{S}}$ and every substitution γ on names, it holds that $[\![S\gamma]\!] = [\![S]\!]\gamma$.

The first semantic criterion is operational correspondence. It consists of a soundness and a completeness condition. *Completeness* requires that every computation of a source term can be emulated by its translation. *Soundness* requires that every computation of a target term corresponds to some computation of the corresponding source term.

Definition 4.4 (Operational Correspondence, [Gor10])**.** An encoding $[\![\cdot]\!]$ is *operationally corresponding* w.r.t. $\preceq$ if it is:

Complete: For all $S \Longmapsto S'$, there exists T such that $[\![S]\!] \Longmapsto T$ and $[\![S']\!] \preceq T$.

Sound: For all $[\![S]\!] \Longmapsto T$, there exists S', T' such that $S \Longmapsto S'$, $T \Longmapsto T'$, and $[\![S']\!] \preceq T'$.

The next criterion concerns the role of infinite computations.

Definition 4.5 (Divergence Reflection, [Gor10])**.** An encoding $[\![\cdot]\!]$ *reflects divergence* if, for every S, $[\![S]\!] \longmapsto^{\omega}$ implies $S \longmapsto^{\omega}$.

The last criterion links the behaviour of source terms to the behaviour of their encodings. Success sensitiveness requires that source configurations reach success if and only if their literal translations do.

Definition 4.6 (Success Sensitiveness, [Gor10])**.** $[\![\cdot]\!]$ is *success sensitive* if, for every S, $S{\Downarrow_{\checkmark}}$ iff $[\![S]\!]{\Downarrow_{\checkmark}}$.

Moreover, $\preceq$ needs to be success sensitive, i.e., $T_1 \preceq T_2$ implies $T_1{\Downarrow_{\checkmark}}$ iff $T_2{\Downarrow_{\checkmark}}$, as required by Definition 4.1. Without this requirement the relation that is induced—as described in [PvG15, Pet19]—by operational correspondence between the source and target is trivial without some notion of barbs. To some up, we use the following notion of *good* encoding, where good refers to classical criteria only.

Definition 4.7 (Classical Criteria)**.** The encoding $[\![\cdot]\!]$ is good, if it is compositional, name invariant, operational corresponding w.r.t. $\preceq$, divergence reflecting, and success sensitive, where $\preceq$ is success sensitive.

There are several other criteria for classical systems that we could have considered (cf. [Pet19]). Since CQS is a typed language, we may consider a criterion for types as discussed e.g. in [KPY16]. As only one language is typed, it suffices to require that the encoding is defined for all terms of the source language. We could also consider a criterion for the preservation of distributability as discussed e.g. in [PNG13], since distribution and communication between distributed locations is of interest. Indeed our encoding satisfies this criterion, because it translates the parallel operator homomorphically. However, already the basic framework of Gorla, on that we rely here, suffices to observe principal design principles of quantum based systems as we discuss with the no-cloning property in Section 7.

5. Encoding Quantum Based Systems

Our encoding, from well-typed CQS-configurations into OQS-configurations that satisfy the conditions Cond1 and Cond2, is given by Definition 5.1.

Definition 5.1 (Encoding $[\![\cdot]\!]$ from CQS into OQS)**.**

$$
\begin{aligned}
[\![(\sigma;\phi;P)]\!] &= \langle [\![P]\!] \setminus \phi, \rho_\sigma \rangle \\
[\![\boxplus_{0\le i<2^r} p_i \bullet (\sigma_i;\phi;P\{\mathsf{b}(i)/v\})]\!] &= \langle \mathsf{D}(q_0,\ldots,q_{r-1};v;[\![P]\!]) \setminus \phi, \rho_\boxplus \rangle \\
[\![\mathbf{0}]\!] &= \mathsf{nil} \\
[\![P \mid Q]\!] &= [\![P]\!] \parallel [\![Q]\!] \\
[\![c?[x].P]\!] &= c?x.[\![P]\!] \\
[\![c![q].P]\!] &= c!q.[\![P]\!] \\
[\![\{\tilde{q} *= U\}.P]\!] &= U[\tilde{q}].[\![P]\!] \\
[\![(v := \mathsf{measure}\ \tilde{q}).P]\!] &= \mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q};v;[\![P]\!]) \\
[\![(\mathsf{new}\ c)P]\!] &= \tau.([\![P]\!] \setminus \{c\}) \\
[\![(\mathsf{qubit}\ x)P]\!] &= \mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P]\!]\{q_{|\mathcal{V}|}/x\}\big) \\
[\![\mathsf{if}\ bv = bv'\ \mathsf{then}\ P]\!] &= \mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P]\!] \\
[\![\checkmark]\!] &= \checkmark
\end{aligned}
$$

where $\rho_\sigma = |\psi\rangle\langle\psi|$ for $\sigma = |\psi\rangle$, $\rho_\boxplus = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for $\sigma_i = |\psi_i\rangle$,

$$
\mathsf{D}(\tilde{q};v;Q) = \begin{cases} Q & \text{, if } \tilde{q} \text{ is empty} \\ \mathsf{if}\ 0..0 = \mathcal{M}[\tilde{q}]\ \mathsf{then}\ \tau.Q\{0..0/v\} + \ldots + & \text{, otherwise} \\ \mathsf{if}\ \mathsf{b}\big(2^{|\tilde{q}|-1}\big) = \mathcal{M}[\tilde{q}]\ \mathsf{then}\ \tau.Q\big\{\mathsf{b}\big(2^{|\tilde{q}|-1}\big)/v\big\} & \end{cases},
$$

$\mathcal{E}_{|0\rangle}[\mathcal{V}]$ adds a new qubit $q_{|\mathcal{V}|}$ initialised with 0 to the current state ρ.

The translation of configurations maps the vector σ to the density matrix ρ_σ (obtained by the outer product) and restricts all names in ϕ to the translation of the sub-term. In the translation of probability distributions, the state $\rho_\boxplus$ is the sum of the density matrices obtained from the σ_i multiplied with their respective probability. Again, the names in ϕ are restricted in the translation. The nondeterminism in choosing one of the possible branches of the probability distribution in CQS by (R-Prob$_{\mathsf{CQS}}$) is translated into the OQS-choice $\mathsf{D}(\tilde{q};v;[\![P]\!])$ with $\tilde{q} = q_0,\ldots,q_{r-1}$, where each case is guarded by a conditional to compare to a possible outcome of measurement followed by the continuation with a substitution to hand the result of measurement to the process. Note that, the translation of a configuration $(\sigma;\phi;P)$ is a special case of the second line. A practical motivated encoding example using such a OQS-choice is given in Example 5.15.

The application of unitary transformations and the creation of new qubits are translated to the corresponding super-operators. Measurement is translated into the super-operator for measurement followed by the choice $\mathsf{D}(\tilde{q};v;[\![P]\!])$ over the branches of the possible outcomes of measurement, i.e., after the first measurement the translation is similar to the translation of a probability distribution in the second case. Note that we measure twice in this translation. The outer measurement—that is a super-operator for measurement—dissolves entanglement on the measured qubits and ensures that the density matrix after this first measurement is the sum of the density matrices of the respective cases in the distribution (compare with

$\rho_{\boxplus}$ and Example 5.2). The measurements within $\mathsf{D}(\tilde{q}; v; [\![P]\!])$—that are not performed by a super-operator but require to indeed physically measure the qubits—then check whether the respective case i occurs with non-zero probability and adjust the density matrix to this result of measurement if case i is picked. The creation of new channel names is translated to restriction, where a τ-guard simulates the step that is necessary in CQS to create a new channel. The restriction ensures that this new name cannot be confused with any other translated source term name. Since in the derivative of a source term step creating a new channel the new channel is added to ϕ in the configuration, we restrict all channels in ϕ. A condition in CQS is translated to a conditional in OQS. We add a τ to guard the continuation of the conditional in the target, since resolving a conditional in CQS (in contrast to OQS) requires a step. The remaining translations are homomorphic.

Example 5.2. Consider the CQS-configuration $S = (\sigma; \phi; (v := \mathsf{measure}\ q_0).P)$, where $\sigma = q_0, q_1 = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = |\psi\rangle$ consists of two entangled qubits. By Rule (R-Measure$_{\mathsf{CQS}}$) in Figure 1, $S \longmapsto S' = \frac{1}{2} \bullet (\sigma = q_0, q_1 = |00\rangle; \phi; P\{00/v\}) \boxplus \frac{1}{2} \bullet (\sigma = q_0, q_1 = |11\rangle; \phi; P\{11/x\})$, where we omitted branches with probability zero.

By Definition 5.1, $[\![S]\!] = \langle (\mathcal{M}[q_0].\mathsf{D}(q_0; v; [\![P]\!])) \setminus \phi, \rho\rangle$ with $\rho = |\psi\rangle\langle\psi|$. By the rules (Oper$_{\mathsf{OQS}}$) and (Red$_{\mathsf{OQS}}$) in Figure 3, then $[\![S]\!] \longmapsto T = \langle \mathsf{D}(q_0; x; [\![P]\!]) \setminus \phi, \mathcal{M}_{q_0}(\rho)\rangle$. Accordingly, the probability distribution in S' is mapped on a choice in T. The outer measurement $\mathcal{M}[q_0]$ resolves the entanglement and yields a density matrix that is the sum of the density matrices of the choice branches, i.e., $\mathcal{M}_{q_0}(\rho) = |00\rangle\langle 00|\rho|00\rangle\langle 00|^\dagger + |11\rangle\langle 11|\rho|11\rangle\langle 11|^\dagger$. □

By analysing the encoding function, we observe that for all source terms the type system of CQS ensures that their literal translation satisfies the conditions Cond1 and Cond2. Hence, the encoding is defined on all source terms.

Corollary 5.3. *For all $S \in \mathfrak{C}_{\mathsf{C}}$ the term $[\![S]\!]$ is defined.*

Before we can start to prove the quality of our encoding, i.e., that it satisfies the criteria in Definition 4.7, we have to fix a relation $\preceq$ on the target language OQS that is used in the definition of operational correspondence in Definition 4.4. We instantiate $\preceq$ with correspondence similarity as given in Definition 4.1. In the literature, operational correspondence is often considered w.r.t. a bisimulation on the target; simply because bisimilarity is a standard behavioural equivalence in process calculi, whereas correspondence simulation is not. For our encoding, we cannot use bisimilarity.

Example 5.4. Consider $S = (\sigma; c; (v := \mathsf{measure}\ q).P \mid Q)$, where S is a 1-qubit system with $\sigma = q = |+\rangle$ and $P, Q \in \mathfrak{P}_{\mathsf{C}}$ with $\mathsf{fc}(P) = \{c\} = \mathsf{fc}(Q)$ and $v \notin \mathsf{fv}(Q)$. By the rules (R-Measure$_{\mathsf{CQS}}$) and (R-Par$_{\mathsf{CQS}}$) of Figure 1,

$$S \longmapsto S' = \frac{1}{2} \bullet (\sigma = q = |0\rangle; c; P\{0/v\} \mid Q) \boxplus \frac{1}{2} \bullet (\sigma = q = |1\rangle; c; P\{1/v\} \mid Q)\,,$$

i.e., (R-Par$_{\mathsf{CQS}}$) pulls the parallel component Q into the probability distribution that results from measuring q. Since our encoding is compositional—and indeed we require compositionality, the translation $[\![S]\!]$ behaves slightly differently. By Definition 5.1, $[\![S]\!] = \langle (\mathcal{M}[q].\mathsf{D}(q; v; [\![P]\!]) \parallel [\![Q]\!]) \setminus \{c\}, \rho\rangle$, where here $\mathsf{D}(q; v; [\![P]\!]) = \mathsf{if}\ 0 = \mathcal{M}[q]\ \mathsf{then}\ \tau.[\![P]\!]\{0/v\} + \mathsf{if}\ 1 = \mathcal{M}[q]\ \mathsf{then}\ \tau.[\![P]\!]\{1/v\}$, $\rho = |+\rangle\langle +|$, and $[\![S']\!] = \langle \mathsf{D}(q; v; [\![P]\!] \parallel [\![Q]\!]) \setminus \{c\}, \rho'\rangle$ with $\rho' = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. By Figure 3, $[\![S]\!] \longmapsto T = \langle (\mathsf{D}(q; v; [\![P]\!]) \parallel [\![Q]\!]) \setminus \{c\}, \rho'\rangle$, because $\mathcal{M}_q(\rho) = \rho'$. Unfortunately, $[\![S']\!]$ and T are not bisimilar. As a counterexample consider

$P = c![q].\mathbf{0}$ and $Q = (\mathsf{new}\ c')c?[x].(v := \mathsf{measure}\ x).\mathsf{if}\ v = 0\ \mathsf{then}\ \checkmark$. The problem is, that a step on $[\![Q]\!]$ in $[\![S']\!]$ forces us to immediately pick a case and resolve the choice, whereas after performing the same step on $[\![Q]\!]$ in T all cases of the choice remain available. After emulating the first step of $[\![Q]\!]$ in $[\![S']\!]$, either we reach a configuration that has to reach success eventually or we reach a configuration that cannot reach success; whereas there is just one way to do the respective step in T and in the resulting configuration success may or may not be reached depending on the next step. Fortunately, $[\![S']\!]$ and T are correspondence similar. □

The encoding $[\![\cdot]\!]$ in Definition 5.1 emulates a source term step by exactly one step on the target, except for source term steps on (R-Perm$_{\mathsf{CQS}}$) that are not emulated at all. Steps on (R-Perm$_{\mathsf{CQS}}$) are necessary in CQP and CQS, because they assume that unitary transformations and measurement is always applied to the first r qubits. With (R-Perm$_{\mathsf{CQS}}$) the quantum register is permuted to bring the relevant qubits to the front. In OQS this is not necessary. Lemma 5.5 captures this observation, by showing that the translation of source term steps on (R-Perm$_{\mathsf{CQS}}$) are indistinguishable in the target modulo $\preceq$.

Lemma 5.5. *If $S \longmapsto S'$ is by* (R-Perm$_{\mathsf{CQS}}$)*, then $[\![S]\!] \preceq [\![S']\!]$ and $[\![S']\!] \preceq [\![S]\!]$.*

Proof. Since $S \longmapsto S'$ is by (R-Perm$_{\mathsf{CQS}}$), there are $q_0, \ldots, q_{n-1}, \psi, \phi, P, \pi$, and Π such that:

$$S = (q_0, \ldots, q_{n-1} = |\psi\rangle; \phi; P) \quad \text{and} \quad S' = \big(q_{\pi(0)}, \ldots, q_{\pi(n-1)} = \Pi|\psi\rangle; \phi; P\pi\big)$$

Let $|\psi'\rangle = \Pi|\psi\rangle$ be the state that results from applying the unitary transformation Π. Then $[\![S]\!] = \langle [\![P]\!] \setminus \phi, \rho\rangle$ with $\rho = |\psi\rangle\langle\psi|$ and $[\![S']\!] = \langle [\![P\pi]\!] \setminus \phi, \rho'\rangle$ with $\rho' = |\psi'\rangle\langle\psi'|$. Note that, $\Pi_{q_0,\ldots,q_{n-1}}(\rho) = \rho'$, where $\Pi[q_0, \ldots, q_{n-1}]$ is the super-operator obtained from the unitary transformation Π. By Lemma 5.8, $[\![S']\!] = \langle [\![P\pi]\!] \setminus \phi, \rho'\rangle = \langle ([\![P]\!]\pi) \setminus \phi, \rho'\rangle$. Since OQS-terms such as $[\![P]\!] \setminus \phi$ and $([\![P]\!]\pi) \setminus \phi$ do not address qubits by their position in the density matrix but their name, $\mathcal{R} = \left\{ \left(\langle Q, \rho_Q\rangle, \left\langle Q\pi, \rho'_Q \right\rangle \right) \mid \Pi_{q_0,\ldots,q_{n-1}}(\rho_Q) = \rho'_Q \right\}$ is a bisimulation and thus $\mathcal{R}$ as well as $\mathcal{R}^{-1}$ are correspondence simulations. Then $[\![S]\!] \preceq [\![S']\!]$ and $[\![S']\!] \preceq [\![S]\!]$. □

Since structural congruence is defined similarly on CQS and OQS, does consider in both cases only alpha conversion, the inactive process, and parallel composition, and since $[\![\cdot]\!]$ translates the inactive process and parallel composition homomorphically, the encoding preserves structural congruence.

Lemma 5.6 (Preservation of Structural Congruence, $[\![\cdot]\!]$)**.**

$$\forall C_1, C_2 \in \mathfrak{C}_{\mathsf{C}}.\ C_1 \equiv C_2 \textit{ implies } [\![C_1]\!] \equiv [\![C_2]\!] \qquad \textit{and}$$
$$\forall S_1, S_2 \in \mathfrak{P}_{\mathsf{C}}.\ S_1 \equiv S_2 \textit{ implies } [\![S_1]\!] \equiv [\![S_2]\!]$$

Proof. By straightforward induction on the rules of structural congruence. □

By [Gor10], good encodings are allowed to use a renaming policy that structures the way in that the translations of source term names are used in target terms and how to treat names that are introduced by the encoding function. The encoding $[\![\cdot]\!]$ simply translates names by themselves and does not introduce any other names. Because of that, we can choose the identity relation as renaming policy and are able to prove a stronger variant of name invariance. Note that, name invariance considers substitutions on names only.

Lemma 5.7 (Name Invariance, $[\![\cdot]\!]$)**.** *Let γ be a substitution on names.*

$$\forall S_C \in \mathfrak{C}_{\mathsf{C}}.\ [\![S_C\gamma]\!] = [\![S_C]\!]\gamma \quad \textit{and} \quad \forall S \in \mathfrak{P}_{\mathsf{C}}.\ [\![S\gamma]\!] = [\![S]\!]\gamma$$

Proof. Assume a substitution γ on names. Let $S_C = (\sigma; \phi; S)$. Then $S_C\gamma = (\sigma; \phi\gamma; S\gamma)$. Moreover, let $\sigma = |\psi\rangle$ and $\rho = |\psi\rangle\langle\psi|$. Then $[\![S_C\gamma]\!] = \langle [\![S\gamma]\!] \setminus (\phi\gamma), \rho\rangle = \langle ([\![S]\!]\gamma) \setminus (\phi\gamma), \rho\rangle = \langle [\![S]\!] \setminus \phi, \rho\rangle\,\gamma = [\![S_C]\!]\gamma$ holds if $[\![S\gamma]\!] = [\![S]\!]\gamma$.

Similarly, let $S_C = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi; S\{\mathsf{b}(i)/v\})$. Then we have $S_C\gamma = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi\gamma; S\{\mathsf{b}(i)/v\}\gamma)$. Moreover, let $\sigma_i = |\psi_i\rangle$, $\rho = \sum_i p i_i |\psi_i\rangle\langle\psi_i|$, $\tilde{q} = q_0, \ldots, q_{r-1}$, and $r = |\tilde{q}| \le n$. Then we have $[\![S_C\gamma]\!] = \langle \mathsf{D}(\tilde{q}; v; [\![S\gamma]\!]) \setminus (\phi\gamma), \rho\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]\gamma) \setminus (\phi\gamma), \rho\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]) \setminus \phi, \rho\rangle\,\gamma = [\![S_C]\!]\gamma$ holds if $[\![S\gamma]\!] = [\![S]\!]\gamma$.

We show $[\![S\gamma]\!] = [\![S]\!]\gamma$ by induction on the structure of S.

Case $S = \mathbf{0}$**:** In this case $S\gamma = S$ and, thus, $[\![S\gamma]\!] = [\![S]\!] = \mathsf{nil} = [\![S]\!]\gamma$.

Case $S = P \mid Q$**:** In this case $S\gamma = P\gamma \mid Q\gamma$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$ and $[\![Q\gamma]\!] = [\![Q]\!]\gamma$. Then $[\![S\gamma]\!] = [\![P\gamma]\!] \parallel [\![Q\gamma]\!] = [\![P]\!]\gamma \parallel [\![Q]\!]\gamma = ([\![P]\!] \parallel [\![Q]\!])\gamma = [\![S]\!]\gamma$.

Case $S = c?[x].P$**:** In this case $S\gamma = (c\gamma)?[x].(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = (c\gamma)?x.[\![P\gamma]\!] = (c\gamma)?x.([\![P]\!]\gamma) = (c?x.[\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = c![q].P$**:** In this case $S\gamma = (c\gamma)![q].(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = (c\gamma)!q.[\![P\gamma]\!] = (c\gamma)!q.([\![P]\!]\gamma) = (c!q.[\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = \{\tilde{q} \mathrel{*}= U\}.P$**:** In this case $S\gamma = \{\tilde{q} \mathrel{*}= U\}.(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then $[\![S\gamma]\!] = U[\tilde{q}].[\![P\gamma]\!] = U[\tilde{q}].([\![P]\!]\gamma) = (U[\tilde{q}].[\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = (v := \mathsf{measure}\ \tilde{q}).P$**:** In this case $S\gamma = (v := \mathsf{measure}\ \tilde{q}).(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then $[\![S\gamma]\!] = \mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v; [\![P\gamma]\!]) = \mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v; [\![P]\!]\gamma) = (\mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v; [\![P]\!]))\gamma = [\![S]\!]\gamma$.

Case $S = (\mathsf{new}\ c)P$**:** In this case $S\gamma = (\mathsf{new}\ d)(P'\gamma)$, where d is fresh and $P' = P\{d/c\}$. By the induction hypothesis, $[\![P'\gamma]\!] = [\![P']\!]\gamma$ and $[\![P']\!] = [\![P]\!]\{d/c\}$. Then $[\![S\gamma]\!] = \tau.([\![P'\gamma]\!] \setminus \{d\}) = (\tau.([\![P']\!] \setminus \{d\}))\gamma = (\tau.([\![P]\!] \setminus \{c\}))\gamma = [\![S]\!]\gamma$.

Case $S = (\mathsf{qubit}\ x)P$**:** In this case $S\gamma = (\mathsf{qubit}\ x)(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then $[\![S\gamma]\!] = \mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P\gamma]\!]\{q_{|\mathcal{V}|}/x\}\big) = \big(\mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P]\!]\{q_{|\mathcal{V}|}/x\}\big)\big)\gamma = [\![S]\!]\gamma$.

Case $S = \mathsf{if}\ bv = bv'\ \mathsf{then}\ P$**:** In this case $S\gamma = \mathsf{if}\ bv = bv'\ \mathsf{then}\ P\gamma$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P\gamma]\!]) = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.([\![P]\!]\gamma)) = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P]\!])\gamma = [\![S]\!]\gamma$. □

For the proof of operational correspondence, we also need qubit invariance, i.e., that also substitutions on qubits are preserved and reflected by the encoding function. The proof of qubit invariance is very similar to the proof of name invariance.

Lemma 5.8 (Qubit Invariance, $[\![\cdot]\!]$)**.** *Let γ be a substitution on qubit names.*

$$\forall S_C \in \mathfrak{C}_{\mathsf{C}}.\ [\![S_C\gamma]\!] = [\![S_C]\!]\gamma \quad \textit{and} \quad \forall S \in \mathfrak{P}_{\mathsf{C}}.\ [\![S\gamma]\!] = [\![S]\!]\gamma$$

Proof. Assume a substitution γ on qubit names. Let $S_C = (\sigma; \phi; S)$. Then $S_C\gamma = (\sigma\gamma; \phi; S\gamma)$. Moreover, let $\sigma = |\psi\rangle$ and $\rho = |\psi\rangle\langle\psi|$. Then $[\![S_C\gamma]\!] = \langle [\![S\gamma]\!] \setminus \phi, \rho\gamma\rangle = \langle ([\![S]\!]\gamma) \setminus \phi, \rho\gamma\rangle = \langle [\![S]\!], \rho\rangle\,\gamma = [\![S_C]\!]\gamma$ holds if $[\![S\gamma]\!] = [\![S]\!]\gamma$.

Similarly, let $S_C = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi; S\{\mathsf{b}(i)/v\})$. Then we have $S_C\gamma = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i\gamma; \phi; S\{\mathsf{b}(i)/v\}\gamma)$. Moreover, let $\sigma_i = |\psi_i\rangle$, $\rho = \sum_i p i_i |\psi_i\rangle\langle\psi_i|$, $\tilde{q} = q_0, \ldots, q_{r-1}$, and $r = |\tilde{q}| \le n$. Then we have $[\![S_C\gamma]\!] = \langle \mathsf{D}(\tilde{q}; v; [\![S\gamma]\!]) \setminus \phi, \rho\gamma\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]\gamma) \setminus \phi, \rho\gamma\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]) \setminus \phi, \rho\rangle\,\gamma = [\![S_C]\!]\gamma$ holds if $[\![S\gamma]\!] = [\![S]\!]\gamma$.

We show $[\![S\gamma]\!] = [\![S]\!]\gamma$ by induction on the structure of S.

Case $S = \mathbf{0}$**:** In this case $S\gamma = S$ and, thus, $[\![S\gamma]\!] = [\![S]\!] = \mathsf{nil} = [\![S]\!]\gamma$.

Case $S = P \mid Q$**:** In this case $S\gamma = P\gamma \mid Q\gamma$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$ and $[\![Q\gamma]\!] = [\![Q]\!]\gamma$. Then $[\![S\gamma]\!] = [\![P\gamma]\!] \parallel [\![Q\gamma]\!] = [\![P]\!]\gamma \parallel [\![Q]\!]\gamma = ([\![P]\!] \parallel [\![Q]\!])\gamma = [\![S]\!]\gamma$.

Case $S = c?[x].P$**:** In this case $S\gamma = c?[y].(P'\gamma)$, where y is fresh and $P' = P\{y/x\}$, i.e., we use alpha conversion to ensure that the variable that stores the received qubit is fresh in γ. By the induction hypothesis, $[\![P'\gamma]\!] = [\![P']\!]\gamma$ and $[\![P']\!] = [\![P]\!]\{y/x\}$. Then we have $[\![S\gamma]\!] = c?y.[\![P'\gamma]\!] = c?y.([\![P']\!]\gamma) = (c?y.[\![P']\!])\gamma = (c?x.[\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = c![q].P$**:** In this case $S\gamma = c![q\gamma].(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = c!(q\gamma).[\![P\gamma]\!] = c!(q\gamma).([\![P]\!]\gamma) = (c!q.[\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = \{\tilde{q} \mathrel{*}= U\}.P$**:** In this case $S\gamma = \{\tilde{q}\gamma \mathrel{*}= U\}.(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then $[\![S\gamma]\!] = U[\tilde{q}\gamma][\![P\gamma]\!] = U[\tilde{q}\gamma]([\![P]\!]\gamma) = (U[\tilde{q}][\![P]\!])\gamma = [\![S]\!]\gamma$.

Case $S = (v := \mathsf{measure}\ \tilde{q}).P$**:** In this case $S\gamma = (v := \mathsf{measure}\ \tilde{q}\gamma).(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = \mathcal{M}[\tilde{q}\gamma].\mathsf{D}(\tilde{q}\gamma; v; [\![P\gamma]\!]) = \mathcal{M}[\tilde{q}\gamma].\mathsf{D}(\tilde{q}\gamma; v; [\![P]\!]\gamma) = (\mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v; [\![P]\!]))\gamma = [\![S]\!]\gamma$.

Case $S = (\mathsf{new}\ x)P$**:** In this case $S\gamma = (\mathsf{new}\ x)(P\gamma)$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then $[\![S\gamma]\!] = \tau.([\![P\gamma]\!] \setminus \{x\}) = \tau.(([\![P]\!]\gamma) \setminus \{x\}) = (\tau.([\![P]\!] \setminus \{x\}))\gamma = [\![S]\!]\gamma$.

Case $S = (\mathsf{qubit}\ x)P$**:** In this case $S\gamma = (\mathsf{qubit}\ y)(P'\gamma)$, where y is fresh and $P' = P\{y/x\}$. By the induction hypothesis, $[\![P'\gamma]\!] = [\![P']\!]\gamma$ and in particular $[\![P']\!] = [\![P]\!]\{y/x\}$. Therefore, we have $[\![S\gamma]\!] = \mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P'\gamma]\!]\{q_{|\mathcal{V}|}/y\}\big) = \mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P']\!]\gamma\{q_{|\mathcal{V}|}/y\}\big) = \big(\mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P']\!]\{q_{|\mathcal{V}|}/y\}\big)\big)\gamma = \big(\mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P]\!]\{q_{|\mathcal{V}|}/x\}\big)\big)\gamma = [\![S]\!]\gamma$.

Case $S = \mathsf{if}\ bv = bv'\ \mathsf{then}\ P$**:** In this case $S\gamma = \mathsf{if}\ bv = bv'\ \mathsf{then}\ P\gamma$. By the induction hypothesis, $[\![P\gamma]\!] = [\![P]\!]\gamma$. Then we have $[\![S\gamma]\!] = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P\gamma]\!]) = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.([\![P]\!]\gamma)) = (\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P]\!])\gamma = [\![S]\!]\gamma$. □

We also show invariance modulo the instantiation of a variable for binary numbers by a number. Again the proof is very similar to the proofs of name and qubit invariance.

Lemma 5.9.

$$\forall S_C \in \mathfrak{C}_{\mathsf{C}}.\ \forall v, b.\ [\![S_C\{b/v\}]\!] = [\![S_C]\!]\{b/v\} \quad \textit{and} \quad \forall S \in \mathfrak{P}_{\mathsf{C}}.\ \forall v, b.\ [\![S\{b/v\}]\!] = [\![S]\!]\{b/v\}$$

Proof. Let $S_C = (\sigma; \phi; S)$. Then $S_C\{b/v\} = (\sigma; \phi; S\{b/v\})$. Moreover, let $\sigma = |\psi\rangle$ and $\rho = |\psi\rangle\langle\psi|$. Then $[\![S_C\{b/v\}]\!] = \langle [\![S\{b/v\}]\!] \setminus \phi, \rho\rangle = \langle ([\![S]\!]\{b/v\}) \setminus \phi, \rho\rangle = \langle [\![S]\!] \setminus \phi, \rho\rangle\{b/v\} = [\![S_C]\!]\{b/v\}$ holds if $[\![S\{b/v\}]\!] = [\![S]\!]\{b/v\}$.

Let $S_C = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi; S\{\mathsf{b}(i)/v'\})$. Then we have $S_C\{b/v\} = \boxplus_{0\le i<2^r} p_i \bullet (\sigma_i; \phi; (S\{\mathsf{b}(i)/v\})\{b/v\})$. Moreover, let $\sigma_i = |\psi_i\rangle$, $\rho = \sum_i p i_i |\psi_i\rangle\langle\psi_i|$, $\tilde{q} = q_0, \ldots, q_{r-1}$, and $r = |\tilde{q}| \le n$. If $v' = v$ then $v \notin \mathsf{fv}(S_C)$ and thus $v \notin \mathsf{fv}([\![S_C]\!])$. Then $[\![S_C\{b/v\}]\!] = [\![S_C]\!] = [\![S_C]\!]\{b/v\}$. Else if $v' \neq v$ then we have $[\![S_C\{b/v\}]\!] = \langle \mathsf{D}(\tilde{q}; v; [\![S\{b/v\}]\!]) \setminus \phi, \rho\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]\{b/v\}) \setminus \phi, \rho\rangle = \langle \mathsf{D}(\tilde{q}; v; [\![S]\!]) \setminus \phi, \rho\rangle\{b/v\} = [\![S_C]\!]\{b/v\}$ holds if $[\![S\{b/v\}]\!] = [\![S]\!]\{b/v\}$.

We show $[\![S\{b/v\}]\!] = [\![S]\!]\{b/v\}$ by induction on the structure of S.

Case $S = \mathbf{0}$**:** In this case $S\{b/v\} = S$ and, thus, $[\![S\{b/v\}]\!] = [\![S]\!] = \mathsf{nil} = [\![S]\!]\{b/v\}$.

Case $S = P \mid Q$**:** In this case $S\{b/v\} = P\{b/v\} \mid Q\{b/v\}$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$ and $[\![Q\{b/v\}]\!] = [\![Q]\!]\{b/v\}$. Then $[\![S\{b/v\}]\!] = [\![P\{b/v\}]\!] \parallel [\![Q\{b/v\}]\!] = [\![P]\!]\{b/v\} \parallel [\![Q]\!]\{b/v\} = ([\![P]\!] \parallel [\![Q]\!])\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = c?[x].P$**:** In this case $S\{b/v\} = c?[x].(P\{b/v\})$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then $[\![S\{b/v\}]\!] = c?x.[\![P\{b/v\}]\!] = c?x.(P\{b/v\}) = (c?x.[\![P]\!])\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = c![q].P$**:** In this case $S\{b/v\} = c![q].(P\{b/v\})$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then we have $[\![S\{b/v\}]\!] = c!q.[\![P\{b/v\}]\!] = c!q.([\![P]\!]\{b/v\}) = (c!q.[\![P]\!])\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = \{\tilde{q} *= U\}.P$**:** In this case $S\{b/v\} = \{\tilde{q} *= U\}.(P\{b/v\})$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then $[\![S\{b/v\}]\!] = U[\tilde{q}].[\![P\{b/v\}]\!] = U[\tilde{q}].([\![P]\!]\{b/v\}) = (U[\tilde{q}].[\![P]\!])\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = (v' := \mathsf{measure}\ \tilde{q}).P$**:** In this case $S\{b/v\} = (v'' := \mathsf{measure}\ \tilde{q}).(P'\{b/v\})$, where v'' is fresh and $P' = P\{v''/v'\}$. By the induction hypothesis, $[\![P'\{b/v\}]\!] = [\![P']\!]\{b/v\}$. Then we have $[\![S\{b/v\}]\!] = \mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v''; [\![P'\{b/v\}]\!]) = \mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v''; [\![P']\!]\{b/v\}) = (\mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v'; [\![P]\!]))\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = (\mathsf{new}\ c)P$**:** In this case $S\{b/v\} = (\mathsf{new}\ c)(P\{b/v\})$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then we have $[\![S\{b/v\}]\!] = \tau.([\![P\{b/v\}]\!] \setminus \{c\}) = (\tau.([\![P]\!] \setminus \{c\}))\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = (\mathsf{qubit}\ x)P$**:** In this case $S\{b/v\} = (\mathsf{qubit}\ x)(P\{b/v\})$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then $[\![S\{b/v\}]\!] = \mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P\{b/v\}]\!]\{q_{|\mathcal{V}|}/x\}\big) = \big(\mathcal{E}_{|0\rangle}[\mathcal{V}].\big([\![P]\!]\{q_{|\mathcal{V}|}/x\}\big)\big)\{b/v\} = [\![S]\!]\{b/v\}$.

Case $S = \mathsf{if}\ bv = bv'\ \mathsf{then}\ P$**:** In this case $S\{b/v\} = \mathsf{if}\ (bv\{b/v\}) = (bv'\{b/v\})\ \mathsf{then}\ P\{b/v\}$. By the induction hypothesis, $[\![P\{b/v\}]\!] = [\![P]\!]\{b/v\}$. Then

$$\begin{aligned}[\![S\{b/v\}]\!] &= \big(\mathsf{if}\ (bv\{b/v\}) = \big(bv'\{b/v\}\big)\ \mathsf{then}\ \tau.([\![P\{b/v\}]\!])\big)\\ &= \big(\mathsf{if}\ (bv\{b/v\}) = \big(bv'\{b/v\}\big)\ \mathsf{then}\ \tau.([\![P]\!]\{b/v\})\big)\\ &= \big(\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.[\![P]\!]\big)\{b/v\} = [\![S]\!]\{b/v\}\end{aligned}$$ □

Then we show the completeness and soundness parts of operational correspondence. For completeness, we have to show how target terms emulate source term steps. Above we observed that steps on (R-Perm$_{\mathsf{CQS}}$) are not emulated at all, i.e., are emulated by an empty sequence of steps, and captured this observation in Lemma 5.5. Moreover, Example 5.4 illustrates that in translating measurement under parallel composition completeness holds w.r.t. correspondence simulation but not bisimulation. All other kinds of source term steps are emulated more tightly by exactly one target term step.

Lemma 5.10 (Operational Completeness, $[\![\cdot]\!]$)**.**

$$\forall S, S' \in \mathfrak{C}_{\mathsf{C}}.\ S \Longmapsto S' \ \textit{implies}\ \exists T \in \mathfrak{C}_{\mathsf{O}}.\ [\![S]\!] \Longmapsto T \wedge \big[\!\big[S'\big]\!\big] \preceq T$$

Proof. We first consider a single step $S \longmapsto S'$ and show that we need in this case at most one step in the sequence $[\![S]\!] \Longmapsto T$ such that $[\![S']\!] \preceq T$. Therefore, we perform an induction over the derivation of $S \longmapsto S'$ using a case split over the rules in Figure 1.

Case (R-Measure$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; (v := \mathsf{measure}\ \tilde{q}).P)$, $\tilde{q} = q_0, \ldots, q_{r-1}$ and $S' = \boxplus_{0 \le m < 2^r} p_m \bullet (\sigma'_m; \phi; P\{\mathsf{b}(m)/x\})$, where $r = |\tilde{q}| \le n$, $\sigma = q_0, \ldots q_{n-1} = |\psi\rangle = \alpha_0|\psi_0\rangle + \cdots + \alpha_{2^n-1}|\psi_{2^n-1}\rangle$, and $\sigma'_m = |\psi'_m\rangle$. The corresponding encodings are given by

$$[\![S]\!] = \langle (\mathcal{M}[\tilde{q}].\mathsf{D}(\tilde{q}; v; [\![P]\!])) \setminus \phi, \rho\rangle \quad \text{and} \quad \big[\!\big[S'\big]\!\big] = \big\langle \mathsf{D}(\tilde{q}; v; [\![P]\!]) \setminus \phi, \rho'\big\rangle\,,$$

where $\rho = |\psi\rangle\langle\psi|$ and $\rho' = \sum_m p_m |\psi'_m\rangle\langle\psi'_m|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ by applying the super-operator $\mathcal{M}[\tilde{q}]$ using the Rule (Oper$_{\mathsf{OQS}}$), i.e., by

$$[\![S]\!] \longmapsto \langle \mathsf{D}(\tilde{q}; v; [\![P]\!]) \setminus \phi, \mathcal{M}_{\tilde{q}}(\rho)\rangle = T.$$

Further, $\sigma'_m = |\psi'_m\rangle = \frac{\alpha_{l_m}}{\sqrt{p_m}}|\psi_{l_m}\rangle + \cdots + \frac{\alpha_{u_m}}{\sqrt{p_m}}|\psi_{u_m}\rangle$ with $l_m = 2^{n-r}m$, $u_m = 2^{n-r}(m+1)-1$, and $p_m = |\alpha_{l_m}|^2 + \cdots + |\alpha_{u_m}|^2$. Let P_m be the base vector for $\mathsf{b}(m)$ in the standard base. Since $\mathcal{M}_{\tilde{q}}(\rho) = \sum_m \mathsf{P}_m \rho \mathsf{P}_m^\dagger$, and $\rho' = \sum_m p_m |\psi'_m\rangle\langle\psi'_m|$, then $\rho' = \mathcal{M}_{\tilde{q}}(\rho)$. Note that $|\psi'_m\rangle = \frac{\mathsf{P}_m|\psi\rangle}{\sqrt{\mathsf{tr}\left(\mathsf{P}_m^\dagger \mathsf{P}_m |\psi\rangle\langle\psi|\right)}}$. Therefore, the measurement using the super-operator $\mathcal{M}[\tilde{q}]$ applied to ρ produces the same probability distribution as measuring σ with $(v := \mathsf{measure}\ q_0, \ldots, q_{r-1}).P$ (modulo the different representations of the qubits). It follows $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-Trans$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; \{\tilde{q} *= U\}.P)$ and $S' = (\sigma'; \phi; P)$, where $\tilde{q} = q_0, \ldots, q_{r-1}$, $r = |\tilde{q}| \leq n$, $\sigma = q_0, \ldots q_{n-1} = |\psi\rangle$, $\sigma' = q_0, \ldots q_{n-1} = |\psi'\rangle$, and $|\psi'\rangle$ is the result of applying U on the first r qubits in $q_0, \ldots q_{n-1} = |\psi\rangle$. The corresponding encodings are given by

$$[\![S]\!] = \langle (U[\tilde{q}].[\![P]\!]) \setminus \phi, \rho\rangle \quad \text{and} \quad [\![S']\!] = \left\langle [\![P]\!] \setminus \phi, \rho'\right\rangle,$$

where $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'\rangle\langle\psi'|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ by applying the super-operator $U[\tilde{q}]$ using the Rule (Oper$_{\mathsf{OQS}}$), i.e., by

$$[\![S]\!] \longmapsto \langle [\![P]\!] \setminus \phi, U_{\tilde{q}}(\rho)\rangle = T.$$

Further, $\sigma' = (U \otimes \mathcal{I}_{\{q_r,\ldots,q_{n-1}\}})|\psi\rangle = |\psi'\rangle$ and $U_{\tilde{q}}(\rho) = (U \otimes \mathcal{I}_{\mathcal{V}-\tilde{q}}) \cdot \rho \cdot (U \otimes \mathcal{I}_{\mathcal{V}-\tilde{q}})^\dagger$. Moreover, since $\rho' = |\psi'\rangle\langle\psi'|$ and $\{q_r, \ldots, q_{n-1}\} = \mathcal{V} - \tilde{q}$, it follows $\rho' = U_{\tilde{q}}(\rho)$ and therefore $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-Perm$_{\mathsf{CQS}}$) : In this case, $[\![S']\!] \preceq [\![S]\!]$, because of Lemma 5.5. We choose $T = [\![S]\!]$ such that $[\![S]\!] \Longmapsto T$ (by doing 0 steps) and $[\![S']\!] \preceq T$.

Case (R-Comm$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; c![q].P \mid c?[x].Q)$ and $S' = (\sigma; \phi; P \mid Q\{q/x\})$, where $\sigma = q_0, \ldots, q_{n-1} = |\psi\rangle$. The corresponding encodings are given by

$$[\![S]\!] = \langle (c!q.[\![P]\!] \parallel c?x.[\![Q]\!]) \setminus \phi, \rho\rangle \quad \text{and} \quad [\![S']\!] = \langle ([\![P]\!] \parallel [\![Q\{q/x\}]\!]) \setminus \phi, \rho\rangle,$$

where $\rho = |\psi\rangle\langle\psi|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ using the rules (Comm$_{\mathsf{OQS}}$), (Input$_{\mathsf{OQS}}$), and (Output$_{\mathsf{OQS}}$) by

$$[\![S]\!] \longmapsto \langle ([\![P]\!] \parallel [\![Q]\!]\{q/x\}) \setminus \phi, \rho\rangle = T.$$

By Lemma 5.8, $[\![Q\{q/x\}]\!] = [\![Q]\!]\{q/x\}$. Then $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-New$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; (\mathsf{new}\ d)P)$ and $S' = (\sigma; \phi, c; P\{c/d\})$, where c is fresh and $\sigma = q_0, \ldots, q_{n-1} = |\psi\rangle$. The corresponding encodings are given by

$$[\![S]\!] = \langle (\tau.([\![P]\!] \setminus \{d\})) \setminus \phi, \rho\rangle \quad \text{and} \quad [\![S']\!] = \langle [\![P\{c/d\}]\!] \setminus \phi, c, \rho\rangle,$$

where $\rho = |\psi\rangle\langle\psi|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ by reducing τ using Rule (Tau$_{\mathsf{OQS}}$), i.e., by

$$[\![S]\!] \longmapsto \langle [\![P]\!] \setminus (\phi \cup \{d\}), \rho\rangle = T.$$

By Lemma 5.7, $[\![P\{c/d\}]\!] = [\![P]\!]\{c/d\}$. Since c is fresh, then $[\![P\{c/d\}]\!] \setminus (\phi \cup \{c\}) = [\![P]\!]\{c/d\} \setminus (\phi \cup \{c\}) = [\![P]\!] \setminus (\phi \cup \{d\})$. Then $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-Qbit$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; (\mathsf{qubit}\ x)P)$ and $S' = (\sigma'; \phi; P\{q_n/x\})$, where $\sigma = q_0, \ldots, q_{n-1} = |\psi\rangle$, $\sigma' = q_0, \ldots, q_{n-1}, q_n = |\psi'\rangle$, $|\psi'\rangle = |\psi\rangle \otimes |0\rangle$, $\mathcal{V} = q_0, \ldots, q_{n-1}$,

and q is fresh. The corresponding encodings are given by the following terms

$$[\![S]\!] = \left\langle \left(\mathcal{E}_{|0\rangle}[\mathcal{V}].([\![P]\!]\{q_n/x\})\right) \setminus \phi, \rho \right\rangle \quad \text{and} \quad [\![S']\!] = \left\langle [\![P\{q_n/x\}]\!] \setminus \phi, \rho' \right\rangle,$$

where $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'\rangle\langle\psi'|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ by applying the super-operator $\mathcal{E}_{|0\rangle}[\mathcal{V}]$ using the Rule ($\text{OPER}_{\mathsf{OQS}}$), i.e., by

$$[\![S]\!] \longmapsto \left\langle ([\![P]\!]\{q_n/x\}) \setminus \phi, \mathcal{E}_{|0\rangle,\mathcal{V}}(\rho) \right\rangle = T.$$

By Lemma 5.8, $[\![P\{q_n/x\}]\!] = [\![P]\!]\{q_n/x\}$. Further, $\mathcal{E}_{|0\rangle,\mathcal{V}}(\rho) = \rho'$. Then $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-Par$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; P \mid Q)$, $S' = \boxplus_{0\le i<2^r} p_i \bullet (\sigma'_i; \phi'; P'\{\mathsf{b}(i)/v\} \mid Q)$, $S_P = (\sigma; \phi; P) \in \mathfrak{C}_{\mathsf{C}}$, and $S_P \longmapsto S'_P = \boxplus_{0\le i<2^r} p_i \bullet (\sigma'_i; \phi'; P'\{\mathsf{b}(i)/v\})$, where $\sigma = q_0, \ldots, q_{n-1} = |\psi\rangle$, $\sigma'_i = q_0, \ldots, q_{n-1} = |\psi'_i\rangle$, $\tilde{q} = q_0, \ldots, q_{r-1}$, $r = |\tilde{q}| \le n$, and v is fresh in Q. By the induction hypothesis, there is some $T_P \in \mathfrak{C}_{\mathsf{O}}$ such that $[\![S_P]\!] \Longmapsto T_P$ and $[\![S'_P]\!] \preceq T_P$. Then either (1) $r = 0$ and $S'_P = \boxplus_{0\le i<2^0} p_i \bullet (\sigma'_i; \phi'; P'\{\mathsf{b}(i)/v\}) = (\sigma'_0; \phi'; P')$, because there is just one case in the probability distribution, or (2) $r > 0$ and the probability distribution in S'_P contains more than one case:

(1) The corresponding encodings are given by

$$\begin{array}{rclcrcl} [\![S]\!] & = & \langle ([\![P]\!] \parallel [\![Q]\!]) \setminus \phi, \rho \rangle, & & [\![S']\!] & = & \langle ([\![P']\!] \parallel [\![Q]\!]) \setminus \phi', \rho' \rangle, \\ [\![S_P]\!] & = & \langle [\![P]\!] \setminus \phi, \rho \rangle, & \text{and} & [\![S'_P]\!] & = & \langle [\![P']\!] \setminus \phi', \rho' \rangle, \end{array}$$

where $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'_0\rangle\langle\psi'_0|$. Since $[\![S'_P]\!] \preceq T_P$, then $T_P = \langle T'_P \setminus \phi', \rho' \rangle$ for some T'_P. By the Rule ($\text{RED}_{\mathsf{OQS}}$) in Figure 3, $[\![S_P]\!] \Longmapsto T_P$ implies $[\![S_P]\!] \xrightarrow{\tau} \ldots \xrightarrow{\tau} T_P$ and, by ($\text{RES}_{\mathsf{OQS}}$), then $\langle [\![P]\!], \rho \rangle \Longmapsto \langle T'_P, \rho' \rangle$. Then $[\![S]\!]$ can emulate the step $S \longmapsto S'$ using the sequence $\langle [\![P]\!], \rho \rangle \Longmapsto \langle T'_P, \rho' \rangle$ and the rules ($\text{INTL}_{\mathsf{OQS}}$) and ($\text{RES}_{\mathsf{OQS}}$) by

$$[\![S]\!] \Longmapsto \left\langle \left(T'_P \parallel [\![Q]\!]\right) \setminus \phi', \rho' \right\rangle = T.$$

Since $[\![S_P]\!] \Longmapsto T_P$ contains at most one step, so does $[\![S]\!] \Longmapsto T$. Finally, we show that $[\![S'_P]\!] \preceq T_P$ implies $[\![S']\!] \preceq T$:

- Assume $[\![S']\!] \xrightarrow{\alpha} C_1$. Then either $[\![Q]\!]$ performs a step on its own, $[\![P']\!]$ does a step on its own, or they perform a communication step together. In the second and third case, $[\![S'_P]\!] \preceq T_P$ ensures that for every $[\![S'_P]\!] = \langle [\![P']\!] \setminus \phi', \rho' \rangle \xrightarrow{\alpha'} T_1$ there is some $T_P = \langle T'_P \setminus \phi', \rho' \rangle \xrightarrow{\alpha'} T'_1$ such that $T_1 \preceq T'_1$. With that, in all three cases, $T \xrightarrow{\alpha} C'_1$ such that $C_1 \preceq C'_1$.
- Assume $T \xrightarrow{\alpha} C'_1$. Then either $[\![Q]\!]$ performs a step on its own, T'_P does a step on its own, or they perform a communication step together. In the second and third case, $[\![S'_P]\!] \preceq T_P$ ensures that for every $T_P = \langle T'_P \setminus \phi', \rho' \rangle \xrightarrow{\alpha'} T'_1$ there are some $[\![S'_P]\!] = \langle [\![P']\!] \setminus \phi', \rho' \rangle \Longmapsto\!\xrightarrow{\alpha'} T_2$ and $T'_1 \Longmapsto T'_2$ such that $T_2 \preceq T'_2$. With that, in all three cases, $[\![S']\!] \Longmapsto\!\xrightarrow{\alpha} C_2$ and $C'_1 \Longmapsto C'_2$ such that $C_2 \preceq C'_2$.
- Since correspondence simulation is stricter than weak trace equivalence, $[\![S']\!]$ and T have the same weak traces and thus $[\![S']\!]\Downarrow_{\checkmark}$ iff $T\Downarrow_{\checkmark}$.

(2) Since v is fresh in Q, the corresponding encodings are given by

$$\begin{array}{rclcrcl} [\![S]\!] & = & \langle ([\![P]\!] \parallel [\![Q]\!]) \setminus \phi, \rho \rangle, & & [\![S']\!] & = & \langle (\mathsf{D}(\tilde{q}; v; [\![P']\!] \parallel [\![Q]\!])) \setminus \phi', \rho' \rangle, \\ [\![S_P]\!] & = & \langle [\![P]\!] \setminus \phi, \rho \rangle, & & [\![S'_P]\!] & = & \langle \mathsf{D}(\tilde{q}; v; [\![P']\!]) \setminus \phi', \rho' \rangle, \end{array}$$

where $\rho = |\psi\rangle\langle\psi|$ and $\rho' = \sum_i p_i |\psi_i'\rangle\langle\psi_i'|$. Since $[\![S_P']\!] \preceq T_P$, then $T_P = \langle \mathsf{D}(\tilde{q}; v; T_P') \setminus \phi', \rho' \rangle$ for some T_P'. By the Rule ($\textsc{Red}_{\mathsf{OQS}}$) in Figure 3, $[\![S_P]\!] \Longmapsto T_P$ implies $[\![S_P]\!] \xrightarrow{\tau} \ldots \xrightarrow{\tau} T_P$ and, by Rule ($\textsc{Res}_{\mathsf{OQS}}$), then $\langle [\![P]\!], \rho \rangle \Longmapsto \langle \mathsf{D}(\tilde{q}; v; T_P'), \rho' \rangle$. Then $[\![S]\!]$ can emulate the step $S \longmapsto S'$ using the sequence $\langle [\![P]\!], \rho \rangle \Longmapsto \langle \mathsf{D}(\tilde{q}; v; T_P'), \rho' \rangle$ and the rules ($\textsc{Intl}_{\mathsf{OQS}}$) and ($\textsc{Res}_{\mathsf{OQS}}$) by

$$[\![S]\!] \Longmapsto \left\langle \left(\mathsf{D}(\tilde{q}; v; T_P') \parallel [\![Q]\!] \right) \setminus \phi', \rho' \right\rangle = T.$$

Since $[\![S_P]\!] \Longmapsto T_P$ contains at most one step, so does $[\![S]\!] \Longmapsto T$. Finally, we show that $[\![S_P']\!] \preceq T_P$ implies $[\![S']\!] \preceq T$:

- Assume $[\![S']\!] \xrightarrow{\alpha} C_1$. Then this step reduces the choice to one branch with non-zero probability with ($\textsc{Cond}_{\mathsf{OQS}}$) and ($\textsc{Choice}_{\mathsf{OQS}}$) and in this branch the respective super-operator to adjust the density matrix to the chosen result of measurement with ($\textsc{Oper}_{\mathsf{OQS}}$), i.e., $\alpha = \tau$ and $C_1 = \left\langle ([\![P']\!]\{\mathsf{b}(j)/v\} \parallel [\![Q]\!]) \setminus \phi' \right.$, $\left. \mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\rho') \right\rangle$ for some $0 \leq j < 2^r$ with $p_j \neq 0$, where $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}$ is measurement with the expected result $\mathsf{b}(j)$ and will adapt the state of the measured qubits to $\mathsf{b}(j)$. Then $T \xrightarrow{\alpha} C_1' = \left\langle (T_P'\{\mathsf{b}(j)/v\} \parallel [\![Q]\!]) \setminus \phi', \mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\rho') \right\rangle$. Because of $\langle \mathsf{D}(\tilde{q}; v; [\![P']\!]) \setminus \phi', \rho' \rangle = [\![S_P']\!] \preceq T_P = \langle \mathsf{D}(\tilde{q}; v; T_P') \setminus \phi', \rho' \rangle$ and Lemma 5.9, then $C_1 \preceq C_1'$.
- Assume $T \xrightarrow{\alpha} C_1'$. Then either the choice on the left is reduced or $[\![Q]\!]$ performs a step on its own. In the former case, $\alpha = \tau$, $C_1' = \left\langle (T_P'\{\mathsf{b}(j)/v\} \parallel [\![Q]\!]) \setminus \phi', \mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\rho') \right\rangle$, $0 \leq j < 2^r$, and $p_j \neq 0$. Then $[\![S']\!] \xrightarrow{\alpha} C_1 = \langle ([\![P']\!]\{\mathsf{b}(j)/v\} \parallel [\![Q]\!]) \setminus \phi', \mathcal{E}_{j,\tilde{q}}(\rho') \rangle$. Because of Lemma 5.9 and $\langle \mathsf{D}(\tilde{q}; v; [\![P']\!]) \setminus \phi', \rho' \rangle = [\![S_P']\!] \preceq T_P = \langle \mathsf{D}(\tilde{q}; v; T_P') \setminus \phi', \rho' \rangle$, then we pick $C_2' = C_1'$ and $C_2 = C_1$ such that $C_2 \preceq C_2'$.
  In the latter case, $C_1' = \langle (\mathsf{D}(\tilde{q}; v; T_P') \parallel T_Q) \setminus \phi'', \rho'' \rangle$. Then we pick an arbitrary case $0 \leq j < 2^r$ of the probability distribution with non-zero probability $p_j \neq 0$ such that $[\![S']\!] \longmapsto \left\langle ([\![P']\!]\{\mathsf{b}(j)/v\} \parallel [\![Q]\!]) \setminus \phi', \mathcal{E}_{\mathsf{b}(j),\tilde{q}} \tilde{\rho'} \right\rangle \xrightarrow{\alpha} C_2$ with $C_2 = \langle ([\![P']\!]\{\mathsf{b}(j)/v\} \parallel T_Q) \setminus \phi'', \rho''' \rangle$, where ρ''' is the result of applying the transformation on the matrix in the step $T \xrightarrow{\alpha} C_1'$ (if there is any) to the density matrix $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\rho')$. Because of the non-cloning principle, applying the super-operator $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}$ on ρ'' again yields ρ''', because $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}$ and the super-operator (if any) applied in $T \xrightarrow{\alpha} C_1'$ need to operate on different sets of qubits. Hence, $C_1' \longmapsto C_2' = \langle (T_P'\{\mathsf{b}(j)/v\} \parallel T_Q) \setminus \phi'', \rho''' \rangle$. Because of $\langle \mathsf{D}(\tilde{q}; v; [\![P']\!]) \setminus \phi', \rho' \rangle = [\![S_P']\!] \preceq T_P = \langle \mathsf{D}(\tilde{q}; v; T_P') \setminus \phi', \rho' \rangle$ and Lemma 5.9, then $C_2 \preceq C_2'$.
- Since correspondence simulation is stricter than weak trace equivalence, $[\![S']\!]$ and T have the same weak traces and thus $[\![S']\!]\downarrow_{\checkmark}$ iff $T\downarrow_{\checkmark}$.

Case (R-Cong$_{\mathsf{CQS}}$) : In this case $S = (\sigma; \phi; Q)$, $S' = \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma_i'; \phi'; Q'\{\mathsf{b}(i)/v\})$, $Q \equiv P$, $P' \equiv Q'$, and $S_P = (\sigma; \phi; P) \longmapsto S_P' = \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma_i'; \phi'; P'\{\mathsf{b}(i)/v\})$, where $\sigma = q_0, \ldots, q_{n-1} = |\psi\rangle$ and $\sigma_i' = q_0, \ldots, q_{n-1} = |\psi'\rangle$. By Lemma 5.6, $Q \equiv P$ implies $[\![S]\!] \equiv [\![S_P]\!]$ and $P' \equiv Q'$ implies $[\![S_P']\!] \equiv [\![S']\!]$. By the induction hypothesis, there is some $T_P \in \mathfrak{C}_{\mathsf{O}}$ such that $[\![S_P]\!] \Longmapsto T_P$ is a sequence of at most one step and $[\![S_P']\!] \preceq T_P$. Because of $[\![S]\!] \equiv [\![S_P]\!]$, i.e., $[\![S_P]\!] \preceq [\![S]\!]$, then there is some $T \in \mathfrak{C}_{\mathsf{O}}$ such that $[\![S]\!] \Longmapsto T$ is a sequence of at most one step and $T_P \preceq T$. Because of $[\![S_P']\!] \equiv [\![S']\!]$, i.e., $[\![S']\!] \preceq [\![S_P']\!]$, then $[\![S']\!] \preceq [\![S_P']\!] \preceq T_P \preceq T$, i.e., $[\![S']\!] \preceq T$.

Case (R-Prob$_{\mathsf{CQS}}$) : Then $S = \boxplus_{0\leq i<2^r} p_i \bullet (\sigma_i; \phi; P\{\mathsf{b}(i)/v\})$ and $S' = (\sigma_j; \phi; P\{\mathsf{b}(j)/v\})$ for some $0 \leq j < 2^r$ with $p_j \neq 0$, where $\sigma_i = q_0, \ldots, q_{n-1} = |\psi_i\rangle$, $\tilde{q} = q_0, \ldots, q_{r-1}$, and $r = |\tilde{q}| \leq n$. The corresponding encodings are given by

$$[\![S]\!] = \langle \mathsf{D}(\tilde{q}; v; [\![P]\!]) \setminus \phi, \rho\rangle \quad \text{and} \quad [\![S']\!] = \left\langle [\![P\{\mathsf{b}(j)/v\}]\!] \setminus \phi, \rho'\right\rangle,$$

where $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\rho' = |\psi_j\rangle\langle\psi_j|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ using the rules (Choice$_{\mathsf{OQS}}$), (Cond$_{\mathsf{OQS}}$), and (Oper$_{\mathsf{OQS}}$) by

$$[\![S]\!] \longmapsto \left\langle [\![P]\!]\{\mathsf{b}(j)/v\} \setminus \phi, \mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\rho)\right\rangle = T,$$

where $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}$ is measurement with the expected result $\mathsf{b}(j)$ and will adapt the state of the measured qubits to $\mathsf{b}(j)$. By Lemma 5.9, $[\![P\{\mathsf{b}(j)/v\}]\!] = [\![P]\!]\{\mathsf{b}(j)/v\}$. Since we restrict in CQS our attention to a probability distributions that results from the measurement of qubits, $\sigma_i = \frac{\alpha_{l_i}}{\sqrt{p_i}}|\psi_{l_i}\rangle + \cdots + \frac{\alpha_{u_i}}{\sqrt{p_i}}|\psi_{u_i}\rangle$ with $l_i = 2^{n-r}i$, $u_i = 2^{n-r}(i+1) - 1$, and $p_i = |\alpha_{l_i}|^2 + \cdots + |\alpha_{u_i}|^2$. Accordingly, $\mathcal{E}_j[\tilde{q}]$ sets the system state to $\frac{\mathcal{E}_{j,\tilde{q}}(\rho)}{\mathsf{tr}(\mathcal{E}_{j,\tilde{q}}(\rho))} = \rho'$. Then $T = [\![S']\!]$, i.e., $[\![S']\!] \preceq T$.

Case (R-Cond$_{\mathsf{CQS}}$) : Then $S = (\sigma; \phi; \mathsf{if}\ b = b'\ \mathsf{then}\ P)$, $b = b'$, and $S' = (\sigma; \phi; P)$, where $\sigma_i = q_0, \ldots, q_{n-1} = |\psi_i\rangle$. The corresponding encodings are given by

$$[\![S]\!] = \left\langle \mathsf{if}\ b = b'\ \mathsf{then}\ \tau.[\![P]\!] \setminus \phi, \rho\right\rangle \quad \text{and} \quad [\![S']\!] = \langle [\![P]\!] \setminus \phi, \rho\rangle,$$

where $\rho = |\psi\rangle\langle\psi|$. We observe that $[\![S]\!]$ can emulate the step $S \longmapsto S'$ using the rules (Cond$_{\mathsf{OQS}}$) and (Tau$_{\mathsf{OQS}}$) by

$$[\![S]\!] \longmapsto \langle [\![P]\!] \setminus \phi, \rho\rangle = T.$$

Since $T = [\![S']\!]$, then $[\![S']\!] \preceq T$.

Finally, the lemma follows from an induction over the number of steps in $S \Longmapsto S'$. □

In the opposite direction, i.e., for soundness, we show that every target term step is the result of emulating a source term step. Thereby, the formulation of soundness allows to perform—after some initial steps $[\![S]\!] \Longmapsto T$ that need to be mapped to the source—some additional steps $T \Longmapsto T'$, to catch up with a source term encoding $[\![S']\!]$. To avoid the problem described in Example 5.4, we use these additional steps on the target to resolve all unguarded choices as they result from translating probability distributions. Accordingly, the sequence $S \Longmapsto S'$ contains the mapping of the steps in $[\![S]\!] \Longmapsto T$, steps to resolve probability distributions to map the steps in $T \Longmapsto T'$, and some additional steps on Rule (R-Perm$_{\mathsf{CQS}}$) to permute qubits. The last kind of steps is necessary in the source to prepare for applications of unitary transformations and measurement, i.e., these steps surround in $S \Longmapsto S'$ the corresponding mappings of steps in $[\![S]\!] \Longmapsto T$ that apply the super-operators for unitary transformations or measurement.

Lemma 5.11 (Operational Soundness, $[\![\cdot]\!]$)**.**

$$\forall S \in \mathfrak{C}_{\mathsf{C}}.\ \forall T \in \mathfrak{C}_{\mathsf{O}}.\ [\![S]\!] \Longmapsto T \textit{ implies}$$
$$\exists S' \in \mathfrak{C}_{\mathsf{C}}.\ \exists T' \in \mathfrak{C}_{\mathsf{O}}.\ S \Longmapsto S' \wedge T \Longmapsto T' \wedge [\![S']\!] \preceq T'$$

Proof. We strengthen the proof goal by replacing $\preceq$ with equality:

$$\forall S \in \mathfrak{C}_{\mathsf{C}}.\ \forall T \in \mathfrak{C}_{\mathsf{O}}.\ [\![S]\!] \Longmapsto T \text{ implies } \exists S' \in \mathfrak{C}_{\mathsf{C}}.\ S \Longmapsto S' \wedge T \Longmapsto [\![S']\!]$$

Moreover, we require that either $S' = S$ or S' is not a probability distribution with $r > 0$ and that every step in the sequence $T \Longmapsto [\![S']\!]$ reduces a choice. Then the proof is by induction on the number of steps in $[\![S]\!] \Longmapsto T$. The base case for zero steps, i.e., $T = [\![S]\!]$, holds trivially by choosing $S' = S$. For the induction step, assume $[\![S]\!] \Longmapsto T^* \longmapsto T$. By the induction hypothesis, there is some S^{**} such that $S \Longmapsto S^{**}$ and $T^* \Longmapsto [\![S^{**}]\!]$, where S^{**} is not a probability distribution and in $T^* \Longmapsto [\![S^{**}]\!]$ only choices are reduced. Let $S^{**} = (\sigma^{**}; \phi^{**}; P^{**})$ with $\sigma^{**} = q_0, \ldots, q_{n^{**}-1} = |\psi^{**}\rangle$. By Definition 5.1, then $[\![S^{**}]\!] = \langle [\![P^{**}]\!] \setminus \phi^{**}, \rho^{**} \rangle$ with $\rho^{**} = |\psi^{**}\rangle\langle\psi^{**}|$.

By Figure 3, $T^* \longmapsto T$ was derived from the Rule ($\textsc{Red}_{\mathsf{OQS}}$), i.e., $T^* \xrightarrow{\tau} T$, and the derivation of $T^* \xrightarrow{\tau} T$ is based on either (1) the Axiom ($\textsc{Tau}_{\mathsf{OQS}}$), (2) the Axiom ($\textsc{Oper}_{\mathsf{OQS}}$), or (3) both of the Axioms ($\textsc{Input}_{\mathsf{OQS}}$) and ($\textsc{Output}_{\mathsf{OQS}}$).

(1) By Definition 5.1, τ cannot guard a branch of a choice. Then τ (a) does not guard the subterm of a conditional, or (b) guards the subterm of a conditional without a measurement, or (c) guards the subterm of a conditional with a measurement.
   (a) Then T^* contains an unguarded subterm $\tau.(T_\tau \setminus c)$ that is reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains an unguarded subterm $(\mathsf{new}\ c)P_{\mathsf{new}}$ that was translated into $\tau.(T_\tau \setminus c)$. Then there is some S' such that $S^{**} \longmapsto S' = (\sigma^{**}; \phi^{**}, c; P'_{\mathsf{new}}\{c/d\})$, where c, d are fresh and P'_{new} is obtained from P^{**} by replacing $(\mathsf{new}\ c)P_{\mathsf{new}}$ with $P_{\mathsf{new}}\{d/c\}$. Then $S \Longmapsto S'$. By Lemma 5.7, then $[\![S']\!] = \langle [\![P'_{\mathsf{new}}\{c/d\}]\!] \setminus (\phi^{**}, c), \rho^{**} \rangle = \langle [\![P'_{\mathsf{new}}]\!] \setminus (\phi^{**}, d), \rho^{**} \rangle$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^*.
   (b) Then T^* contains an unguarded subterm $\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.T_\tau$ that is reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains an unguarded subterm $\mathsf{if}\ bv = bv'\ \mathsf{then}\ P_{\mathsf{cond}}$ that was translated into $\mathsf{if}\ bv = bv'\ \mathsf{then}\ \tau.T_\tau$. Then there is some S' such that $S^{**} \longmapsto S' = (\sigma^{**}; \phi^{**}; P'_{\mathsf{cond}})$, where P'_{cond} is obtained from P^{**} by replacing $\mathsf{if}\ bv = bv'\ \mathsf{then}\ P_{\mathsf{cond}}$ with P_{cond}. Then $S \Longmapsto S'$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^*.
   (c) By Definition 5.1, then the τ guards the subterm of a conditional within a choice. Since $T^* \Longmapsto [\![S^{**}]\!]$ and S^{**} is not a probability distribution (with $r > 0$), then $T^* \Longmapsto [\![S^{**}]\!]$ reduces this choice but not necessarily to the case j that contains the considered τ guard. Accordingly, $S \Longmapsto S^{**}$ contains a step that reduces the corresponding probability distribution, where the respective branch is not further reduced because $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices. Then we replace in $S \Longmapsto S^{**}$ and $T^* \Longmapsto [\![S^{**}]\!]$ the respective steps reducing the probability distribution and the choice in question by a step that reduces this probability distribution and this choice to case j. Note that, because $T^* \longmapsto T$ measures $\tilde{q}$, case j has a non-zero probability. Finally, we reorder the steps on the target such that $S \Longmapsto S'$ and $T^* \longmapsto T \Longmapsto [\![S']\!]$, where S' is obtained from S^{**} by adapting the chosen branch to case j. Note that this is the only case, in that the state of S' is not σ^{**}, because the adaptation of the branch to case j also requires to adapt the state accordingly.

(2) By Definition 5.1, one of the following super-operators was reduced:
   Case of $U[\tilde{q}]$: By Definition 5.1, $U[\tilde{q}]$ cannot guard a branch of a choice nor can $U[\tilde{q}]$ guard the subterm of a conditional. Then T^* contains an unguarded subterm

$U[\tilde{q}].T_{\mathsf{U}}$ that is reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains an unguarded subterm $\{\tilde{q} *= U\}.P_{\mathsf{U}}$ that was translated into $U[\tilde{q}].T_{\mathsf{U}}$. Then there are some $S_{\mathsf{perm}}, S_{\mathsf{U}}, S'$ such that $S^{**} \longmapsto S_{\mathsf{perm}} \longmapsto S_{\mathsf{U}} \longmapsto S' = (\sigma'; \phi^{**}; P'_{\mathsf{U}})$, where $S^{**} \longmapsto S_{\mathsf{perm}}$ is by Rule (R-PERM$_{\mathsf{CQS}}$) and permutes the qubits in $\tilde{q}$ to the front using a permutation π, $S_{\mathsf{perm}} \longmapsto S_{\mathsf{U}}$ performs the unitary transformation, $S_{\mathsf{U}} \longmapsto S'$ permutes the qubits back to their original order, $\sigma' = \Pi\Big(\Big(U \otimes \mathcal{I}_{\{q_{|\tilde{q}|},\ldots,q_{n-1}\}}\Big)(\Pi|\psi^{**}\rangle)\Big) = |\psi'\rangle$, and P'_{U} is obtained from P^{**} by replacing $\{\tilde{q} *= U\}.P_{\mathsf{U}}$ with P_{U}. Then $S \Longmapsto S'$ and $[\![S']\!] = \langle [\![P'_{\mathsf{U}}]\!] \setminus \phi^{**}, \rho' \rangle$, where $\rho' = U_{\tilde{q}}(\rho^{**}) = |\psi'\rangle\langle\psi'|$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^*.

Case of $\mathcal{M}[\tilde{q}]$: By Definition 5.1, $\mathcal{M}[\tilde{q}]$ cannot guard a branch of a choice nor can $\mathcal{M}[\tilde{q}]$ guard the subterm of a conditional. Then T^* contains an unguarded subterm $\mathcal{M}[\tilde{q}].T_{\mathsf{M}}$ that is reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains an unguarded subterm $(v := \mathsf{measure}\ \tilde{q}).P_{\mathsf{M}}$ that was translated into $\mathcal{M}[\tilde{q}].T_{\mathsf{M}}$. Then there are some $S_{\mathsf{perm}}, S_{\mathsf{M}}, S_{\mathsf{dist}}, S'$ such that $S^{**} \longmapsto S_{\mathsf{perm}} \longmapsto S_{\mathsf{M}} \longmapsto S_{\mathsf{dist}} \longmapsto S' = (\sigma'; \phi^{**}; P'_{\mathsf{M}}\{\mathsf{b}(j)/v'\})$, where $S^{**} \longmapsto S_{\mathsf{perm}}$ is by Rule (R-PERM$_{\mathsf{CQS}}$) and permutes the qubits in $\tilde{q}$ to the front using a permutation π, $S_{\mathsf{perm}} \longmapsto S_{\mathsf{M}}$ performs the measurement, $S_{\mathsf{M}} \longmapsto S_{\mathsf{dist}}$ resolves the resulting probability distribution to an arbitrary case j with non-zero probability, $S_{\mathsf{dist}} \longmapsto S'$ permutes the qubits back to their original order, v' is fresh, $\sigma' = |\psi'\rangle$ is the result of measuring the qubits $\tilde{q}$ in σ^{**}, and P'_{M} is obtained from P^{**} by replacing $(v := \mathsf{measure}\ \tilde{q}).P_{\mathsf{M}}$ with $P_{\mathsf{M}}\{v'/v\}$. Then $S \Longmapsto S'$. By Lemma 5.9, then $[\![S']\!] = \langle [\![P'_{\mathsf{M}}\{\mathsf{b}(j)/v'\}]\!] \setminus \phi^{**}, \rho' \rangle = \langle [\![P'_{\mathsf{M}}]\!]\{\mathsf{b}(j)/v'\} \setminus \phi^{**}, \rho' \rangle$, where $\mathcal{E}_{\mathsf{b}(j),\tilde{q}}(\mathcal{M}_{\tilde{q}}\tilde{\rho^{**}})$ sets the system state to $\rho' = |\psi'\rangle\langle\psi'|$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^* and one additional step to reduce the choice that is the outermost operator of T_{M} to case j.

Case of $\mathcal{E}_{|0\rangle}[\mathcal{V}]$: By Definition 5.1, $\mathcal{E}_{|0\rangle}[\mathcal{V}]$ cannot guard a branch of a choice nor can $\mathcal{E}_{|0\rangle}[\mathcal{V}]$ guard the subterm of a conditional. Then T^* contains an unguarded subterm of the form $\mathcal{E}_{|0\rangle}[\mathcal{V}].\big(T_{\mathsf{qbit}}\{q_{|\mathcal{V}|}/x\}\big)$ that is reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains an unguarded subterm $(\mathsf{qubit}\ x)P_{\mathsf{qbit}}$ that was translated into $\mathcal{E}_{|0\rangle}[\mathcal{V}].\big(T_{\mathsf{qbit}}\{q_{|\mathcal{V}|}/x\}\big)$. Then there is some S' such that $S^{**} \longmapsto S' = \Big(\sigma'; \phi^{**}; P'_{\mathsf{qbit}}\{q_{|\mathcal{V}|}/y\}\Big)$, where y is fresh, $\sigma' = |\psi^{**}\rangle \otimes |0\rangle = |\psi'\rangle$, and P'_{qbit} is obtained from P^{**} by replacing $(\mathsf{qubit}\ x)P_{\mathsf{qbit}}$ with $P_{\mathsf{qbit}}\{y/x\}$. Then $S \Longmapsto S'$. By Lemma 5.8, then $[\![S']\!] = \Big\langle \Big[\!\Big[P'_{\mathsf{qbit}}\{q_{|\mathcal{V}|}/y\}\Big]\!\Big] \setminus \phi^{**}, \rho' \Big\rangle = \Big\langle \Big[\!\Big[P'_{\mathsf{qbit}}\Big]\!\Big]\{q_{|\mathcal{V}|}/y\} \setminus \phi^{**}, \rho' \Big\rangle$, where $\rho' = \mathcal{E}_{|0\rangle,\mathcal{V}}(\rho^{**}) = |\psi'\rangle\langle\psi'|$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^*.

(3) By Definition 5.1, inputs or outputs cannot guard a branch of a choice nor can inputs or outputs guard the subterm of a conditional. Then T^* contains two unguarded subterms $c?x.T_{\mathsf{in}}$ and $c!q.T_{\mathsf{out}}$ that are reduced in the step $T^* \longmapsto T$. Because of Definition 5.1 and since $T^* \Longmapsto [\![S^{**}]\!]$ reduces only choices, then S^{**} contains two unguarded subterms $c?[x].P_{\mathsf{in}}$ and $c![q].P_{\mathsf{out}}$ that were translated into $c?x.T_{\mathsf{in}}$ and $c!q.T_{\mathsf{out}}$. Then there is

some S' such that $S^{**} \longmapsto S' = (\sigma^{**}; \phi^{**}; P_{\mathsf{com}})$, where P_{com} is obtained from P^{**} by replacing $c?[x].P_{\mathsf{in}}$ with $P_{\mathsf{in}}\{q/x\}$ and $c![q].P_{\mathsf{out}}$ with P_{out}. Then $S \Longmapsto S'$ and $[\![S']\!] = \langle [\![P_{\mathsf{com}}]\!] \setminus \phi^{**}, \rho^{**} \rangle$. Since $T^* \longmapsto T$ is not in conflict with any of the steps of $T^* \Longmapsto [\![S^{**}]\!]$, $T \Longmapsto [\![S']\!]$ performs the sequence $T^* \Longmapsto [\![S^{**}]\!]$ starting in T instead of T^*. □

Divergence reflection follows from the above soundness proof.

Lemma 5.12 (Divergence Reflection, $[\![\cdot]\!]$)**.**

$$\forall S \in \mathfrak{C}_{\mathsf{C}}.\ [\![S]\!] \longmapsto^{\omega} \ \textit{implies}\ S \longmapsto^{\omega}$$

Proof. By the variant of soundness that we show in the proof of Lemma 5.11, for every sequence $[\![S]\!] \Longmapsto T$ there is some $S' \in \mathfrak{C}_{\mathsf{C}}$ such that $S \Longmapsto S'$ and $T \Longmapsto [\![S']\!]$, where the sequence $S \Longmapsto S'$ is at least as long as $T \Longmapsto [\![S']\!]$ (and often longer). Then for every sequence of target term steps there is a matching sequence of source term steps that is at least as long. This ensures divergence reflection. □

Success sensitiveness follows from the homomorphic translation of ✓ in Definition 5.1 and operational correspondence.

Lemma 5.13 (Success Sensitiveness, $[\![\cdot]\!]$)**.**

$$\forall S \in \mathfrak{C}_{\mathsf{C}}.\ S{\Downarrow_{\checkmark}}\ \textit{iff}\ [\![S]\!]{\Downarrow_{\checkmark}}$$

Proof. By Definition 5.1, $S^*{\downarrow_{\checkmark}}$ iff $[\![S^*]\!]{\downarrow_{\checkmark}}$ for all S^*.

- If $S{\Downarrow_{\checkmark}}$, then $S \Longmapsto S'$ and $S'{\downarrow_{\checkmark}}$. By Lemma 5.10, then $[\![S]\!] \Longmapsto T$ and $[\![S']\!] \preceq T$. Since $\preceq$ is success sensitive and $S'{\downarrow_{\checkmark}}$ implies $[\![S']\!]{\downarrow_{\checkmark}}$, then $T{\downarrow_{\checkmark}}$ and, thus, $[\![S]\!]{\Downarrow_{\checkmark}}$.
- If $[\![S]\!]{\Downarrow_{\checkmark}}$, then $[\![S]\!] \Longmapsto T$ and $T{\downarrow_{\checkmark}}$. By the proof of Lemma 5.11, then $S \Longmapsto S'$ and $T \Longmapsto [\![S']\!]$. Since $[\![S']\!]{\downarrow_{\checkmark}}$ implies $S'{\downarrow_{\checkmark}}$, then $S'{\downarrow_{\checkmark}}$ and, thus, $S{\Downarrow_{\checkmark}}$. □

Compositionality follows directly from the encoding function, i.e., as we can observe in Definition 5.1 every source term operator is translated in a compositional way. With that we can show that the encoding $[\![\cdot]\!]$ satisfies the properties (1) compositionality, (2) name invariance, (3) operational correspondence, (4) divergence reflection, and (5) success sensitiveness.

Theorem 5.14. *The encoding $[\![\cdot]\!]$ is good.*

Proof. By Definition 5.1, $[\![\cdot]\!]$ is compositional, because we can derive the required contexts from the right hand side of the equations by replacing the encodings of the respective sub-terms by holes $[\cdot]$.

By Lemma 5.7, $[\![\cdot]\!]$ is name invariant.

By Lemma 5.10 and Lemma 5.11, $[\![\cdot]\!]$ is operationally corresponding with respect to the success sensitive correspondence simulation $\preceq$.

By Lemma 5.12, $[\![\cdot]\!]$ reflects divergence.

By Lemma 5.13, $[\![\cdot]\!]$ is success sensitive. □

By [PvG15], Theorem 5.14 implies that there is a correspondence simulation that relates source terms S and their literal translations $[\![S]\!]$. To refer to a more standard equivalence, this also implies that S and $[\![S]\!]$ are coupled similar (for the relevance of coupled similarity see e.g. [BNP20]). Proving operational correspondence w.r.t. a bisimulation would not significantly tighten the connection between the source and the target. To really tighten the connection such that S and $[\![S]\!]$ are bisimilar, we need a stricter variant of operational correspondence and for that a more direct translation of probability distributions to avoid the

problem discussed in Example 5.4. Indeed [FDY12] introduces probability distributions to qCCS and a corresponding alternative of measurement that allows to translate this operator homomorphically. However, in this study we are more concerned about the quality criteria. Hence using them to compare languages that treat qubits fundamentally differently is more interesting here. Moreover, to tighten the connection we would need a probabilistic version of operational correspondence and accordingly a probabilistic version of bisimulation. Very recently we introduced probabilistic operational correspondence in [SP23].

To illustrate the encoding $[\![\cdot]\!]$ on a practical relevant example, we present the translation of the quantum teleportation protocol in Example 3.5.

Example 5.15. By Definition 5.1,

$$\begin{aligned}
[\![S]\!] &= \langle \tau.([\![Alice(q_0,q_1)]\!] \parallel [\![Bob(q_2)]\!]), \rho_0\rangle \\
[\![Alice(q_0,q_1)]\!] &= \mathsf{CNOT}[q0,q_1].\mathcal{H}[q_0].\mathcal{M}[q_0,q_1].\mathsf{D}(q_0,q_1;v_0;c!q_0.c!q_1.\mathsf{nil}) \\
[\![Bob(q_2)]\!] &= c?x_0.c?x_1.\mathcal{M}[x_0,x_1].\mathsf{D}(x_0,x_1;v;T_B) \\
T_B &= \mathsf{if}\ v=00\ \mathsf{then}\ \tau.\checkmark \parallel \mathsf{if}\ v=01\ \mathsf{then}\ \tau.\mathcal{X}[q_2].\checkmark \parallel \\
&\qquad \mathsf{if}\ v=10\ \mathsf{then}\ \tau.\mathcal{Z}[q_2].\checkmark \parallel \mathsf{if}\ v=11\ \mathsf{then}\ \tau.\mathcal{Y}[q_2].\checkmark
\end{aligned}$$

where $\rho_0 = |\psi_0\rangle\langle\psi_0|$. By Figure 3, $[\![S]\!]$ can do the following sequence of steps to emulate the sequence in Example 3.5

$$\begin{aligned}
[\![S]\!] &\longmapsto \langle [\![Alice(q_0,q_1)]\!] \parallel [\![Bob(q_2)]\!], \rho_0\rangle \\
&\longmapsto \langle \mathcal{H}[q_0].\mathcal{M}[q_0,q_1].\mathsf{D}(q_0,q_1;v_0;c!q_0.c!q_1.\mathsf{nil}) \parallel [\![Bob(q_2)]\!], \rho_1\rangle \\
&\longmapsto \langle \mathcal{M}[q_0,q_1].\mathsf{D}(q_0,q_1;v_0;c!q_0.c!q_1.\mathsf{nil}) \parallel [\![Bob(q_2)]\!], \rho_2\rangle \\
&\longmapsto \langle \mathsf{D}(q_0,q_1;v_0;c!q_0.c!q_1.\mathsf{nil}) \parallel [\![Bob(q_2)]\!], \rho_3\rangle = T^*
\end{aligned}$$

where $\rho_1 = \mathsf{CNOT}[q_0,q_1](\rho_0)$, $\rho_2 = \mathcal{H}[q_0](\rho_1)$, $\rho_3 = \mathcal{M}[q_0,q_1](\rho_2)$, and the state ρ_3 corresponds to $|\psi_2\rangle = q_0,q_1,q_2 = \frac{1}{2}|001\rangle + \frac{1}{2}|010\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle$ in Example 3.5.

$$\begin{aligned}
\mathsf{D}(q_0,q_1;v_0;c!q_0.c!q_1.\mathsf{nil}) = {} & (\mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.c!q_0.c!q_1.\mathsf{nil}) + \\
& (\mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.c!q_0.c!q_1.\mathsf{nil}) + \\
& (\mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.c!q_0.c!q_1.\mathsf{nil}) + \\
& (\mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.c!q_0.c!q_1.\mathsf{nil}) +
\end{aligned}$$

As in Example 3.5 we choose again the first branch:

$$\begin{aligned}
T^* &\longmapsto \langle c!q_0.c!q_1.\mathsf{nil} \parallel [\![Bob(q_2)]\!], \rho_4\rangle \\
&\longmapsto \langle c!q_1.\mathsf{nil} \parallel c?x_1.\mathcal{M}[q_0,x_1].\mathsf{D}(q_0,x_1;v;T_B), \rho_4\rangle \\
&\longmapsto \langle \mathcal{M}[q_0,q_1].\mathsf{D}(q_0,q_1;v;T_B), \rho_4\rangle \\
&\longmapsto \langle \mathsf{D}(q_0,q_1;v;T_B), \rho_4\rangle = T^{**}
\end{aligned}$$

where $\rho_4 = \mathcal{E}_{0,q_0,q_1}(\rho_3) = |001\rangle\langle 001|$. Note that the measurement in the last of the above steps has no effect on the state, since q_0 and q_1 are already both in the base state $|0\rangle$. Because of that $\mathsf{D}(q_0,q_1;v;T_B)$ can only reduce to the first state of T_B.

$$\begin{aligned}
T^{**} &\longmapsto \left\langle \begin{array}{l} \mathsf{if}\ 00=00\ \mathsf{then}\ \tau.\checkmark \parallel \mathsf{if}\ 00=01\ \mathsf{then}\ \tau.\mathcal{X}[q_2].\checkmark \parallel \\ \mathsf{if}\ 00=10\ \mathsf{then}\ \tau.\mathcal{Z}[q_2].\checkmark \parallel \mathsf{if}\ 00=11\ \mathsf{then}\ \tau.\mathcal{Y}[q_2].\checkmark \end{array}, \rho_4 \right\rangle \\
&\longmapsto \left\langle \begin{array}{l} \checkmark \parallel \mathsf{if}\ 00=01\ \mathsf{then}\ \tau.\mathcal{X}[q_2].\checkmark \parallel \\ \mathsf{if}\ 00=10\ \mathsf{then}\ \tau.\mathcal{Z}[q_2].\checkmark \parallel \mathsf{if}\ 00=11\ \mathsf{then}\ \tau.\mathcal{Y}[q_2].\checkmark \end{array}, \rho_4 \right\rangle
\end{aligned}$$

□

6. Separating Quantum Based Systems

Since super-operators are more expressive than unitary transformations, an encoding from qCCS or OQS into CQP or CQS is more difficult.

Example 6.1 (Phase Flip Channel)**.** Consider the operator $\mathcal{Q}(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger$, where $E_0 = \sqrt{0.5}\mathcal{I} = \begin{pmatrix}\sqrt{0.5} & 0\\ 0 & \sqrt{0.5}\end{pmatrix}$ and $E_1 = \sqrt{0.5}\mathcal{Z} = \begin{pmatrix}\sqrt{0.5} & 0\\ 0 & -\sqrt{0.5}\end{pmatrix}$, that is presented under the name *phase flip* channel in [NC10, Section 8.3.3] (for $p = 0.5$) as an operator to introduce noise. Note that $E_0^\dagger E_0 + E_1^\dagger E_1 = \mathcal{I}$. By Definition 2.1, $\mathcal{Q}$ is then a trace-preserving super-operator (in sum representation). $\mathcal{Q}$ sometimes behaves as identity, in particular we have $\mathcal{Q}(|0\rangle\langle 0|) = |0\rangle\langle 0|$ and $\mathcal{Q}(|1\rangle\langle 1|) = |1\rangle\langle 1|$, and sometimes it changes a qubit, in particular we have $\mathcal{Q}(|+\rangle\langle +|) = \begin{pmatrix}0.5 & 0\\ 0 & 0.5\end{pmatrix} = \mathcal{Q}(|-\rangle\langle -|)$. □

It is easy to show that there is no unitary transformation with the behaviour of $\mathcal{Q}$. However, to prove that there is no encoding from qCCS into CQP, we have to show additionally that this operator can also not be emulated using measurement. Therefore, we use the fact that measurement destroys entanglement. More precisely, we consider 2-qubit systems and use a bell pair as starting state to prove that even with measurement the behaviour of $\mathcal{Q}$ cannot be emulated.

Example 6.2 (Counterexample)**.** Consider $\mathcal{Q}$ of Example 6.1 applied to the second bit of a 2-qubit system:

$$\begin{aligned}\mathcal{Q}_2(\rho) =\ & (\mathcal{I}\otimes E_0)\,\rho\,(\mathcal{I}\otimes E_0)^\dagger + (\mathcal{I}\otimes E_1)\,\rho\,(\mathcal{I}\otimes E_1)^\dagger\\ =\ & \begin{pmatrix}\sqrt{0.5} & 0 & 0 & 0\\ 0 & \sqrt{0.5} & 0 & 0\\ 0 & 0 & \sqrt{0.5} & 0\\ 0 & 0 & 0 & \sqrt{0.5}\end{pmatrix}\rho\begin{pmatrix}\sqrt{0.5} & 0 & 0 & 0\\ 0 & \sqrt{0.5} & 0 & 0\\ 0 & 0 & \sqrt{0.5} & 0\\ 0 & 0 & 0 & \sqrt{0.5}\end{pmatrix} +\\ & \begin{pmatrix}\sqrt{0.5} & 0 & 0 & 0\\ 0 & -\sqrt{0.5} & 0 & 0\\ 0 & 0 & \sqrt{0.5} & 0\\ 0 & 0 & 0 & -\sqrt{0.5}\end{pmatrix}\rho\begin{pmatrix}\sqrt{0.5} & 0 & 0 & 0\\ 0 & -\sqrt{0.5} & 0 & 0\\ 0 & 0 & \sqrt{0.5} & 0\\ 0 & 0 & 0 & -\sqrt{0.5}\end{pmatrix}\end{aligned}$$

Accordingly, $\mathcal{Q}_2(x) = x$ for all $x \in \{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$, $\mathcal{Q}_2(|0+\rangle\langle 0+|) = \begin{pmatrix}0.5 & 0 & 0 & 0\\ 0 & 0.5 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$, and $\mathcal{Q}_2\left(\begin{pmatrix}0.5 & 0 & 0 & 0.5\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0.5 & 0 & 0 & 0.5\end{pmatrix}\right) = \begin{pmatrix}0.5 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0.5\end{pmatrix}$ for the bell pair that resembles $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. To observe this strange behaviour of $\mathcal{Q}$ we measure directly or apply Hadamard and then measure. Therefore we use the OQS-terms

$$\begin{aligned}S_{00} =\ & \mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark + \mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} +\\ & \mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil}\\ S_{01} =\ & \mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark +\\ & \mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil}\\ S_{10} =\ & \mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} +\end{aligned}$$

$$\begin{aligned}
&\mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark + \mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil}\\
S_{11} = {}&\mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} +\\
&\mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark\\
S_{00+11} = {}&\mathsf{if}\ 00 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark + \mathsf{if}\ 01 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} +\\
&\mathsf{if}\ 10 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\mathsf{nil} + \mathsf{if}\ 11 = \mathcal{M}[q_0,q_1]\ \mathsf{then}\ \tau.\checkmark
\end{aligned}$$

such that S_{ij} reaches success if and only if ij is measured and S_{00+11} reaches success if and only if 00 or 11 is measured. From that we build the OQS-configurations

$$\begin{aligned}
\mathsf{S}_{\mathsf{ce1}}(\rho) &= \langle \mathcal{Q}[q_1].S_{00}, \rho\rangle\\
\mathsf{S}_{\mathsf{ce2}}(\rho) &= \langle \mathcal{Q}[q_1].S_{01}, \rho\rangle\\
\mathsf{S}_{\mathsf{ce3}}(\rho) &= \langle \mathcal{Q}[q_1].S_{10}, \rho\rangle\\
\mathsf{S}_{\mathsf{ce4}}(\rho) &= \langle \mathcal{Q}[q_1].S_{11}, \rho\rangle\\
\mathsf{S}_{\mathsf{ce5}}(\rho) &= \langle \mathcal{Q}[q_1].\mathcal{H}[q_1].S_{01}, \rho\rangle\\
\mathsf{S}_{\mathsf{ce6}}(\rho) &= \langle \mathcal{Q}[q_1].S_{00+11}, \rho\rangle
\end{aligned}$$

for the 2-qubit system $\rho = q_0, q_1$. In particular, we use that $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$, $\mathsf{S}_{\mathsf{ce2}}(|01\rangle\langle 01|)$, $\mathsf{S}_{\mathsf{ce3}}(|10\rangle\langle 10|)$, and $\mathsf{S}_{\mathsf{ce4}}(|11\rangle\langle 11|)$ must reach success, whereas $\mathsf{S}_{\mathsf{ce5}}(|0+\rangle\langle 0+|)$ may but not must reach success, to show that $\mathcal{Q}$ cannot be emulated by unitary transformations. Since Hadamard $\mathcal{H}$ applied to $\mathcal{Q}(|+\rangle\langle +|)$ is again $\mathcal{Q}(|+\rangle\langle +|)$, we measure in $\mathsf{S}_{\mathsf{ce5}}$ after applying $\mathcal{Q}[q_1].\mathcal{H}[q_1]$ either 00 or 01 with equal probability. In the latter case success $\checkmark$ is unguarded, whereas the former case does not unguard success, i.e., $\mathsf{S}_{\mathsf{ce5}}(|0+\rangle\langle 0+|)$ may but not must reach success. Finally, we use that $\mathsf{S}_{\mathsf{ce6}}$ for the bell pair that resembles $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ must reach success, to show that also measurement does not allow to emulate $\mathcal{Q}$. Note that the first qubit is only relevant for this last step, i.e., for $\mathsf{S}_{\mathsf{ce6}}$. □

An encoding from qCCS or OQS into CQP or CQS needs to emulate the behaviour of $\mathcal{Q}[q_1]$. Since CQP and CQS do not allow for super-operators but only unitary transformations and since there is no unitary transformation with the same effect as $\mathcal{Q}[q_1]$, there is no good encoding from OQS into CQS or qCCS into CQP. To prove this separation result we borrow a technical result from [PNG13]. By success sensitiveness, a source term S reaches success if and only if its literal translation $[\![S]\!]$ reaches success. As a consequence S cannot reach success if and only if $[\![S]\!]$ cannot reach success. The next lemma shows that operational correspondence and success sensitiveness also imply that S must reach success, i.e., reaches success in all finite traces, if and only if $[\![S]\!]$ must reach success.

Lemma 6.3. *For all operationally corresponding, success sensitive encodings $[\![\cdot]\!]$ w.r.t. some success respecting preorder $\preceq$ on the target and for all source configurations S, S must reach success in all finite traces iff $[\![S]\!]$ must reach success in all finite traces.*

Proof. We consider both directions separately.

if S must reach success then also $[\![S]\!]$: Assume the opposite, i.e., there is an encoding that satisfies the criteria operational soundness and success sensitiveness, $\preceq$ is success respecting, and there is some source configuration S such that for all S' with $S \Longmapsto S'$ we have $S'\Downarrow_{\checkmark}$, i.e., S must reach success in all finite traces, but there is some target configuration T such that $[\![S]\!] \Longmapsto T$ and T cannot reach success.

Since $[\![\cdot]\!]$ is operationally sound, $[\![S]\!] \Longmapsto T$ implies that there exist some S'', T'' such that $S \Longmapsto S''$, $T \Longmapsto T''$, and $[\![S'']\!] \preceq T''$. Since T cannot reach success and

$T \Longmapsto T''$, then T'' cannot reach success. Since $\preceq$ respects success, $[\![S'']\!] \preceq T''$ and that T'' cannot reach success imply that $[\![S'']\!]$ cannot reach success. Because $[\![\cdot]\!]$ is success sensitive, then also S'' cannot reach success, which contradicts the assumption that S must reach success. We conclude that if S must reach success in all finite traces then $[\![S]\!]$ must reach success in all finite traces.

if $[\![S]\!]$ must reach success then also S: Assume the opposite, i.e., there is an encoding that satisfies the criteria operational completeness and success sensitiveness, $\preceq$ is success respecting, and there is some source configuration S such that for all T with $[\![S]\!] \Longmapsto T$ we have $T{\Downarrow_{\checkmark}}$, i.e., $[\![S]\!]$ must reach success in all finite traces, but there is some source configuration S' such that $S \Longmapsto S'$ and S' cannot reach success.

Since $[\![\cdot]\!]$ is operationally complete, $S \Longmapsto S'$ implies that there exists some T' such that $[\![S]\!] \Longmapsto T'$ and $[\![S']\!] \preceq T'$. Because $[\![\cdot]\!]$ is success sensitive and S' cannot reach success, then also $[\![S']\!]$ cannot reach success. Since $\preceq$ respects success, $[\![S']\!] \preceq T'$ and that $[\![S']\!]$ cannot reach success imply that T' cannot reach success. Since T' cannot reach success and $[\![S]\!] \Longmapsto T'$, this contradicts the assumption that $[\![S]\!]$ must reach success. We conclude that if $[\![S]\!]$ must reach success in all finite traces then S must reach success in all finite traces. □

To prove the non-existence of an encoding from OQS into CQS, we use $\mathcal{Q}$ on a 2-quit system as described in Example 6.2 as a counterexample and show that it is not possible in CQS to emulate the behaviour of $\mathcal{Q}[q_1]$ modulo compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness. More precisely, since there is no unitary transformation with this behaviour and also measurement or additional qubits do not help to emulate this behaviour on the state of the qubit (see the proof of Theorem 6.4), there is no encoding from OQS into CQS that satisfies compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness.

Theorem 6.4. *There is no encoding from* OQS *into* CQS *that satisfies compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness.*

Proof. The proof is by contradiction, i.e., we assume that there is an encoding $[\![\cdot]\!]$ from OQS into CQS that satisfies compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness. In OQS we start with a configuration that contains two qubits (represented as a density matrix in ρ). The encoding translates this OQS-configuration into a CQS-configuration such that its state is captured in a vector σ. The encoding may use the qubits inside ρ directly for σ, or it may measure these qubits and uses the information gained in this measurement to construct σ. Remember that it is impossible to determine the exact state of a qubit and hence the entries for the density matrix. Using the original qubits directly results in a 2-qubit vector σ. From measuring the original qubits we cannot gain more than two bit information such that we again capture all the information in a 2-qubit vector σ. In other words, we can assume that the encoding translates a 2-qubit density matrix ρ into a 2-qubit vector σ, because there is no more information available to justify the use of more qubits in CQS, i.e., systems with more qubits won't provide more information.

By compositionality, then there is a CQS-context $\mathcal{C}_{\mathcal{Q}}([\cdot])$ such that

$$[\![\mathsf{S}_{\mathsf{ce1}}(\rho)]\!] = \big(\sigma; \phi_2; \mathcal{C}_{\mathcal{Q}}(T_1)\big)$$
$$[\![\mathsf{S}_{\mathsf{ce2}}(\rho)]\!] = \big(\sigma; \phi_2; \mathcal{C}_{\mathcal{Q}}(T_2)\big)$$

$$[\![\mathsf{S}_{\mathsf{ce3}}(\rho)]\!] = \big(\sigma;\phi_2;\mathcal{C}_{\mathcal{Q}}(T_3)\big)$$
$$[\![\mathsf{S}_{\mathsf{ce4}}(\rho)]\!] = \big(\sigma;\phi_2;\mathcal{C}_{\mathcal{Q}}(T_4)\big)$$
$$[\![\mathsf{S}_{\mathsf{ce5}}(\rho)]\!] = \big(\sigma;\phi_2;\mathcal{C}_{\mathcal{Q}}(T_5)\big)$$
$$[\![\mathsf{S}_{\mathsf{ce6}}(\rho)]\!] = \big(\sigma;\phi_2;\mathcal{C}_{\mathcal{Q}}(T_6)\big)$$

where

$$[\![\langle S_{00},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_1)$$
$$[\![\langle S_{01},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_2)$$
$$[\![\langle S_{10},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_3)$$
$$[\![\langle S_{11},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_4)$$
$$[\![\langle \mathcal{H}[q_1].S_{01},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_5)$$
$$[\![\langle S_{00+11},\rho\rangle]\!] = (\sigma;\phi_{\mathcal{M}};T_6)$$

and σ is the translation of ρ. Since the OQS-configurations in the source are parametric on ρ, the behaviour of the resulting CQS-configurations depends on σ. By operational correspondence and success sensitiveness, these contexts have to behave exactly as their respective sources w.r.t. the reachability of success (including the reachability of success in all finite traces as in Lemma 6.3). Since the behaviour of the translations depends only on σ as input, we can focus on the translation of $\mathcal{Q}[q_1]$ on the quantum register σ that $\mathcal{C}_{\mathcal{Q}}([\cdot])$ constructs from the input ρ. In CQP as well as CQS the only operators with direct influence on the quantum register are unitary transformations, measurement, and the creation of new qubits. Moreover, e.g. by communication or the probability distributions after measurement CQP-configurations or CQS-configurations can introduce branching and thus provide different results on different branches.

With the creation of new qubits the size of the vector is increased. Intuitively, $\mathcal{C}_{\mathcal{Q}}([\cdot])$ gets as input a 2-qubit vector and has to produce another 2-qubit vector as output, because $T_1 - T_6$ and $\mathcal{C}_{\mathcal{Q}}([\cdot])$ require a 2-qubit vector. Because of that, the creation of new qubits can only contribute to $\mathcal{C}_{\mathcal{Q}}([\cdot])$ by allowing to set a qubit to $|0\rangle$. Since this can also be done by measurement followed by a bit-flip if 1 was measured, we do not need to consider the creation of new qubits, i.e., this behaviour is subsumed by the other operations.

Note that we consider 2-bit vectors. Measuring one qubit in CQP or CQS creates a probability distribution with two cases that consist of their respective probability, which can be zero, followed by the configuration in the respective case. The overall evolution of closed systems—and CQP and CQS can express only closed systems—can be described by a unitary transformation. Accordingly, for the way in that $\mathcal{C}_{\mathcal{Q}}([\cdot])$ manipulates the 2-qubit vector the only relevant effect of measurement is (1) that it creates branches, (2) that some of these branches might have a zero-probability w.r.t. particular inputs but not necessarily all inputs, and (3) that the evolution of the 2-qubit vector in every of these branches is described by a unitary transformation, at least if we consider as inputs only the values $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, $|0+\rangle$, and $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

There are two sources for branching: either branching results from the probability distribution after measurement or from communication. Since the matrix multiplication of two unitary transformations is again a unitary transformation, sequences of unitary transformations can be abbreviated by a single unitary transformation. Accordingly, if we consider a single branch without measurement in $\mathcal{C}_{\mathcal{Q}}([\cdot])$ from the beginning to the end, the

transformation on the 2-qubit vector can be abbreviated by a single unitary transformation that is a 4×4-matrix.

Assume that all branches in $\mathcal{C}_{\mathcal{Q}}([\cdot])$ result from communication, i.e., $\mathcal{C}_{\mathcal{Q}}([\cdot])$ does not use measurement. Then for every branch there is a unitary transformation $U = \begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ u_{21} & u_{22} & u_{23} & u_{24} \\ u_{31} & u_{32} & u_{33} & u_{34} \\ u_{41} & u_{42} & u_{43} & u_{44} \end{pmatrix}$ that emulates $\mathcal{Q}[q_1]$ in this branch. Considering the behaviour of $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$ it follows

$$\begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ u_{21} & u_{22} & u_{23} & u_{24} \\ u_{31} & u_{32} & u_{33} & u_{34} \\ u_{41} & u_{42} & u_{43} & u_{44} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{array}{ll} \text{and therefore} & u_{11} = 1 \\ \text{and} & u_{21} = u_{31} = u_{41} = 0 \end{array}$$

for all branches, because $|00\rangle = (1,0,0,0)^{\mathsf{T}}$ is the only state such that T_1 applied to this state always unguards ✓ and $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$ must reach success. Repeating this calculation for $\mathsf{S}_{\mathsf{ce2}}(|01\rangle\langle 01|)$, $\mathsf{S}_{\mathsf{ce3}}(|10\rangle\langle 10|)$, and $\mathsf{S}_{\mathsf{ce1}}(|11\rangle\langle 11|)$, we conclude that $u_{ii} = 1$ for all $i \in \{1,2,3,4\}$ and $u_{ij} = 0$ for all $i,j \in \{1,2,3,4\}$ with $i \neq j$, i.e., that $U = \mathcal{I} \otimes \mathcal{I}$ is identity. But, if we apply this identity transformation U to $|0+\rangle$ we obtain $|0+\rangle$ and T_5 applied in this state cannot reach success, whereas $\mathsf{S}_{\mathsf{ce5}}(|0+\rangle\langle 0+|)$ may reach success. This is a contradiction, i.e., there is no such unitary transformation that emulates $\mathcal{Q}[q_1]$. Therefore, our assumption that all branches in $\mathcal{C}_{\mathcal{Q}}([\cdot])$ result from communication must be wrong, i.e., $\mathcal{C}_{\mathcal{Q}}([\cdot])$ has to measure.

Of course $\mathcal{C}_{\mathcal{Q}}([\cdot])$ may consist of a sequence of steps containing several measurements. From $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$, $\mathsf{S}_{\mathsf{ce2}}(|01\rangle\langle 01|)$, $\mathsf{S}_{\mathsf{ce3}}(|10\rangle\langle 10|)$, and $\mathsf{S}_{\mathsf{ce4}}(|11\rangle\langle 11|)$ it is obvious that measuring the first qubit does not contribute to the implementation of $\mathcal{Q}[q_1]$. It suffices to consider implementations of $\mathcal{C}_{\mathcal{Q}}([\cdot])$ that measure only the second qubit. More precisely, we consider only the last measurement of the second qubit that is performed in $\mathcal{C}_{\mathcal{Q}}([\cdot])$ in each of its branches. Without loss of generality we can assume that this measurement was performed w.r.t. the standard base, because all other cases can be implemented by a unitary transformation right before the measurement. Then there are two possible outcomes of every last measurement, $|0\rangle$ and $|1\rangle$, i.e., there are two possible branches but one of them might occur with probability zero. As usual we ignore branches that occur with probability zero. All transformations in $\mathcal{C}_{\mathcal{Q}}([\cdot])$ after the last measurement can again be subsumed in a single unitary transformation. Accordingly, $\mathcal{C}_{\mathcal{Q}}([\cdot])$ does perform some arbitrary initial steps that may contain an arbitrary number of measurements and might produce an arbitrary number of branches and each branch with measurement ends with the final measurement of the second qubit that produces one or two branches whose behaviour after the final measurement can be described respectively by a single unitary transformation.

We consider once more the case $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$. The last measurement of q_2 sets in every branch the qubit q_2 in σ to $|0\rangle$ or $|1\rangle$. Since $|00\rangle$ is the only state such that T_1 applied to this state always unguards ✓ and $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$ must reach success, the unitary transformation after the last measurement has to map the current state in every branch to $|00\rangle$. Let us call this unitary transformation U_0. Note that for instance $U_0 = \mathcal{I} \otimes \mathcal{I}$ would do the job, if the first qubit is still in state $|0\rangle$ before its application. Similarly, in all branches in that 1 was measured, the unitary transformation has to result in $|00\rangle$. Let us call this transformation U_1 and note that e.g. $\mathcal{I} \otimes \mathcal{X}$ can do this, if the first qubit is still in state $|0\rangle$. Accordingly,

in all branches in that the last measurement results in $|0\rangle$ this measurement is followed by U_0 and in all branches in that the last measurement results in $|1\rangle$ this measurement is followed by U_1, because this ensures that each branch of $\mathcal{C}_{\mathcal{Q}}([\cdot])$ for $|00\rangle$ finally results in $|00\rangle$ as required by T_1.

We apply the same argumentation for $|01\rangle$ instead of $|00\rangle$ and $\mathsf{S}_{\mathsf{ce2}}(|01\rangle\langle 01|)$ instead of $\mathsf{S}_{\mathsf{ce1}}(|00\rangle\langle 00|)$ to obtain the following: In all branches in that the last measurement results in $|0\rangle$ this measurement is followed by U_0 and in all branches in that the last measurement results in $|1\rangle$ this measurement is followed by some U_1 such that U_0, U_1 both ensure that the respective branch of $\mathcal{C}_{\mathcal{Q}}([\cdot])$ for $|01\rangle$ finally results in $|01\rangle$.

Note that this is not yet a contradiction. By compositionality, $\mathcal{C}_{\mathcal{Q}}([\cdot])$ has to be implemented by the same term regardless of whether we start with $|00\rangle$ or $|01\rangle$ and, thus, the mentioned U_0 and U_1 indeed have to be the same in both cases. And, obviously, there is no U_0 that applied to $|0\rangle$ for the second qubit sometimes results in $|0\rangle$ and sometimes in $|1\rangle$. But we do not necessarily always have two branches as result of measurement. So there are so far still two plausible scenarios: Either if we start with $|0\rangle$ for the second qubit only 0 is measured and if we start with $|1\rangle$ for the second qubit only 1 is measured or vice versa. In the former case we could e.g. pick $U_0 = U_1 = \mathcal{I} \times \mathcal{I}$ and in the latter case we could e.g. pick $U_0 = U_1 = \mathcal{I} \times \mathcal{X}$ (if the first qubit remains in its initial state). However, we have a contradiction for the case $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

In the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ measuring the second qubit we obtain either 0 or 1 with equal probability. Because of that, the implementation of $\mathcal{C}_{\mathcal{Q}}([\cdot])$ will have at least two branches with measurement on the second qubit such that in one branch after the last measurement of the second qubit U_0 is applied and in the other branch after the last measurement of the second qubit U_1 is applied. For both of the two plausible scenarios that are left, this means that in one branch the second qubit is set to $|0\rangle$ and in the other to $|1\rangle$. Note that the entanglement between the two qubits is destroyed (if not before then by this last measurement). Then it cannot be avoided that a subsequent measurement of both qubits will result in different values. This is in contradiction to $\mathsf{S}_{\mathsf{ce6}}$, because $\mathsf{S}_{\mathsf{ce6}}$ applied on the considered bell pair must reach success and therefore T_6 requires two qubits that always return the same value in measurement.

Accordingly, our original assumption, i.e., that there is an encoding $[\![\cdot]\!]$ from OQS into CQS that satisfies compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness is wrong: there is no such encoding. □

As we claim, the counterexample in Example 6.2 can be expressed similarly, i.e., with strongly bisimilar behaviour, in variants of qCCS with measurement operators as in [FDJY07, FDY12]. Moreover, even the full expressive power of CQP does not help to correctly emulate this super-operator. Hence, there is also no encoding from qCCS into CQP.

Corollary 6.5. *There is no encoding from qCCS with a measurement operator into CQP that satisfies compositionality, operational correspondence w.r.t. a success respecting preorder, and success sensitiveness.*

7. Quality Criteria for Quantum Based Systems

Sections 5 and 6 show that the quality criteria of Gorla in [Gor10] can be applied to quantum based systems and are still meaningful in this setting. They might, however, not be exhaustive, i.e., there might be aspects of quantum based systems that are relevant but not sufficiently covered by this set of criteria. To obtain these criteria, Gorla studied a large number of encodings, i.e., this set of criteria was built upon the experience of many researchers and years of work. Accordingly, we do not expect to answer the question 'what are good quality criteria for quantum based systems' now, but rather want to start the discussion.

A closer look at the criteria in Section 4 reveals a first candidate for an additional quality criterion. Name invariance ensures that encodings cannot cheat by treating names differently. It requires that good encodings preserve substitutions to some extend. CQP and qCCS model the dynamics of quantum registers in fundamentally different ways, but both languages address qubits by qubit names. It seems natural to extend name invariance to also cover qubit names.

As in [Gor10], we let our definition of qubit invariance depend on a renaming policy φ, where this renaming policy is for qubit names. The renaming policy translates qubit names of the source to tuples of qubit names in the target, i.e., $\varphi : \mathcal{V} \to \mathcal{V}^n$, where we require that $\varphi(q) \cap \varphi(q') = \emptyset$ whenever $q \neq q'$.

The new criterion *qubit invariance*, then requires that encodings preserve and reflect substitutions on qubits modulo the renaming policy on qubits.

Definition 7.1 (Qubit Invariance)**.** The encoding $[\![\cdot]\!]$ is *qubit invariant* if, for every $S \in \mathfrak{C}_{\mathsf{S}}$ and every substitution γ on qubit names, it holds that $[\![S\gamma]\!] = [\![S]\!]\gamma'$, where $\varphi(\gamma(q)) = \gamma'(\varphi(q))$ for every $q \in \mathcal{V}$.

In [Gor10], name invariance allows the slightly weaker condition $[\![S\gamma]\!] \preceq [\![S]\!]\gamma'$ for non-injective substitutions. In contrast, substitutions on qubits always have to be injective such that they cannot violate the no-cloning principle. Since $[\![\cdot]\!]$ translates qubit names to themselves and introduces no other qubit names, it satisfies qubit invariance for φ being the identity and $\gamma' = \gamma$. The corresponding proof is given above in Lemma 5.8.

Note that the qubits discussed so far are so-called *logical qubits*, i.e., they are abstractions of the physical qubits. To implement a single *logical qubit* as of today several *physical qubits* are necessary. These additional physical qubits are used to ensure stability and fault-tolerance in the implementation of logical qubits. Since the number of necessary physical qubits can be much larger than the number of logical qubits, already a small increase in the number of logical qubits might seriously limit the practicability of a system. Accordingly, one may require that encodings preserve the number of logical qubits.

Definition 7.2 (Size of Quantum Registers)**.** An encoding $[\![\cdot]\!]$ *preserves the size of quantum registers*, if for all $S \in \mathfrak{C}_{\mathsf{S}}$, the number of qubits in $[\![S]\!]$ is not greater than in S.

Again, the encoding $[\![\cdot]\!]$ in Definition 5.1 satisfies this criterion, which can be verified easily by inspection of the encoding function.

Lemma 7.3. *The encoding $[\![\cdot]\!]$ preserves the size of quantum registers, i.e., for all $S \in \mathfrak{C}_{\mathsf{S}}$, the number of qubits in $[\![S]\!]$ is not greater than in S.*

Proof. By Definition 5.1, the number of qubits in $[\![S]\!]$ is the same as the number of qubits in S. Moreover, $[\![\cdot]\!]$ does not introduce new qubits in any of its cases except as the encoding

of the creation of a new qubit in the source. Because of that, also the derivatives of source term translations have the same number of qubits as their respective source term equivalents. Thus, $[\![\cdot]\!]$ preserves the size of quantum registers. □

Similarly to success sensitiveness, requiring the preservation of the size of quantum registers on literal encodings is not enough. To ensure that all reachable target terms preserve the size of quantum registers, we again link this criterion with the target term relation $\preceq$. More precisely, we require that $\preceq$ is sensible to the size of quantum registers, i.e., $T_1 \preceq T_2$ implies that the quantum registers in T_1 and T_2 have the same size. The correspondence simulation $\preceq$ that we used as target relation for the encoding $[\![\cdot]\!]$ is not sensible to the size of quantum registers, but we can easily turn it into such a relation. Therefore, we simply add the condition that $|\rho| = |\sigma|$ whenever $\langle P, \rho\rangle \,\mathcal{R}\, \langle Q, \sigma\rangle$ to Definition 4.1. Fortunately, all of the already shown results remain valid for the altered version of $\preceq$.

In contrast to CQP, the semantics of OQS yields a non-probabilistic transition system, where probabilities are captured in the density matrices. The encoding $[\![\cdot]\!]$ translates probability distributions into non-deterministic choices. Thereby, branches with zero probability are correctly eliminated, but all remaining branches are treated similarly and their probabilities are forgotten. To check also the probabilities of branches, we can strengthen operational correspondence e.g. to a labelled variant, where labels capture the probability of a step. The challenge here is to create a meaningful criterion that correctly accumulates the probabilities in sequences of steps as e.g. a single source term step might be translated into a sequence of target term steps, but the product of the probabilities contained in the sequence has to be equal to the probability of the single source term step. As, to the best of our knowledge, there are no well-accepted probabilistic versions of operational correspondence. Because of that, we started to study probabilistic versions of operational correspondence and the nature of the relation between source and target they imply. Just recently we were able to publish three variants of probabilistic operational correspondence [SP23]. These criteria allow to more closely and more naturally connect the usually probabilistic quantum based systems.

Another important aspect is in how far the quality criteria capture the fundamental principles of quantum based systems such as the *no-cloning principle*: By the laws of quantum mechanics, it is not possible to exactly copy a qubit. Technically, such a copying would require some form of interaction with the qubit and this interaction would destroy its superposition, i.e., alter its state. Interestingly, the criteria of Gorla are even strong enough to observe a violation of this principle in the encoding from CQS into OQS, i.e., if we allow CQS to violate this principle but require that OQS respects it, then we obtain a negative result. Therefore, we remove the type system from CQS. Without this type system, we can use the same qubit at different locations, violating the no-cloning principle. As an example, consider $S = (\sigma; \phi; c![q].\mathbf{0} \mid c![q].\mathbf{0})$. Then the encoding $[\![\cdot]\!]$ in Definition 5.1 is not valid any more, because $[\![S]\!] = \langle (c!q.\mathsf{nil} \parallel c!q.\mathsf{nil}) \setminus \phi, \rho\rangle$ violates condition Cond2. Using S as counterexample, it should be possible to show that there exists no encoding that satisfies compositionality, operational correspondence, and success sensitiveness.

Of course, even if we succeed with this proof, this does not imply that the criteria are strong enough to sufficiently capture the no-cloning principle. Indeed, the other direction is more interesting, i.e., criteria that rule out encodings such that the source language respects the no-cloning principle but not all literal translations or their derivatives respect it. We believe that capturing the no-cloning principle and the other fundamental principles of quantum based systems is an interesting research challenge.

8. Conclusions

We proved that CQS can be encoded by OQS w.r.t. the quality criteria compositionality, name invariance, operational correspondence, divergence reflection, and success sensitiveness. Additionally, this encoding satisfies two new, quantum specific criteria: it is invariant to qubit names and preserves the size of quantum registers. We think that these new criteria are relevant for translations between quantum based systems.

The encoding proves that the way in that qCCS treats qubits—using density matrices and super-operators—can emulate the way in that CQP treats qubits. The other direction is more difficult. We showed that there exists no encoding from OQS into CQS that satisfies compositionality, operational correspondence, and success sensitiveness and claim that this also implies that there is no encoding from qCCS into CQP.

The results themselves may not necessarily be very surprising. The unitary transformations used in CQS/CQP are a subset of the super-operators used in OQS/qCCS and also density matrices can express more than the vectors used in CQS/CQP. What our case study proves is that the quality criteria that were originally designed for classical systems are still meaningful in this quantum based setting. They may, however, not be exhaustive. Accordingly, in Section 7 we start the discussion on quality criteria for this new setting of quantum based systems. The first two candidate criteria that we propose, namely qubit invariance and preservation of quantum register sizes, are relevant, but rather basic. Since the semantics of quantum based systems is often probabilistic, a variant of operational correspondence that requires the preservation and reflection of probabilities in the respective traces might be meaningful. The encoding $[\![\cdot]\!]$ presented above does not satisfy probabilistic operational correspondence as presented in [SP23]. More difficult and thus also more interesting are criteria that capture the fundamental principles of quantum based systems such as the no-cloning principle. Hereby, we pose the task of identifying such criteria as research challenge.

References

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.

[BNP20] Benjamin Bisping, Uwe Nestmann, and Kirstin Peters. Coupled similarity: the first 32 years. *Acta Informatica*, 57(3–5):439–463, 2020. doi:10.1007/s00236-019-00356-4.

[DGNP12] Timothy A. S. Davidson, Simon J. Gay, Rajagopal Nagarajan, and Ittoop V. Puthoor. Analysis of a Quantum Error Correcting Code using Quantum Process Calculus. In *Proceedings of QPL*, volume 95 of *EPTCS*, pages 67–80, 2012. doi:10.4204/EPTCS.95.7.

[DRMT+04] Hugues De Riedmatten, Ivan Marcikic, Wolfgang Tittel, Hugo Zbinden, Daniel Collins, and Nicolas Gisin. Long Distance Quantum Teleportation in a Quantum Relay Configuration. *Physical Review Letters*, 92:047904, 2004. doi:10.1103/PhysRevLett.92.047904.

[FDJY07] Yuan Feng, Runyao Duan, Zhengfeng Ji, and Mingsheng Ying. Probabilistic bisimulations for quantum processes. *Information and Computation*, 205(11):1608–1639, 2007. doi:10.1016/j.ic.2007.08.001.

[FDY12] Yuan Feng, Runyao Duan, and Mingsheng Ying. Bisimulation for Quantum Processes. *ACM Transactions on Programming Languages and Systems*, 34(4), 2012. doi:10.1145/2400676.2400680.

[FGP13] Sonja Franke-Arnold, Simon J. Gay, and Ittoop V. Puthoor. Quantum Process Calculus for Linear Optical Quantum Computing. In *Proceedings of Reversible Computation*, volume 7948 of *LNCS*, pages 234–246. Springer, 2013. doi:10.1007/978-3-642-38986-3_19.

[FGP14] Sonja Franke-Arnold, Simon J. Gay, and Ittoop V. Puthoor. Verification of Linear Optical Quantum Computing using Quantum Process Calculus. In *Preoceedings of EXPRESS/SOS*, volume 160 of *EPTCS*, pages 111–129, 2014. doi:10.4204/EPTCS.160.10.

[Gay06] Simon J. Gay. Quantum programming languages: survey and bibliography. *Mathematical Structures of Computer Science*, 16(4):581–600, 2006. doi:10.1017/S0960129506005378.

[GN05] Simon J. Gay and Rajagopal Nagarajan. Communicating quantum processes. In *Proceedings of POPL*, pages 145–157, 2005. doi:10.1145/1040305.1040318.

[Gor10] Daniele Gorla. Towards a Unified Approach to Encodability and Separation Results for Process Calculi. *Information and Computation*, 208(9):1031–1053, 2010. doi:10.1016/j.ic.2010.05.002.

[GP12] Simon J. Gay and Ittoop V. Puthoor. Application of Quantum Process Calculus to Higher Dimensional Quantum Protocols. In *Proceedings of Quantum Physics and Logic*, volume 158 of *EPTCS*, pages 15–28, 2012. doi:10.4204/EPTCS.158.2.

[Gru09] Jozef Gruska. Quantum Computing. In *Wiley Encyclopedia of Computer Science and Engineering*. John Wiley & Sons, Inc., 2009. doi:10.1002/9780470050118.ecse720.

[JL04] Philippe Jorrand and Marie Lalire. Toward a Quantum Process Algebra. In *Proceedings of CF*, pages 111–119, 2004. doi:10.1145/977091.977108.

[KKK+12] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. Application of a process calculus to security proofs of quantum protocols. In *Proceedings of FCS*, 2012.

[KKK+13] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. Automated Verification of Equivalence on Quantum Cryptographic Protocols. *EPiC Series in Computing*, 15:64–69, 2013.

[KPY16] Dimitrios Kouzapas, Jorge A. Pérez, and Nobuko Yoshida. On the Relative Expressiveness of Higher-Order Session Processes. In *Proceedings of ESOP*, volume 9632 of *LNCS*, pages 446–475, 2016. doi:10.1007/978-3-662-49498-1_18.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2010. doi:10.1017/cbo9780511976667.016.

[Pet19] Kirstin Peters. Comparing Process Calculi Using Encodings. In *Proceedings of EXPRESS/SOS*, volume 300 of *EPCTS*, pages 19–38, 2019. doi:10.4204/EPTCS.300.2.

[Plo04] Gordon D. Plotkin. A Structural Approach to Operational Semantics. *Journal of Logic and Algebraic Programming*, 60:17–140, 2004. [An earlier version of this paper was published as technical report at Aarhus University in 1981.].

[PNG13] Kirstin Peters, Uwe Nestmann, and Ursula Goltz. On Distributability in Process Calculi. In *Proceedings of ESOP*, volume 7792 of *LNCS*, pages 310–329, 2013. doi:10.1007/978-3-642-37036-6_18.

[PvG15] Kirstin Peters and Rob van Glabbeek. Analysing and Comparing Encodability Criteria. In *Proceedings of EXPRESS/SOS*, volume 190 of *EPTCS*, pages 46–60, 2015. doi:10.4204/EPTCS.190.4.

[RP00] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, 2000. doi:10.1145/367701.367709.

[SP23] Anna Schmitt and Kirstin Peters. Probabilistic Operational Correspondence. In *Proceedings of CONCUR*, volume 279 of *LIPIcs*, pages 15:1–15:17, 2023. doi:10.4230/LIPIcs.CONCUR.2023.15.

[SPD22a] Anna Schmitt, Kirstin Peters, and Yuxin Deng. Encodability Criteria for Quantum Based Systems. In *Proceedings of Forte*, volume 13273 of *LNCS*, pages 151–169. Springer, 2022. doi:10.1007/978-3-031-08679-3_10.

[SPD22b] Anna Schmitt, Kirstin Peters, and Yuxin Deng. Encodability Criteria for Quantum Based Systems (Technical Report). Technical report, 2022. doi:10.48550/ARXIV.2204.06068.

[YFDJ09] Mingsheng Ying, Yuan Feng, Runyao Duan, and Zhengfeng Ji. An algebra of quantum processes. *ACM Transactions on Computational Logic*, 10(3):1–36, 2009. doi:10.1145/1507244.1507249.

[YKK14] Kazuya Yasuda, Takahiro Kubota, and Yoshihiko Kakutani. Observational Equivalence Using Schedulers for Quantum Processes. In *Proceedings of Quantum Physics and Logic*, volume 172 of *EPTCS*, pages 191–203, 2014. doi:10.4204/EPTCS.172.13.

Appendix A. Type System of Closed Quantum Systems

Lemma 3.2 states that:

If $\Sigma \vdash P$ then $\mathsf{fq}(P) \subseteq \Sigma$.

Proof of Lemma 3.2. Assume $\Sigma \vdash P$. We perform an induction on the structure of P.

$P = \mathbf{0}$**:** Then $\mathsf{fq}(P) = \emptyset \subseteq \Sigma$.
$P = \checkmark$**:** Then $\mathsf{fq}(P) = \emptyset \subseteq \Sigma$.
$P = Q \mid R$**:** By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash Q$, $\Sigma_2 \vdash R$, and $\Sigma = \Sigma_1 \cup \Sigma_2$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma_1$ and $\mathsf{fq}(R) \subseteq \Sigma_2$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q) \cup \mathsf{fq}(R)$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = c?[x].Q$**:** By (T-In), then $c \in \mathcal{N}$, $x \in \mathcal{V} \setminus \Sigma$, and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma \cup \{x\}$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q) \setminus \{x\}$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = c![x].Q$**:** By (T-Out), then $c \in \mathcal{N}$, $x \in \mathcal{V} \cap \Sigma$, and $\Sigma \setminus \{x\} \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma \setminus \{x\}$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q) \cup \{x\}$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = \{x_1, \ldots, x_n \mathrel{*}= U\}.Q$**:** By (T-Trans), then $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, $\vdash U{:}\mathsf{Op}(n)$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q)$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = (v' := \mathsf{measure}\ x_1, \ldots, x_n).Q$**:** By (T-Msure), then $v' \in \mathcal{B}$, $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q)$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = (\mathsf{new}\ c)Q$**:** By (T-New), then $c \in \mathcal{N}$ and $\Sigma \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q)$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = (\mathsf{qubit}\ x)Q$**:** By (T-Qbit), then $x \in \mathcal{V} \setminus \Sigma$ and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma \cup \{x\}$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q) \setminus \{x\}$, then $\mathsf{fq}(P) \subseteq \Sigma$.
$P = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ Q$**:** By (T-Cond), then $bv_1 \in \mathcal{B}$ or $\vdash bv_1{:}\mathsf{Bin}$, $bv_2 \in \mathcal{B}$ or $\vdash bv_2{:}\mathsf{Bin}$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\mathsf{fq}(Q) \subseteq \Sigma$. Since $\mathsf{fq}(P) = \mathsf{fq}(Q)$, then $\mathsf{fq}(P) \subseteq \Sigma$. □

Well-typedness is preserved modulo structural congruence.

Lemma A.1. *If $\Sigma \vdash P$ and $P \equiv Q$ then $\Sigma \vdash Q$.*

Proof. Remember that we assume that there are no name clashes in P or Q. The proof is then by straightforward induction on the rules of structural congruence. □

Well-typedness is also preserved modulo substitutions of variables for binary numbers.

Lemma A.2. *If $\Sigma \vdash P$, $v \in \mathcal{B}$, and $bv \in \mathcal{B}$ or $\vdash bv{:}\mathsf{Bin}$ then $\Sigma \vdash P\{bv/v\}$.*

Proof. Assume $\Sigma \vdash P$, $v \in \mathcal{B}$, and $bv \in \mathcal{B}$ or $\vdash bv{:}\mathsf{Bin}$. We perform an induction on the structure of P.

$P = \mathbf{0}$**:** Then $P = P\{bv/v\}$ and thus $\Sigma \vdash P$ implies $\Sigma \vdash P\{bv/v\}$.
$P = \checkmark$**:** Then $P = P\{bv/v\}$ and thus $\Sigma \vdash P$ implies $\Sigma \vdash P\{bv/v\}$.
$P = Q \mid R$**:** By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash Q$, $\Sigma_2 \vdash R$, $\Sigma = \Sigma_1 \cup \Sigma_2$, and $\Sigma_1 \cap \Sigma_2 = \emptyset$. By the induction hypothesis, then $\Sigma_1 \vdash Q\{bv/b\}$ and $\Sigma_2 \vdash R\{bv/v\}$. Since $P\{bv/v\} = Q\{bv/b\} \mid R\{bv/v\}$ and because of (T-Par), then $\Sigma \vdash P\{bv/v\}$.
$P = c?[x].Q$**:** By (T-In), then $c \in \mathcal{N}$, $x \in \mathcal{V} \setminus \Sigma$, and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \cup \{x\} \vdash Q\{bv/v\}$. Since $P\{b_2/b_1\} = c?[x].\,(Q\{bv/v\})$ and because of (T-In), then $\Sigma \vdash P\{bv/v\}$.

$P = c![x].Q$**:** By (T-Out), then $c \in \mathcal{N}$, $x \in \mathcal{V} \cap \Sigma$, and $\Sigma \setminus \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \setminus \{x\} \vdash Q\{bv/v\}$. Since $P\{bv/v\} = c![x].\,(Q\{bv/v\})$ and because of (T-Out), then $\Sigma \vdash P\{bv/v\}$.

$P = \{x_1, \ldots, x_n \mathrel{*}= U\}.Q$**:** By (T-Trans), then $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, $\vdash U{:}\mathsf{Op}(n)$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{bv/v\}$. Since $P\{bv/v\} = \{x_1, \ldots, x_n \mathrel{*}= U\}.\,(Q\{bv/v\})$ and because of (T-Trans), then $\Sigma \vdash P\{bv/v\}$.

$P = (v' := \mathsf{measure}\ x_1, \ldots, x_n).Q$**:** By (T-Msure), then $v' \in \mathcal{B}$, $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{bv/v\}$. If $v' = v$ then $P\{bv/v\} = P$, since v' is bound. Then $\Sigma \vdash P$ implies $\Sigma \vdash P\{bv/v\}$. Else if $v' \neq v$ then $P\{bv/v\} = (v' := \mathsf{measure}\ x_1, \ldots, x_n).\,(Q\{bv/v\})$. By (T-Msure), then $\Sigma \vdash P\{bv/v\}$.

$P = (\mathsf{new}\ c)Q$**:** By (T-New), then $c \in \mathcal{N}$ and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{bv/v\}$. Since $P\{bv/v\} = (\mathsf{new}\ c)\,(Q\{bv/v\})$ and because of (T-New), then $\Sigma \vdash P\{bv/v\}$.

$P = (\mathsf{qubit}\ x)Q$**:** By (T-Qbit), then $x \in \mathcal{V} \setminus \Sigma$ and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \cup \{x\} \vdash Q\{bv/v\}$. Since $P\{bv/v\} = (\mathsf{qubit}\ x)\,(Q\{bv/v\})$ and because of (T-Qbit), then $\Sigma \vdash P\{bv/v\}$.

$P = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ Q$**:** By (T-Cond), then $bv_1 \in \mathcal{B}$ or $\vdash bv_1{:}\mathsf{Bin}$, $bv_2 \in \mathcal{B}$ or $\vdash bv_2{:}\mathsf{Bin}$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{bv/v\}$. Then $P\{bv/v\} = \mathsf{if}\ bv_1^* = bv_2^*\ \mathsf{then}\ (Q\{bv/v\})$, where $bv_1^* = bv$ if $bv_1 = v$ and else $bv_1^* = bv_1$ and similarly $bv_2^* \in \{bv_2, bv\}$. By (T-Msure) and $bv \in \mathcal{B}$ or $\vdash bv{:}\mathsf{Bin}$, then $\Sigma \vdash P\{bv/v\}$. □

Let $\mathsf{bq}(P)$ denote the set of bound qubit (variables) in P. Well-typedness is preserved modulo adding qubit names to Σ that are not bound in P.

Lemma A.3. *If $\Sigma \vdash P$ and $x \in \mathcal{V} \setminus \mathsf{bq}(P)$ then $\Sigma \cup \{x\} \vdash P$.*

Proof. Assume $\Sigma \vdash P$ and $x \in \mathcal{V} \setminus \mathsf{bq}(P)$. The proof is by straightforward induction on the rules in Figure 2 to derive $\Sigma \vdash P$. The only interesting cases are for (T-In) and (T-Qbit).

(T-In) : Then $P = c?[y].Q$, $c \in \mathcal{N}$, $y \in \mathcal{V} \setminus \Sigma$, and $\Sigma \cup \{y\} \vdash Q$. Since $x \in \mathcal{V} \setminus \mathsf{bq}(P)$, $x \neq y$. By the induction hypothesis, then $\Sigma \cup \{x, y\} \vdash Q$. By (T-In), then $\Sigma \cup \{x\} \vdash P$.

The case of (T-Qbit) is similar. Note that for (T-Par) it does not matter to which parallel component we give the additional x. □

Well-typedness is also preserved modulo removing qubit names from Σ that are not free in P.

Lemma A.4. *If $\Sigma \vdash P$ and $x \in \mathcal{V} \setminus \mathsf{fq}(P)$ then $\Sigma \setminus \{x\} \vdash P$.*

Proof. Assume $\Sigma \vdash P$ and $x \in \mathcal{V} \setminus \mathsf{fq}(P)$. The proof is by straightforward induction on the rules in Figure 2 to derive $\Sigma \vdash P$. The only interesting case is for (T-Out).

(T-Out) : Then $P = c![y].Q$, $c \in \mathcal{N}$, $y \in \mathcal{V} \cap \Sigma$, and $\Sigma \setminus \{y\} \vdash Q$. Since $x \in \mathcal{V} \setminus \mathsf{fq}(P)$, $x \neq y$. By the induction hypothesis, then $\Sigma \setminus \{x, y\} \vdash Q$. By (T-Out), then $\Sigma \setminus \{x\} \vdash P$. □

Well-typedness is preserved modulo substitutions of qubit names. To prove this property we have to rely on the condition that substitutions on qubit names are not allowed to rename two qubits to the same qubit (see Section 3). We use s to denote substitutions on qubits of the form $\{q_1/x_1, \ldots, q_n/x_n\}$. Let $\Sigma\mathsf{s}$ be the result of applying the substitution s simultaneously on all qubit names in the set Σ. Similarly, $\tilde{x}\mathsf{s}$ is the result of applying the substitution s simultaneously on all qubit names in $\tilde{x}$. Moreover, let $\mathsf{fq}(\mathsf{s})$ return all qubit names in the substitution s, i.e., $\mathsf{fq}(\{q_1/x_1, \ldots, q_n/x_n\}) = \{x_1, q_1, \ldots, x_n, q_n\}$. As usual we

require for $\mathsf{s} = \{q_1/x_1, \ldots, q_n/x_n\}$ that the $x_1, \ldots, x_n$ are pairwise distinct. For the next Lemma we additionally explicitly require that also the $q_1, \ldots, q_n$ are pairwise distinct.

Lemma A.5. *If $\Sigma \vdash P$, $\mathsf{s} = \{q_1/x_1, \ldots, q_n/x_n\}$, $\mathsf{fq}(\mathsf{s}) \in \mathcal{V} \setminus \mathsf{bq}(P)$, and $q_1, \ldots, q_n$ are pairwise distinct, then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.*

Proof. Assume $\Sigma \vdash P$, $\mathsf{s} = \{q_1/x_1, \ldots, q_n/x_n\}$, $\mathsf{fq}(\mathsf{s}) \in \mathcal{V} \setminus \mathsf{bq}(P)$, and $q_1, \ldots, q_n$ are pairwise distinct. We perform an induction on the structure of P.

- $P = \mathbf{0}$**:** Then $P = P\mathsf{s}$. By (T-Nil), then $\vdash P\mathsf{s}$. By applying Lemma A.3 potentially several times, then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
- $P = \checkmark$**:** Then $P = P\mathsf{s}$. By (T-Suc), then $\vdash P\mathsf{s}$. By applying Lemma A.3 potentially several times, then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
- $P = Q \mid R$**:** By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash Q$, $\Sigma_2 \vdash R$, $\Sigma = \Sigma_1 \cup \Sigma_2$, and $\Sigma_1 \cap \Sigma_2 = \emptyset$. By Lemma 3.2, then $\mathsf{fq}(Q) \subseteq \Sigma_1$ and $\mathsf{fq}(R) \subseteq \Sigma_2$. Then we can split s into $\mathsf{s}_1 = \{q_{1,1}/x_{1,1}, \ldots, q_{1,n_1}/x_{1,n_1}\}$ and $\mathsf{s}_2 = \{q_{2,1}/x_{2,1}, \ldots, q_{2,n_2}/x_{2,n_2}\}$, i.e., $\mathsf{s} = \mathsf{s}_1 \cup \mathsf{s}_2$, and $x_{1,1}, \ldots, x_{1,n_1} \notin \mathsf{fq}(R)$, $x_{2,1}, \ldots, x_{2,n_2} \notin \mathsf{fq}(Q)$, and $\{x_{1,1}, \ldots, x_{1,n_1}\} \cap \{x_{2,1}, \ldots, x_{2,n_2}\} = \emptyset$. Then $P\mathsf{s} = Q\mathsf{s}_1 \mid R\mathsf{s}_2$. Since $\mathsf{bq}(P) = \mathsf{bq}(Q) \cup \mathsf{bq}(R)$, we have $\mathsf{fq}(\mathsf{s}_1) \notin \mathsf{bq}(Q)$ and $\mathsf{fq}(\mathsf{s}_2) \notin \mathsf{bq}(R)$. By the induction hypothesis, then $\Sigma_1\mathsf{s}_1 \vdash Q\mathsf{s}_1$ and $\Sigma_2\mathsf{s}_2 \vdash R\mathsf{s}_2$. Because the $q_1, \ldots, q_n$ are pairwise distinct and $\Sigma_1 \cap \Sigma_2 = \emptyset$ and since substitutions on qubits cannot rename two qubits to the same qubit, then $(\Sigma_1\mathsf{s}_1) \cap (\Sigma_2\mathsf{s}_2) = \emptyset$ and $(\Sigma_1\mathsf{s}_1) \cup (\Sigma_2\mathsf{s}_2) = \Sigma\mathsf{s}$. By (T-Par), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
- $P = c?[x].Q$**:** By (T-In), then $c \in \mathcal{N}$, $x \in \mathcal{V} \setminus \Sigma$, and $\Sigma \cup \{x\} \vdash Q$. Note that $\mathsf{bq}(P) = \mathsf{bq}(Q) \cup \{x\}$. By the induction hypothesis, then $(\Sigma \cup \{x\})\,\mathsf{s} \vdash Q\mathsf{s}$. Since $\mathsf{fq}(\mathsf{s}) \notin \mathsf{bq}(P)$, we have $x \notin \{x_1, \ldots, x_n\}$. Then $P\mathsf{s} = c?[x].\,(Q\mathsf{s})$ and $(\Sigma \cup \{x\})\,\mathsf{s} = \Sigma\mathsf{s} \cup \{x\}$. By (T-In), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
- $P = c![x].Q$**:** By (T-Out), then $c \in \mathcal{N}$, $x \in \mathcal{V} \cap \Sigma$, and $\Sigma \setminus \{x\} \vdash Q$. Note that $\mathsf{bq}(P) = \mathsf{bq}(Q)$. If $x \notin \{x_1, \ldots, x_n\}$, then $P\mathsf{s} = c![x].\,(Q\mathsf{s})$. Remember that substitutions on qubits are not allowed to rename two qubits to the same qubit. Then either (1) $x \notin \{q_1, \ldots, q_n\}$ or (2) $x = q_i \in \{q_1, \ldots, q_n\}$ but $x_i \notin \mathsf{fq}(Q)$.
  (1) By the induction hypothesis, then $(\Sigma \setminus \{x\})\,\mathsf{s} \vdash Q\mathsf{s}$ and $(\Sigma \setminus \{x\})\,\mathsf{s} = \Sigma\mathsf{s} \setminus \{x\}$. By (T-Out), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
  (2) In this case, we can ignore the substitution q_i/x_i, i.e., $\mathsf{s}' = \mathsf{s} \setminus \{q_i/x_i\}$ and $Q\mathsf{s} = Q\mathsf{s}'$ as well as $P\mathsf{s} = P\mathsf{s}'$. By the induction hypothesis, then $(\Sigma \setminus \{x\})\,\mathsf{s}' \vdash Q\mathsf{s}'$ and we have that $(\Sigma \setminus \{x\})\,\mathsf{s}' = \Sigma\mathsf{s}' \setminus \{x\}$. By (T-Out), then $\Sigma\mathsf{s}' \vdash P\mathsf{s}'$. If $x_i \notin \Sigma$ then also $\Sigma\mathsf{s} \vdash P\mathsf{s}$. Else if $x_i \in \Sigma$, then $x_i \in \Sigma\mathsf{s}'$. By Lemma A.4 and since $x_i \notin \mathsf{fq}(Q)$, then $\Sigma\mathsf{s}' \setminus \{x_i\} \vdash P\mathsf{s}'$. By Lemma A.3 and since $q_i \notin \mathsf{bq}(P)$, then $(\Sigma\mathsf{s}' \setminus \{x_i\}) \cup \{q_i\} \vdash P\mathsf{s}'$. If $x_i \notin \{q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n\}$ then $\Sigma\mathsf{s} \vdash P\mathsf{s}$. Else we apply once more Lemma A.3 to add the respective q_j and have again $\Sigma\mathsf{s} \vdash P\mathsf{s}$.

  Else $x = x_i \in \{x_1, \ldots, x_n\}$. Then $P\mathsf{s} = c![q_i].\,(Q\mathsf{s})$. By Lemma 3.2, $\Sigma \setminus \{x\} \vdash Q$ implies $x \notin \mathsf{fq}(Q)$. Then we can ignore the substitution q_i/x_i for Q, i.e., $\mathsf{s}' = \mathsf{s} \setminus \{q_i/x_i\}$ and $Q\mathsf{s} = Q\mathsf{s}'$. By the induction hypothesis, then $(\Sigma \setminus \{x\})\,\mathsf{s}' \vdash Q\mathsf{s}'$. Since the substitution cannot rename two qubits to the same qubit, then $(\Sigma \setminus \{x\})\,\mathsf{s}' = (\Sigma\mathsf{s}) \setminus \{q_i\}$. By (T-Out), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.
- $P = \{\tilde{x} \mathrel{*}= U\}.Q$**:** By (T-Trans), then $\tilde{x} \in \mathcal{V} \cap \Sigma$, $\vdash U{:}\mathsf{Op}(n)$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma\mathsf{s} \vdash Q\mathsf{s}$. Since $P\mathsf{s} = \{\tilde{x}\mathsf{s} \mathrel{*}= U\}.\,(Q\mathsf{s})$ and because of (T-Trans), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.

$P = (v' := \mathsf{measure}\ \tilde{x}).Q$**:** By (T-Msure), then $v' \in \mathcal{B}$, $\tilde{x} \in \mathcal{V} \cap \Sigma$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma\mathsf{s} \vdash Q\mathsf{s}$. Since $P\mathsf{s} = (v' := \mathsf{measure}\ \tilde{x}\mathsf{s}).\,(Q\mathsf{s})$ and because of (T-Msure), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.

$P = (\mathsf{new}\ c)Q$**:** By (T-New), then $c \in \mathcal{N}$ and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma\mathsf{s} \vdash Q\mathsf{s}$. Since $P\mathsf{s} = (\mathsf{new}\ c)\,(Q\mathsf{s})$ and because of (T-New), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.

$P = (\mathsf{qubit}\ x)Q$**:** By (T-Qbit), then $x \in \mathcal{V} \setminus \Sigma$ and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $(\Sigma \cup \{x\})\,\mathsf{s} \vdash Q\mathsf{s}$. Since $\mathsf{fq}(\mathsf{s}) \notin \mathsf{bq}(P)$, $x \notin \mathsf{fq}(\mathsf{s})$ and thus $(\Sigma \cup \{x\})\,\mathsf{s} = \Sigma\mathsf{s} \cup \{x\}$. Since $P\mathsf{s} = (\mathsf{qubit}\ x)\,(Q\mathsf{s})$ and because of (T-Qbit), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$.

$P = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ Q$**:** By (T-Cond), then $bv_1 \in \mathcal{B}$ or $\vdash bv_1{:}\mathsf{Bin}$, $bv_2 \in \mathcal{B}$ or $\vdash bv_2{:}\mathsf{Bin}$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma\mathsf{s} \vdash Q\mathsf{s}$. Since $P\mathsf{s} = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ (Q\mathsf{s})$ and because of (T-Msure), then $\Sigma\mathsf{s} \vdash P\mathsf{s}$. □

Well-typedness is also preserved modulo substitutions of channel names. Let $\mathsf{bc}(P)$ return the set of bound names in P.

Lemma A.6. *If $\Sigma \vdash P$ and $a, c \in \mathcal{N} \setminus \mathsf{bc}(P)$ then $\Sigma \vdash P\{a/c\}$.*

Proof. Assume $\Sigma \vdash P$ and $a, c \in \mathcal{N} \setminus \mathsf{bc}(P)$. We perform an induction on the structure of P.

$P = \mathbf{0}$**:** Then $P = P\{a/c\}$ and thus $\Sigma \vdash P$ implies $\Sigma \vdash P\{a/c\}$.

$P = \checkmark$**:** Then $P = P\{a/c\}$ and thus $\Sigma \vdash P$ implies $\Sigma \vdash P\{a/c\}$.

$P = Q \mid R$**:** By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash Q$, $\Sigma_2 \vdash R$, $\Sigma = \Sigma_1 \cup \Sigma_2$, and $\Sigma_1 \cap \Sigma_2 = \emptyset$. By the induction hypothesis, then $\Sigma_1 \vdash Q\{a/c\}$ and $\Sigma_2 \vdash R\{a/c\}$. Since $P\{a/c\} = Q\{a/c\} \mid R\{a/c\}$ and because of (T-Par), then $\Sigma \vdash P\{a/c\}$.

$P = d?[x].Q$**:** By (T-In), then $d \in \mathcal{N}$, $x \in \mathcal{V} \setminus \Sigma$, and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \cup \{x\} \vdash Q\{a/c\}$. Since $P\{a/c\} = d^*?[x].\,(Q\{a/c\})$ with $d^* \in \{a, d\}$ and because of (T-In), then $\Sigma \vdash P\{a/c\}$.

$P = d![x].Q$**:** By (T-Out), then $d \in \mathcal{N}$, $x \in \mathcal{V} \cap \Sigma$, and $\Sigma \setminus \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \setminus \{x\} \vdash Q\{a/c\}$. Since $P\{a/c\} = d^*![x].\,(Q\{a/c\})$ with $d^* \in \{a, d\}$ and because of (T-Out), then $\Sigma \vdash P\{a/d\}$.

$P = \{x_1, \ldots, x_n \mathrel{*}\!= U\}.Q$**:** By (T-Trans), then $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, $\vdash U{:}\mathsf{Op}(n)$, and $\Sigma \vdash Q$. By the induction hypothesis, then we have $\Sigma \vdash Q\{a/c\}$. Since $P\{a/c\} = \{x_1, \ldots, x_n \mathrel{*}\!= U\}.\,(Q\{a/c\})$ and because of (T-Trans), then $\Sigma \vdash P\{a/c\}$.

$P = (v := \mathsf{measure}\ x_1, \ldots, x_n).Q$**:** By (T-Msure), then $v \in \mathcal{B}$, $x_1, \ldots, x_n \in \mathcal{V} \cap \Sigma$, and $\Sigma \vdash Q$. By the induction hypothesis, then we have $\Sigma \vdash Q\{a/c\}$. Since $P\{a/c\} = (v := \mathsf{measure}\ x_1, \ldots, x_n).\,(Q\{a/c\})$ and because of (T-Msure), then $\Sigma \vdash P\{a/c\}$.

$P = (\mathsf{new}\ d)Q$**:** By (T-New), then $d \in \mathcal{N}$ and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{a/c\}$. Since $a, c \notin \mathsf{bc}(P)$, $d \notin \{a, c\}$. Then $P\{a/c\} = (\mathsf{new}\ d)\,(Q\{a/c\})$. By (T-New), then $\Sigma \vdash P\{a/c\}$.

$P = (\mathsf{qubit}\ x)Q$**:** By (T-Qbit), then $x \in \mathcal{V} \setminus \Sigma$ and $\Sigma \cup \{x\} \vdash Q$. By the induction hypothesis, then $\Sigma \cup \{x\} \vdash Q\{a/c\}$. Since $P\{a/c\} = (\mathsf{qubit}\ x)\,(Q\{a/c\})$ and because of (T-Qbit), then $\Sigma \vdash P\{a/c\}$.

$P = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ Q$**:** By (T-Cond), then $bv_1 \in \mathcal{B}$ or $\vdash bv_1{:}\mathsf{Bin}$, $bv_2 \in \mathcal{B}$ or $\vdash bv_2{:}\mathsf{Bin}$, and $\Sigma \vdash Q$. By the induction hypothesis, then $\Sigma \vdash Q\{a/c\}$. Since $P\{a/c\} = \mathsf{if}\ bv_1 = bv_2\ \mathsf{then}\ (Q\{a/c\})$ and because of (T-Msure), then $\Sigma \vdash P\{a/c\}$. □

Lemma 3.3 states:

> If $\Sigma \vdash P$ and $(\sigma; \phi; P) \longmapsto \boxplus_{0 \le i < 2^r} p_i \bullet (\sigma'_i; \phi'; P_i)$ or if $\Sigma \vdash P_k$ for all $0 \le k < 2^t$ and $\boxplus_{0 \le k < 2^t} p'_k \bullet (\sigma; \phi; P'_k) \longmapsto \boxplus_{0 \le i < 2^r} p_i \bullet (\sigma'_i; \phi'; P_i)$ then there is some $\Sigma' \in \{\Sigma, \Sigma \cup \{q_n\}\}$ for some fresh q_n such that $\Sigma' \vdash P_i$ for all $0 \le i < 2^r$.

Proof of Lemma 3.3. Assume $\Sigma \vdash P$ and $(\sigma;\phi;P) \longmapsto \boxplus_{0\leq i<2^r} p_i \bullet (\sigma'_i;\phi';P_i)$ or if $\Sigma \vdash P_k$ for all $0 \leq k < 2^t$ and $\boxplus_{0\leq k<2^t} p_k \bullet (\sigma;\phi;P_k) \longmapsto \boxplus_{0\leq i<2^r} p_i \bullet (\sigma'_i;\phi';P_i)$. We perform an induction on the reduction rules in Figure 1.

(R-Measure$_{\mathsf{CQS}}$) : Then $P = (v := \mathsf{measure}\ q_1,\ldots,q_{r-1}).Q$ and all $P_i = Q\{\mathsf{b}(i)/v\}$ for all $0 \leq i < 2^r$. Fix some i with $0 \leq i < 2^r$. By (T-Msure), then $v \in \mathcal{B}$ and $\Sigma \vdash Q$. By (T-Bin), $\vdash \mathsf{b}(i){:}\mathsf{Bin}$. By Lemma A.2, then $\Sigma \vdash P_i$.

(R-Trans$_{\mathsf{CQS}}$) : Then $P = \{q_0,\ldots,q_{r'-1} \mathrel{*}= U\}.Q$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q$. By (T-Trans), then $\Sigma \vdash Q$, i.e., $\Sigma \vdash P_i$.

(R-Perm$_{\mathsf{CQS}}$) : Then $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = P\pi$, where π is a permutation of qubit names that are free, i.e., $\mathsf{fq}(\pi) \subseteq \mathsf{fq}(P)$. By Lemma 3.2, then $\mathsf{fq}(\pi) \subseteq \Sigma$. Then $\Sigma\pi = \Sigma$. By Lemma A.5, then $\Sigma \vdash P$ implies $\Sigma \vdash P_i$.

(R-Prob$_{\mathsf{CQS}}$) : Then $P'_j = Q\{\mathsf{b}(j)/v\}$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q\{\mathsf{b}(j)/v\} = P'_j$ for some $0 \leq j < 2^t$. Hence, $\Sigma \vdash P'_j$ implies $\Sigma \vdash P_i$.

(R-New$_{\mathsf{CQS}}$) : Then $P = (\mathsf{new}\ c)Q$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q\{a/c\}$, where a is fresh. By (T-New), then $c \in \mathcal{N}$ and $\Sigma \vdash Q$. By Lemma A.6, then $\Sigma \vdash P_i$.

(R-Qbit$_{\mathsf{CQS}}$) : Then $P = (\mathsf{qubit}\ x)Q$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q\{q_n/x\}$ for some fresh q_n. By (T-Qbit), $x \in \mathcal{V} \setminus \Sigma$ and $\Sigma \cup \{x\} \vdash Q$. Because we assume the absence of name clashes and since no qubit variable has a name of the form q_j, $x \notin \mathsf{bq}(Q)$. Since q_n is fresh, $q_n \notin \mathsf{bq}(Q)$. Note that $\Sigma \subseteq (\Sigma \cup \{x\})\{q_n/x\}$. By Lemma A.5, then $(\Sigma \cup \{x\})\{q_n/x\} \vdash P_i$.

(R-Comm$_{\mathsf{CQS}}$) : Then $P = c![q].Q \mid c?[x].R$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q \mid R\{q/x\}$. By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash c![q].Q$, $\Sigma_2 \vdash c?[x].R$, $\Sigma_1 \cap \Sigma_2 = \emptyset$, and $\Sigma_1 \cup \Sigma_2 = \Sigma$. By (T-Out), then $c \in \mathcal{N}$, $q \in \mathcal{V} \cap \Sigma_1$, and $\Sigma_1 \setminus \{q\} \vdash Q$. By (T-In), then $x \in \mathcal{V} \setminus \Sigma_2$ and $\Sigma_2 \cup \{x\} \vdash R$. Since $q \in \Sigma_1$ and $\Sigma_1 \cap \Sigma_2 = \emptyset$, $q \notin \Sigma_2$. Because we assume that there are no name clashes for P, $x, q \notin \mathsf{bq}(R)$. By Lemma A.5, then $(\Sigma_2 \cup \{x\})\{q/x\} \vdash R\{q/x\}$. Since $x \notin \Sigma_2$, $(\Sigma_2 \cup \{x\})\{q/x\} = \Sigma_2 \cup \{q\}$. Note that $(\Sigma_1 \setminus \{q\}) \cap (\Sigma_2 \cup \{q\}) = \emptyset$ and $(\Sigma_1 \setminus \{q\}) \cup (\Sigma_2 \cup \{q\}) = \Sigma$. By (T-Par), then $\Sigma \vdash P_i$.

(R-Par$_{\mathsf{CQS}}$) : Then $P = Q \mid R$, $(\sigma;\phi;Q) \longmapsto \boxplus_{0\leq i<2^r} p_i\,(\sigma'_i;\phi;Q_i)$, and $P_i = Q_i \mid R$ for all $0 \leq i < 2^r$. Fix some i with $0 \leq i < 2^r$. By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash Q$, $\Sigma_2 \vdash R$, $\Sigma_1 \cap \Sigma_2 = \emptyset$, and $\Sigma_1 \cup \Sigma_2 = \Sigma$. By the induction hypothesis, then there is some $\Sigma'_1 \in \{\Sigma_1, \Sigma'_1 \cup \{q\}\}$ for some fresh q such that $\Sigma'_1 \vdash Q_i$. Since q is fresh, $\Sigma'_1 \cap \Sigma_2 = \emptyset$. By (T-Par), then $\Sigma' \vdash P_i$, where $\Sigma' \in \{\Sigma, \Sigma' \cup \{q\}\}$.

(R-Cong$_{\mathsf{CQS}}$) : Then $P \equiv Q$, $(\sigma;\phi;Q) \longmapsto \boxplus_{0\leq i<2^r} p_i\,(\sigma'_i;\phi;Q'_i)$, and $P_i \equiv Q'_i$ for all $0 \leq i < 2^r$. Fix some i with $0 \leq i < 2^r$. By Lemma A.1, then $\Sigma \vdash Q$. By the induction hypothesis, then there is some $\Sigma' \in \{\Sigma, \Sigma' \cup \{q\}\}$ for some fresh q such that $\Sigma' \vdash Q'_i$. By Lemma A.1, then $\Sigma' \vdash P_i$.

(R-Cond$_{\mathsf{CQS}}$) : Then $P = \mathsf{if}\ b = b'\ \mathsf{then}\ Q$, $b = b'$, $r = 0$, there is just one i such that $0 \leq i < 2^r$, and $P_i = P_0 = Q$. By (T-Cond), then $\Sigma \vdash P_i$. □

Finally, Lemma 3.4 states:

If $\Sigma \vdash P \mid Q$ then $\mathsf{fq}(P) \cap \mathsf{fq}(Q) = \emptyset$.

Proof of Lemma 3.4. Assume $\Sigma \vdash P \mid Q$. By (T-Par), then there are Σ_1, Σ_2 such that $\Sigma_1 \vdash P$, $\Sigma_2 \vdash Q$, $\Sigma_1 \cap \Sigma_2 = \emptyset$, and $\Sigma_1 \cup \Sigma_2 = \Sigma$. By Lemma 3.2, then $\mathsf{fq}(P) \subseteq \Sigma_1$ and $\mathsf{fq}(Q) \subseteq \Sigma_2$. Since $\Sigma_1 \cap \Sigma_2 = \emptyset$, then $\mathsf{fq}(P) \cap \mathsf{fq}(Q) = \emptyset$. □