Observational Equivalence Using Schedulers for Quantum Processes

Kazuya Yasuda Takahiro Kubota Yoshihiko Kakutani

Dept. of Computer Science
Graduate School of Information Science and Technology
The University of Tokyo
Tokyo, Japan

{kyasuda, takahiro.k11_30, kakutani}@is.s.u-tokyo.ac.jp

In the study of quantum process algebras, researchers have introduced different notions of equivalence between quantum processes like bisimulation or barbed congruence. However, there are intuitively equivalent quantum processes that these notions do not regard as equivalent. In this paper, we introduce a notion of equivalence named observational equivalence into qCCS. Since quantum processes have both probabilistic and nondeterministic transitions, we introduce schedulers that solve nondeterministic choices and obtain probability distribution of quantum processes. By definition, restrictions of schedulers change observational equivalence. We propose some definitions of schedulers, and investigate the relation between the restrictions of schedulers and observational equivalence.

1 Introduction

Quantum communication protocols have been proposed since Bennett and Brassard [2] proposed a quantum key distribution (QKD) protocol. However, proving the correctness or security of communication protocols is very complicated and error-prone because quantum mechanical behavior is often different from our intuition based on classical mechanics. In order to analyze or verify quantum protocols successfully, quantum process calculi have been proposed, for example, QPAlg [10], CQP [8], and qCCS [6, 7, 14].

In quantum process calculi, it is one of the important notions whether two processes behave similarly or not, in other words, whether they are behaviorally equivalent or not. One of the benefits of this notion is to provide the following technique to verify the correctness of a communication protocol. First, write a process that models the procedure of the communication protocol. Second, define a simpler process that is the specification of the protocol. Then, if these two processes are behaviorally equivalent, it is proved that the protocol satisfies the specification. For instance, the correctness of quantum teleportation is shown by using qCCS in [7]. In the paper, the model and the specification of quantum teleportation are defined with qCCS as $Tel = (Alice_t || Bob_t) \backslash \{e\}$ and $Tel_{spec} = \mathtt{c}?q.SWAP_{1,3}[q, q_1, q_2].\mathtt{d}!q_2.\mathbf{nil}$ respectively, where

$$Alice_t := \mathtt{c}?q.CN[q, q_1].H[q].M[q, q_1; x].e!x.\mathbf{nil},\ Bob_t := e?x.\sum_{0 \le i \le 3} \left(\mathbf{if}\ x = i\ \mathbf{then}\ \sigma^i[q_2].\mathtt{d}!q_2.\mathbf{nil}\right),$$

and it is proved that the model Tel and the specification Tel_{spec} are behaviorally equivalent (definitions of some symbols are in [7]).

There is a variety of the notions of behavioral equivalence such as (weak) bisimulation and barbed congruence. For example, these notions for qCCS are defined in [5, 7]. Intuitively, bisimulation is the

B. Coecke, I. Hasuo & P. Panangaden (Eds.):
Quantum Physics and Logic 2014 (QPL 2014).
EPTCS 172, 2014, pp. 191–203, doi:10.4204/EPTCS.172.13

notion that one process can simulate the other's behavior, and barbed congruence is the notion that any observers (or attackers) cannot distinguish two processes.

These two notions have widely been used in formal verification of processes. However, there are some processes that are not regarded as equivalent by these notions but intuitively equivalent. This problem occurs when the processes include quantum operations or communication. For example, consider the following two processes: one sends a qubit $|0\rangle$ or $|1\rangle$ with the same probability, the other sends $|+\rangle$ or $|-\rangle$ with the same probability. These two processes are not regarded as equivalent by the notion of bisimulation. However, we have intuitively regarded these two processes as the same process because these qubits are expressed as the same density matrix. This kind of equation was used in the security proof of BB84 by Shor and Preskill [13].

The aim of this paper is to define the notion of equivalence that regards above cases as equivalent into the quantum process calculus qCCS. This notion is called observational equivalence. Intuitively, two processes are observationally equivalent when they are observed the same by any attackers. Because attackers can observe their behavior only by watching the channels that they use, processes are observed the same when they use the channels with the same probability. In addition, we must consider the probability of using channels although the quantum processes of qCCS have both probabilistic and nondeterministic transitions. In order to solve this inconvenience, we define schedulers that solve nondeterministic choices and obtain probability distribution of quantum processes. By definition, the restrictions of schedulers change observational equivalence. We propose some definitions of schedulers, and investigate the relation between the restrictions of schedulers and observational equivalence.

2 Definitions of qCCS

In this section, we introduce the language qCCS proposed in [6, 7, 14].

2.1 Syntax

Three types of data are considered in qCCS: `Bool` for booleans, `Real` for real numbers and `Qbt` for qubits. Let $cVar$ be the set of classical variables, ranged over by $x, y, \ldots$, and $qVar$ be the set of quantum variables, ranged over by $q, r, \ldots$. We assume that $cVar$ and $qVar$ are both countably infinite and $cVar \cap qVar = \emptyset$. The indexed set $\{q_1, \ldots, q_n\}$ is often abbreviated to $\tilde{q}$. Let Exp be the set of classical data expressions over `Real`, ranged over by $e, e', \ldots$, which includes $cVar$ as a subset. Let $BExp$ be the set of boolean-valued expressions, ranged over by $b, b', \ldots$.

Two types of channels are used in qCCS: $cChan$ for classical channels and $qChan$ for quantum channels. $c, d, \ldots$ range over $cChan$ and $\mathtt{c}, \mathtt{d}, \ldots$ range over $qChan$. We assume that $cChan \cap qChan = \emptyset$. Let $Chan$ be the set of all channels, that is, $Chan = cChan \cup qChan$. A *relabeling function* is a function $f : Chan \to Chan$ such that $f(cChan) \subset cChan$ and $f(qChan) \subset qChan$.

The set of *quantum processes* $qProc$ is defined inductively as follows:

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

where $c \in cChan$, $x \in cVar$, $e \in Exp$, $\mathtt{c} \in qChan$, $b \in BExp$, $q \in qVar$, $A(\tilde{q};\tilde{x})$ is a process constant, τ is the silent action, f is a relabeling function, $L \subset_{\text{fin}} Chan$, $\mathscr{E}$ and M are respectively a trace-preserving super-operator and a non-degenerate projective measurement applying on the Hilbert space associated with the systems $\tilde{q}$. The process **nil** may be omitted, for instance, $c!0$ is used instead of $c!0.\mathbf{nil}$.

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

Figure 1: Definition of qv

The *free classical variable function* $fv : qProc \to 2^{cVar}$ is defined in the usual way. Note that the quantum measurement $M[\tilde{q};x]$ binds the variable x, that is, $fv(M[\tilde{q};x].P) = fv(P) - \{x\}$. A process P is *closed* if $fv(P) = \emptyset$. The *free quantum variable function* $qv : qProc \to 2^{qVar}$ is defined inductively as in Figure 1. For quantum processes to be legal, we require that

1. $q \notin qv(P)$ in the process $\mathtt{c}!q.P$;
2. $qv(P) \cap qv(Q) = \emptyset$ in the process $P||Q$;
3. each process constant $A(\tilde{q};\tilde{x})$ has a defining equation $A(\tilde{q};\tilde{x}) := P$, where $P \in qProc$, $qv(P) \subset \tilde{q}$ and $fv(P) \subset \tilde{x}$.

We use $P\{v/x\}$ to denote the substitution of v for x in P. We abbreviate $P\{v_1/x_1\}\ldots\{v_n/x_n\}$ to $P\{\tilde{v}/\tilde{x}\}$.

2.2 Configuration

For each $q \in qVar$, we assume a 2-dimensional Hilbert space $\mathscr{H}_q$ to be the state space associated with the system q. Let

$$\mathscr{H}_S = \bigotimes_{q \in S} \mathscr{H}_q$$

for any $S \subset qVar$. In particular, $\mathscr{H} = \mathscr{H}_{qVar}$ is the whole state space associated with all of the quantum variables.

A *configuration* is a pair $\langle P, \rho \rangle$, where $P \in qProc$ is closed and ρ is a density operator on $\mathscr{H}$. Let Con be the set of all configurations, ranged over by $C, D, \ldots$. If the state associated with the system q is $|\psi\rangle\langle\psi|$, the notation $|\psi\rangle\langle\psi|_q \otimes \rho$ or $[|\psi\rangle]_q \otimes \rho$ is used to denote this whole state, where ρ is a state associated with the systems $qVar - \{q\}$.

Let $D(Con)$ be the set of finite-support probability distribution over Con, ranged over by $\mu, \nu, \ldots$. When $\mu(C) = 1$ for some $C \in Con$, we use C instead of μ to denote the distribution. We sometimes use a form $\mu = \boxplus_{i \in I} p_i \bullet C_i$ to denote the distribution μ, where C_i are distinct elements of Con and $\mu(C_i) = p_i$. For any $\mu = \boxplus_{i \in I} p_i \bullet \langle P_i, \rho_i \rangle$ and trace-preserving super-operator $\mathscr{E}$, the notation $\boxplus_{i \in I} p_i \bullet \langle P_i, \mathscr{E}(\rho_i) \rangle$ is often abbreviated to $\mathscr{E}(\mu)$.

2.3 Operational semantics

Let $Act = \{\tau\} \cup \{c?v, c!v \mid c \in cChan, v \in \mathtt{Real}\} \cup \{\mathtt{c}?r, \mathtt{c}!r \mid \mathtt{c} \in qChan, r \in qVar\}$. For each $\alpha \in Act$, let $cn(\alpha)$ be the set of channel names used in the action α, that is, $cn(\tau) = \emptyset$, $cn(c?v) = cn(c!v) = \{c\}$ and $cn(\mathtt{c}?r) = cn(\mathtt{c}!r) = \{\mathtt{c}\}$. For each $\alpha \in Act$ and relabeling function f, we use $f(\alpha)$ to denote the action of which channel is relabeled by f. For example, $f(\tau) = \tau$, $f(c?v) = f(c)?v$ and $f(\mathtt{c}!q) = f(\mathtt{c})!q$.

The operational semantics of qCCS is defined by the probabilistic labeled transition system [5] $(Con, Act, \longrightarrow)$, where $\longrightarrow \subset Con \times Act \times D(Con)$ is the smallest relation satisfying the rules defined in

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

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

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

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

$$\frac{r \notin qv(\texttt{c}?q.P)}{\langle \texttt{c}?q.P,\rho\rangle \xrightarrow{\texttt{c}?r} \langle P\{r/q\},\rho\rangle} \text{(Q-Inp)}$$

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

$$\frac{\langle P_1,\rho\rangle \xrightarrow{\texttt{c}?r} \langle P_1',\rho\rangle,\ \ \langle P_2,\rho\rangle \xrightarrow{\texttt{c}!r} \langle P_2',\rho\rangle}{\langle P_1||P_2,\rho\rangle \xrightarrow{\tau} \langle P_1'||P_2',\rho\rangle} \text{(Q-Com)}$$

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

$$\frac{M = \sum_{i\in I}\lambda_i E^i \quad p_i = \mathrm{tr}(E_{\tilde{q}}^{i\dagger}\rho)}{\langle M[\tilde{q};x].P,\rho\rangle \xrightarrow{\tau} \sum_{i\in I\wedge p_i\neq 0} p_i \left\langle P\{\lambda_i/x\}, E_{\tilde{q}}^i \rho E_{\tilde{q}}^{i\dagger}/p_i\right\rangle} \text{(Meas)}$$

$$\frac{\langle P_1,\rho\rangle \xrightarrow{c?r} \langle P_1',\rho\rangle,\ \ r \notin qv(P_2)}{\langle P_1||P_2,\rho\rangle \xrightarrow{c?r} \langle P_1'||P_2,\rho\rangle} \text{(Inp-Int)}$$

$$\frac{\langle P_1,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i',\rho_i\rangle,\ \ \alpha \neq \texttt{c}?r}{\langle P_1||P_2,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i'||P_2,\rho_i\rangle} \text{(Oth-Int)}$$

$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu}{\langle P+Q,\rho\rangle \xrightarrow{\alpha} \mu} \text{(Sum)}$$

$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i,\rho_i\rangle}{\langle P[f],\rho\rangle \xrightarrow{f(\alpha)} \boxplus_{i\in I} p_i \bullet \langle P_i[f],\rho_i\rangle} \text{(Rel)}$$

$$\frac{\langle P,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i,\rho_i\rangle,\ \ cn(\alpha)\cap L = \emptyset}{\langle P\backslash L,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i\backslash L,\rho_i\rangle} \text{(Res)}$$

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

$$\frac{\langle P\{\tilde{r}/\tilde{q}\}\{\tilde{v}/\tilde{x}\},\rho\rangle \xrightarrow{\alpha} \mu,\ \ A(\tilde{q};\tilde{x}) := P}{\langle A(\tilde{r};\tilde{v}),\rho\rangle \xrightarrow{\alpha} \mu} \text{(Def)}$$

Figure 2: Transition rules of qCCS

Figure 2 (the symmetric forms for rules C-Com, Q-Com, Inp-Int, Oth-Int and Sum are omitted). Here, $[\![e]\!]$ and $[\![b]\!]$ are the usual interpretations of $e \in Exp$ and $b \in BExp$ respectively, and $\mathscr{E}_{\tilde{q}}$ means that the super-operator $\mathscr{E}$ applys on the state associated with the systems $\tilde{q}$. We write $C \xrightarrow{\alpha} \mu$ instead of $(C,\alpha,\mu) \in \longrightarrow$. We write $C \xrightarrow{\alpha}$ when there exists $\mu \in D(Con)$ such that $C \xrightarrow{\alpha} \mu$. We write $C \not\xrightarrow{}$ when there do not exist α and μ such that $C \xrightarrow{\alpha} \mu$.

The transition relation $\longrightarrow$ is lifted to $D(Con) \times Act \times D(Con)$ as follows: we write $\mu \xrightarrow{\alpha} \nu$ if for any $C \in supp(\mu)$, $C \xrightarrow{\alpha} \nu_C$ for some ν_C, and $\nu = \sum_{C\in supp(\mu)} \mu(C)\nu_C$.

3 Bisimulation

In this section, we recall the relation called open bisimulation. To define it, we need to define the relation $\Longrightarrow$ and a weight function. These definitions are introduced in [7].

Definition 1. The relation $\Longrightarrow \subset D(Con) \times D(Con)$ is the smallest relation satisfying the following conditions:

1. $C \Longrightarrow C$;
2. if $C \xrightarrow{\tau} \mu$ and $\mu \Longrightarrow \nu$, then $C \Longrightarrow \nu$;
3. if $\mu = \sum_{i\in I} p_i C_i$, and for any $i \in I$, $C_i \Longrightarrow \nu_i$ for some ν_i, then $\mu \Longrightarrow \sum_{i\in I} p_i \nu_i$.

For any $\mu,\nu \in D(Con)$ and $s = \alpha_1 \ldots \alpha_n \in Act^*$, we say that μ can evolve into ν by a weak s-transition, denoted by $\mu \overset{s}{\Longrightarrow} \nu$, if there exist $\mu_1,\ldots,\mu_{n+1},\nu_1,\ldots,\nu_n \in D(Con)$, such that $\mu \Longrightarrow \mu_1$, $\mu_{n+1} = \nu$, and for each $i = 1,\ldots,n$, $\mu_i \xrightarrow{\alpha_i} \nu_i$ and $\nu_i \Longrightarrow \mu_{i+1}$.

For any $s \in Act^*$, $\hat{s}$ is the string obtained from s by deleting all the occurrences of τ.

Definition 2. Let $\mathscr{R} \subset Con \times Con$ and $\mu, \nu \in D(Con)$. A *weight function* for (μ, ν) w.r.t. $\mathscr{R}$ is a function $\delta : Con \times Con \to [0,1]$ that satisfies the following conditions:

1. for all $C, D \in Con$,

$$\sum_{D' \in supp(\nu)} \delta(C, D') = \mu(C), \quad \sum_{C' \in supp(\mu)} \delta(C', D) = \nu(D);$$

2. for all $C, D \in Con$, if $\delta(C, D) > 0$, then $C \mathscr{R} D$.

We write $\mu \mathscr{R} \nu$ if there exists a weight function for (μ, ν) w.r.t. $\mathscr{R}$.

Lemma 1. *Let $\mu, \nu \in D(Con)$. Then $\mu \mathscr{R} \nu$ if and only if there exist $\{p_i\}_{i \in I}$, $\{C_i\}_{i \in I}$, and $\{D_i\}_{i \in I}$ such that $\mu = \sum_{i \in I} p_i C_i$, $\nu = \sum_{i \in I} p_i D_i$, and $C_i \mathscr{R} D_i$ for each $i \in I$. In particular, if $C \mathscr{R} \mu$ then $C \mathscr{R} D$ for each $D \in supp(\mu)$.*

Now we introduce open bisimulation on qCCS defined in [5].

Definition 3. A relation $\mathscr{R} \subset Con \times Con$ is an *open bisimulation* if $\langle P, \rho \rangle \mathscr{R} \langle Q, \sigma \rangle$ implies that $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and for any super-operator $\mathscr{E}$ acting on $\mathscr{H}_{\overline{qv(P)}}$,

1. whenever $\langle P, \mathscr{E}(\rho) \rangle \xrightarrow{\alpha} \mu$, there exists ν such that $\langle Q, \mathscr{E}(\sigma) \rangle \xRightarrow{\hat{\alpha}} \nu$ and $\mu \mathscr{R} \nu$;
2. whenever $\langle Q, \mathscr{E}(\sigma) \rangle \xrightarrow{\alpha} \nu$, there exists μ such that $\langle P, \mathscr{E}(\rho) \rangle \xRightarrow{\hat{\alpha}} \mu$ and $\mu \mathscr{R} \nu$.

Let $\approx_o$ be the largest open bisimulation.

There are other notions of equivalence like open bisimulation on qCCS. For example, *bisimulation* is defined in [7] and *reduction barbed congruence* is defined in [5]. According to [5], the largest open bisimulation is strictly coarser than the largest bisimulation, and the reduction barbed congruence coincides with the largest open bisimulation.

4 Observational equivalence

In this section, we introduce the notion of observational equivalence on qCCS. Intuitively, two configurations are observationally equivalent when they are observed by foreign processes in the same way, in other words, when they use the same channels with the same probability in any contexts.

First of all, we describe why we want to define the notion of observational equivalence with an example. There are two different ways to express quantum measurements in qCCS: $M[q;x]$ and $\mathscr{E}[q]$, where M is the 1-qubit projective measurement such that $M = \sum_{i=0}^{1} i \, |i\rangle \langle i|$, $\mathscr{E}$ is the trace-preserving super-operator such that $\mathscr{E}(\rho) = \sum_{i=0}^{1} |i\rangle \langle i| \, \rho \, |i\rangle \langle i|$. We intuitively want to consider that these two processes are equivalent, but they are not bisimilar. This gap is an obstacle to formalize Shor and Preskill's security proof of BB84 [12]. For simplicity, we consider the following example.

Example 1. Consider these two configurations:

$$C = \left\langle M[q;x].(c!0 + d!0), [|+\rangle]_q \otimes \rho \right\rangle, \quad D = \left\langle \mathscr{E}[q].(c!0 + d!0), [|+\rangle]_q \otimes \rho \right\rangle$$

where M and $\mathscr{E}$ are described above. The pLTSs for these configurations are depicted as in Figure 3. It is obvious that $C \not\approx_o D$. We want to consider that C and D are equivalent.

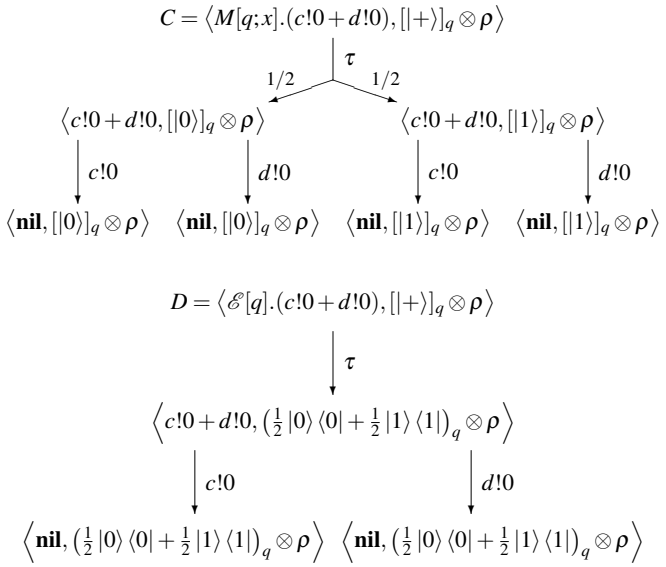

Figure 3: pLTSs for Example 1

4.1 Scheduler

Even though quantum processes on qCCS have both probabilistic and nondeterministic transitions, we have to consider a probability to use channels in order to define observational equivalence. So, we define schedulers to solve nondeterministic choices and to obtain probability distribution of configurations.

Definition 4. A function $F : Con \to (Act \times D(Con)) \cup \{\bot\}$ is a *scheduler* if the following conditions are satisfied:

1. $F(C) = (\alpha, \mu)$ implies $C \xrightarrow{\alpha} \mu$,
2. $F(C) = \bot$ implies $C \not\to$.

We write $C \xrightarrow{\alpha}_F \mu$ when $F(C) = (\alpha, \mu)$. We write $C \xrightarrow{\alpha}_F$ when $F(C) = (\alpha, \mu)$ for some $\mu \in D(Con)$.

The relation $\Longrightarrow$ is limited by a scheduler as follows:

Definition 5. The relation $\Longrightarrow_F \subset D(Con) \times D(Con)$ is the smallest relation satisfying the following conditions:

1. $C \Longrightarrow_F C$;
2. if $C \xrightarrow{\tau}_F \mu$ and $\mu \Longrightarrow_F \nu$, then $C \Longrightarrow_F \nu$;
3. if $\mu = \sum_{i \in I} p_i C_i$, and for any $i \in I$, $C_i \Longrightarrow_F \nu_i$ for some ν_i, then $\mu \Longrightarrow_F \sum_{i \in I} p_i \nu_i$.

4.2 Observational equivalence

We write $C \Downarrow^p_F c$ when there exists $\mu \in D(Con)$ such that

- $C \Longrightarrow_F \mu$ holds;
- for each $C' \in supp(\mu)$, either $F(C') = \bot$ or $C' \xrightarrow{\lambda}_F$ holds for some $\lambda \neq \tau$; and

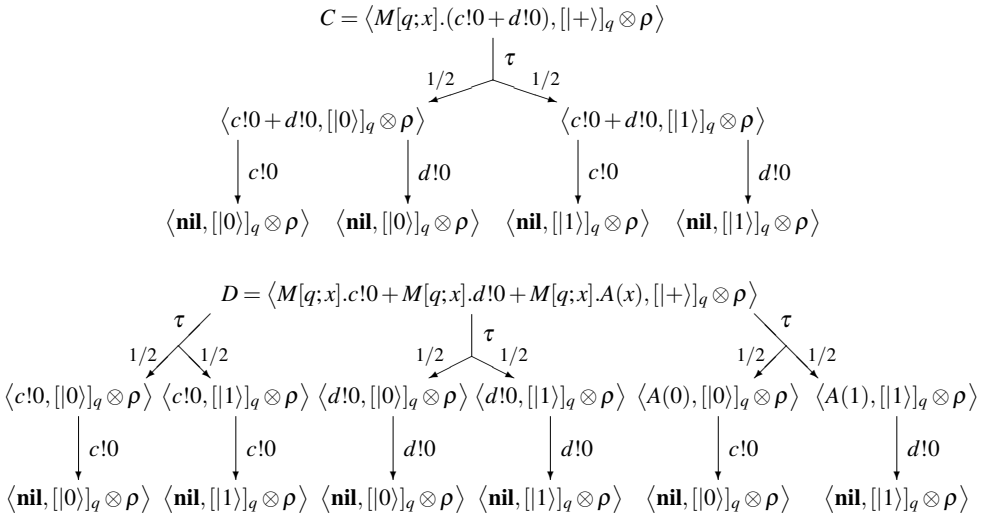

Figure 4: pLTSs for Example 2

- the equation $\sum\{\mu(C') \mid C' \xrightarrow{c!v}_F \text{ for some } v\} = p$ holds.

This means, intuitively, that the configuration C uses the channel c with the probability p after all internal transitions in accordance with the scheduler F.

Now, we define observational equivalence on qCCS.

Definition 6. Two configurations $\langle P, \rho \rangle, \langle Q, \sigma \rangle \in Con$ are *observationally equivalent*, we write $\langle P, \rho \rangle \approx_{oe} \langle Q, \sigma \rangle$, if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$ and for any quantum processes $R \in qProc$,

1. for each scheduler F there exists a scheduler F' such that, for any classical channel $c \in cChan$ $\langle P||R, \rho \rangle \Downarrow^p_F c$ implies that $\langle Q||R, \sigma \rangle \Downarrow^p_{F'} c$;
2. for each scheduler F there exists a scheduler F' such that, for any classical channel $c \in cChan$ $\langle Q||R, \sigma \rangle \Downarrow^p_F c$ implies that $\langle P||R, \rho \rangle \Downarrow^p_{F'} c$.

We can prove that $\approx_{oe}$ is an equivalence relation easily.

For example, we show two configurations that are not equivalent in the notion of open bisimulation but observationally equivalent.

Example 2. Consider these two configurations:

$$C = \left\langle M[q;x].(c!0+d!0), [|+\rangle]_q \otimes \rho \right\rangle,$$

$$D = \left\langle M[q;x].c!0 + M[q;x].d!0 + M[q;x].A(x), [|+\rangle]_q \otimes \rho \right\rangle$$

where $A(x) := (\textbf{if } x = 0 \textbf{ then } c!0) + (\textbf{if } x = 1 \textbf{ then } d!0)$ and M is as defined in Example 1. The pLTSs for these configurations are depicted as in Figure 4. It is obvious that $C \not\approx_o D$. However, we can prove that $C \approx_{oe} D$.

Proposition 1. *Let C, D be the configurations in Example 2. Then* $C \approx_{oe} D$.

Proof. Let $P = M[q;x].(c!0+d!0)$ and $Q = M[q;x].c!0 + M[q;x].d!0 + M[q;x].A(x)$.

We have $qv(P) = qv(Q) = \{q\}$ and $\mathrm{tr}_{qv(P)}([|+\rangle]_q \otimes \rho) = \mathrm{tr}_{qv(Q)}([|+\rangle]_q \otimes \rho) = \rho$.

Let R be an arbitrary quantum process. First, we need to show that, for each scheduler F, there exists a scheduler F' such that, for any classical channel c $\langle P||R, [|+\rangle]_q \otimes \rho \rangle \Downarrow^p_F c$ implies $\langle Q||R, [|+\rangle]_q \otimes \rho \rangle \Downarrow^p_{F'} c$. To prove it, we divide several cases of the scheduler F and construct a scheduler F' in each case.

1. The scheduler F does not choose the τ transition caused by P. In this case, we can easily construct a scheduler F' such that $\langle Q||R,[|+\rangle]_q\otimes\rho\rangle \Downarrow^p_{F'} c$.

2. The scheduler F chooses the τ transition caused by P. In this case, we have

$$\langle P||R,[|+\rangle]_q\otimes\rho\rangle \Longrightarrow_F \boxplus_{i\in I}\left(\frac{1}{2}p_i\bullet\langle c!0+d!0||R_i,[|0\rangle]_q\otimes\rho_i\rangle \boxplus \frac{1}{2}p_i\bullet\langle c!0+d!0||R_i,[|1\rangle]_q\otimes\rho_i\rangle\right)$$

after all τ transitions caused by P and R independently in accordance with F. Then, there exists a scheduler F' such that

$$\langle Q||R,[|+\rangle]_q\otimes\rho\rangle \Longrightarrow_{F'} \boxplus_{i\in I} p_i\bullet\langle Q||R_i,[|+\rangle]_q\otimes\rho_i\rangle.$$

For each $i\in I$, we again divide some cases of F and construct F' in each cases. Here we show only one case and omit the others.

When

$$\langle c!0+d!0||R_i,[|0\rangle]_q\otimes\rho_i\rangle \xrightarrow{c!0}_F \langle \mathbf{nil}||R_i,[|0\rangle]_q\otimes\rho_i\rangle,$$

$$\langle c!0+d!0||R_i,[|1\rangle]_q\otimes\rho_i\rangle \xrightarrow{c!0}_F \langle \mathbf{nil}||R_i,[|1\rangle]_q\otimes\rho_i\rangle,$$

the channel c is used with the probability 1. So, we can construct a scheduler F' such that

$$\langle Q||R_i,[|+\rangle]_q\otimes\rho_i\rangle \xrightarrow{\tau}_{F'} \frac{1}{2}\bullet\langle c!0||R_i,[|0\rangle]_q\otimes\rho_i\rangle \boxplus \frac{1}{2}\bullet\langle c!0||R_i,[|1\rangle]_q\otimes\rho_i\rangle,$$

$$\langle c!0||R_i,[|0\rangle]_q\otimes\rho_i\rangle \xrightarrow{c!0}_{F'} \langle \mathbf{nil}||R_i,[|0\rangle]_q\otimes\rho_i\rangle, \quad \langle c!0||R_i,[|1\rangle]_q\otimes\rho_i\rangle \xrightarrow{c!0}_{F'} \langle \mathbf{nil}||R_i,[|1\rangle]_q\otimes\rho_i\rangle.$$

The scheduler F' satisfies the requirement.

□

We show another example that means there exist configurations C,D that $C\not\approx_{oe} D$ but $C\approx_o D$.

Example 3. Consider these two configurations:

$$C=\langle M[q;x].A(q;x),[|+\rangle]_q\otimes\rho\rangle, \qquad D=\langle c!0.\mathscr{I}[q]+d!0.\mathscr{I}[q],[|0\rangle]_q\otimes\rho\rangle$$

where

$$A(q;x):=(\textbf{if } x=0 \textbf{ then } (c!0.\mathscr{I}[q]+d!0.\mathscr{I}[q]))+(\textbf{if } x=1 \textbf{ then } (c!0.\mathscr{X}[q]+d!0.\mathscr{X}[q])),$$

$\mathscr{I}$ is an operator that does nothing, $\mathscr{X}$ is the Pauli-X operator, and M is as defined in Example 1. The pLTSs for these configurations are depicted as in Figure 5.

We can prove that $C\approx_o D$. However, $C\not\approx_{oe} D$. Consider a scheduler F such that

$$F(\langle A(q;0),[|0\rangle]_q\otimes\rho\rangle)=(c!0,\langle\mathscr{I}[q],[|0\rangle]_q\otimes\rho\rangle),$$

$$F(\langle A(q;1),[|1\rangle]_q\otimes\rho\rangle)=(d!0,\langle\mathscr{X}[q],[|1\rangle]_q\otimes\rho\rangle).$$

Then both $C\Downarrow^{1/2}_F c$ and $C\Downarrow^{1/2}_F d$ hold. But, for any schedulers F', neither $D\Downarrow^{1/2}_{F'} c$ nor $D\Downarrow^{1/2}_{F'} d$ holds.

Proposition 2. *$\approx_o$ and $\approx_{oe}$ are incomparable.*

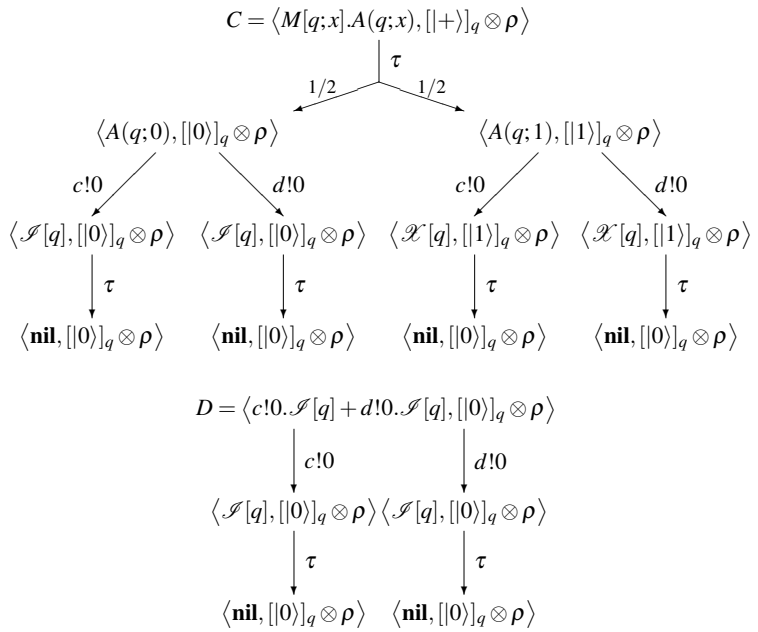

Figure 5: pLTSs for Example 3

4.3 Strategy: a limited scheduler

In previous section, we define schedulers and the observational equivalence. However, the processes in Example 1 are not observationally equivalent. Consider a scheduler F such that

$$F(\langle (c!0 + d!0), [|0\rangle]_q \otimes \rho \rangle) = (c!0, \langle \mathbf{nil}, [|0\rangle]_q \otimes \rho \rangle),$$
$$F(\langle (c!0 + d!0), [|1\rangle]_q \otimes \rho \rangle) = (d!0, \langle \mathbf{nil}, [|1\rangle]_q \otimes \rho \rangle).$$

Then both $C \Downarrow_F^{1/2} c$ and $C \Downarrow_F^{1/2} d$ hold. But, for any schedulers F', neither $D \Downarrow_{F'}^{1/2} c$ nor $D \Downarrow_{F'}^{1/2} d$ holds.

This problem is due to the definition of schedulers, that is, because schedulers can choose different transitions even though the processes are the same. In order to solve this problem, we propose strategies, limited schedulers.

Definition 7. A function $F : Con \to (Act \times D(Con)) \cup \{\bot\}$ is a *strategy* if the following conditions are satisfied:

1. $F(C) = (\alpha, \mu)$ implies $C \xrightarrow{\alpha} \mu$,
2. $F(C) = \bot$ implies $C \not\to$,
3. if $F(\langle P, \rho \rangle) = (\alpha, \mu)$, then there exist a set of processes $\{P_i\}_{i \in I}$, a set of super-operators $\{\mathscr{E}_i\}_{i \in I}$, acting on $\mathscr{H}_{qv(P)}$, and a set of projectors $\{E_i\}_{i \in I}$, acting on $\mathscr{H}_{qv(P)}$ and $\sum_{i \in I} E_i = I$, such that for any density operators σ,

$$F(\langle P, \sigma \rangle) = \left(\alpha, \sum_{i \in I \wedge q_i^\sigma \neq 0} q_i^\sigma \langle P_i, \mathscr{E}_i(\sigma)/q_i^\sigma \rangle \right)$$

and

$$\mu = \sum_{i \in I \wedge q_i^\rho \neq 0} q_i^\rho \langle P_i, \mathscr{E}_i(\rho)/q_i^\rho \rangle$$

where $q_i^\sigma = \mathrm{tr}(E_i\sigma)$.

The difference between schedulers and strategies is only the condition 3 in Definition 7. This condition means that strategies must choose the same transition for any density operators if the processes of the configurations are the same. In order to validate this condition, we use the following lemma. This lemma is stronger than Lemma 3.3 (2) in [7], but can still be easily observed from the transition rules of qCCS.

Lemma 2. *If $\langle P,\rho\rangle \xrightarrow{\alpha} \mu$, then there exists a set of processes $\{P_i\}_{i\in I}$, a set of super-operators $\{\mathscr{E}_i\}_{i\in I}$, acting on $\mathscr{H}_{qv(P)}$, and a set of projectors $\{E_i\}_{i\in I}$, acting on $\mathscr{H}_{qv(P)}$ and $\sum_{i\in I}E_i = I$, such that for any density operators σ,*

$$\langle P,\sigma\rangle \xrightarrow{\alpha} \sum_{i\in I\wedge q_i^\sigma\neq 0} q_i^\sigma \langle P_i, \mathscr{E}_i(\sigma)/q_i^\sigma\rangle,$$

and

$$\mu = \sum_{i\in I\wedge q_i^\rho\neq 0} q_i^\rho \left\langle P_i, \mathscr{E}_i(\rho)/q_i^\rho\right\rangle$$

where $q_i^\sigma = \mathrm{tr}(E_i\sigma)$.

We use the notations $C \xrightarrow{\alpha}_F \mu$, $C \xrightarrow{\alpha}_F$ and $\Longrightarrow_F$ for strategies F in the same way as schedulers.

4.4 Observational equivalence with strategies

We write $C \Downarrow_F^p c$ for strategies F in the same way as schedulers. Now, we define observational equivalence using strategies instead of schedulers.

Definition 8. Two configurations $\langle P,\rho\rangle, \langle Q,\sigma\rangle \in Con$ are *observationally equivalent with strategies*, we write $\langle P,\rho\rangle \approx_{oe}^{st} \langle Q,\sigma\rangle$, if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$ and for any quantum processes $R \in qProc$,

1. for each strategy F there exists a strategy F' such that, for any classical channel $c \in cChan$ $\langle P||R,\rho\rangle \Downarrow_F^p c$ implies that $\langle Q||R,\sigma\rangle \Downarrow_{F'}^p c$;
2. for each strategy F there exists a strategy F' such that, for any classical channel $c \in cChan$ $\langle Q||R,\sigma\rangle \Downarrow_F^p c$ implies that $\langle P||R,\rho\rangle \Downarrow_{F'}^p c$.

We can prove that $\approx_{oe}^{st}$ is an equivalence relation easily.

Now, we can check that the two configurations in Example 1 are observationally equivalent with strategies.

Proposition 3. *Let C and D be configurations in Example 1. Then $C \approx_{oe}^{st} D$.*

Let us consider the relation among open bisimulation $\approx_o$, observational equivalence $\approx_{oe}$, and observational equivalence with strategies $\approx_{oe}^{st}$.

By Example 1 and Proposition 3, there exist some configurations C and D that $C \not\approx_{oe} D$ but $C \approx_{oe}^{st} D$. However, $\approx_{oe} \subset \approx_{oe}^{st}$ does not hold. Consider Example 2 again. The configurations in Example 2 are observationally equivalent, but they are not observationally equivalent with strategies. Consider the strategy F such that

$$F(D) = \left(\tau, \frac{1}{2}\bullet\left\langle A(0), [|0\rangle]_q\otimes\rho\right\rangle \boxplus \frac{1}{2}\bullet\left\langle A(1), [|1\rangle]_q\otimes\rho\right\rangle\right),$$

$$F(\left\langle A(0), [|0\rangle]_q\otimes\rho\right\rangle) = \left(c!0, \left\langle \mathbf{nil}, [|0\rangle]_q\otimes\rho\right\rangle\right), \quad F(\left\langle A(1), [|1\rangle]_q\otimes\rho\right\rangle) = \left(d!0, \left\langle \mathbf{nil}, [|1\rangle]_q\otimes\rho\right\rangle\right).$$

Then both $D \Downarrow_F^{1/2} c$ and $D \Downarrow_F^{1/2} d$ are hold. However, neither $C \Downarrow_{F'}^{1/2} c$ nor $C \Downarrow_{F'}^{1/2} d$ holds for any strategies F'. It is because, for any strategies F', if

$$F'(\langle c!0 + d!0, [|0\rangle]_q \otimes \rho \rangle) = (\alpha_0, \mu_0), \quad F'(\langle c!0 + d!0, [|1\rangle]_q \otimes \rho \rangle) = (\alpha_1, \mu_1),$$

then α_0 and α_1 must be the same action by the definition of strategies.

Proposition 4. *$\approx_{oe}$ and $\approx_{oe}^{st}$ are incomparable.*

In addition, $\approx_o \subset \approx_{oe}^{st}$ does not also hold, although there exist some configurations C and D that $C \not\approx_o D$ but $C \approx_{oe}^{st} D$. Consider Example 3 again. It is proved that $C \approx_o D$, but $C \not\approx_{oe}^{st} D$. Consider the strategy F such that

$$F(C) = \left(\tau, \frac{1}{2} \bullet \langle A(q;0), [|0\rangle]_q \otimes \rho \rangle \boxplus \frac{1}{2} \bullet \langle A(q;1), [|1\rangle]_q \otimes \rho \rangle\right),$$

$$F(\langle A(q;0), [|0\rangle]_q \otimes \rho \rangle) = \left(c!0, \langle \mathscr{I}[q], [|0\rangle]_q \otimes \rho \rangle\right),$$
$$F(\langle A(q;1), [|1\rangle]_q \otimes \rho \rangle) = \left(d!0, \langle \mathscr{X}[q], [|1\rangle]_q \otimes \rho \rangle\right).$$

Then both $C \Downarrow_F^{1/2} c$ and $C \Downarrow_F^{1/2} d$ are hold. However, neither $D \Downarrow_{F'}^{1/2} c$ nor $D \Downarrow_{F'}^{1/2} d$ holds for any strategies F'.

Proposition 5. *$\approx_o$ and $\approx_{oe}^{st}$ are incomparable.*

5 Related work

There already exists "observational equivalence" or "observational congruence" on other process calculi such as applied pi calculus [1] and probabilistic applied pi calculus [9]. However, they are essentially the same as reduction barbed congruence because they are reduction-closed by definition. So, they are also the same as the notion of open bisimulation.

The same notion of observational equivalence in this paper is defined along the line of applied pi calculi in [11]. However, the study in [11] was not so sophisticated and many unsolved problems were taken over by this study.

On the other hand, probabilistic branching bisimilarity, another notion of behavioral equivalence, is defined on CQP in [3, 4]. The same idea as strategies in our work is used in its definition.

6 Conclusion

In this paper, we proposed the notion of observational equivalence. To define it, we used schedulers that solve nondeterministic choices. Some processes that are not bisimilar became observationally equivalent, but others remained nonequivalent. And so, we defined strategies, which are limited schedulers, and the notion of observational equivalence with strategies. Some processes that are intuitively equivalent became observationally equivalent with strategies. After that, we investigated the relation among three notions, that is, open bisimulation $\approx_o$, observational equivalence $\approx_{oe}$, and observational equivalence with strategies $\approx_{oe}^{st}$, and we found that it is impossible to compare these three notions. Even so, we think that $\approx_{oe}^{st}$ is the most intuitive of the three when we consider the situation like Example 1 or the formal security proof of BB84.

However, there remains a question whether our definition of observational equivalence is really intuitive. In order to solve this question, we must formalize the "intuition" at first. And then, we can discuss whether our definition of equivalence is intuitive or not.

We should also discuss the congruence of our observational equivalences. Congruence is the property that the equivalence is preserved under process constructs. The congruence property for parallel compositions $P||R$, which are the most important case, holds by definition of our observational equivalences. In addition, the property for relabelling functions $P[f]$ and conditional executions **if** b **then** P also holds. However, the property for channel restrictions $P\backslash L$ does not hold. For example, $\langle c!0+d!0,\rho\rangle \approx_{oe} \langle \tau.c!0+\tau.d!0,\rho\rangle$ but $\langle (c!0+d!0)\backslash\{c\},\rho\rangle \not\approx_{oe} \langle (\tau.c!0+\tau.d!0)\backslash\{c\},\rho\rangle$ for any density operator ρ. It remains for future work to investigate whether they are preserved under other constructs or not.

References

[1] Martín Abadi & Cédric Fournet (2001): *Mobile Values, New Names, and Secure Communication*. In: *Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '01*, ACM Press, New York, New York, USA, pp. 104–115, doi:10.1145/360204.360213.

[2] Charles H. Bennett & Gilles Brassard (1984): *Quantum cryptography: Public key distribution and coin tossing*. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

[3] Timothy A. S. Davidson (2012): *Formal verification techniques using quantum process calculus*. Phd thesis, University of Warwick.

[4] Timothy A. S. Davidson, Simon J. Gay, Rajagopal Nagarajan & Ittoop Vergheese Puthoor (2012): *Analysis of a Quantum Error Correcting Code using Quantum Process Calculus*. *Electronic Proceedings in Theoretical Computer Science* 95, pp. 67–80, doi:10.4204/EPTCS.95.7.

[5] Yuxin Deng & Yuan Feng (2012): *Open Bisimulation for Quantum Processes*. In: *Theoretical Computer Science, Lecture Notes in Computer Science* 7604, Springer Berlin Heidelberg, pp. 119–133, doi:10.1007/978-3-642-33475-7_9.

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

[7] Yuan Feng, Runyao Duan & Mingsheng Ying (2012): *Bisimulation for Quantum Processes*. *ACM Transactions on Programming Languages and Systems* 34(4), pp. 17:1–17:43, doi:10.1145/2400676.2400680.

[8] Simon J. Gay & Rajagopal Nagarajan (2005): *Communicating Quantum Processes*. In: *Proceedings of the 32nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '05*, ACM Press, New York, New York, USA, pp. 145–157, doi:10.1145/1040305.1040318.

[9] Jean Goubault-larrecq, Catuscia Palamidessi & Angelo Troina (2007): *A Probabilistic Applied Pi-Calculus*. In: *Programming Languages and Systems, Lecture Notes in Computer Science* 4807, Springer Berlin Heidelberg, pp. 175–190, doi:10.1007/978-3-540-76637-7_12.

[10] Philippe Jorrand & Marie Lalire (2004): *Toward a Quantum Process Algebra*. In: *Proceedings of the first conference on computing frontiers on Computing frontiers - CF'04*, ACM Press, New York, New York, USA, pp. 111–119, doi:10.1145/977091.977108.

[11] Takahiro Kubota (2011): *Formalization and Automation of Unconditional Security Proof of QKD*. Master's thesis, University of Tokyo.

[12] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano & Hideki Sakurada (2012): *Application of a Process Calculus to Security Proofs of Quantum Protocols*. In: *Proceedings of Foundations of Computer Science in WORLDCOMP*, pp. 141–147. Available at `http://worldcomp-proceedings.com/proc/p2012/FCS.html`.

[13] Peter W. Shor & John Preskill (2000): *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*. Physical Review Letters 85(2), pp. 441–444, doi:10.1103/PhysRevLett.85.441.

[14] Mingsheng Ying, Yuan Feng, Runyao Duan & Zhengfeng Ji (2009): *An Algebra of Quantum Processes*. ACM Transactions on Computational Logic 10(3), pp. 19:1–19:36, doi:10.1145/1507244.1507249.