Verifying Quantum Communication Protocols with Distribution-based Bisimulation

Xudong Qin[1,2], Yuxin Deng[1,2], and Yuan Feng

[1] Shanghai Key Laboratory of Trustworthy Computing
[2] East China Normal University, China
[3] XXXXXXX

Abstract. The process algebra is one of the useful techniques in formal verification. It has been extended to several quantum versions for describing quantum communication protocols in a number of works. Bisimulation presents the behavioural equivalence between processes through process algebra. It enables us to check whether an implementation of a protocol is consistent with its specification. Considering the quantum state depends on the history of the quantum operations applied on it, we give a distribution-based quantum ground bisimulation which is more suitable to present the equivalence between quantum operations. We also implement a algorithm to check if two given quantum processes are distribution-based ground bisimilar and then we make the experiments on several interesting quantum protocols so that we can compare it with the checking algorithm of the state-based bisimulation.

Keywords: Quantum process algebra · Bisimulation · Verification · Quantum communication protocols.

1 Introduction

Quantum mechanical principles such as non-cloning property and entanglement have been used in a number of previous works to design quantum communication protocols which are more efficient and secure ranging from the teleportation protocol [5] to key distribution protocols like BB84 [4] and B92 [3]. It brings difficulty to verify the correctness of the quantum protocols as the general quantum computer is still under developing. Formal methods are introduced to check the protocols at the design stage.

Process algebra is one of the useful techniques in the formal method providing the specification and verification of communicating and concurrent systems. Their extensions to the quantum setting have already appeared in the literature. Jorrand and Lalire [16,18] defined the *Quantum Process Algebra* (QPAlg) and presented a branching bisimulation to identify quantum processes with the same branching structure. Gay and Nagarajan [13] developed *Communicating Quantum Processes* (CQP), for which Davidson [6] established a bisimulation congruence. Feng et al. [10] have proposed a quantum variant of classical value-passing CCS [19], called qCCS, and a notion of probabilistic bisimulation for quantum processes, which is then improved to be a general notion of bisimulation that enjoys a congruence property [12]. Later on, motivated by [20], Deng and Feng [7] defined an open bisimulation for quantum processes that makes it possible to separate ground bisimulation and the closedness under super-operator applications, thus providing not only a neater and simpler definition, but also a new technique for proving bisimilarity. In order to avoid the problem of instantiating quantum variables by potentially infinitely many quantum states, Feng et al. [11] extended the idea of symbolic bisimulation [14] for value-passing CCS and provided a symbolic version of open bisimulation for qCCS. They proposed an algorithm for checking symbolic ground bisimulation.

In the current work, we consider a distribution-based ground bisimulation rather than the state-based ground bisimualtion proposed in [7]. The processes are encoded in qCCS with fixed initial quantum states. We compute a bisimulation matrix to check if two process are bisimilar. The algorithm extends the general distribution-based bisimulation checking method in [15] taking the check on the quantum states into account.

The definition the distribution-based ground bisimulation is based on the definition of the state-based ground bisimulation proposed in [7], changing the transition from a state to a distribution of states into the transition between distributions. It is already known that for any convex and continuous equivalence relation there exists a characteristic matrix for it which can check if two distributions satisfy the relation. As the distribution-based quantum ground bisimulation is also a convex and continuous equivalence relation, we can compute its characteristic matrix, called bisimulation matrix, for bisimilarity checking. We have developed a tool that implements the algorithm and check if two given bisimulations are strongly or weakly bisimilar. Then we have conducted experiments on a few interesting quantum communication protocols including super-dense coding, teleportation, secret sharing, and several quantum key distribution protocols. We also have made a comparison between the distribution-based version and state-based version of bisimilarity checking algorithms.

Other related work In the equivalence checking for the quantum processes, Ardeshir-Larijani et al. [2] proposed a quantum variant of CCS called Quantum Programming Language (QPL) [21], to describe quantum protocols. The syntax of that variant is similar to qCCS but its semantics is very different. The behaviour of a concurrent process is described as a finite tree and an interleaving is a path from the root to a leaf. By interpreting an interleaving as a superoperator, the semantics of a process is a set of superoperators. Then they introduce the stabiliser simulation algorithm invented by Aaronson and Gottesman [1] for the equivalence checking between two processes. Ardeshir-Larijani et al. have implemented their approach in an automated equivalence checker in Java and verified several quantum protocols from teleportation to secret sharing. However the input of the states are limited to the stabilizer states.

Kubota et al. [17] implemented a semi-automated tool to check a notion of symbolic bisimulation and used it to verify the equivalence of BB84 and another quantum key distribution protocol based on entanglement distillation [22]. The checking algorithm is based on the equational reasoning in which users need to provide equations during the checking procedure thus it is semi-automated.

The the distribution-based weak bisimulations has been introduced in [9]. After that several works distribution-based bisimulations have been proposed. A decision algorithm for the weak bisimulation of the probabilistic automata is proposed in [8]. Then a general and natural notion of the distribution-based bisimulation is given in [15] together with algorithms for computing such bisimulation relation in both finite and a part of infinite systems. Motivated by the unrealistic requirement of the current general scheduler on distributed systems, Zhang et al. [24] have proposed a coarser weak bisimilarity called late distribution bisimilarity.

The rest of the paper is structured as follows. In Section 2 we recall the syntax and semantics of the quantum process algebra qCCS. In Section 3 we define a distribution-based quantum ground bisimulations and show the relation between the state-based version and distribution-based version. In Section 4 we present an algorithm for checking distribution-based ground bisimulation. In Section 5 we extend the method to check the weak distribution-based ground bisimulation which abstract invisible actions away. In Section 6 we report some experimental results on verifying a few quantum communication protocols and make a comparison with the state-based version of the bisimulation checking algorithm. Finally, we conclude in Section 7 and discuss some future work.

2 Preliminary

We introduce a quantum extension of classical CCS (qCCS) which was originally studied in [10,23,12]. 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 [19]. We briefly explain

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

Fig. 1. Free quantum variables

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 $P \mid\mid Q$;
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. The second condition says that parallel composition $\mid\mid$ 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 also give the semantics of qCCS. We start at the definition of probabilistic labelled transition systems (pLTSs) by which we present the behavior of the quantum processes. We first introduce the notation of the probability distribution. A discrete probability distribution over a set S is a function $\Delta : S \to [0,1]$ with $\sum_{s\in S} \Delta(s) = 1$ and the support of the distribution Δ is the set $\lceil \Delta \rceil = \{s \in S | \Delta(s) > 0\}$. The point distribution $\overline{s}$ assigns probability 1 to the element s and 0 to all other elements of S, so that $\lceil \overline{s} \rceil = \{s\}$. The empty distribution ϵ assigns 0 to all other elements of S and $\lceil \epsilon \rceil = \emptyset$.

Let S be the set of states and $Dist(S)$ be the probability distribution over S, ranged over by Δ, Θ, etc. The probabilistic labelled transition system can be defined as follow.

(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 $\tilde{q}$.

Definition 1. *A probabilistic labelled transition system (pLTS) is a tuple $P = \langle S, Act_\tau, \rightarrow\rangle$ where $\rightarrow \in S \times Dist(S)$ is the smallest relation satisfying:*

- *if $s \xrightarrow{\alpha} \Delta$ then $\overline{s} \xrightarrow{\alpha} \Delta$;*
- *if $s \not\xrightarrow{\alpha}$ then $\overline{s} \xrightarrow{\alpha} \epsilon$;*

The operational semantics of qCCS are given in Figure 2. 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 $\mathcal{H}$[4], 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 $\mathcal{D}$. The trace of ρ is defined as $tr(\rho)$.

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.

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

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:

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

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

3 Distribution-based Bisimulation

We introduce the definition of the state-based bisimulation [7,11] first. Here we still need to consider the relations between distributions, so we make the use of the lifting operation.

Definition 2. *Let $\mathcal{R} \in S \times S$ be a relation between states of pLTSs. We can lift $\mathcal{R}$ to $\mathcal{R}^\circ \in Dist(S) \times Dist(S)$ which is the smallest relation satisfying:*

- *$s \mathcal{R} s'$ implies that $\overline{s} \mathcal{R}^\circ \overline{s'}$;*
- *$\Delta_i \ \mathcal{R}^\circ \ \Theta_i$ for all $i \in I$ implies $(\sum_i p_i \Delta_i) \ \mathcal{R}^\circ \ (\sum_i p_i \Theta_i)$ for any p_i with $\sum_i p_i = 1 \wedge p_i \geq 0$,*

where I is a finite set of the distribution indices.

We give the definition of the state-based bisimulation as follow. The notation $tr_{qv(P)}(\rho)$ is the partial trace over system P at the configuration $\langle P, \rho\rangle$ whose result is a reduced density operator presenting the state of the environment.

Definition 3. *A state-based strong ground bisimulation is a symmetry relation $\mathcal{R} \in Con \times Con$ for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$ such that $\langle P, \rho\rangle \ \mathcal{R} \ \langle Q, \sigma\rangle$ implies*

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

– *$qv(P) = qv(Q)$ and $tr_{qv(P)}(\rho) = tr_{qv(Q)}(\sigma)$;*
– *whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \Delta'$, there exists Θ' such that $\langle Q, \sigma\rangle \xrightarrow{\alpha} \Theta'$ and $\Delta'\ \mathcal{R}^\circ\ \Theta'$.*

We set $\langle P, \rho\rangle \sim \langle Q, \sigma\rangle$ if there is a strong ground bisimulation $\mathcal{R}$ such that $\langle P, \rho\rangle\ \mathcal{R}\ \langle Q, \sigma\rangle$.

If we take the history of the superoperator applied on ρ into account, we should consider the transition between distributions instead of the transition from a single state to a distribution.

We change the transitions in pLTS into the transition between distributions. For the relation $\rightarrow\ \in Dist(S) \times Dist(S)$, we write $\Delta \xrightarrow{\alpha} \Theta$ where $\Theta = \sum_{s\in\lceil\Delta\rceil} \Delta(s)\cdot\Delta_s$ and $s \xrightarrow{\alpha} \Delta_s$. After that, the distribution-based bisimulation is as follows.

Definition 4. *A distribution-based strong ground bisimulation is a symmetry relation $\mathcal{R}^D \in Dist(Con)\times Dist(Con)$ for any $\Delta, \Theta \in Dist(Con)$, $\Delta = \sum_i p_i\langle t_i, \rho_i\rangle$, $\Theta = \sum_j q_j\langle u_j, \sigma_j\rangle$ such that $\Delta\ \mathcal{R}^D\ \Theta$ implies*

– *$qv(\Delta) = qv(\Theta)$ and $\sum_i p_i tr_{qv(\Delta)}(\rho_i) = \sum_j q_j tr_{qv(\Theta)}(\sigma_j)$;*
– *whenever $\Delta \xrightarrow{\alpha} \Delta'$, there exists Θ' such that $\Theta \xrightarrow{\alpha} \Theta'$ and $\Delta'\ \mathcal{R}^D\ \Theta'$.*

We set $\Delta \sim_D \Theta$ if there is a strong ground bisimulation $\mathcal{R}^D$ such that $\Delta\ \mathcal{R}^D\ \Theta$.

Then we discuss the relation between the lifted state-based bismulation $\mathcal{R}^\circ$ and the distribution-based bisimulation $\mathcal{R}^D$. For any $\mathcal{R}$, if there are $\Delta, \Theta \in Dist(Con)$ and $\Delta\ \mathcal{R}^\circ\ \Theta$, we can take $\mathcal{R}^D{=}\mathcal{R}^\circ$ and then there is $\Delta\ \mathcal{R}^D\ \Theta$. In the other direction, we consider the example in Fig. 3.

We take two distributions $\Delta, \Theta \in Dist(Con)$ where $\Delta = \frac{1}{2}s_1 + \frac{1}{4}s_2 + \frac{1}{4}s_3$ and $\Theta = \frac{1}{4}t_1 + \frac{1}{4}t_2 + \frac{1}{2}s_3$. There are transitions $\Delta \rightarrow \Lambda$ and $\Theta \rightarrow \Lambda$ where $\Lambda \in Dist(Con)$, $\Lambda = \frac{1}{4}a + \frac{1}{4}b + \frac{1}{4}c + \frac{1}{4}d$.

Assume that the quantum variables used in each configuration of the pLTS are the same. Then we have $\Delta\ \mathcal{R}^D\ \Theta$ according to Definition 4. Meanwhile, for each s_i, there is no t_i such that $s_i\ \mathcal{R}\ t_i$, so $\Delta\ \mathcal{R}^\circ\ \Theta$ cannot be satisfied.

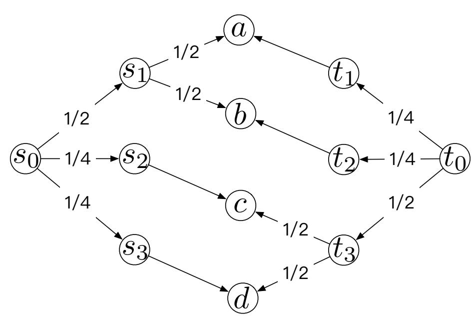

Fig. 3. The example.

4 The Algorithm

In this section, we introduce an algorithm to check the distribution-based bisimulation between two pLTSs with fixed initial quantum configurations. We use the algorithm in [15] to check the distribution-based bisimulation between such pLTSs. The algorithm try finding a characteristic matrix of the equivalence relation.

Definition 5. *A matrix E is a characteristic matrix of a relation $\mathcal{R}$ if for any $\mu, \nu \in \mathbb{R}^n$,*

$$\mu \,\mathcal{R}\, \nu \quad \textbf{\textit{iff}} \quad (\mu - \nu)E = 0.$$

The relation between the characteristic matrix and the equivalence relation. There are several properties for the relations need to declare first.

Let $\mathbb{P}^n \subseteq \mathbb{R}^n$ be the set of probability vectors.

Definition 6. *A relation $\mathcal{R}$ on $\mathbb{P}^n$ is said to be continuous if*

$$\mu_i \,\mathcal{R}\, \nu_i \wedge \lim_{i\to\infty} \mu_i = \mu \wedge \lim_{i\to\infty} \nu_i = \nu \implies \mu \,\mathcal{R}\, \nu.$$

Lemma 1. *If the relation $\mathcal{R}$ is a convex and continuous equivalence relation over probability distributions then $\mathcal{R}$ is affine as well. That is for any $\mu_i \,\mathcal{R}\, \nu$ where $i \in \{1, 2\}$, $\forall p \in \mathbb{R}^n$, there is $\mu = p\mu_1 + (1-p)\mu_2$ and $\mu \,\mathcal{R}\, \nu$ provided that $\mu \in \mathbb{P}^n$.*

Proof. *We consider the problem in two cases. If $0 \le p \le 1$, then from the convexity of $\mathcal{R}$, we have $\mu = p\mu_1 + (1-p)\mu_2$ directly.*

Otherwise, without loss of generality, suppose $p < 0$. Let $p^* = \dfrac{-p}{1-p}$, then there is $0 \le p^* \le 1$. Note that $\mu_2 = (1-p^*)\mu + p^*\mu_1$. So we have

$$\mu_2 \,\mathcal{R}\, (1-p^*)\mu + p^*\mu_1 \,\mathcal{R}\, \nu.$$

From the result of first case, as $\mu_1 \,\mathcal{R}\, \nu$ and $\mu_2 \,\mathcal{R}\, \nu$, we can swap μ_1 with μ_2 here. Then we have

$$\mu_2 \,\mathcal{R}\, (1-p^*)\mu + p^*[(1-p^*)\mu + p^*\mu_1]$$

$$\mu_2 \,\mathcal{R}\, [1-(p^*)^n]\mu + (p^*)^n\mu_1$$

for all $n \ge 0$. Thus $\mu \,\mathcal{R}\, \mu_2$ when n tends to infinity as $\mathcal{R}$ is continuous, and we get $\mu \,\mathcal{R}\, \nu$.

Lemma 2. *A relation $\mathcal{R}$ is a convex and continuous equivalence relation over $\mathbb{P}^n$ if and only if there is a characteristic matrix E of it.*

Proof. *If there is a characteristic matrix E of $\mathcal{R}$. It is obvious that $\mathcal{R}$ is a convex and continuous equivalence relation.*

For the necessity part, suppose $\mathcal{R}$ is a convex equivalence relation and define the set Γ as follow

$$\Gamma = \{\mu - \nu | \mu \,\mathcal{R}\, \nu, \mu, \nu \in \mathbb{P}^n\}.$$

Then let $\overline{\Gamma}$ be the affine closure of Γ, for any $\rho_i \in \Gamma$ and $p_i \in \mathbb{R} \wedge \sum_i p_i = 1$, there is $\sum_i p_i \rho_i \in \overline{\Gamma}$. As $\mathcal{R}$ is a reflexive relation, there is $\mu - \mu = \boldsymbol{0} \in \Gamma$, and there also exists $\boldsymbol{0} \in \overline{\Gamma}$. For any $\rho' \in \overline{\Gamma}$ and $\rho_i \in \overline{\Gamma}$, $p_i \in \mathbb{R} \wedge \sum_i p_i \neq 1$, we can take $p' = 1 - \sum_i p_i$ and $p' + \sum_i p_i = 1$, such that

$$p'\rho' + \sum_i p_i \rho_i \in \overline{\Gamma}.$$

Let $\rho' = \boldsymbol{0}$, then we have $\sum_i p_i \rho_i \in \overline{\Gamma}$ for some $\rho_i \in \Gamma$. So for any $p_i \in \mathbb{R}$, there is $\sum_i p_i \rho_i \in \overline{\Gamma}$ for some $\rho_i \in \overline{\Gamma}$. Hence $\overline{\Gamma}$ is a linear subspace of $\mathbb{R}^n$.

Therefore, there exists a matrix E whose columns consist of an orthonormal basis of the kernal space of $\overline{\Gamma}$ such that for any $\rho \in \mathbb{R}^n$,

$$\rho \in \overline{\Gamma} \quad \textbf{\textit{iff}} \quad \rho E = 0.$$

We are going to show that E is a characteristic matrix for $\mathcal{R}$. For any $\mu, \nu \in \mathbb{P}^n$, if $\mu \mathrel{\mathcal{R}} \nu$, let $\rho = \mu - \nu$, $\rho \in \Gamma$, then from $\Gamma \subseteq \overline{\Gamma}$ we have $\rho \in \overline{\Gamma}$ thus $\rho E = 0$.

Conversely, suppose $(\mu - \nu)E = 0$, then $(\mu - \nu) \in \overline{\Gamma}$. There is a collection of $\{\mu_i\}$ and $\{\nu_i\}$ s.t. $\mu - \nu = \sum_i p_i(\mu_i - \nu_i)$ and $\forall i, \mu_i \mathrel{\mathcal{R}} \nu_i$. Note that

$$\mu = \sum_i p_i \mu_i - \sum_i p_i \nu_i + \nu$$

$$\nu = \sum_i p_i \mu_i - \sum_i p_i \mu_i + \nu.$$

Thus according to Lemma 1, $\mathcal{R}$ is affine, so we have $\mu \mathrel{\mathcal{R}} \nu$. From Definition 5, E is a characteristic matrix of $\mathcal{R}$.

Then we apply the lemmas to the quantum configuration distributions. In order to represent $\sim$ using linear algebra, we index all the configurations in the pLTSs so that every distribution of configurations has its corresponding distribution of indexes which is in a space of real value. Given a set of configurations S, if we give a linear order on the state space $S = \{s_1, s_2, \ldots, s_n\}$, we can see that the spaces $\mathbb{R}^n$ and $\mathbb{R}^{|S|}$ are isomorphic, so do the spaces $\mathbb{P}^n$ and $\mathbb{P}^{|S|}$. And obviously, $\mathbb{P}^{|S|} = Dist(S)$. So the distribution Δ can be presented in form of a real-valued vector $(\Delta(s_1), \cdots, \Delta(s_{|S|}))$.

Then we can find a characteristic matrix E of the distribution-based quantum ground bisimulation as it is also a convex and continuous equivalence relation.

Lemma 3. *$\sim$ is a convex and continuous equivalence relation.*

Proof. First, according to Definition 4, we have already known that $\sim$ is a equivalence relation.

Then we prove its convexity. Let $p \in \mathbb{R}$, we show that for any $\Delta_1 \sim \Theta_1, \Delta_2 \sim \Theta_2$, there is $\Delta \sim \Theta$ where $\Delta = p\Delta_1 + (1-p)\Delta_2$ and $\Theta = p\Theta_1 + (1-p)\Theta_2$.

We can prove following conditions.

- *From $qv(\Delta_1) = qv(\Theta_1)$ and $qv(\Delta_2) = qv(\Theta_2)$, we have $qv(\Delta) = qv(\Delta_1) \cup qv(\Delta_2) = qv(\Theta_1) \cup qv(\Theta_2) = qv(\Theta)$.*

- *From* $|\Delta_1| = |\Theta_1|$ *and* $|\Delta_2| = |\Theta_2|$, *we have* $|\Delta| = |p\Delta_1 + (1-p)\Delta_2| = p|\Delta_1| + (1-p)|\Delta_2| = p|\Theta_1| + (1-p)|\Theta_2| = |\Theta|$.
- *For any* $\Delta_1 \xrightarrow{\alpha} \Delta'_1$, *there exists* Θ'_1, $\Theta_1 \xrightarrow{\alpha} \Theta'_1 \wedge \Delta'_1 \sim \Theta'_1$. *So do the* Δ_2 *and* Θ_2. *Since* $\Delta' = p\Delta'_1 + (1-p)\Delta'_2 \sim p\Theta'_1 + (1-p)\Theta'_2 = \Theta'$, *for any* $\Delta \xrightarrow{\alpha} \Delta'$ *there is* Θ' *such that* $\Theta \xrightarrow{\alpha} \Theta' \wedge \Delta' \sim \Theta'$.

According to Definition 4, it comes out that there is $\Delta \sim \Theta$.

Then we show that it is continuous. That is for any $i \in I$, $\Delta_i, \Theta_i \in Dist(S)$, $\Delta_i \sim \Theta_i \wedge \lim_{i\to\infty} \Delta_i = \Delta \wedge \lim_{i\to\infty} \Theta_i = \Theta$ *implies that* $\Delta \sim \Theta$. *For the first conditions,* Δ_i *should keep the same set of quantum variables as* Θ_i. *When* Δ_i *tends to* Δ *this set does not changed, so the first condition holds. Similarly,* $|\Delta| = |\Theta|$ *holds.*

For the transition $\Delta_i \xrightarrow{\alpha} \Delta'_i$, *there exists transition* $\Theta_i \xrightarrow{\alpha} \Theta'_i$ *such that* $\Delta'_i \sim \Theta'_i$. *When* Δ_i *tends to* Δ, *suppose* Δ'_i *tends to a distribution* Δ'. *Similarly, a distribution* Θ' *is supposed. As* Δ_i *and* Θ_i *always keep the relation* $\Delta_i \sim \Theta_i$, *we have* $\Delta' \sim \Theta'$. *Then there is* $\Delta \sim \Theta$.

Lemma 4. *There is a characteristic matrix* E *such that for any* $\Delta, \Theta \in Dist(S)$ *we have* $\Delta \sim \Theta$ *iff* $(\Delta - \Theta)E = 0$.

Proof. *For any distribution* $\Delta \in Dist(S)$, *there is a vector* $\Delta^o \in \mathbb{P}^n$ *s.t.* $\Delta(s_i) = \Delta^o(i)$ *for each* i.

For any bisimulation $\mathcal{R} \subseteq Dist(S) \times Dist(S)$, *there exists the relation* $\mathcal{R}^o \subseteq \mathbb{P}^n \times \mathbb{P}^n$ *s.t.* $\Delta\ \mathcal{R}\ \Theta$ *iff* $\Delta^o\ \mathcal{R}^o\ \Theta^o$.

By following Lemma 3, we have $\sim^o$ *is a convex and continuous equivalence relation. Let* $\mathscr{R}$ *be the set of all convex and continuous equivalence relations* $\mathcal{R}' \subseteq \mathbb{R}^n \times \mathbb{R}^n$. *By Lemma 2, since* $\sim^o \in \mathscr{R}$, *there is a characteristic matrix* E *of* $\sim^o$. *As a consequence, for any subdistribution* Δ, Θ, *we have*

$$\Delta \sim \Theta \quad \textbf{\textit{iff}} \quad \Delta^o \sim^o \Theta^o \quad \textbf{\textit{iff}} \quad (\Delta^o - \Theta^o)E = 0.$$

We introduce the algorithm in [15] to find the characteristic matrix E of the quantum bisimulation relation, called the bisimulation matrix, through a transition matrix generated from the configurations of the pLTSs. The transition matrix shows the change of the distributions of states.

4.1 Action-deterministic Systems

We first consider checking bisimulation between action-deterministic pLTSs.

Let $P_\alpha = (\mathcal{E}_{ij})$ denote the superoperator matrix for each action $\alpha \in \mathbf{Act}_\tau$ such that for all i, j, if there is $\langle t_i, \rho_i \rangle \xrightarrow{\alpha} \Delta$ and $\Delta = \sum_j p_{ij} \langle t_j, \mathcal{E}(\rho_i) \rangle$, $\mathcal{E}_{ij}$ is set to the superoperator $\mathcal{E}$, otherwise it is set to the zero operator O.

Furthermore, given an input quantum state we can compute the possibility p_{ij} and construct a real-valued transition matrix. Let $P_\alpha(\rho) = (p_{ij})$ denote the transition matrix for each action $\alpha \in \mathbf{Act}_\tau$ and input quantum state $\rho \in D(\mathcal{H})$ where $D(\mathcal{H})$ is the set of the density operators.

We denote $\mathbf{1} = (1, \cdots, 1)^\top$. The stability of the matrix E is required to present the second condition of Definition 4 which means that for any pair of distributions, if they are contained in $\mathcal{R}$, their next distributions are also contained.

Definition 7. *For a matrix E with $|S|$ rows and a $|S| \times |S|$ matrix P, E is said P-stable if for every distribution Δ,*

$$\Delta E = 0 \longrightarrow \Delta P E = 0.$$

Let matrix P to be the transition matrix of the pLTS, then the distribution ΔP is the result distribution after one step of movement and it should be still contained in the bisimulation relation.

Proposition 1. *Between two pLTSs $\langle S_1, \boldsymbol{Act}_\tau, \rightarrow_1\rangle$ and $\langle S_2, \boldsymbol{Act}_\tau, \rightarrow_2\rangle$ with no non-deterministic choice, a $(|S_1| + |S_2|)$ rows real-valued matrix E containing $\boldsymbol{1}$ is a bisimulation matrix if and only if it is $P_\alpha(\rho)$-stable for all $\alpha \in \boldsymbol{Act}_\tau$. For those states whose corresponding positions are non-zero in the same column, their sets of quantum variables should also be the same.*

Proof. *Let $\Delta, \Theta \in Dist(S)$ be the distributions from two pLTSs and $\Delta\ \mathcal{R}\ \Theta$. If E containing $\boldsymbol{1}$ is a bisimulation matrix, there is $(\Delta - \Theta)E = 0$ by Lemma 2. Since E containing $\boldsymbol{1}$, we have $|\Delta| = |\Theta|$. Let $\Delta' = \Delta P_\alpha$, then $\Delta \xrightarrow{\alpha} \Delta'$. According to definition, there exists $\Theta' = \Theta P_\alpha$, $\Theta \xrightarrow{\alpha} \Theta' \wedge \Delta'\ \mathcal{R}\ \Theta'$. Therefore, $(\Delta' - \Theta')E = (\Delta P_\alpha - \Theta P_\alpha)E = (\Delta - \Theta)P_\alpha E = 0$. Conversely, let E be a matrix containing $\boldsymbol{1}$ and $P_\alpha(\rho)$-stable for all $\alpha \in \boldsymbol{Act}_\tau$. We show that $\mathcal{R}$ defined by $\Delta\ \mathcal{R}\ \Theta$ iff $(\Delta - \Theta)P_\alpha E = 0$ for $\Delta, \Theta \in Dist(S)$ is a bisimulation relation. According to Definition 4, as the non-zero value in the same column present the states could be matched, the set of the quantum variables of the distributions to match are the same. So $qv(\Delta) = qv(\Theta)$. Then $\sum_i p_i tr_{qv(\Delta)(\rho_i)} = \sum_j q_j tr_{qv(\Theta)(\sigma_j)}$ follows from $(\Delta - \Theta)P_\alpha \boldsymbol{1} = 0$. As E is $P_\alpha(\rho)$-stable, the second condition follows from $(\Delta P_\alpha - \Theta P_\alpha)E = 0$. Thus $\mathcal{R}$ is a bisimulation relation.*

Given $\rho \in D(\mathcal{H})$, the set of all column of E is given by the iteration $\{P_\alpha(\rho) : \alpha \in \mathbf{Act}_\tau\}^* \mathbf{1}$ modulo linear dependency. Since P_α has $|S_1| + |S_2|$ rows, the fixed point reached within $|S_1| + |S_2|$ iterations yielding $1 \leq d \leq (|S_1| + |S_2|)$ equations.

4.2 Non-deterministic Systems

Then we consider checking bisimulation between pLTSs containing non-deterministic choices.

When there exists non-deterministic choices in the pLTS, the transition matrix $P_\alpha(\rho)$ may contain symbolic variables used to present the probability of a transition will be taken. For each $\langle t_i, \rho_i\rangle \in S$, $\alpha \in \mathbf{Act}_\tau$, let c_i^α be the number of non-deterministic choices of $\langle t_i, \rho_i\rangle$ under action α, w_i^k, $0 \leq k \leq c_i^\alpha$ be the probability that the k-th choice is taken.

Let the transition be $\langle t_i, \rho_i\rangle \xrightarrow{\alpha} \Delta_i^k$ where $\Delta_i^k = \sum_j p_{ij}^k \langle t_j, \rho_j\rangle$. Let the collection W keeps the probability of each choice and the matrix $P_\alpha^W(\rho)$ sums up the choices under action α. Then the transition matrix is presented as $P_\alpha^W(\rho) = (\sum_{k=1}^{c_i^\alpha} w_i^k \cdot p_{ij}^k)$.

The value of the w_i^k is taken by a Spoiler-Duplicator bisimulation game in s_i. That is, for a pair of distribution $\{\Delta_0, \Delta_1\}$, Spoiler chooses $i \in \{0,1\}$, $\alpha \in \mathsf{Act}$, $\Delta_i \xrightarrow{\alpha} \Delta_i'$ and Duplicator has to reply $\Delta_{1-i} \xrightarrow{\alpha} \Delta_{1-i}'$ such that $\Delta_i(S_\alpha) = \Delta_{1-i}(S_\alpha)$, and the game continues in $\{\Delta_0', \Delta_1'\}$ where S_α is a set of states $\{s | \exists \Theta : s \xrightarrow{\alpha} \Theta\}$. Spoiler wins the games if and only if Duplicator cannot reply at some point.

The fundamental idea of the algorithm is that if two distributions are matched on the finitely many "extremal" choices, we can check they are bisimilar. When we compute the matrix by the same iteration method, there are variable w_i^k in the matrix $M_\alpha^W(\rho) = P_\alpha^W(\rho)E$ where E is the result of the last iteration. The i-th row of $M_\alpha^W(\rho)$ over W is a vector containing variables w_i^k, denoted by $m_{il}(w_i^1, \cdots, w_i^{c_i^\alpha})$. As there are random and mixed choices to take, the set of vectors

$$\{m_{i1}(w_i^1, \cdots, w_i^{c_i}), \cdots, m_{ib}(w_i^1, \cdots, w_i^{c_i}) | w_i^1, \cdots, w_i^{c_i} \geq 0, \sum_{k=1}^{c_i} w_i^k = 1\}$$

constructs a convex polytope denoted by C_i. The extremal points of C_i is denoted by $\mathcal{E}(C_i)$.

For all the rows, $C = \{\sum_{i=1}^{|S|} c_i' | \forall i : c_i' \in C_i\}$ is also a polytope. Let the set $\mathcal{E}(C) \subseteq \prod_{i=1}^{|S|} \mathcal{E}(C_i)$ contain a tuple $c = (c_1, \cdots, c_{|S|})$ if and only if they are extremal in the same direction that is $\sum_{i=1}^{|S|} c_i$ is a vertex of the polytope. The particular choices corresponding to $c \in \mathcal{E}(C)$ is denoted by $W(c)$. Then the elements of the transition matrix $P_\alpha^{W(c)}$ can be confirmed with $W(c)$ plugged in.

Denote the $|S|$-dimensional vector of C_i's by $\mathbf{C}$. For a distribution Δ, the Δ-combination of polytope C_i is

$$\Delta \mathbf{C}^\top = \{\sum_{i=1}^{|S|} \Delta(s_i) c_i | \forall i : c_i \in C_i\}.$$

Furthermore, the set $\mathcal{E}(\Delta \mathbf{C}^\top)$ is $\{\Delta c^\top | c \in \mathcal{E}(C)\}$. Note that these points are mapped to pure strategies and achieve Pareto extremal values when applied to any distributions, i.e. $\Delta c^\top$ is a corner of $\Delta \mathbf{C}^\top$ for every distribution µ.

Proposition 2. *Between two pLTSs $\langle S_1, \boldsymbol{Act}_\tau, \rightarrow_1\rangle$ and $\langle S_2, \boldsymbol{Act}_\tau, \rightarrow_2\rangle$. Let E be a $(|S_1|+|S_2|)$ rows real-valued matrix containing $\mathbf{1}$. It is a bisimulation matrix if and only if it is $P_\alpha^{W(c)}(\rho)$-stable for all $\alpha \in L$ and $c \in \mathcal{E}(C)$. For those states whose corresponding positions are non-zero in the same column, their sets of quantum variables should also be the same.*

Proof. *Other parts are similar to the proof in Proposition 1 except proving E is $P_\alpha^{W(c)}(\rho)$-stable for all $\alpha \in L$ and $c \in \mathcal{E}(C)$.*

Let $\Delta, \Theta \in Dist(S)$ be the distributions from two pLTSs. Observe that if $\Delta \mathrel{\mathcal{R}} \Theta$ then $\Delta \boldsymbol{C}^\top$ and $\Theta \boldsymbol{C}^\top$ are the same polytopes as for every choice on one side there must be a choice on the other side matching it in all states. Conversly, if $\Delta \boldsymbol{C}^\top$ and $\Theta \boldsymbol{C}^\top$ are not the same, then $\Delta \mathrel{\mathcal{R}} \Theta$ also does not hold. Spoiler can choose a distribution that cannot be matched by Duplicator. Note that equality of the polytopes $\Delta \boldsymbol{C}^\top$ and $\Theta \boldsymbol{C}^\top$ can be tested by the equality of the sets of the extremal points $\mathcal{E}(\Delta \boldsymbol{C}^\top)$ and $\mathcal{E}(\Theta \boldsymbol{C}^\top)$. Hence two facts need to be proved:

- *The extremal choices $\mathcal{E}(C)$ are sufficient for Spoiler, that is $W_S = W(c)$.*
- *For an extremal choice $W(c)$ from Spoiler, $W(c)$ is an optimal reply of Duplicator for any distrbutions Δ and Θ, that is $W_D = W(c)$.*

As to the first fact, intuitively, if two polytopes are different, there must be a corner of one of them not in the other by the convexity of the polytope. If $\Delta \boldsymbol{C}^\top$ and $\Theta \boldsymbol{C}^\top$ are not the same, then the optimal choice of Spoiler is a $W(c)$ such that $\Delta c^\top \notin \Theta \boldsymbol{C}^\top$ (or $\Theta c^\top \notin \Delta \boldsymbol{C}^\top$).

As to the second fact, intuitively, if two polytopes are the same and Spoiler checks whether a corner c_1 is also a corner of the other one, then Duplicator needs to reply the corner c_2 which is extremal in the same direction as c_1. Let $\Delta \mathrel{\mathcal{R}} \Theta$ and $W(s)$ be an extremal choice of Spoiler on Δ, $W(d)$ be an optimal choice of Duplicator on Θ. For a contradiction, suppose $W(d)$ is different from $W(s)$. Since s is extreme in some direction v for which d is not, and since $W(s)$ achieves on Δ the same as $W(d)$ on Θ, there is a choice $W(d')$ where d' is extreme in direction v and achieves strictly better Pareto value on Θ than d, hence also strictly better than $W(s)$ on Δ. Then if Spoiler choose $W(d)$ on Θ, a matching reply would be $W(s)$ on Δ. Furthermore, if Spoiler choose $W(d')$ on Θ, this choice is strictly dominates $W(d)$ on Θ in direction v and thus all choices on Δ in direction v, as s is already the extremal choice in direction v. Hence Duplicator has no choice to reply, this is a contradiction.

As a result, the bisimulation matrix requirement can be simplified. In the game fashion it is written as follows:

$$\forall \alpha \in \mathsf{Act}, (\Delta - \Theta)E = 0 \implies \forall W_S, \exists W_D, \Delta P_\alpha^{W_S} \boldsymbol{1} = \Theta P_\alpha^{W_D} \boldsymbol{1} \wedge (P_\alpha^{W_S} - \Theta P_\alpha^{W_D})E = 0.$$

Since $W_S = W(c)$, $W_D = W(c)$ and E contains $\boldsymbol{1}$, there is

$$\forall \alpha \in \mathsf{Act}, (\Delta - \Theta)E = 0 \implies \forall W(c), (\Delta - \Theta)P_\alpha^{W(c)} E = 0$$

which shows that E is $P_\alpha^{W(c)}(\rho)$-stable for all $\alpha \in L$ and $c \in \mathcal{E}(C)$.

Algorithm 1 computes the bisimulation matrix of a pLTS which may contain non-deterministic choices. The algorithm is divided into two parts.The first part traverses the pLTSs to compute the transition matrix with the input quantum state $\rho \in D(\mathcal{H})$. Then the algorithm compute the columns of E by the iteration $\{P_\alpha^{W(c)} : \alpha \in \mathbf{Act}_\tau, W \in \mathcal{W}_\tau\}^* \mathbf{1}$. According to the condition given in Definition 4, the algorithm also matches the quantum variables of two corresponding distributions when a new column is added (Line 12).

Algorithm 1 Checking Symbolic Ground Bisimulation

Require: Two pLTSs.
Ensure: A minimal bisimulation matrix E.

function SymbolicBisimulation =
  for each $\alpha \in L$ **do**
    traverse the pLTSs to compute $P_\alpha^W(\rho)$
  $E \leftarrow (\mathbf{1})$
  repeat
    for each $\alpha \in L$ **do**
      $M_\alpha^W(\rho) \leftarrow P_\alpha^W(\rho)E$
      compute $\mathcal{E}(C)$ from M_α^W
      for each $c \in \mathcal{E}(C)$ **do**
        $M_\alpha^{W(c)}(\rho) \leftarrow M_\alpha^W(\rho)$ with $W(c)$ plugged in
        for each column E_{new} in $M_\alpha^{W(c)}(\rho)$ independent of E **do**
          check the sets of quantum variables of non-zero rows
          if these sets are equal **then**
            $E \leftarrow (E \;\; E_{new})$
          else skip
  until E does not change
  return E

5 Weak Distribution-based Bisimulation

To abstract the invisible actions caused by internal communications, as well as quantum operations, we refer to the idea of saturation which extends an automaton to a weak automaton through adding weak transitions.

We write $\Delta \xrightarrow{\hat{\tau}} \Theta$ if either $\Delta \xrightarrow{\tau} \Theta$ or $\Theta = \Delta$. 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 $\Delta \xRightarrow{\hat{\tau}}\xrightarrow{a}\xRightarrow{\hat{\tau}} \Theta$.

We denote P' as the pLTS P adding weak transitions according to the following rules.

$$weak1 \; \frac{}{\Delta \xRightarrow{\epsilon} \Delta} \qquad weak2 \; \frac{\Delta \xrightarrow{\gamma} \Delta}{\Delta \xRightarrow{\gamma} \Delta}$$

$$weak3 \; \frac{\Delta \xRightarrow{\gamma} \sum_{s \in \lceil \Delta \rceil} \Delta_s \qquad \forall s \in \lceil \Delta \rceil : \; \Delta_s \xrightarrow{\tau} \Theta_s}{\Delta \xRightarrow{\gamma} \sum_{s \in \lceil \Delta \rceil} \Theta_s}$$

$$weak4 \; \frac{\Delta \xrightarrow{\tau} \sum_{s \in \lceil \Delta \rceil} \Delta_s \qquad \forall s \in \lceil \Delta \rceil : \; \Delta_s \xRightarrow{\gamma} \Theta_s}{\Delta \xRightarrow{\gamma} \sum_{s \in \lceil \Delta \rceil} \Theta_s}$$

Fig. 4. Weak Transition Rules

Then we can apply the same algorithm in 4 to the result pLTSs to check the weak bisimulation.

6 Experimental Results

We implement the algorithm in Python and then we conducted experiments on several quantum communication protocols with a set of given input variables (both quantum and classical). Firstly, we make a brief introduction about the examples we used.

Measurement on two qubits. In quantum mechanics, measuring a two-qubit state should be equal to measuring each qubit separately with the same basis. These two ways of measurement can be defined as follows:

$$\begin{aligned} S1 \overset{def}{=} Set_{\Psi}[q1, q2].M_1[q_1; x_1].(&\mathbf{if}\ x_1 = 0\ \mathbf{then}\ M_1[q_2; x_2].(\mathbf{if}\ x_2 = 0\ \mathbf{then}\ d!0.\mathbf{nil} \\ &\qquad\qquad\qquad\qquad\qquad + \mathbf{if}\ x_2 = 1\ \mathbf{then}\ d!1.\mathbf{nil}) \\ &+ \mathbf{if}\ x_1 = 1\ \mathbf{then}\ M_1[q_2; x_2].(\mathbf{if}\ x_2 = 0\ \mathbf{then}\ d!2.\mathbf{nil} \\ &\qquad\qquad\qquad\qquad\qquad + \mathbf{if}\ x_2 = 1\ \mathbf{then}\ d!3.\mathbf{nil})); \end{aligned}$$

$$S2 \overset{def}{=} Set_{\Psi}[q1, q2].M_1[q_1, q_2; x_1].(\sum_{i=0}^{3} \mathbf{if}\ x_1 = i\ \mathbf{then}\ d!i.\mathbf{nil})$$

where $Set_{\Psi}[\tilde{q}]$ sets the two-qubit state $|q1\rangle|q2\rangle$ to the state $|+\rangle|+\rangle$.

Communication protocols. Many quantum protocols use the property of the maximally entangled state, EPR state, to achieve a more efficient communication, such as super-dense coding protocol, teleportation protocol and secret sharing protocol. In these examples, we make the use of their quantum circuit presentation to encode them into qCCS programs and match them with their specifications.

Key distribution protocols. Quantum key distribution protocols also use the some properties in quantum mechanics to encrypt the key. For example, because of the quantum no-cloning theorem, a third party will be detected if he eavesdrops the qubits. When the protocol randomly decide which key the protocol to transport, it can use the result of a measurement on a qubit which leads to a probability distribution. In another way, non-deterministic choices can be used instead of it to present the randomness of the generation of the key.

Table 1 provides a summary of our experimental results obtained on a macOS machine with an Intel Core i7 2.5 GHz processor and 16GB of RAM.

In the result of 2-qubit measurement, the distribution-based bisimulation checking algorithm succeed verifying that two processes are bisimilar. From the last column of the table, we can see that with the distribution-based method the bisimulation checking has been finished in less time. The time cost excludes the part of pLTS generation which takes around 1 second in all the examples.

State-based weak bisimulation					
Program	**Arguments**	**Bisim**	**Impl**	**Spec**	**Sec**
Teleportation	$q_1q_2q_3 = \frac{1}{\sqrt{2}}\|000\rangle + \frac{1}{\sqrt{2}}\|100\rangle$	Yes	54	8	1015
Super-dense coding	$q_1q_2 = \|00\rangle$, $x = 5$	Yes	8	5	141
Secret Sharing	$q_1q_2q_3q_4 = \frac{1}{\sqrt{2}}\|0000\rangle + \frac{1}{\sqrt{2}}\|1000\rangle$	Yes	143	8	5565
BB84	$q_1q_2q_3 = \|00\rangle$	Yes	152	80	147792
B92	$q_1q_2 = \|00\rangle$	Yes	64	80	32541
E91	$q_1q_2q_3q_4 = \|0000\rangle$	Yes	124	80	124015
BB84 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	93	25	21752
B92 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	37	23	2785
E91 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	79	25	1712
2-qubit measurement	$q_1q_2 = \|00\rangle$	No	12	16	156
Distribution-based weak bisimulation					
Program	**Arguments**	**Bisim**	**Impl**	**Spec**	**Sec**
Teleportation	$q_1q_2q_3 = \frac{1}{\sqrt{2}}\|000\rangle + \frac{1}{\sqrt{2}}\|100\rangle$	Yes	54	8	252
Super-dense coding	$q_1q_2 = \|00\rangle$, $x = 5$	Yes	8	5	10
Secret Sharing	$q_1q_2q_3q_4 = \frac{1}{\sqrt{2}}\|0000\rangle + \frac{1}{\sqrt{2}}\|1000\rangle$	Yes	143	8	16143
BB84	$q_1q_2q_3 = \|00\rangle$	Yes	152	80	5357
B92	$q_1q_2 = \|00\rangle$	Yes	64	80	1390
E91	$q_1q_2 = \|0000\rangle$	Yes	124	80	3533
BB84 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	93	25	1177
B92 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	37	23	310
E91 (non-deterministic)	$q_1q_2 = \|00\rangle$	Yes	79	25	902
2-qubit measurement	$q_1q_2 = \|00\rangle$	Yes	12	16	54

Table 1. Experimental results. The columns headed by **Impl** and **Spec** show the numbers of nodes contained in the generated pLTSs of the implementations and specifications, respectively. Column **Sec** shows the time cost of the verification in milliseconds.

7 Conclusion

In this paper, we have defined a distribution-based quantum ground bisimulation which is coarser than the state-based one introduced in previous work so that some operations which are equivalent in quantum mechanics can also be checked bisimilar. We have extended the classical distribution-based bisimulation checking algorithm into the quantum setting for quantum ground bisimulation checking. We have carried out several non-trivial experiments on the algorithm and compared the results with the results of state-based bisimulation algorithm. The result shows that the distribution-based algorithm completes the checking in less time.

As future work we intend to study quantum symbolic bisimulation in order to verify the quantum programs with arbitrary input quantum states. Without the input quantum states, the transition matrix becomes a superoperator-valued matrix which leads to the difficulty in computing.

References

1. Aaronson, S., Gottesman, D.: Improved simulation of stabilizer circuits. Physical Review A **70**(052328) (2004)
2. Ardeshir-Larijani, E., Gay, S.J., Nagarajan, R.: Automated equivalence checking of concurrent quantum systems. ACM Transactions on Computational Logic **19**(4), 28:1–28:32 (2018)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Physical Review Letters **68**, 3121–3124 (1992)
4. 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)
5. Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.: Teleporting an unknown quantum state via dual classical and EPR channels. Physical Review Letters **70**, 1895–1899 (1993)
6. Davidson, T.A.S.: Formal Verification Techniques using Quantum Process Calculus. Ph.D. thesis, University of Warwick (2011)
7. Deng, Y., Feng, Y.: Open bisimulation for quantum processes. In: Proceedings of the 7th IFIP International Conference on Theoretical Computer Science. Lecture Notes in Computer Science, vol. 7604, pp. 119–133. Springer (2012)
8. Eisentraut, C., Hermanns, H., Krämer, J., Turrini, A., Zhang, L.: Deciding bisimilarities on distributions. In: Joshi, K.R., Siegle, M., Stoelinga, M., D'Argenio, P.R. (eds.) Quantitative Evaluation of Systems - 10th International Conference, QEST 2013, Buenos Aires, Argentina, August 27-30, 2013. Proceedings. Lecture Notes in Computer Science, vol. 8054, pp. 72–88. Springer (2013). https://doi.org/10.1007/978-3-642-40196-1_6, https://doi.org/10.1007/978-3-642-40196-1_6
9. Eisentraut, C., Hermanns, H., Zhang, L.: On probabilistic automata in continuous time. In: Proc. LICS'10. pp. 342–351. IEEE Computer Society (2010)
10. Feng, Y., Duan, R., Ji, Z., Ying, M.: Probabilistic bisimulations for quantum processes. Information and Computation **205**(11), 1608–1639 (2007)
11. Feng, Y., Deng, Y., Ying, M.: Symbolic bisimulation for quantum processes. ACM Transactions on Computational Logic **15**(2), 1–32 (2014)
12. Feng, Y., Duan, R., Ying, M.: Bisimulation for quantum processes. In: Proceedings of the 38th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 523–534. ACM (2011)
13. Gay, S.J., Nagarajan, R.: Communicating quantum processes. In: Palsberg, J., Abadi, M. (eds.) Proceedings of the 32Nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 145–157 (2005)
14. Hennessy, M., Lin, H.: Symbolic bisimulations. Theoretical Computer Science **138**(2), 353–389 (1995)
15. Hermanns, H., Krcál, J., Kretínský, J.: Probabilistic bisimulation: Naturally on distributions. In: CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings. pp. 249–265 (2014). https://doi.org/10.1007/978-3-662-44584-6_18, https://doi.org/10.1007/978-3-662-44584-6_18
16. Jorrand, P., Lalire, M.: Toward a quantum process algebra. In: Proceedings of the 1st Conference on Computing Frontiers. pp. 111–119. ACM (2004)
17. Kubota, T., Kakutani, Y., Kato, G., Kawano, Y., Sakurada, H.: Semi-automated verification of security proofs of quantum cryptographic protocols. Journal of Symbolic Computa **73**, 192–220 (2016)

18. Lalire, M.: Relations among quantum processes: Bisimilarity and congruence. Mathematical Structures in Computer Science **16(3)**, 407–428 (2006)
19. Milner, R.: Communication and Concurrency. Prentice-Hall (1989)
20. Sangiorgi, D.: A theory of bisimulation for the pi-calculus. Acta Informatica **33**(1), 69–97 (1996)
21. Selinger, P.: Towards a quantum programming language. Mathematical Structures in Computer Science **14**(4), 527–586 (2004)
22. Shor, P., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters **85**(2), 441–444 (2000)
23. Ying, M., Feng, Y., Duan, R., Ji, Z.: An algebra of quantum processes. ACM Transactions on Computational Logic **10**(3), 1–36 (2009)
24. Zhang, L., Yang, P., Song, L., Hermanns, H., Eisentraut, C., Jansen, D.N., Godskesen, J.C.: Probabilistic bisimulation for realistic schedulers. Acta Informatica **55**(6), 461–488 (2018). https://doi.org/10.1007/s00236-018-0313-1, https://doi.org/10.1007/s00236-018-0313-1