Open Bisimulation for Quantum Processes

Yuxin Deng[1],* and Yuan Feng[2],**

[1] Shanghai Jiao Tong University
and Chinese Academy of Sciences, China
[2] University of Technology, Sydney, Australia
and Tsinghua University, China

Abstract. Quantum processes describe concurrent communicating systems that may involve quantum information. We propose a notion of open bisimulation for quantum processes and show that it provides both a sound and complete proof methodology for a natural extensional behavioural equivalence between quantum processes. We also give a modal characterisation of the behavioural equivalence, by extending the Hennessy-Milner logic to a quantum setting.

1 Introduction

The theory of quantum computing has attracted considerable research efforts in the past twenty years. Benefiting from the superposition of quantum states and linearity of quantum operations, quantum computing may provide considerable speedup over its classical analogue [30,13,14].

As is well known, it is very difficult to guarantee the correctness of classical communication protocols at the design stage, and some simple protocols were eventually found to have fundamental flaws. One expects that the design of complex quantum protocols is at least as error-prone, if not more, than in the classical case. In view of the success that classical process algebras [23,18,1] achieved in analyzing and verifying classical communication protocols, several research groups proposed various quantum process algebras with the purpose of modeling quantum protocols. Jorrand and Lalire [21,22] defined a language QPAlg (Quantum Process Algebra) by adding primitives expressing unitary transformations and quantum measurements, as well as communications of quantum states, to a CCS-like classical process algebra. An operational semantics of QPAlg is given, and further a probabilistic branching bisimulation between quantum processes is defined. Gay and Nagarajan [12,11] proposed a language CQP (Communicating Quantum Processes), which is obtained from the pi-calculus [24] by adding primitives for measurements and transformations of quantum states, and allowing transmission of qubits. They presented a type system for CQP, and in particular proved that the semantics preserves typing and that typing guarantees that each qubit is owned by a unique process within a system. A probabilistic branching

* Supported by the Natural Science Foundation of China (61173033 and 61033002).
** Supported by Australian Research Council (FT100100218 and DP110103473).

J.C.M. Baeten, T. Ball, and F.S. de Boer (Eds.): TCS 2012, LNCS 7604, pp. 119–133, 2012.

bisimulation for CQP was proposed by Davidson [3] and shown to be a congruence. The second author of the current paper, together with his colleagues, proposed a language named qCCS [8,31,9] for quantum communicating systems by adding quantum input/output and quantum operation/measurement primitives to classical value-passing CCS [15,16]. One distinctive feature of qCCS, compared to QPAlg and CQP, is that it provides a framework to describe, as well as reason about, the communication of quantum systems which are entangled with other systems. Furthermore, a bisimulation for processes in qCCS has been introduced, and the associated bisimilarity is proven to be a congruence with respect to all process constructors of qCCS. Uniqueness of the solutions to recursive process equations is also established, which provides a powerful proof technique for verifying complex quantum protocols.

In the study of quantum systems, as well as classical communicating systems, an important problem is to tell if two given systems exhibit the same behaviour, as this may allow us to replace a complex system with a simplified but equivalent one. To approach the problem we first need to give criteria for reasonable behavioural equivalence. Two systems should only be distinguished on the basis of the chosen criteria. Therefore, these criteria induce an extensional equivalence between systems, $\approx_{\text{behav}}$, namely the largest equivalence which satisfies them.

Having an independent notion of which systems should, and which should not, be distinguished, one can then justify a particular notion of equivalence, e.g. bisimulation, by showing that it captures precisely the touchstone equivalence. In other words, a particular definition of bisimulation is appropriate because the associated bisimulation equivalence, say $\approx_{\mathit{bis}}$, is *sound* with respect to the touchstone equivalence and provides for it a *complete* proof methodology, i.e. $s_1 \approx_{\mathit{bis}} s_2$ if and only if $s_1 \approx_{\text{behav}} s_2$.

This approach originated in [19] but has now been widely used for different process description languages; for example, see [20,28] for its application to higher-order process languages, [26] for mobile ambients, [10] for asynchronous languages and [6] for probabilistic timed languages. Moreover, in each case the distinguishing criteria are almost the same. The touchstone equivalence should be *compositional* (preserved by some natural operators for constructing systems), *barb-preserving* (equivalent processes exhibit the same observables) and *reduction-closed* (nondeterministic choices are in some sense preserved).

We adapt this approach to quantum processes. Using natural versions of these criteria we obtain an appropriate touchstone equivalence, which we call *reduction barbed congruence*, $\approx_r$. We then develop a theory of bisimulations which is both sound and complete for $\approx_r$. Moreover, we provide a modal characterisation of $\approx_r$ in a quantum logic based on Hennessy-Milner logic [17] by establishing the coincidence of the largest bisimulation with logical equivalence.

Due to lack of space, we omit all proofs; they can be found in [5]. We also refer the readers to [25] for the basic notions of linear algebra and quantum information theory used in this paper.

2 A Probabilistic Model

We review the model of probabilistic labelled transition systems (pLTSs). Later on we will interpret the behaviour of quantum processes in terms of pLTSs because quantum measurements give rise to probability distributions naturally.

We begin with some notations. A (discrete) probability distribution over a set S is a function $\Delta : S \to [0,1]$ with $\sum_{s\in S} \Delta(s) = 1$; the support of such a Δ is the set $\lceil \Delta \rceil = \{\, s \in S \mid \Delta(s) > 0 \,\}$. The point distribution $\overline{s}$ assigns probability 1 to s and 0 to all other elements of S, so that $\lceil \overline{s} \rceil = \{s\}$. In this paper we only need to use distributions with finite support, and let $Dist(S)$ denote the set of finite support distributions over S, ranged over by Δ, Θ etc. If $\sum_{k\in K} p_k = 1$ for some collection of $p_k \geq 0$, and the Δ_k are distributions, then so is $\sum_{k\in K} p_k \cdot \Delta_k$ with $(\sum_{k\in K} p_k \cdot \Delta_k)(s) \ = \ \sum_{k\in K} p_k \cdot \Delta_k(s)$.

Definition 1. *A* probabilistic labelled transition system *is a triple* $\langle S, \mathsf{Act}_\tau, \to \rangle$*, where* S *is a set of states,* Act_τ *is a set of labels* Act *augmented with distinguished element* τ*, and* $\to$ *is a subset of* $S \times \mathsf{Act}_\tau \times Dist(S)$*.*

We often write $s \xrightarrow{\alpha} \Delta$ for $(s, \alpha, \Delta) \in \to$, and $s \xrightarrow{\alpha}$ for $\exists \Delta : s \xrightarrow{\alpha} \Delta$. In a pLTS actions are only performed by states, in that actions are given by relations from states to distributions. But in general we allow distributions over states to perform an action. For this purpose, we *lift* these relations so that they also apply to distributions [7].

Definition 2. *Let* $\mathcal{R} \subseteq S \times Dist(S)$ *be a relation from states to distributions in a pLTS. Then* $\mathcal{R}^\circ \subseteq Dist(S) \times Dist(S)$ *is the smallest relation that satisfies the two rules: (i)* $s \ \mathcal{R} \ \Theta$ *implies* $\overline{s} \ \mathcal{R}^\circ \ \Theta$*; (ii)* $\Delta_i \ \mathcal{R}^\circ \ \Theta_i$ *for all* $i \in I$ *implies* $(\sum_{i\in I} p_i \cdot \Delta_i) \ \mathcal{R}^\circ \ (\sum_{i\in I} p_i \cdot \Theta_i)$ *for any* $p_i \in [0,1]$ *with* $\sum_{i\in I} p_i = 1$*, where* I *is a countable index set.*

We apply this operation to the relations $\xrightarrow{\alpha}$ in the pLTS for $\alpha \in \mathsf{Act}_\tau$, where we also write $\xrightarrow{\alpha}$ for $(\xrightarrow{\alpha})^\circ$. Thus as source of a relation $\xrightarrow{\alpha}$ we now also allow distributions. But note that $\overline{s} \xrightarrow{\alpha} \Delta$ is more general than $s \xrightarrow{\alpha} \Delta$ because if $\overline{s} \xrightarrow{\alpha} \Delta$ then there is a collection of distributions Δ_i and probabilities p_i such that $s \xrightarrow{\alpha} \Delta_i$ for each $i \in I$ and $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$ with $\sum_{i\in I} p_i = 1$.

We write $s \xrightarrow{\hat{\tau}} \Delta$ if either $s \xrightarrow{\tau} \Delta$ or $\Delta = \overline{s}$. We define weak transitions $\xRightarrow{\hat{a}}$ by letting $\xRightarrow{\hat{\tau}}$ be the reflexive and transitive closure of $\xrightarrow{\hat{\tau}}$ and writing $\Delta \xRightarrow{\hat{a}} \Theta$ for $a \in \mathsf{Act}$ whenever $\Delta \xRightarrow{\hat{\tau}}\xrightarrow{a}\xRightarrow{\hat{\tau}} \Theta$. If Δ is a point distribution, we often write $s \xRightarrow{\hat{a}} \Theta$ instead of $\overline{s} \xRightarrow{\hat{a}} \Theta$.

Let $\mathcal{R} \subseteq S \times S$ be a relation between states. It induces a special relation $\hat{\mathcal{R}} \subseteq S \times Dist(S)$ between states and distributions by letting $\hat{\mathcal{R}} \overset{def}{=} \{(s, \overline{t}) \mid s \ \mathcal{R} \ t\}$. Then we can use Definition 2 to lift $\hat{\mathcal{R}}$ to be a relation $(\hat{\mathcal{R}})^\circ$ between distributions. For simplicity, we combine the above two lifting operations and directly write $\mathcal{R}^\circ$ for $(\hat{\mathcal{R}})^\circ$ in the sequel, with the intention that a relation between states can be lifted to a relation between distributions via a special application of Definition 2. In this particular case, it holds that $\Delta \ \mathcal{R}^\circ \ \Theta$ implies $\Theta \ (\mathcal{R}^{-1})^\circ \ \Delta$, where $s \ \mathcal{R} \ t$ iff

$t\,\mathcal{R}^{-1}\,s$ for any $s, t \in S$. This way of lifting relations has elegant mathematical characterisations; see [4] for more details.

3 Quantum CCS

We introduce a quantum extension of classical CCS (qCCS) which was originally studied in [8,31,9]. Three types of data are considered in qCCS: as classical data we have `Bool` for booleans and `Real` for real numbers, and as quantum data we have `Qbt` for qubits. Consequently, two countably infinite sets of variables are assumed: $cVar$ for classical variables, ranged over by $x, y, ...$, and $qVar$ for quantum variables, ranged over by $q, r, ...$ We assume a set Exp, which includes $cVar$ as a subset and is ranged over by $e, e', \ldots$, of classical data expressions over `Real`, and a set of boolean-valued expressions $BExp$, ranged over by $b, b', \ldots$, with the usual boolean constants `true`, `false`, and operators $\neg$, $\wedge$, $\vee$, and $\rightarrow$. In particular, we let $e \bowtie e'$ be a boolean expression for any $e, e' \in Exp$ and $\bowtie \in \{>, <, \geq, \leq, =\}$. We further assume that only classical variables can occur freely in both data expressions and boolean expressions. Two types of channels are used: $cChan$ for classical channels, ranged over by $c, d, ...$, and $qChan$ for quantum channels, ranged over by $\underline{c}, \underline{d}, ...$ A relabelling function f is a map on $cChan \cup qChan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$. Sometimes we abbreviate a sequence of distinct variables $q_1, ..., q_n$ into $\tilde{q}$.

The terms in qCCS are given by:

$$\begin{aligned} P, Q ::= \mathbf{nil} \mid \tau.P \mid c?x.P \mid c!e.P \mid \underline{c}?q.P \mid \underline{c}!q.P \mid \mathcal{E}[\tilde{q}].P \mid M[\tilde{q}; x].P \mid \\ P + Q \mid P \,||\, Q \mid P[f] \mid P\backslash L \mid \mathbf{if}\ b\ \mathbf{then}\ P \mid A(\tilde{q}; \tilde{x}) \end{aligned}$$

where f is a relabelling function and $L \subseteq cChan \cup qChan$ is a set of channels. Most of the constructors are standard as in CCS [23]. We briefly explain a few new constructors. The process $\underline{c}?q.P$ receives a quantum datum along quantum channel $\underline{c}$ and evolves into P, while $\underline{c}!q.P$ sends out a quantum datum along quantum channel $\underline{c}$ before evolving into P. The symbol $\mathcal{E}$ represents a trace-preserving super-operator applied on the systems $\tilde{q}$. The process $M[\tilde{q}; x].P$ measures the state of qubits $\tilde{q}$ according to the observable M and stores the measurement outcome into the classical variable x of P.

Free classical variables can be defined in the usual way, except for the fact that the variable x in the quantum measurement $M[\tilde{q}; x]$ is bound. A process P is closed if it contains no free classical variable, i.e. $fv(P) = \emptyset$.

The set of free quantum variables for process P, denoted by $qv(P)$ can be inductively defined as in Figure 1. For a process to be legal, we require that

1. $q \notin qv(P)$ in the process $\underline{c}!q.P$;
2. $qv(P) \cap qv(Q) = \emptyset$ in the process $P \,||\, Q$;
3. Each constant $A(\tilde{q}; \tilde{x})$ has a defining equation $A(\tilde{q}; \tilde{x}) := P$, where P is a term with $qv(P) \subseteq \tilde{q}$ and $fv(P) \subseteq \tilde{x}$.

The first condition says that a quantum system will not be referenced after it has been sent out. This is a requirement of the quantum no-cloning theorem.

$$
\begin{array}{rlrl}
qv(\mathsf{nil}) &= \emptyset & qv(\tau.P) &= qv(P)\\
qv(c?x.P) &= qv(P) & qv(c!e.P) &= qv(P)\\
qv(\underline{c}?q.P) &= qv(P) - \{q\} & qv(\underline{c}!q.P) &= qv(P) \cup \{q\}\\
qv(\mathcal{E}[\tilde{q}].P) &= qv(P) \cup \tilde{q} & qv(M[\tilde{q};x].P) &= qv(P) \cup \tilde{q}\\
qv(P+Q) &= qv(P) \cup qv(Q) & qv(P \mid\mid Q) &= qv(P) \cup qv(Q)\\
qv(P[f]) &= qv(P) & qv(P\backslash L) &= qv(P)\\
qv(\textbf{if } b \textbf{ then } P) &= qv(P) & qv(A(\tilde{q};\tilde{x})) &= \tilde{q}.
\end{array}
$$

Fig. 1. Free quantum variables

The second condition says that parallel composition $||$ models separate parties that never reference a quantum system simultaneously.

Throughout the paper we implicitly assume the convention that processes are identified up to α-conversion, bound variables differ from each other and they are different from free variables.

We now give the semantics of qCCS. For each quantum variable q we assume a 2-dimensional Hilbert space $\mathcal{H}_q$. For any nonempty subset $S \subseteq qVar$ we write $\mathcal{H}_S$ for the tensor product space $\bigotimes_{q\in S} \mathcal{H}_q$ and $\mathcal{H}_{\overline{S}}$ for $\bigotimes_{q\notin S} \mathcal{H}_q$. In particular, $\mathcal{H} = \mathcal{H}_{qVar}$ is the state space of the whole environment consisting of all the quantum variables, which is a countably infinite dimensional Hilbert space.

Let P be a closed quantum process and ρ a density operator on $\mathcal{H}$,[1] the pair $\langle P, \rho\rangle$ is called a *configuration*. We write *Con* for the set of all configurations, ranged over by $\mathcal{C}$ and $\mathcal{D}$. We interpret qCCS with a pLTS whose states are all the configurations definable in the language, and whose transitions are determined by the rules in Figure 2; we have omitted the obvious symmetric counterparts to the rules *(C-Com)*, *(Q-Com)*, *(Int)* and *(Sum)*. The set of actions Act takes the following form, consisting of classical/quantum input/output actions.

$$\{c?v, c!v \mid c \in cChan, v \in \texttt{Real}\} \cup \{\underline{c}?r, \underline{c}!r \mid \underline{c} \in qChan, r \in qVar\}$$

We use $cn(\alpha)$ for the set of channel names in action α. For example, we have $cn(\underline{c}?x) = \{\underline{c}\}$ and $cn(\tau) = \emptyset$.

In the first eight rules in Figure 2, the targets of arrows are point distributions, and we use the slightly abbreviated form $\mathcal{C} \xrightarrow{\alpha} \mathcal{C}'$ to mean $\mathcal{C} \xrightarrow{\alpha} \overline{\mathcal{C}'}$.

The rules use the obvious extension of the function $||$ on terms to configurations and distributions. To be precise, $\mathcal{C} \mid\mid P$ is the configuration $\langle Q \mid\mid P, \rho\rangle$ where $\mathcal{C} = \langle Q, \rho\rangle$, and $\Delta \mid\mid P$ is the distribution defined by:

$$(\Delta \mid\mid P)(\langle Q, \rho\rangle) \overset{def}{=} \begin{cases} \Delta(\langle Q', \rho\rangle) & \text{if } Q = Q' \mid\mid P \text{ for some } Q' \\ 0 & \text{otherwise.} \end{cases}$$

Similar extension applies to $\Delta[f]$ and $\Delta\backslash L$.

[1] As $\mathcal{H}$ is infinite dimensional, ρ should be understood as a density operator on some finite dimensional subspace of $\mathcal{H}$ which contains $\mathcal{H}_{qv(P)}$.

(Tau)
$$\langle \tau.P,\rho\rangle \xrightarrow{\tau} \langle P,\rho\rangle$$

(C-Outp)
$$\frac{v=[[e]]}{\langle c!e.P,\rho\rangle \xrightarrow{c!v} \langle P,\rho\rangle}$$

(Q-inp)
$$\frac{r \notin qv(\underline{c}?q.P)}{\langle \underline{c}?q.P,\rho\rangle \xrightarrow{\underline{c}?r} \langle P[r/q],\rho\rangle}$$

(Q-Com)
$$\frac{\langle P_1,\rho\rangle \xrightarrow{\underline{c}?r} \langle P_1',\rho\rangle \qquad \langle P_2,\rho\rangle \xrightarrow{\underline{c}!r} \langle P_2',\rho\rangle}{\langle P_1 \mid\mid P_2,\rho\rangle \xrightarrow{\tau} \langle P_1' \mid\mid P_2',\rho\rangle}$$

(Meas)
$$\frac{M=\sum_{i\in I}\lambda_i E^i \qquad p_i = tr(E^i_{\tilde q}\rho)}{\langle M[\tilde q;x].P,\rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i\langle P[\lambda_i/x], E^i_{\tilde q}\rho E^i_{\tilde q}/p_i\rangle}$$

(Int)
$$\frac{\langle P_1,\rho\rangle \xrightarrow{\alpha} \Delta \qquad qbv(\alpha)\cap qv(P_2)=\emptyset}{\langle P_1 \mid\mid P_2,\rho\rangle \xrightarrow{\alpha} \Delta \mid\mid P_2}$$

(Rel)
$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \Delta}{\langle P[f],\rho\rangle \xrightarrow{f(\alpha)} \Delta[f]}$$

(Cho)
$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \Delta \qquad [[b]]=\texttt{true}}{\langle \textbf{if } b \textbf{ then } P,\rho\rangle \xrightarrow{\alpha} \Delta}$$

(C-Inp)
$$\frac{v\in \texttt{Real}}{\langle c?x.P,\rho\rangle \xrightarrow{c?v} \langle P[v/x],\rho\rangle}$$

(C-Com)
$$\frac{\langle P_1,\rho\rangle \xrightarrow{c?v} \langle P_1',\rho\rangle \qquad \langle P_2,\rho\rangle \xrightarrow{c!v} \langle P_2',\rho\rangle}{\langle P_1 \mid\mid P_2,\rho\rangle \xrightarrow{\tau} \langle P_1' \mid\mid P_2',\rho\rangle}$$

(Q-Outp)
$$\langle \underline{c}!q.P,\rho\rangle \xrightarrow{\underline{c}!q} \langle P,\rho\rangle$$

(Oper)
$$\langle \mathcal{E}[\tilde q].P,\rho\rangle \xrightarrow{\tau} \langle P,\mathcal{E}_{\tilde q}(\rho)\rangle$$

(Sum)
$$\frac{\langle P_1,\rho\rangle \xrightarrow{\alpha} \Delta}{\langle P_1+P_2,\rho\rangle \xrightarrow{\alpha} \Delta}$$

(Res)
$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \Delta \qquad cn(\alpha)\cap L=\emptyset}{\langle P\backslash L,\rho\rangle \xrightarrow{\alpha} \Delta\backslash L}$$

(Cons)
$$\frac{\langle P[\tilde v/\tilde x, \tilde r/\tilde q],\rho\rangle \xrightarrow{\alpha} \Delta \qquad A(\tilde x,\tilde q):=P}{\langle A(\tilde v,\tilde r),\rho\rangle \xrightarrow{\alpha} \Delta}$$

Fig. 2. Operational semantics of qCCS. Here in rule *(C-Outp)*, $[[e]]$ is the evaluation of e, and in rule *(Meas)*, $E^i_{\tilde q}$ denotes the operator E^i acting on the quantum systems $\tilde q$.

4 An Extensional Equivalence

Let $\mathcal{C}=\langle P,\rho\rangle$. We use the notation $qv(\mathcal{C}):=qv(P)$ for free quantum variables and $\mathrm{env}(\mathcal{C}):=\mathrm{tr}_{qv(P)}(\rho)$ for partial traces. Let $\Delta=\sum_{i\in I} p_i\cdot\overline{\langle P_i,\rho_i\rangle}$. We write $\mathcal{E}(\Delta)$ for the distribution $\sum_{i\in I} p_i\cdot\overline{\langle P_i,\mathcal{E}(\rho_i)\rangle}$.

We formally define three criteria, namely barb-preservation, reduction-closedness and compositionality, in order to judge whether two processes are equivalent.

Definition 3. *A relation $\mathcal{R}$ is*

- barb-preserving *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $\mathcal{C}\Downarrow_c^{\geq p}$ iff $\mathcal{D}\Downarrow_c^{\geq p}$ for any $p\in[0,1]$ and any classical channel c, where $\mathcal{C}\Downarrow_c^{\geq p}$ holds if $\mathcal{C}\stackrel{\hat\tau}{\Longrightarrow}\Delta$ for some Δ with*
$$\sum\{\Delta(\mathcal{C}') \mid \mathcal{C}' \xrightarrow{c!v} \textit{for some } v\} \ \geq\ p;$$
- reduction-closed *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies*
  - *whenever $\mathcal{C}\stackrel{\hat\tau}{\Longrightarrow}\Delta$, there exists Θ such that $\mathcal{D}\stackrel{\hat\tau}{\Longrightarrow}\Theta$ and $\Delta\ \mathcal{R}^\circ\ \Theta$,*
  - *whenever $\mathcal{D}\stackrel{\hat\tau}{\Longrightarrow}\Theta$, there exists Δ such that $\mathcal{C}\stackrel{\hat\tau}{\Longrightarrow}\Delta$ and $\Delta\ \mathcal{R}^\circ\ \Theta$;*

- compositional *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies $(\mathcal{C}||R)\ \mathcal{R}\ (\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$, and $\mathcal{R}$ is closed under super-operator application, namely $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies $\mathcal{E}(\mathcal{C})\ \mathcal{R}\ \mathcal{E}(\mathcal{D})$ for any $\mathcal{E} \in \mathcal{TSO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$, where $\mathcal{TSO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ stands for the set of trace-preserving super-operators on finite dimensional subspaces of $\mathcal{H}_{\overline{qv(\mathcal{C})}}$.*

Here barb-preservation means that two related configurations have the same probability to send out values on classical channels. Reduction-closure ensures that non-deterministic choices are in some sense preserved. In the definition of compositionality, it is worth noting that we only allow the super-operator $\mathcal{E}$ to be applied on $\mathcal{H}_{\overline{qv(\mathcal{C})}}$. The intuition behind this restriction is that systems in $qv(\mathcal{C})$ are actually the *local* quantum variables of $\mathcal{C}$, and they cannot be manipulated by the outer environment.

Definition 4 (Reduction barbed congruence). *Let* reduction barbed congruence*, written $\approx_r$, be the largest relation over configurations which is barb-preserving, reduction-closed and compositional, and furthermore, if $\mathcal{C} \approx_r \mathcal{D}$ then $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$.*

With the above definition, it is difficult to prove if two given configurations are related by reduction barbed congruence. Therefore, we need to discover some proof techniques which are easy to use.

4.1 Open Bisimulations

We now introduce a coinductively defined relation which will be used later on to characterise reduction barbed congruence.

Definition 5. *A relation $\mathcal{R} \subseteq Con \times Con$ is an* open simulation *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$, $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$, and for any $\mathcal{E} \in \mathcal{TSO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$,*

- *whenever $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, there is some Θ with $\mathcal{E}(\mathcal{D}) \overset{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta\ \mathcal{R}^\circ\ \Theta$.*

A relation $\mathcal{R}$ is an open bisimulation *if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are open simulations. We let $\approx_o$ be the largest open bisimulation.*

Two quantum processes P and Q are bisimilar, denoted by $P \approx_o Q$, if for any quantum state ρ and any indexed set $\tilde{v}$ of classical values, we have

$$\langle P\{\tilde{v}/\tilde{x}\}, \rho\rangle \approx_o \langle Q\{\tilde{v}/\tilde{x}\}, \rho\rangle.$$

Here $\tilde{x}$ is the set of free classical variables contained in P and Q.

The above definition is inspired by the work of Sangiorgi [27], where a notion of bisimulation is defined for the π-calculus by treating name instantiation in an "open" style (name instantiation happens before any transition). Here we deal with super-operator application in an "open" style, but the instantiation of variables is in an "early" style (variables are instantiated when input actions are performed) because the operational semantics given in Figure 2 is essentially an early semantics. For more variants of semantics, see e.g. [29].

4.2 A Useful Proof Technique

In Definition 5 super-operator application and transitions are considered at the same time. In fact, we can separate the two issues and approach the concept of open bisimulation in an incremental way, which turns out to be very useful when proving that two configurations are bisimilar.

Definition 6. *A relation $\mathcal{R} \subseteq Con \times Con$ is a* ground simulation *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$, $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$, and*

- *whenever $\mathcal{C} \xrightarrow{\alpha} \Delta$, there is some distribution Θ with $\mathcal{D} \overset{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta\ \mathcal{R}^\circ\ \Theta$.*

A relation $\mathcal{R}$ is a ground bisimulation *if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are ground simulations.*

Proposition 1. *Suppose that a relation $\mathcal{R}$*

1. *is a ground bisimulation, and*
2. *is closed under all super-operator application.*

Then $\mathcal{R}$ is an open bisimulation.

Proposition 1 provides us with a useful proof technique: in order to show that two configurations $\mathcal{C}$ and $\mathcal{D}$ are open bisimilar, it suffices to exhibit a binary relation including the pair $(\mathcal{C}, \mathcal{D})$, and then to check that the relation is a ground bisimulation and is closed under all super-operator application. This is analogous to a proof technique of open bisimulation for the π-calculus [27], where name instantiation is playing the same role as super-operator application here.

Proposition 2. *$\approx_o$ is the largest ground bisimulation that is closed under all super-operator application.*

For a sanity check, we can prove that $\approx_o$ is an equivalence relation. As a relation between configurations, $\approx_o$ is preserved by all static constructors.

Proposition 3. *If $\langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle$ then*

1. *$\langle P\|R, \rho\rangle \approx_o \langle Q\|R, \sigma\rangle$;*
2. *$\langle P[f], \rho\rangle \approx_o \langle Q[f], \sigma\rangle$;*
3. *$\langle P\backslash L, \rho\rangle \approx_o \langle Q\backslash L, \sigma\rangle$;*
4. *$\langle \textbf{if } b \textbf{ then } P, \rho\rangle \approx_o \langle \textbf{if } b \textbf{ then } Q, \sigma\rangle$.*

We do not have a counterpart of the above proposition for dynamic constructors such as prefix. For example, consider the two configurations taken from [9]: $\langle P, \rho\rangle$ and $\langle Q, \rho\rangle$, where $P = M_{0,1}[q; x].\mathbf{nil}$ with $M_{0,1} = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$ being the 1-qubit measurement according to the computational basis, $Q = I[q].\mathbf{nil}$, and $\rho = |0\rangle\langle 0|_q \otimes \sigma$ with σ being a state on $\mathcal{H}_{\overline{q}}$. We have $\langle P, \rho\rangle \approx_o \langle Q, \rho\rangle$, but $\langle H[q].P, \rho\rangle \not\approx_o \langle H[q].Q, \rho\rangle$, where H is the Hadamard operator.

Nevertheless, as a relation between processes, $\approx_o$ is preserved by almost all constructors of qCCS.

Theorem 1. *The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.*

It turns out that reduction barbed congruence can be captured by open bisimulation precisely. This gives a coinductive technique to judge if two configurations are behaviourally equivalent.

Theorem 2 (Soundness). *If $\mathcal{C} \approx_o \mathcal{D}$ then $\mathcal{C} \approx_r \mathcal{D}$.*

In order to obtain completeness, the converse of Theorem 2, we make use of a proof technique that involves examining the barbs of processes in certain contexts; the following technical lemma enhances this technique.

Lemma 1. *If $\Delta||c!0 \; (\approx_r)^\circ \; \Theta||c!0$ where c is a fresh channel, then $\Delta \; (\approx_r)^\circ \; \Theta$.*

We are now in a position to show that $\approx_r$ is complete with respect to $\approx_o$.

Theorem 3 (Completeness). *If $\mathcal{C} \approx_r \mathcal{D}$ then $\mathcal{C} \approx_o \mathcal{D}$.*

Proof. (*Schema*) Since $\approx_r$ is closed under any super-operator application, by Proposition 1 it suffices to show that $\approx_r$ is a ground bisimulation. The key idea is the following. For any transition $\mathcal{C} \xrightarrow{\alpha} \Delta$, we design a test process T, depending on the form of α, such that $\mathcal{C}||T \overset{\hat{\tau}}{\Longrightarrow} \Gamma_1$ for some distribution Γ_1 which exhibits certain barbs. Since $\mathcal{C} \approx_r \mathcal{D}$ we know $\mathcal{C}||T \approx_r \mathcal{D}||T$ by the compositionality of $\approx_r$. Since $\approx_r$ is reduction-closed, there is some Γ_2 such that $\mathcal{D}||T \overset{\hat{\tau}}{\Longrightarrow} \Gamma_2$ and $\Gamma_1 \; (\approx_r)^\circ \; \Gamma_2$. Since $\approx_r$ is barb-preserving, Γ_2 must exhibit similar barbs as Γ_1. The careful design of T ensures that $\mathcal{D} \overset{\hat{\alpha}}{\Longrightarrow} \Theta$ for some Θ with $\Delta \; (\approx_r)^\circ \; \Theta$, and the last step involves Proposition 1. See [5] for more details. □

4.3 Modal Characterisation

We extend the Hennessy-Milner logic by adding a probabilistic choice modality to express the behaviour of distributions, as in [7], and a super-operator modality to express trace-preserving super-operator application, as well as atomic formulae involving projectors for dealing with density operators.

Definition 7. *The class $\mathcal{L}$ of modal formulae over* Act*, ranged over by ϕ, is defined by the following grammar:*

$$\begin{aligned} \phi &:= E_{\tilde{q}}^{\geq p} \mid \textstyle\bigwedge_{i\in I} \phi_i \mid \langle\alpha\rangle\psi \mid \neg\phi \mid \mathcal{E}.\phi \\ \psi &:= \textstyle\bigoplus_{i\in I} p_i \cdot \phi_i \end{aligned}$$

where $\alpha \in \mathsf{Act}_\tau$, $\mathcal{E}$ is a super-operator, and E is a projector associated with a certain subspace of $\mathcal{H}_{\tilde{q}}$. We call ϕ a configuration formula *and ψ a* distribution formula*. Note that a distribution formula ψ only appears as the continuation of a diamond modality $\langle\alpha\rangle\psi$.*

The satisfaction relation *$\models \subseteq Con \times \mathcal{L}$ is defined by*

- *$\mathcal{C} \models E_{\tilde{q}}^{\geq p}$ if $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$ where $\mathcal{C} = \langle P, \rho\rangle$.*
- *$\mathcal{C} \models \bigwedge_{i\in I} \phi_i$ if $\mathcal{C} \models \phi_i$ for all $i \in I$.*

- *$\mathcal{C} \models \langle\alpha\rangle\psi$ if for some $\Delta \in Dist(Con)$, $\mathcal{C} \overset{\hat{\alpha}}{\Longrightarrow} \Delta$ and $\Delta \models \psi$.*
- *$\mathcal{C} \models \neg\phi$ if it is not the case that $\mathcal{C} \models \phi$.*
- *$\mathcal{C} \models \mathcal{E}.\phi$ if $\mathcal{E} \in \mathcal{TSO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ and $\mathcal{E}(\mathcal{C}) \models \phi$.*
- *$\Delta \models \bigoplus_{i\in I} p_i \cdot \phi_i$ if there are $\Delta_i \in Dist(Con)$ for all $i \in I$, and for all $\mathcal{D} \in \lceil \Delta_i \rceil$, with $\mathcal{D} \models \phi_i$, such that $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$.*

With a slight abuse of notation, we write $\Delta \models \psi$ above to mean that Δ satisfies the distribution formula ψ. A logical equivalence arises from the logic naturally: we write $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ if $\mathcal{C} \models \phi \Leftrightarrow \mathcal{D} \models \phi$ for all $\phi \in \mathcal{L}$. Using the logical equivalence, we provide a modal characterisation of reduction barbed congruence as follows.

Theorem 4. *$\mathcal{C} \approx_r \mathcal{D}$ if and only if $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$.*

Proof. (*Schema*) In view of Theorems 2 and 3, it suffices to prove that $\mathcal{C} \approx_o \mathcal{D}$ if and only if $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$. For one direction, we show that $\mathcal{C} \models \phi \Leftrightarrow \mathcal{D} \models \phi$ for all $\phi \in \mathcal{L}$ by structural induction on ϕ; for the other direction, we show that $=^{\mathcal{L}}$ is an open bisimulation by using Proposition 1. □

5 Examples

BB84, the first quantum key distribution protocol developed by Bennett and Brassard in 1984 [2], provides a provably secure way to create a private key between two parties, say, Alice and Bob. Its security relies on the basic property of quantum mechanics that information gain about a quantum state is only possible at the expense of changing the state, if the states to be distinguished are not orthogonal. The basic BB84 protocol goes as follows:

(1) Alice randomly creates two strings of bits $\tilde{B}_a$ and $\tilde{K}_a$, each with size n.
(2) Alice prepares a string of qubits $\tilde{q}$, with size n, such that the ith qubit of $\tilde{q}$ is $|x_y\rangle$ where x and y are the ith bits of $\tilde{B}_a$ and $\tilde{K}_a$, respectively, and $|0_0\rangle = |0\rangle$, $|0_1\rangle = |1\rangle$, $|1_0\rangle = |+\rangle$, and $|1_1\rangle = |-\rangle$. Here the symbols $|+\rangle$ and $|-\rangle$ have their usual meaning: $|+\rangle \overset{def}{=} (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle \overset{def}{=} (|0\rangle - |1\rangle)/\sqrt{2}$.
(3) Alice sends the qubit string $\tilde{q}$ to Bob.
(4) Bob randomly generates a string of bits $\tilde{B}_b$ with size n.
(5) Bob measures each qubit received from Alice according to a basis determined by the bits he generated: if the ith bit of $\tilde{B}_b$ is k then he measures with $\{|k_0\rangle, |k_1\rangle\}$, $k = 0, 1$. Let the measurement results be $\tilde{K}_b$, which is also a string of bits with size n.
(6) Bob sends his choice of measurement bases $\tilde{B}_b$ back to Alice, and upon receiving the information, Alice sends her bases $\tilde{B}_a$ to Bob.
(7) Alice and Bob determine at which positions the bit strings $\tilde{B}_a$ and $\tilde{B}_b$ are equal. They discard the bits in $\tilde{K}_a$ and $\tilde{K}_b$ where the corresponding bits of $\tilde{B}_a$ and $\tilde{B}_b$ do not match.

After the execution of the basic BB84 protocol above, the remaining bits of $\tilde{K}_a$ and $\tilde{K}_b$, denoted by $\tilde{K}'_a$ and $\tilde{K}'_b$ respectively, should be the same, provided that the channels used are perfect, and no eavesdropper exists.

To detect a potential eavesdropper Eve, Alice and Bob proceed as follows:

(8) Alice randomly chooses $\lceil k/2 \rceil$, where k is the size of $\tilde{K}'_a$, bits of $\tilde{K}'_a$, denoted by $\tilde{K}''_a$, and sends Bob $\tilde{K}''_a$ and their indexes in the original string $\tilde{K}'_a$.

(9) Upon receiving the information from Alice, Bob sends back to Alice his substring $\tilde{K}''_b$ of $\tilde{K}'_b$ according to the indexes received from Alice.

(10) Alice and Bob check if the strings $\tilde{K}''_a$ and $\tilde{K}''_b$ are equal. If yes, then the remaining substring $\tilde{K}^f_a$ (resp. $\tilde{K}^f_b$) of $\tilde{K}'_a$ (resp. $\tilde{K}'_b$) by deleting $\tilde{K}''_a$ (resp. $\tilde{K}''_b$) is the secure key shared by Alice (reps. Bob). Otherwise, an eavesdropper is detected, and the protocol halts without generating any secure keys.

For simplicity, we omit the processes of information reconciliation and privacy amplification. Now we describe the above protocol in qCCS. To ease the notations, we assume a special measurement $Ran[\tilde{q};\tilde{x}]$ which can create a string of n random bits, independent of the initial states of the $\tilde{q}$ system, and store it to $\tilde{x}$. In effect, $Ran[\tilde{q};\tilde{x}] = Set^n_+[\tilde{q}].M^n_{0,1}[\tilde{q};\tilde{x}].Set^n_0[\tilde{q}]$ where Set^n_+ (resp. Set^n_0) is the super-operator which sets each of the n qubits it applies on to $|+\rangle$ (resp. $|0\rangle$), $M^n_{0,1}[\tilde{q};\tilde{x}]$ is the quantum measurement on $\tilde{q}$ according to the basis $\{|0\rangle, |1\rangle\}$, and stores the result into $\tilde{x}$. Then the basic BB84 protocol can be defined as

$$\begin{aligned}
Alice &\overset{def}{=} Ran[\tilde{q};\tilde{B}_a].Ran[\tilde{q};\tilde{K}_a].Set_{\tilde{K}_a}[\tilde{q}].H_{\tilde{B}_a}[\tilde{q}].\mathsf{A2B}!\tilde{q}.WaitA(\tilde{B}_a,\tilde{K}_a)\\
WaitA(\tilde{B}_a,\tilde{K}_a) &\overset{def}{=} b2a?\tilde{B}_b.a2b!\tilde{B}_a.key_a!cmp(\tilde{K}_a,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}\\
Bob &\overset{def}{=} \mathsf{A2B}?\tilde{q}.Ran[\tilde{q}';\tilde{B}_b].M_{\tilde{B}_b}[\tilde{q};\tilde{K}_b].b2a!\tilde{B}_b.WaitB(\tilde{B}_b,\tilde{K}_b)\\
WaitB(\tilde{B}_b,\tilde{K}_b) &\overset{def}{=} a2b?\tilde{B}_a.key_b!cmp(\tilde{K}_b,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}\\
BB84 &\overset{def}{=} (Alice\|Bob)\backslash\{a2b, b2a, \mathsf{A2B}\}
\end{aligned}$$

where $Set_{\tilde{K}_a}[\tilde{q}]$ sets the ith qubit of $\tilde{q}$ to the state $|\tilde{K}_a(i)\rangle$, $H_{\tilde{B}_a}[\tilde{q}]$ applies H or does nothing on the ith qubit of $\tilde{q}$ depending on whether the ith bit of $\tilde{B}_a$ is 1 or 0, and $M_{\tilde{B}_b}[\tilde{q};\tilde{K}_b]$ is the quantum measurement on $\tilde{q}$ according to the basis determined by $\tilde{B}_b$, i.e., for each $1 \le k \le n$, it measures q_k with respect to the basis $\{|0\rangle, |1\rangle\}$ (reps. $\{|+\rangle, |-\rangle\}$) if $\tilde{B}_b(k) = 0$ (resp. 1), and stores the result into $\tilde{K}_b(k)$. We also abuse the notation slightly by writing $\mathcal{E}_{\tilde{B}}[\tilde{q}].P$ when we mean $\sum_{\tilde{x}=0^n}^{1^n}(\textbf{if } \tilde{B} = \tilde{x} \textbf{ then } \mathcal{E}_{\tilde{x}}[\tilde{q}].P)$ where i^n is the all i string of size n, $i = 0, 1$. The function cmp takes a triple of strings $\tilde{x}, \tilde{y}, \tilde{z}$ with the same size as inputs, and returns the substring of $\tilde{x}$ where the corresponding bits of $\tilde{y}$ and $\tilde{z}$ match. When $\tilde{y}$ and $\tilde{z}$ match nowhere, we let $cmp(\tilde{x},\tilde{y},\tilde{z}) = \epsilon$, the empty string.

To show the correctness of this basic form of BB84 protocol, we let

$$\begin{aligned}
BB84_{spe} \overset{def}{=} {} & Ran[\tilde{q};\tilde{B}_a].Ran[\tilde{q};\tilde{K}_a].Ran[\tilde{q}';\tilde{B}_b].\\
& (key_a!cmp(\tilde{K}_a,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}\|key_b!cmp(\tilde{K}_a,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}).
\end{aligned}$$

The pLTSs of $BB84$ and $BB84_{spe}$ for the special case of $n = 2$ can be depicted as in Figure 3, where for simplicity, we only specify the branch where $\tilde{B}_a = \tilde{K}_a = 00$. Each arrow in the graph denotes a sequence of τ actions, and all probabilistic

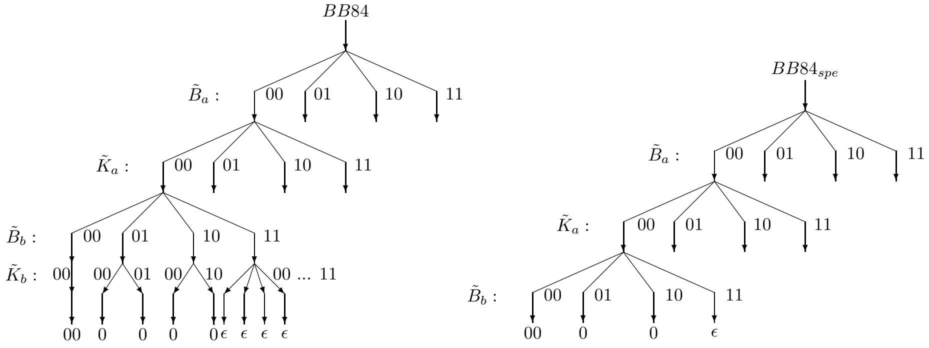

Fig. 3. pLTSs for $BB84$ and $BB84_{spe}$

distributions are uniform. The strings at the bottom line are the outputs of the protocol. Then it can be easily checked from the pLTSs that $BB84 \approx_o BB84_{spe}$. The key is, for each extra branch in $BB84$ caused by the measurement of Bob (the $\tilde{K}_b$ line), the final states are bisimilar; they all output the same string.

Now we proceed to describe the protocol with an eavesdropper. Let

$$\begin{aligned} Alice' \overset{def}{=} &\ (Alice\|key_a?\tilde{K}'_a.Pstr_{|\tilde{K}'_a|}[\tilde{q}_a;\tilde{x}].a2b!\tilde{x}.a2b!SubStr(\tilde{K}'_a,\tilde{x}).b2a?\tilde{K}''_b.\\ &\ (\textbf{if } SubStr(\tilde{K}'_a,\tilde{x}) = \tilde{K}''_b \textbf{ then } key'_a!RemStr(\tilde{K}'_a,\tilde{x}).\textbf{nil}\\ &\ \qquad\qquad\qquad\qquad\qquad \textbf{else } alarm_a!0.\textbf{nil})))\backslash\{key_a\}\\ Bob' \overset{def}{=} &\ (Bob\|key_b?\tilde{K}'_b.a2b?\tilde{x}.a2b?\tilde{K}''_a.b2a!SubStr(\tilde{K}'_b,\tilde{x}).\\ &\ (\textbf{if } SubStr(\tilde{K}'_b,\tilde{x}) = \tilde{K}''_a \textbf{ then } key'_b!RemStr(\tilde{K}'_b,\tilde{x}).\textbf{nil}\\ &\ \qquad\qquad\qquad\qquad\qquad \textbf{else } alarm_b!0.\textbf{nil}))\backslash\{key_b\} \end{aligned}$$

where $|\tilde{x}|$ is the size of $\tilde{x}$, the function $SubStr(\tilde{K}'_a,\tilde{x})$ returns the substring of $\tilde{K}'_a$ at the indexes specified by $\tilde{x}$, and $RemStr(\tilde{K}'_a,\tilde{x})$ returns the remaining substring of $\tilde{K}'_a$ by deleting $SubStr(\tilde{K}'_a,\tilde{x})$. The special measurement $Pstr_m$, which is similar to Ran, randomly generates a $\lceil m/2 \rceil$-sized string of indexes from $1,\ldots,m$.

To get a taste of the security of $BB84$, we consider a special case where Eve's strategy is to simply measure the qubits sent by Alice, according to randomly guessed bases, to get the keys. She then prepares and sends to Bob a fresh sequence of qubits, employing the same method Alice used to encode keys, but using her own guess of bases and the keys she obtained. That is, we define

$$\begin{aligned} Eve &\overset{def}{=} \mathsf{A2E}?\tilde{q}.Ran[\tilde{q}'';\tilde{B}_e].M_{\tilde{B}_e}[\tilde{q};\tilde{K}_e].Set_{\tilde{K}_e}[\tilde{q}].H_{\tilde{B}_e}[\tilde{q}].\mathsf{E2B}!\tilde{q}.key'_e!\tilde{K}_e,\\ BB84_E &\overset{def}{=} (Alice'[f_a]\|Eve\|Bob'[f_b])\backslash\{a2b, b2a, \mathsf{A2E}, \mathsf{E2B}\}. \end{aligned}$$

where $f_a(\mathsf{A2B}) = \mathsf{A2E}$, and $f_b(\mathsf{A2B}) = \mathsf{E2B}$. Let

$$\begin{aligned} TestBB84 \overset{def}{=} & (BB84_E \| key'_a?\tilde{x}.key'_b?\tilde{y}.key'_e?\tilde{z}. \\ & (\mathbf{if}\ \tilde{x} \neq \tilde{y}\ \mathbf{then}\ fail!0.\mathbf{nil}\ \mathbf{else}\ key_e!\tilde{z}.skey!\tilde{x}.\mathbf{nil}))\backslash K \end{aligned}$$

where $K = \{key'_a, key'_b, key'_e\}$. It is generally very complicated to prove the security of the full $BB84$ protocol. Here we choose to reduce $TestBB84$ to a simpler process which is easier for further verification. To be specific, we can show that $TestBB84$ is bisimilar to the following process:

$$\begin{aligned} TB \overset{def}{=} & Ran[\tilde{q}; \tilde{B}_a].Ran[\tilde{q}; \tilde{K}_a].Ran[\tilde{q}''; \tilde{B}_e].Ran'_{\tilde{B}_a, \tilde{B}_e, \tilde{K}_a}[\tilde{q}; \tilde{K}_e].Ran[\tilde{q}'; \tilde{B}_b]. \\ & Ran'_{\tilde{B}_e, \tilde{B}_b, \tilde{K}_e}[\tilde{q}; \tilde{K}_b].Pstr_{|\tilde{K}_{ab}|}[\tilde{q}_a; \tilde{x}]. \\ & (\mathbf{if}\ \tilde{K}_{ab} = \tilde{K}_{ba}\ \mathbf{then}\ key_e!\tilde{K}_e.skey!RemStr(\tilde{K}_{ab}, \tilde{x}).\mathbf{nil} \\ & \ \mathbf{else}\ (\mathbf{if}\ \tilde{K}^{\tilde{x}}_{ab} \neq \tilde{K}^{\tilde{x}}_{ba}\ \mathbf{then}\ alarm_a!0.\mathbf{nil} \| alarm_b!0.\mathbf{nil}\ \mathbf{else}\ fail!0.\mathbf{nil})) \end{aligned}$$

where to ease the notations, we let $\tilde{K}_{ab} = cmp(\tilde{K}_a, \tilde{B}_a, \tilde{B}_b)$, $\tilde{K}_{ba} = cmp(\tilde{K}_b, \tilde{B}_a, \tilde{B}_b)$, $\tilde{K}^{\tilde{x}}_{ab} = SubStr(\tilde{K}_{ab}, \tilde{x})$, and $\tilde{K}^{\tilde{x}}_{ba} = SubStr(\tilde{K}_{ba}, \tilde{x})$. Similar to Ran, the special measurement Ran' here, which takes three parameters, delivers a string of n bits. For example, $Ran'_{\tilde{B}_a, \tilde{B}_e, \tilde{K}_a}[\tilde{q}; \tilde{K}_e]$ will first generate a string of $n - |\tilde{K}_{ae}|$ random bits $\tilde{x}$, replace with $\tilde{x}$ the substring of $\tilde{K}_a$ at the positions where $\tilde{B}_a$ and $\tilde{B}_e$ do not match, and store the string after the replacement in $\tilde{K}_e$.

6 Conclusion and Related Work

In our opinion, bisimulation should be considered as a proof methodology for demonstrating behavioural equivalence between systems, rather than providing the definition of the extensional behavioural equivalence itself. We have adapted the well-known *reduction barbed congruence* to obtain a touchstone extensional behavioural equivalence for quantum processes considered in [9], and equipped it with a coinductive proof technique and a modal characterisation.

Below we briefly compare our open bisimulation with other bisimulations for quantum processes proposed in the literature. A branching bisimulation was defined for QPAlg [21,22]. However, it cannot always distinguish different quantum operations, as quantum states are only compared when they are input or output. And the derived bisimilarity is not a congruence; it is not preserved by restriction. Bisimulation defined in [8] indeed distinguishes different quantum operations but it works well only for finite processes. Again, it is not preserved by restriction. In [31], a congruent (strong) bisimulation was proposed for a special model where no classical datum is involved. However, as many important quantum communication protocols such as superdense coding and teleportation cannot be described in that model, its applicability is very limited. Furthermore, as all quantum operations are regarded as visible in [31], the bisimulation is too strong to identify some intuitively equivalent quantum processes.

The first general (both classical and quantum data are involved, and recursive definition is allowed), weak (quantum operations are regarded as invisible, thus can be combined arbitrarily), and congruent bisimulation for quantum processes was defined in [9]. It differentiates quantum input from other actions because, to match a quantum input, an arbitrarily chosen super-operator should be considered. The open bisimulation in this paper makes a step further by treating the super-operator application in an *open* style: applying super-operators before an action to be matched is selected. This makes it possible to separate ground bisimulation and the closedness under super-operator application, and by doing so, we are able to provide not only a neater and simpler definition, but also a powerful technique for proving bisimilarity. Comparing our open bisimulation with the bisimulation in [9], there are two main differences:

1. In [9] a non-standard weak transition $\Longrightarrow\xrightarrow{\underline{c}?q}$ is used to match the transition $\xrightarrow{\underline{c}?q}$. This is for a purely technical reason but makes possible the following example which demonstrates that open bisimulation is strictly coarser. Let $P = \underline{c}?q.(\tau + c!0)$ and $Q = P + \underline{c}?q$. Then P and Q are open bisimilar but not bisimilar in the sense of [9]. This is actually a *classical* example, however, as no quantum operation is included; restricting to this special form of transitions also makes classical bisimulation strictly stronger.
2. In [9] any super-operator application is performed on $\mathcal{H}_{\overline{qv(\mathcal{C}')-q}}$, provided that $\mathcal{C} \xrightarrow{\underline{c}?q} \mathcal{C}'$; while in open bisimulation of this paper, it is performed on $\mathcal{H}_{\overline{qv(\mathcal{C})}}$. As $qv(\mathcal{C}')-q$ can be a proper subset of $qv(\mathcal{C})$, there are more choices of super-operators in the former case. This observation suggests letting $P = \underline{c}?q.\mathcal{E}[q, \widetilde{r}_1]+I[\widetilde{r}_2]$ and $Q = \underline{c}?q.\mathcal{F}[q, \widetilde{r}_1]+I[\widetilde{r}_2]$. We conjecture that by taking suitable $\mathcal{E}$ and $\mathcal{F}$, we will have a real *quantum* example showing that open bisimilarity in this paper is strictly coarser than the bisimilarity in [9].

References

1. Baeten, J.C.M., Weijland, W.P.: Process Algebra. Cambridge University Press (1990)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing, pp. 175–179 (1984)
3. Davidson, T.A.S.: Formal Verification Techniques using Quantum Process Calculus. PhD thesis, University of Warwick (2011)
4. Deng, Y., Du, W.: Logical, metric, and algorithmic characterisations of probabilistic bisimulation. Technical Report CMU-CS-11-110. Carnegie Mellon University (March 2011)
5. Deng, Y., Feng, Y.: Open bisimulation for quantum processes. Full Version of the current paper, `http://arxiv.org/abs/1201.0416`
6. Deng, Y., Hennessy, M.: On the Semantics of Markov Automata. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011, Part II. LNCS, vol. 6756, pp. 307–318. Springer, Heidelberg (2011)
7. Deng, Y., van Glabbeek, R., Hennessy, M., Morgan, C.: Testing Finitary Probabilistic Processes (Extended Abstract). In: Bravetti, M., Zavattaro, G. (eds.) CONCUR 2009. LNCS, vol. 5710, pp. 274–288. Springer, Heidelberg (2009)

8. Feng, Y., Duan, R., Ji, Z., Ying, M.: Probabilistic bisimulations for quantum processes. Information and Computation 205(11), 1608–1639 (2007)
9. Feng, Y., Duan, R., Ying, M.: Bisimulation for quantum processes. In: Proc. POPL 2011, pp. 523–534. ACM (2011)
10. Fournet, C., Gonthier, G.: A hierarchy of equivalences for asynchronous calculi. Journal of Logic and Algebraic Programming 63(1), 131–173 (2005)
11. Gay, S.J., Nagarajan, R.: Types and typechecking for communicating quantum processes. Mathematical Structures in Computer Science 16(03), 375–406 (2006)
12. Gay, S.J., Nagarajan, R.: Communicating quantum processes. In: Palsberg, J., Abadi, M. (eds.) Proc. POPL 2005, pp. 145–157 (2005)
13. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proc. ACM STOC, pp. 212–219 (1996)
14. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters 78(2), 325 (1997)
15. Hennessy, M.: A proof system for communicating processes with value-passing. Formal Aspects of Computer Science 3, 346–366 (1991)
16. Hennessy, M., Ingólfsdóttir, A.: A theory of communicating processes value-passing. Information and Computation 107(2), 202–236 (1993)
17. Hennessy, M., Milner, R.: Algebraic laws for nondeterminism and concurrency. Journal of the ACM 32(1), 137–161 (1985)
18. Hoare, C.A.R.: Communicating Sequential Processes. Prentice Hall (1985)
19. Honda, K., Tokoro, M.: On reduction-based process semantics. Theoretical Computer Science 151(2), 437–486 (1995)
20. Jeffrey, A., Rathke, J.: Contextual equivalence for higher-order pi-calculus revisited. Logical Methods in Computer Science 1(1:4) (2005)
21. Jorrand, P., Lalire, M.: Toward a quantum process algebra. In: Proceedings of the 1st Conference on Computing Frontiers, pp. 111–119. ACM (2004)
22. Lalire, M.: Relations among quantum processes: Bisimilarity and congruence. Mathematical Structures in Computer Science 16(3), 407–428 (2006)
23. Milner, R.: Communication and Concurrency. Prentice-Hall (1989)
24. Milner, R., Parrow, J., Walker, D.: A calculus of mobile processes, Parts I and II. Information and Computation 100, 1–77 (1992)
25. Nielsen, M., Chuang, I.: Quantum computation and quantum information. Cambridge University Press (2000)
26. Rathke, J., Sobociński, P.: Deriving Structural Labelled Transitions for Mobile Ambients. In: van Breugel, F., Chechik, M. (eds.) CONCUR 2008. LNCS, vol. 5201, pp. 462–476. Springer, Heidelberg (2008)
27. Sangiorgi, D.: A theory of bisimulation for the pi-calculus. Acta Informatica 33(1), 69–97 (1996)
28. Sangiorgi, D., Kobayashi, N., Sumii, E.: Environmental bisimulations for higher-order languages. In: Proc. LICS 2007, pp. 293–302. IEEE Computer Society (2007)
29. Sangiorgi, D., Walker, D.: The π-calculus: a Theory of Mobile Processes. Cambridge University Press (2001)
30. Shor, P.W.: Algorithms for quantum computation: discrete log and factoring. In: Proc. FOCS 1994, pp. 124–134 (1994)
31. Ying, M., Feng, Y., Duan, R., Ji, Z.: An algebra of quantum processes. ACM Transactions on Computational Logic 10(3), 1–36 (2009)