Encodability Criteria for Quantum Based Systems

Anna Schmitt[1 [0000−0001−6675−2879]], Kirstin Peters[1 [0000−0002−4281−0074]], and Yuxin Deng[2 [0000−0003−0753−418X]]

[1] TU Darmstadt, Germany
[2] East China Normal University, Shanghai

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 sublanguage of CQP into 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 (or its sublanguage) that is compositional, operationally corresponding, and success sensitive.

Keywords: Process calculi · Quantum Based Systems · Encodings

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. 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 [8,5,4,18]. 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, 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 [6] for the classical setting. As a case study we want to compare *Communicating Quantum Processes* (CQP) introduced in [5] and the *Algebra of Quantum Processes* (qCCS) introduced in [18]. 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 is non-probabilistic. (Unitary transformations and super-operators are discussed in the next section.)

Unfortunately, the languages also differ in classical aspects: CQP has pi-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 [5] 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 CQP^-, a 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.

We then show that there exists an encoding from CQP^- into qCCS that satisfies the quality criteria of Gorla and thereby that the treatment of qubits in qCCS is strong enough to emulate the treatment of qubits in 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 qCCS into CQP that satisfies compositionality, operational correspondence, and success sensitiveness.

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 CQP^- into qCCS and comments on its correctness. The negative result from qCCS into CQP is presented in §6. In §7 we discuss directions for criteria specific to quantum based systems. We conclude in §8. The missing proofs are provided by a technical report in [17].

2 Quantum Based Systems

We briefly introduce the aspects of quantum based systems, which are needed for the rest of the paper. For more details, we refer to the books by Nielsen and Chuang [10], Gruska [7], and Rieffel and Polak [16].

A *quantum bit* or *qubit* is a physical system which has the two base states $|0\rangle$, $|1\rangle$. 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 $(\alpha, \beta)^T$. The vector space of these vectors is a *Hilbert space* and is denoted by $\mathcal{H}$. We consider finite-dimensional and countably infinite-dimensional Hilbert spaces, where the latter are treated as tensor products of countably infinitely many finite-dimensional Hilbert spaces.

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* [10]. 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 H, as it creates the superpositions $\mathsf{H}|0\rangle = |+\rangle$ and $\mathsf{H}|1\rangle = |-\rangle$.

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

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. Unitary transformations can be performed on single or several qubits.

The multi-qubit systems can exhibit *entanglement*, meaning that states of qubits are correlated, e.g. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. 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*. In contrast to the vector description of states, density matrices allow to describe the states of open systems. We further discuss density matrices in Section 3.2.

3 Process Calculi

Assume two countably-infinite sets $\mathcal{N}$ of *names* and $\mathcal{V}$ of *qubit variables*. Let $\tau \notin \mathcal{V} \cup \mathcal{N}$. The *semantics* of a process calculus is given as a *structural operational semantics* consisting of inference rules defined on the operators of the language [14]. Thereby, 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* $\mathcal{C}([\cdot]_1, \ldots, [\cdot]_n) : \mathcal{P}^n \to \mathcal{P}$ with n holes is a function from n terms into one term, i.e., given $P_1, \ldots, P_n \in \mathcal{P}$, 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 use $\{y/x\}$ to denote the capture avoiding substitution of x by y on either names or qubits. The definition of substitution on names in the respective calculi is standard. Substitutions on qubits additionally have to be bijective, i.e., 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 [18]. We equate terms and configurations modulo alpha conversion on (qubit) names.

For the last criterion of [6] in Section 4, we need a special constant $\checkmark$, called *success(ful termination)*, in both considered languages. Therefore, we add $\checkmark$ to the grammars of both languages without explicitly mentioning them. Success is used as a barb, where $P{\downarrow_{\checkmark}}$ if P has an unguarded occurrence of $\checkmark$ and $P{\Downarrow_{\checkmark}} = \exists P'.\, P \Longmapsto P' \wedge P'{\downarrow_{\checkmark}}$, to implement some form of (fair) testing.

3.1 Communicating Quantum Processes

Communicating Quantum Processes (CQP) is introduced in [5]. We need a sub-language CQP$^-$ of CQP without name passing. We simplify the definition of CQP by removing contexts, the additional layer on expressions in the syntax and semantics, do not allow to construct channel names from expressions (though we allow to use the values obtained by measurement as channel names), and by using a monadic version of communication in that only qubits can be transmitted. CQP$^-$ is a strictly less expressive sublanguage of CQP. 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.

Definition 1 (CQP$^-$). *The CQP$^-$ terms, denoted by $\mathcal{P}_C$, are given by:*

$$\begin{aligned} P \ ::= \ & \mathbf{0} \ \mid \ P \mid P \ \mid \ c?[x].P \ \mid \ c![q].P \ \mid \ \{\tilde{q} \mathrel{*}= U\}.P \\ \mid \ & (x \ := \ \mathsf{measure}\ \tilde{q}).P \ \mid \ (\mathsf{new}\ x)P \ \mid \ (\mathsf{qbit}\ x)P \end{aligned}$$

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

$$
\begin{array}{rl}
(\text{R-Measure}_{CQP}) & (\sigma; \phi; (x := \mathsf{measure}\ q_0, \ldots q_{r-1}).P) \\
& \longmapsto \boxplus_{0 \leq m < 2^r} p_m \bullet (\sigma'_m; \phi; P\{m/x\}) \\
(\text{R-Trans}_{CQP}) & (q_0, \ldots, q_{n-1} = |\psi\rangle; \phi; \{q_0, \ldots, q_{r-1} \mathrel{*}= U\}.P) \\
& \longmapsto \big(q_0, \ldots, q_{n-1} = (U \otimes \mathcal{I}_{\{q_r, \ldots, q_{n-1}\}})|\psi\rangle; \phi; P\big) \\
(\text{R-Perm}_{CQP}) & (q_0, \ldots, q_{n-1} = |\psi\rangle; \phi; P) \longmapsto \big(q_{\pi(0)}, \ldots, q_{\pi(n-1)} = \prod |\psi\rangle; \phi; P\pi\big) \\
(\text{R-Prob}_{CQP}) & \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma_i; \phi; P\{i/x\}) \\
& \longmapsto (\sigma_j; \phi; P\{j/x\}) \quad \text{where } p_j \neq 0 \text{ and } r > 0 \\
(\text{R-New}_{CQP}) & (\sigma; \phi; (\mathsf{new}\ x)P) \longmapsto (\sigma; \phi, c; P\{c/x\}) \quad \text{where } c \text{ is fresh} \\
(\text{R-Qbit}_{CQP}) & (q_0, \ldots, q_{n-1} = |\psi\rangle; \phi; (\mathsf{qbit}\ x)P) \\
& \longmapsto (q_0, \ldots, q_{n-1}, q_n = |\psi\rangle \otimes |0\rangle; \phi; P\{q_n/x\}) \\
(\text{R-Comm}_{CQP}) & (\sigma; \phi; c![q].P \mid c?[x].Q) \longmapsto (\sigma; \phi; P \mid Q\{q/x\}) \\
(\text{R-Par}_{CQP}) & \dfrac{(\sigma; \phi; P) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; P'\{i/x\})}{(\sigma; \phi; P \mid Q) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; P'\{i/x\} \mid Q)} \\
(\text{R-Cong}_{CQP}) & \dfrac{Q \equiv P \quad (\sigma; \phi; P) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; P'\{i/x\}) \quad P' \equiv Q'}{(\sigma; \phi; Q) \longmapsto \boxplus_{0 \leq i < 2^r} p_i \bullet (\sigma'_i; \phi'; Q'\{i/x\})}
\end{array}
$$

Fig. 1. Semantics of CQP^-

The syntax of CQP^- is pi-calculus like. It adds the term $\{\tilde{q} \mathrel{*}= U\}.P$ to apply the unitary transformation U to the qubits in sequence $\tilde{q}$ and the term $(\mathsf{qbit}\ x)P$ to create a fresh qubit q_n (for $\sigma = q_0, \ldots, q_{n-1}$) which then proceeds as $P\{q_n/x\}$. The process $(x := \mathsf{measure}\ \tilde{q}).P$ measures the qubits in $\tilde{q}$ with $|\tilde{q}| > 0$ and saves the result in x. The configuration $\boxplus_{0 \leq i < 2^r} p_i \bullet C_i$ denotes a probability distribution over configurations $C_i = (\sigma_i; \phi; P\{i/x\})$, where $\sum_i p_i = 1$ and where the terms within the configurations C_i may differ only by instantiating channel name x by i. It results from measuring the first r qubits, where p_i is the probability of obtaining result i from measuring the qubits $q_0, \ldots, q_{r-1}$ and C_i is the configuration of case i after the measurement. We may also write a distribution as $p_1 \bullet C_1 \boxplus \ldots \boxplus p_j \bullet C_j$ with $j = 2^r - 1$. We equate $(\sigma_0; \phi; P)$ and $\boxplus_{0 \leq i < 2^0} 1 \bullet (\sigma_i; \phi; P\{i/x\})$, i.e., if $|\tilde{q}| = 0$ then we assume that x is not free in P. We naturally extend the definition of contexts to configurations, i.e., consider also contexts $\mathcal{C}([\cdot]_1, \ldots, [\cdot]_n) : \mathcal{P}^n \to \mathfrak{C}$.

The variable x is bound in P by $c?[x].P$, $(x := \mathsf{measure}\ \tilde{q}).P$, $(\mathsf{new}\ x)P$, and $(\mathsf{qbit}\ x)P$. A variable is free if it is not bound. Let $\mathsf{fq}(P)$ and $\mathsf{fc}(P)$ denote the sets of free qubits and free channels in P.

The state σ is represented by a list of qubits $q_0, \ldots, q_{n-1}$ 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 $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})^T$. As done in [5], we sometimes write as an abbreviated form $\sigma = q_0, \ldots, q_{n-1}$ or $\sigma = |\psi\rangle$.

The semantics of CQP^- is defined by the reduction rules in Figure 1. Rule (R-Measure$_{CQP}$) measures the first r qubits of σ, where $\sigma = \alpha_0|\psi_0\rangle + \cdots + \alpha_{2^n-1}|\psi_{2^n-1}\rangle$, $\sigma'_m = \dfrac{\alpha_{l_m}}{\sqrt{p_m}}|\psi_{l_m}\rangle + \cdots + \dfrac{\alpha_{u_m}}{\sqrt{p_m}}|\psi_{u_m}\rangle$, $l_m = 2^{n-r}m$, $u_m = 2^{n-r}(m + 1) - 1$, and $p_m = |\alpha_{l_m}|^2 + \cdots + |\alpha_{u_m}|^2$. As a result a probability distribution over the possible base vectors is generated, where σ'_m is the accordingly updated qubit vector. Rule (R-Trans$_{CQP}$) applies the unitary operator U on the first r qubits. In contrast to [5], we explicitly list in the subscript of $\mathcal{I}$ the qubits it is applied to. As the rules (R-Measure$_{CQP}$) and (R-Trans$_{CQP}$) operate on the first r qubits within σ, Rule (R-Perm$_{CQP}$) allows to permute the qubits in σ. Thereby, π is a permutation and $\prod$ is the corresponding unitary operator.

The Rule (R-Prob$_{CQP}$) reduces a probability distribution with $r > 0$ to a single of its configurations $(\sigma_j; \phi; P\{j/x\})$ with non-zero probability p_j. The rules (R-New$_{CQP}$) and (R-Qbit$_{CQP}$) 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 remaining rules are standard pi-calculus rules and also structural congruence $\equiv$ is standard.

We inherit the type system from [5]. It ensures that two parallel components cannot share qubits, which is the realisation of the no-cloning property of qubits. To illustrate this type system, we present the rules for parallel composition, input, and output from [5]:

$$\text{(T-Par)}\ \frac{\Gamma_1 \vdash P \quad \Gamma_2 \vdash Q}{\Gamma_1 + \Gamma_2 \vdash P \mid Q} \qquad \text{(T-In)}\ \frac{\Gamma \vdash x : \hat{}[\widetilde{T}] \quad \Gamma, \tilde{y} : \widetilde{T} \vdash P}{\Gamma \vdash x?[\tilde{y} : \widetilde{T}].P}$$

$$\text{(T-Out)}\ \frac{\Gamma \vdash x : \hat{}[\widetilde{T}, \widetilde{\mathsf{Qbit}}] \quad \forall i.\ T_i \neq \mathsf{Qbit} \quad \forall i.\ \Gamma \vdash y_i : T_i \quad z_i \text{ distinct} \quad \Gamma \vdash P}{\Gamma, \tilde{z} : \widetilde{\mathsf{Qbit}} \vdash x![\tilde{y}, \tilde{z}].P}$$

Rule (T-Par) ensures that parallel components cannot share qubits, where $\Gamma_1 + \Gamma_2$ implies that Γ_1 and Γ_2 do not share assignments for the same qubit. Rule (T-In) adds the types of the received values and qubits to the type environment for the continuation P such that P can use the received qubits. Therefore, Rule (T-Out) removes the transmitted qubits from the type environment of the continuation such that these qubits can no longer be used by the continuation. For the remaining rules of the type system we refer to [5]. These rules straightforwardly implement the idea that parallel components cannot share qubits. To adapt this type system to CQP$^-$ it suffices to adapt the multiplicity in communication to the monadic case, where the message is always of type Qbit for qubits.

As an example for a CQP$^-$ configuration and the application of the rules in Figure 1 consider Example 1. This example contains an implementation of the quantum teleportation protocol as given in [1]. The quantum teleportation protocol is a procedure for transmitting a quantum state via a non-quantum medium. This protocol is particularly important: not only is it 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 [15] which will be necessary in large-scale quantum communication networks.

Example 1. Consider the CQP^--configuration S

$$S = \left(q_0, q_1, q_2 = \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{\sqrt{2}}|111\rangle; \emptyset; \mathit{System}\,(0,1,2,3,q_0,q_1,q_2)\right) \text{ where}$$
$$\mathit{System}\,(0,1,2,3,q_0,q_1,q_2) = (\mathsf{new}\ 0)(\mathsf{new}\ 1)(\mathsf{new}\ 2)(\mathsf{new}\ 3)(\mathit{Alice}\,(q_0,q_1,0,1,2,3) \mid \mathit{Bob}\,(q_2,0,1,2,3))$$
$$\mathit{Alice}\,(q_0,q_1,0,1,2,3) = \{q_0, q_1 \mathrel{*}= \mathsf{CNOT}\}.\{q_0 \mathrel{*}= \mathsf{H}\}.(x \ := \ \mathsf{measure}\ q_0, q_1).x![a].\mathbf{0}$$
$$\mathit{Bob}\,(q_2,0,1,2,3) = (0?[y].\{q_2 \mathrel{*}= \mathcal{I}\}.\checkmark) \mid (1?[y].\{q_2 \mathrel{*}= \mathcal{X}\}.\checkmark) \mid (2?[y].\{q_2 \mathrel{*}= \mathcal{Z}\}.\checkmark) \mid (3?[y].\{q_2 \mathrel{*}= \mathcal{Y}\}.\checkmark)$$

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 $|0\rangle$, 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

$$\begin{aligned}
S \longmapsto^4 &(|\psi_0\rangle; 0,1,2,3; (\mathit{Alice}\,(q_0,0,1,2,3,q_2) \mid \mathit{Bob}\,(q_1,0,1,2,3)))\\
\longmapsto &(|\psi_1\rangle; 0,1,2,3; (\{q_0 \mathrel{*}= \mathsf{H}\}.(x \ := \ \mathsf{measure}\ q_0, q_1).x![a].\mathbf{0} \mid \\
&\quad \mathit{Bob}\,(q_2,0,1,2,3)))\\
\longmapsto &(|\psi_2\rangle; 0,1,2,3; ((x \ := \ \mathsf{measure}\ q_0, q_1).x![a].\mathbf{0} \mid \mathit{Bob}\,(q_2,0,1,2,3)))\\
\longmapsto &\frac{1}{4} \bullet (q_0,q_1,q_2 = |001\rangle; 0,1,2,3; (0![a].\mathbf{0} \mid \mathit{Bob}\,(q_2,0,1,2,3)))\boxplus\\
&\frac{1}{4} \bullet (q_0,q_1,q_2 = |010\rangle; 0,1,2,3; (1![a].\mathbf{0} \mid \mathit{Bob}\,(q_2,0,1,2,3)))\boxplus\\
&\frac{1}{4} \bullet (q_0,q_1,q_2 = |101\rangle; 0,1,2,3; (2![a].\mathbf{0} \mid \mathit{Bob}\,(q_2,0,1,2,3)))\boxplus\\
&\frac{1}{4} \bullet (q_0,q_1,q_2 = |110\rangle; 0,1,2,3; (3![a].\mathbf{0} \mid \mathit{Bob}\,(q_2,0,1,2,3))) = S^*,
\end{aligned}$$

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$_{CQP}$).

$$\begin{aligned}
S^* \longmapsto &(q_0,q_1,q_2 = |001\rangle; 0,1,2,3; (0![a].\mathbf{0} \mid (0?[y].\{q_2 \mathrel{*}= \mathcal{I}\}.\checkmark) \mid \\
&\quad (1?[y].\{q_2 \mathrel{*}= \mathcal{X}\}.\checkmark) \mid (2?[y].\{q_2 \mathrel{*}= \mathcal{Z}\}.\checkmark) \mid (3?[y].\{q_2 \mathrel{*}= \mathcal{Y}\}.\checkmark)))\\
\longmapsto &(q_0,q_1,q_2 = |001\rangle; 0,1,2,3; (\mathbf{0} \mid (\{q_2 \mathrel{*}= \mathcal{I}\}.\checkmark) \mid \\
&\quad (1?[y].\{q_2 \mathrel{*}= \mathcal{X}\}.\checkmark) \mid (2?[y].\{q_2 \mathrel{*}= \mathcal{Z}\}.\checkmark) \mid (3?[y].\{q_2 \mathrel{*}= \mathcal{Y}\}.\checkmark)))\\
\longmapsto &(q_0,q_1,q_2 = |001\rangle; 0,1,2,3; (\mathbf{0} \mid \checkmark \mid \\
&\quad (1?[y].\{q_2 \mathrel{*}= \mathcal{X}\}.\checkmark) \mid (2?[y].\{q_2 \mathrel{*}= \mathcal{Z}\}.\checkmark) \mid (3?[y].\{q_2 \mathrel{*}= \mathcal{Y}\}.\checkmark)))
\end{aligned}$$

□

3.2 An Algebra of Quantum Processes

The algebra of quantum processes (qCCS) is introduced in [18,3] as a process calculus for quantum based systems. As qCCS is designed to model open systems, its states are described by density matrices or operators. A density operator in a Hilbert space $\mathcal{H}$ 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 $\mathsf{tr}(\rho)$ is the sum of elements on the main diagonal of the matrix ρ. A positive operator ρ is called a partial density operator if $\mathsf{tr}(\rho) \leq 1$. By slightly abusing notation, we use $\mathcal{V}$ to denote the current set of qubit names of a given density matrix ρ. We write $\mathcal{D}(\mathcal{H})$ for the set of partial density operators on $\mathcal{H}$. Every density matrix can be represented as $\sum_i p_i |\psi_i\rangle\langle\psi_i|$, i.e., by an ensemble of pure states $|\psi_i\rangle$ with their probabilities $p_i \geq 0$. Accordingly, the density matrix of a pure state $|\psi\rangle$ is $|\psi\rangle\langle\psi|$.

The dynamics of open quantum systems cannot be described solely by unitary transformations. Instead *super-operators* are used. Unitary transformations as well as measurement can be transformed to super-operators on density matrices. We illustrate this with the Hadamard transformation and measurement.

Example 2. Let $X \subseteq \mathcal{V}$. The super-operator that represents the Hadamard transformation on X is denoted as $\mathsf{H}[X]$, where its application to ρ is defined as $\mathsf{H}_X(\rho) = (\mathsf{H} \otimes \mathcal{I}_{\mathcal{V}-X}) \cdot \rho \cdot (\mathsf{H} \otimes \mathcal{I}_{\mathcal{V}-X})^\dagger$.

The super-operator to measure the qubits in X with the result of measurement unknown is denoted as $\mathcal{M}[X]$. Its application to ρ is defined as $\mathcal{M}_X(\rho) = \sum_m (\mathsf{P}_m \otimes \mathcal{I}_{\mathcal{V}-X}) \rho (\mathsf{P}_m \otimes \mathcal{I}_{\mathcal{V}-X})^\dagger$, where P_m is the outer product of m as a base vector.

The super-operator to measure the qubits in X with the expected result i is denoted as $\mathcal{E}_i[X]$. Its application to ρ is defined as $\mathcal{E}_{i,X}(\rho) = (\mathsf{P}_i \otimes \mathcal{I}_{\mathcal{V}-X}) \rho (\mathsf{P}_i \otimes \mathcal{I}_{\mathcal{V}-X})^\dagger$. If X is empty, then $\mathcal{E}_i[X]$ is the identity operator $\mathcal{I}_{\mathcal{V}}$. □

Super-operators that go beyond the expressive power of unitary transformations are e.g. the super-operators that are used to model the noise in quantum communication. Intuitively, noise is a form of partial entanglement with an unkown environment. Note that, as in CQP, the channels that are used to transfer qubit-systems in qCCS, are modelled as noise-free channels, i.e., noise has to be added explicitly by respective super-operators as discussed in [18].

Definition 2 (Super-Operator). *Let $X \subseteq \mathcal{V}$. A* super-operator $\mathcal{E}[X]$ *on a Hilbert space $\mathcal{H}$ is a linear operator $\mathcal{E}$ (from the space of linear operators on $\mathcal{H}$ into itself) which is defined as $\mathcal{E}_X = \mathcal{E} \otimes \mathcal{I}_{\mathcal{V}-X}$ and therefore $\mathcal{E}_X(\rho) = (\mathcal{E} \otimes \mathcal{I}_{\mathcal{V}-X}) \cdot \rho \cdot (\mathcal{E} \otimes \mathcal{I}_{\mathcal{V}-X})^\dagger$. Further, $\mathcal{E}$ is required to be completely positive and satisfies $\mathsf{tr}(\mathcal{E}_X(\rho)) \leq \mathsf{tr}(\rho)$. For any extra Hilbert space $\mathcal{H}_R$, $(\mathcal{I}_R \otimes \mathcal{E})(A)$ is positive provided A is a positive operator on $\mathcal{H}_R \otimes \mathcal{H}$, where $\mathcal{I}_R$ is the identity operation on $\mathcal{H}_R$.*

The syntax of qCCS adds an operator to standard CCS to apply super-operators and a standard conditional, where P is executed if b is true. Further, it alters the communication prefixes such that only qubits can be transmitted via standard channels ([18,3]).

$$(\textsc{Input}_{\text{QCCS}})\ \langle c?x.P, \rho\rangle \xrightarrow{c?q} \langle P\{q/x\}, \rho\rangle \quad q \notin \mathsf{fq}(c?x.P)$$

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

$$(\textsc{Comm}_{\text{QCCS}})\ \frac{\langle P, \rho\rangle \xrightarrow{c?q} \langle P', \rho\rangle \quad \langle Q, \rho\rangle \xrightarrow{c!q} \langle Q', \rho\rangle}{\langle P \parallel Q, \rho\rangle \xrightarrow{\tau} \langle P' \parallel Q', \rho\rangle} \qquad (\textsc{Tau}_{\text{QCCS}})\ \langle \tau.P, \rho\rangle \xrightarrow{\tau} \langle P, \rho\rangle$$

$$(\textsc{Choice}_{\text{QCCS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle P + Q, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle} \qquad (\textsc{IfThen}_{\text{QCCS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle \quad b = \mathsf{true}}{\langle \mathsf{if}\ b\ \mathsf{then}\ P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}$$

$$(\textsc{Def}_{\text{QCCS}})\ \frac{\langle P\{\tilde{q}/\tilde{x}\}, \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle}{\langle A(\tilde{q}), \rho\rangle \xrightarrow{\alpha} \langle P', \rho'\rangle} \quad A(\tilde{x}) \overset{def}{=} P \qquad (\textsc{Close}_{\text{QCCS}})\ \frac{\langle P, \rho\rangle \xrightarrow{\tau} \langle P', \rho'\rangle}{\langle P, \rho\rangle \longmapsto \langle P', \rho'\rangle}$$

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

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

Fig. 2. Semantics of qCCS

Definition 3 (qCCS). *The qCCS* terms*, denoted by* $\mathcal{P}_q$*, are given by:*

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

The qCCS configurations $\mathfrak{C}_q$ *are given by* $\langle P, \rho\rangle$*, where* $P \in \mathcal{P}_q$ *and* $\rho \in \mathcal{D}(\mathcal{H})$*.*

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 $A(\tilde{x}) \overset{def}{=} P$ with $P \in \mathcal{P}_q$ and $\mathsf{fq}(P) \subseteq \tilde{x}$ is assumed. As done in [18], we require the following two conditions:

$$c!q.P \in \mathcal{P}_{qCCS} \text{ implies } q \notin \mathsf{fq}(P) \qquad \text{(Cond1)}$$

$$P \parallel Q \in \mathcal{P}_{qCCS} \text{ implies } \mathsf{fq}(P) \cap \mathsf{fq}(Q) = \emptyset \qquad \text{(Cond2)}$$

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

The semantics of qCCS is defined by the inference rules given in Figure 2. We start with a labelled variant of the semantics from [18] and then add the Rule ($\textsc{Close}_{\text{QCCS}}$) to obtain a reduction semantics. We omit the symmetric forms of the rules ($\textsc{Choice}_{\text{QCCS}}$), ($\textsc{Intl}_{\text{QCCS}}$), and ($\textsc{Comm}_{\text{QCCS}}$). Let $\mathsf{cn}(\alpha)$ return the possibly empty set of channels in the label α.

Rule ($\textsc{Oper}_{\text{QCCS}}$) implements the application of a super-operator. It updates the state of the configuration as defined in Definition 2. To simplify the definition of a reduction semantics, we use (in contrast to [18]) the label τ.

Rule ($\textsc{Input}_{\text{QCCS}}$) ensures that the received qubits are fresh in the continuation of the input. The rules ($\textsc{Intl}_{\text{QCCS}}$) and ($\textsc{Intr}_{\text{QCCS}}$) forbid to receive qubits within parallel contexts that do posses this qubit. Rule ($\textsc{Res}_{\text{QCCS}}$) allows to do a step under a restriction. The other rules are self-explanatory.

4 Encodings and Quality Criteria

Let $\mathcal{L}_{\mathsf{S}} = \langle \mathfrak{C}_{\mathsf{S}}, \longmapsto_{\mathsf{S}} \rangle$ and $\mathcal{L}_{\mathsf{T}} = \langle \mathfrak{C}_{\mathsf{T}}, \longmapsto_{\mathsf{T}} \rangle$ be two process calculi, denoted as *source* and *target* language. An *encoding* from $\mathcal{L}_{\mathsf{S}}$ into $\mathcal{L}_{\mathsf{T}}$ is a function $\llbracket \cdot \rrbracket : \mathfrak{C}_{\mathsf{S}} \to \mathfrak{C}_{\mathsf{T}}$. 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 [6] suggests five criteria well suited for language comparison. We start with these criteria for classical systems, which are described in more detail in [17].

Definition 4 (Quality Criteria, [6]). *The encoding $\llbracket \cdot \rrbracket$ is good, if it is*

compositional: *For every operator* **op** *with arity n of $\mathcal{L}_{\mathsf{S}}$ and for every subset of names N, there exists a context $\mathcal{C}_{\mathbf{op}}^{N}([\cdot]_1, \ldots, [\cdot]_n)$ such that, for all $S_1, \ldots, S_n$ with $\mathsf{fv}(S_1) \cup \ldots \cup \mathsf{fv}(S_n) = N$, it holds that $\llbracket \mathbf{op}\,(S_1, \ldots, S_n) \rrbracket = \mathcal{C}_{\mathbf{op}}^{N}(\llbracket S_1 \rrbracket, \ldots, \llbracket S_n \rrbracket)$.*

name invariant: *For every $S \in \mathfrak{C}_{\mathsf{S}}$ and every substitution γ on names, it holds that $\llbracket S\gamma \rrbracket = \llbracket S \rrbracket \gamma$.*

operational corresponding w.r.t. $\preceq$:

Complete: For all $S \Longmapsto S'$, there is T such that $\llbracket S \rrbracket \Longmapsto T$ and $\llbracket S' \rrbracket \preceq T$.

Sound: For all $\llbracket S \rrbracket \Longmapsto T$, there is S', T' such that $S \Longmapsto S'$, $T \Longmapsto T'$, and $\llbracket S' \rrbracket \preceq T'$.

divergence reflecting: *For every S, $\llbracket S \rrbracket \longmapsto^{\omega}$ implies $S \longmapsto^{\omega}$.*

success sensitive: *For every S, $S \Downarrow_{\checkmark}$ iff $\llbracket S \rrbracket \Downarrow_{\checkmark}$.*

We use here a stricter variant of name invariance compared to [6], since we translate names by themselves in our encoding. Operational correspondence 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.

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 [12], we pair operational correspondence as of [6] with correspondence simulation.

Definition 5 (Correspondence Simulation, [12]). *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.*

There are several other criteria for classical systems that we could have considered (cf. [11]). Since CQP$^-$ is a typed language, we may consider a criterion for types as discussed e.g. in [9]. 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 [13], 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 CQP$^-$ configurations into qCCS-configurations that satisfy the conditions Cond1 and Cond2, is given by Definition 6.

Definition 6 (Encoding $[\![\cdot]\!]$ from CQP$^-$ into qCCS).

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

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

$$
\begin{aligned}
\mathsf{D}(\tilde{q};x;Q) = {}&\mathsf{if}\ \mathsf{tr}(\mathcal{E}_0[\tilde{q}]) \neq 0\ \mathsf{then}\ \mathcal{E}_0[\tilde{q}].Q\{0/x\} + \ldots +\\
&\mathsf{if}\ \mathsf{tr}(\mathcal{E}_{2^{|\tilde{q}|}-1}[\tilde{q}]) \neq 0\ \mathsf{then}\ \mathcal{E}_{2^{|\tilde{q}|}-1}[\tilde{q}].Q\{2^{|\tilde{q}|}-1/x\},
\end{aligned}
$$

$\mathcal{E}_{|0\rangle}[\mathcal{V}]$ *adds a new qubit* $q_{|\mathcal{V}|}$ *initialised with* 0 *to the current state* ρ*,* $\mathcal{M}$ *is measurement with the result unkown, and the super-operator* $\mathcal{E}_i[Y]$ *is measurement of* Y *with the expected result* i*.*

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 CQP$^-$ by (R-PROB$_{CQP}$) is translated into the qCCS-choice $\mathsf{D}(\tilde{q};x;[\![P]\!])$ with $\tilde{q} = q_0,\ldots,q_{r-1}$, where each case is guarded by a conditional which checks whether the result of measurement is not zero, i.e., whether the respective case occurs with a non-zero probability, followed by a super-operator that adjusts the state to the respective result of measurement. Note that, the translation of a configuration $(\sigma; \phi; P)$ is a special case of the second line with an additional step to resolve the conditional, since $|\psi\rangle\langle\psi| = \sum 1|\psi\rangle\langle\psi|$, $r = 0$ implies that $\tilde{q} = q_0, \ldots, q_{r-1}$ is empty, and thus $\mathsf{D}(\tilde{q}; x; [\![P]\!]) = \mathsf{if}\ \mathsf{tr}(\mathcal{I}[\mathcal{V}]) \neq 0\ \mathsf{then}\ \mathcal{I}[\mathcal{V}].[\![P]\!]$. An encoding example using such a qCCS-choice is given in Example 5.

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 with unkown result followed by the choice $\mathsf{D}(\tilde{q}; x; [\![P]\!])$ 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 combine two kinds of measurement in this translation. The outer measurement w.r.t. an unkown result 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 3). The measurements w.r.t. $0 \leq i < 2^r$ within $\mathsf{D}(\tilde{q}; x; [\![P]\!])$ 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 CQP$^-$ 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. The remaining translations are homomorphic.

Example 3. Consider $S = (\sigma; \phi; (x := \mathsf{measure}\ q_0).P)$, 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 Figure 1, $S \longmapsto S' = \frac{1}{2} \bullet (\sigma = q_0, q_1 = |00\rangle; \phi; P\{0/x\}) \boxplus \frac{1}{2} \bullet (\sigma = q_0, q_1 = |11\rangle; \phi; P\{1/x\})$. By Definition 6, $[\![S]\!] = \langle(\mathcal{M}[q_0].\mathsf{D}(q_0; x; [\![P]\!])) \setminus \phi, \rho\rangle$ with $\rho = |\psi\rangle\langle\psi|$. By Figure 2, 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., $\mathcal{M}_{q_0}(\rho) = (|0\rangle\langle 0| \otimes \mathcal{I}_{q_1})\rho(|0\rangle\langle 0| \otimes \mathcal{I}_{q_1})^\dagger + (|1\rangle\langle 1| \otimes \mathcal{I}_{q_1})\rho(|1\rangle\langle 1| \otimes \mathcal{I}_{q_1})^\dagger$. □

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

Corollary 1. *For all $S \in \mathfrak{C}_C$ the term $[\![S]\!]$ is defined.*

Considering Figure 1, we observe that in CQP$^-$ we have to permute the matrix σ, in order to apply unitary transformations or measure qubits in the middle of σ. Such permutations are not necessary in qCCS. More precisely, since these steps only reorder qubits in σ, they do not change the state of the translated system modulo correspondence simulation.

Lemma 1. *If $S \longmapsto S'$ is by* (R-PERM$_{CQP}$)*, then $[\![S]\!] \preceq [\![S']\!]$ and $[\![S']\!] \preceq [\![S]\!]$.*

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 4. Consider $S = (\sigma; \emptyset; (x := \mathsf{measure}\ q).P \mid Q)$, where S is a 1-qubit system with $\sigma = q = |+\rangle$ and $P, Q \in \mathcal{P}_C$ with $\mathsf{fc}(P) \subseteq \{x\}$ and $\mathsf{fc}(Q) = \emptyset$. By the rules (R-Measure$_{CQP}$) and (R-Par$_{CQP}$) of Figure 1,

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

i.e., (R-Par$_{CQP}$) 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 6, $[\![S]\!] = \langle \mathcal{M}[q].\mathsf{D}(q; x; [\![P]\!]) \parallel [\![Q]\!], \rho \rangle$, where $\mathsf{D}(q; x; [\![P]\!]) =$ $\mathsf{if}\ \mathsf{tr}(\mathcal{E}_0[q]) \neq 0\ \mathsf{then}\ \mathcal{E}_0[q].[\![P]\!]\{0/x\} + \mathsf{if}\ \mathsf{tr}(\mathcal{E}_1[q]) \neq 0\ \mathsf{then}\ \mathcal{E}_1[q].[\![P]\!]\{1/x\}$ and $\rho = |+\rangle\langle+|$, and $[\![S']\!] = \langle \mathsf{D}(q; x; [\![P]\!] \parallel [\![Q]\!]), \rho' \rangle$ with $\rho' = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. By Figure 2, $[\![S]\!] \longmapsto T = \langle \mathsf{D}(q; x; [\![P]\!]) \parallel [\![Q]\!], \rho' \rangle$, because $\mathcal{M}_q(\rho) = \rho'$. Unfortunately, $[\![S']\!]$ and T are not bisimilar. As a counterexample consider $P = x![q].\mathbf{0}$ and $Q = (\mathsf{new}\ y)0?[z].\checkmark$. 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. □

We also present the translation of the quantum teleportation protocol in Example 1.

Example 5. By Definition 6

$$\begin{aligned}
&[\![S]\!] = \langle (\tau.(\tau.(\tau.(P) \setminus 3) \setminus 2) \setminus 1) \setminus 0, \rho_0 \rangle, \text{ where} \\
&\quad P = [\![\mathit{Alice}\,(q_0, q_1, 0, 1, 2, 3)]\!] \parallel [\![\mathit{Bob}\,(q_2, 0, 1, 2, 3)]\!], \\
&\quad [\![\mathit{Alice}\,(q_0, q_1, 0, 1, 2, 3)]\!] = \mathsf{CNOT}[q_0, q_1].\mathsf{H}[q_0].\mathcal{M}[q_0, q_1].\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil}), \\
&\quad [\![\mathit{Bob}\,(q_2, 0, 1, 2, 3)]\!] = \\
&\qquad\quad (0?y.\mathcal{I}[q_2].\checkmark) \parallel (1?y.\mathcal{X}[q_2].\checkmark) \parallel (2?y.\mathcal{Z}[q_2].\checkmark) \parallel (3?y.\mathcal{Y}[q_2].\checkmark)\,, \text{ and} \\
&\quad \rho_0 = |\psi_0\rangle\langle\psi_0|.
\end{aligned}$$

By Figure 2, $[\![S]\!]$ can do the following steps

$$\begin{aligned}
[\![S]\!] &\longmapsto^4 \langle ((((P) \setminus 3) \setminus 2) \setminus 1) \setminus 0, \rho_0 \rangle \\
&\longmapsto \langle (\mathsf{H}[q_0].\mathcal{M}[q_0, q_1].\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil})) \parallel [\![\mathit{Bob}\,(q_2, 0, 1, 2, 3)]\!], \rho_1 \rangle \\
&\longmapsto \langle (\mathcal{M}[q_0, q_1].\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil})) \parallel [\![\mathit{Bob}\,(q_2, 0, 1, 2, 3)]\!], \rho_2 \rangle \\
&\longmapsto \langle \mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil}) \parallel [\![\mathit{Bob}\,(q_2, 0, 1, 2, 3)]\!], \rho_3 \rangle = T^*,
\end{aligned}$$

with $\rho_1 = \mathcal{CNOT}_{q_0,q_1}(\rho_0)$, $\rho_2 = \mathcal{H}_{q_0}(\rho_1)$, $\rho_3 = \mathcal{M}_{q_0,q_1}(\rho_2)$, and where the qCCS-choice $\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil})$ is given by

$$\begin{aligned}\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil}) = {} & \mathsf{if}\ \mathsf{tr}(\mathcal{E}_0[q_0, q_1]) \neq 0\ \mathsf{then}\ \mathcal{E}_0[q_0, q_1].\,((x!a.\mathsf{nil})\,\{0/x\})\ + \\ & \mathsf{if}\ \mathsf{tr}(\mathcal{E}_1[q_0, q_1]) \neq 0\ \mathsf{then}\ \mathcal{E}_1[q_0, q_1].\,((x!a.\mathsf{nil})\,\{1/x\})\ + \\ & \mathsf{if}\ \mathsf{tr}(\mathcal{E}_2[q_0, q_1]) \neq 0\ \mathsf{then}\ \mathcal{E}_2[q_0, q_1].\,((x!a.\mathsf{nil})\,\{2/x\})\ + \\ & \mathsf{if}\ \mathsf{tr}(\mathcal{E}_3[q_0, q_1]) \neq 0\ \mathsf{then}\ \mathcal{E}_3[q_0, q_1].\,((x!a.\mathsf{nil})\,\{3/x\})\,.\end{aligned}$$

To emulate the behaviour of S we choose again the first branch within $\mathsf{D}(q_0, q_1; x; x!a.\mathsf{nil})$.

$$\begin{aligned}T^* & \longmapsto \langle (0!a.\mathsf{nil}) \parallel [\![Bob\,(q_2, 0, 1, 2, 3)]\!], \rho_4 \rangle \\ & \longmapsto \langle \mathsf{nil} \parallel (\mathcal{I}[q_2].\checkmark) \parallel (1?y.\mathcal{X}[q_2].\checkmark) \parallel (2?y.\mathcal{Z}[q_2].\checkmark) \parallel (3?y.\mathcal{Y}[q_2].\checkmark)\,, \rho_4 \rangle \\ & \longmapsto \langle \mathsf{nil} \parallel \checkmark \parallel (1?y.\mathcal{X}[q_2].\checkmark) \parallel (2?y.\mathcal{Z}[q_2].\checkmark) \parallel (3?y.\mathcal{Y}[q_2].\checkmark)\,, \rho_4 \rangle,\end{aligned}$$

with $\rho_4 = \mathcal{E}_{0,q_0,q_1}(\rho_3)$. □

Except for permutation, a source term step is translated by the encoding $[\![\cdot]\!]$ into exactly one target term step. In the other direction, every target term step is translated by exactly one source term step possibly surrounded by two steps on (R-Perm$_{CQP}$) to permute qubits and put them back in the original order. From that, we obtain operational correspondence. Compositionality holds by definition and name invariance is trivially satisfied, because names are translated by themselves and the encoding does not use names for any other purpose. Divergence reflection results from operational soundness, since all source term steps are translated to a finite number of target term steps. Finally, operational correspondence and the homomorphic translation of success ensure that $[\![\cdot]\!]$ is success sensitive. With that, $[\![\cdot]\!]$ satisfies all the criteria that we discussed in Section 4. The corresponding proofs can be found in [17].

Theorem 1. *The encoding* $[\![\cdot]\!]$ *is good.*

By [12], Theorem 1 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. [2]). 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 4. Indeed [3] 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. We leave the study of these probabilistic versions for future research.

6 Separating Quantum Based Systems

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

Example 6. Consider the super-operator $\mathcal{Q}_q(\rho) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1+p} \end{pmatrix} \rho \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1+p} \end{pmatrix} - \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix} \rho \begin{pmatrix} 0 & 0 \\ \sqrt{p} & 0 \end{pmatrix}$ where p is a probability. With $p = 1$ we obtain $\mathcal{Q}_q(\rho) = \begin{pmatrix} \rho_{00} - \rho_{11} & \sqrt{2}\rho_{01} \\ \sqrt{2}\rho_{10} & 2\rho_{11} \end{pmatrix}$ that sometimes behaves as identity, i.e., $\mathcal{Q}_q(|0\rangle\langle 0|) = |0\rangle\langle 0|$, and sometimes changes the qubit, e.g. $\mathcal{Q}_q(|1\rangle\langle 1|) = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}$, $\mathcal{Q}_q(|+\rangle\langle +|) = \begin{pmatrix} 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & 1 \end{pmatrix}$, and $\mathcal{Q}_q(|-\rangle\langle -|) = \begin{pmatrix} 0 & -\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} & 1 \end{pmatrix}$. To observe this strange behaviour of $\mathcal{Q}[q]$, we measure the resulting qubit using the qCCS-configuration

$$\mathsf{S}_{\mathsf{ce}}(\rho) = \langle \mathcal{Q}[q].\mathsf{if}\ \mathsf{tr}(\mathcal{E}_0[q]) \neq 0\ \mathsf{then}\ \tau.\checkmark + \mathsf{if}\ \mathsf{tr}(\mathcal{E}_1[q]) \neq 0\ \mathsf{then}\ \tau.\mathsf{nil}, \rho \rangle$$

for the 1-qubit system $\rho = q$, where the choice allows to unguard success if 0 can be measured. We observe that $\mathsf{S}_{\mathsf{ce}}(|0\rangle\langle 0|)$ must reach success, $\mathsf{S}_{\mathsf{ce}}(|1\rangle\langle 1|)$ may but not must reach success, and $\mathsf{S}_{\mathsf{ce}}(|+\rangle\langle +|)$ as well as $\mathsf{S}_{\mathsf{ce}}(|-\rangle\langle -|)$ cannot reach success. □

An encoding from qCCS into CQP needs to emulate the behaviour of $\mathcal{Q}[q]$, which is inspired by an operator used for amplitude-damping (see e.g. [10]). 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 2), there is no encoding from qCCS into CQP that satisfies compositionality, operational correspondence, and success sensitiveness, i.e., we can use Example 6 as a counterexample to prove that there is no good encoding from qCCS into CQP. The proof of Theorem 2 is given in [17]. Note that we reason here about CQP instead of CQP$^-$, since even the full expressive power of CQP does not help to correctly emulate this super-operator.

Theorem 2. *There is no encoding from qCCS into CQP that satisfies compositionality, operational correspondence, and success sensitiveness.*

7 Quality Criteria for Quantum Based Systems

Sections 5 and 6 show that the quality criteria of Gorla in [6] 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 critria 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 [6], 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 (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 [6], 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 in [17].

Lemma 2. *The encoding* $[\![\cdot]\!]$ *is qubit invariant.*

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 8 (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 6 satisfies this criterion, which can be verified easily by inspection of the encoding function. The full proof can be found [17].

Lemma 3. *The encoding* $[\![\cdot]\!]$ *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 5. Fortunately, all of the already shown results remain valid for the altered version of $\preceq$.

In contrast to CQP$^-$, the semantics of qCCS 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 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. We leave the derivation of a suitable probabilistic version of operational correspondence to future work.

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 CQP$^-$ into qCCS, i.e., if we allow CQP$^-$ to violate this principle but require that qCCS respects it, then we obtain a negative result. Therefore, we remove the type system from CQP$^-$. 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 6 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 CQP^- can be encoded by qCCS 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 qCCS into CQP that satisfies compositionality, operational correspondence, and success sensitiveness.

The results themselves may not necessarily be very surprising. The unitary transformations used in $\mathrm{CQP}^-/\mathrm{CQP}$ are a subset of the super-operators used in qCCS and also density matrices can express more than the vectors used in $\mathrm{CQP}^-/\mathrm{CQP}$. 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. Such a criterion would rule out the encoding $[\![\cdot]\!]$ presented above. 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.

As, to the best of our knowledge, there are no well-accepted probabilistic versions of operational correspondence. As a first step we will study probabilistic versions of operational correspondence and the nature of the relation between source and target they imply.

References

1. Bennett, C.H., Brassard, G., Crépeau, C., RichardJozsa, Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (Mar 1993). https://doi.org/10.1103/PhysRevLett.70.1895, `https://link.aps.org/doi/10.1103/PhysRevLett.70.1895`
2. Bisping, B., Nestmann, U., Peters, K.: Coupled similarity: the first 32 years. Acta Informatica **57**(3–5), 439–463 (2020). https://doi.org/10.1007/s00236-019-00356-4
3. Feng, Y., Duan, R., Ying, M.: Bisimulation for quantum processes. ACM Trans. Program. Lang. Syst. **34**(4) (Dec 2012). https://doi.org/10.1145/2400676.2400680, `https://doi.org/10.1145/2400676.2400680`

4. Gay, S.J.: Quantum programming languages: survey and bibliography. Mathematical Structures of Computer Science **16**(4), 581 – 600 (2006). https://doi.org/10.1017/S0960129506005378
5. Gay, S.J., Nagarajan, R.: Communicating quantum processes. In: Proceedings of SIGPLAN-SIGACT (ACM). pp. 145–157 (2005). https://doi.org/10.1145/1040305.1040318
6. Gorla, D.: Towards a Unified Approach to Encodability and Separation Results for Process Calculi. Information and Computation **208**(9), 1031–1053 (2010). https://doi.org/10.1016/j.ic.2010.05.002
7. Gruska, J.: Quantum Computing. In: Wiley Encyclopedia of Computer Science and Engineering. John Wiley & Sons, Inc. (2008). https://doi.org/10.1002/9780470050118.ecse720
8. Jorrand, P., Lalire, M.: Toward a Quantum Process Algebra. In: Proceedings of CF. pp. 111–119 (2004). https://doi.org/10.1145/977091.977108
9. Kouzapas, D., Pérez, J.A., Yoshida, N.: On the Relative Expressiveness of Higher-Order Session Processes. In: Proceedings of ESOP. LNCS, vol. 9632, pp. 446–475 (2016). https://doi.org/10.1007/978-3-662-49498-1_18
10. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2010)
11. Peters, K.: Comparing Process Calculi Using Encodings. In: Proceedings of EXPRESS/SOS. EPCTS, vol. 300, pp. 19–38 (2019). https://doi.org/10.4204/EPTCS.300.2
12. Peters, K., van Glabbeek, R.: Analysing and Comparing Encodability Criteria. In: Crafa, S., Gebler, D. (eds.) Proceedings of EXPRESS/SOS. EPTCS, vol. 190, pp. 46–60 (2015). https://doi.org/10.4204/EPTCS.190.4
13. Peters, K., Nestmann, U., Goltz, U.: On Distributability in Process Calculi. In: Proceedings of ESOP. LNCS, vol. 7792, pp. 310–329 (2013). https://doi.org/10.1007/978-3-642-37036-6_18
14. Plotkin, G.D.: A structural approach to operational semantics. Log. Algebraic Methods Program. **60-61**, 17–139 (2004)
15. de Riedmatten, H., Marcikic, I., Tittel, W., Zbinden, H., Collins, D., Gisin, N.: Long distance quantum teleportation in a quantum relay configuration. Phys. Rev. Lett. **92**, 047904 (Jan 2004). https://doi.org/10.1103/PhysRevLett.92.047904, `https://link.aps.org/doi/10.1103/PhysRevLett.92.047904`
16. Rieffel, E.G., Polak, W.: An introduction to quantum computing for non-physicists. ACM Comput. Surv. **32**(3), 300–335 (2000). https://doi.org/10.1145/367701.367709
17. Schmitt, A., Peters, K., Deng, Y.: Encodability criteria for quantum based systems (technical report). Tech. rep., TU Darmstadt, Germany (2022). https://doi.org/10.48550/ARXIV.2204.06068, `https://arxiv.org/abs/2204.06068`
18. Ying, M., Feng, Y., Duan, R., Ji, Z.: An algebra of quantum processes. ACM Trans. Comput. Log. **10**(3), 19:1–19:36 (2009). https://doi.org/10.1145/1507244.1507249