Model checking quantum Markov chains

Yuan Feng, Nengkun Yu, and Mingsheng Ying
University of Technology, Sydney, Australia,
Tsinghua University, China

Abstract. Although the security of quantum cryptography is provable based on the principles of quantum mechanics, it can be compromised by the flaws in the design of quantum protocols and the noise in their physical implementations. So, it is indispensable to develop techniques of verifying and debugging quantum cryptographic systems. Model-checking has proved to be effective in the verification of classical cryptographic protocols, but an essential difficulty arises when it is applied to quantum systems: the state space of a quantum system is always a continuum even when its dimension is finite. To overcome this difficulty, we introduce a novel notion of quantum Markov chain, specially suited to model quantum cryptographic protocols, in which quantum effects are entirely encoded into super-operators labelling transitions, leaving the location information (nodes) being classical. Then we define a quantum extension of probabilistic computation tree logic (PCTL) and develop a model-checking algorithm for quantum Markov chains.

Keywords: Quantum Markov chains, quantum protocols, model checking

1 Introduction

Quantum cryptography, employing quantum mechanical effects to accomplish cryptographic tasks, has been developed so rapidly that quantum cryptographic systems are already commercially available by a number of companies such as Id Quantique, Cerberis, MagiQ Technologies, SmartQuantum, and NEC. One of the greatest advantages of quantum cryptography over its classical counterpart is that the security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics. In practice, however, errors which comprise this absolute security will still creep in at the following two levels:

- **Protocol design level.** As quantum mechanics is more or less anti-intuitive, quantum cryptographic protocol designers will inevitably make more mistakes than classical protocol designers, especially when more and more complicated quantum protocols can be implemented by future physical technology.
- **Physical implementation level.** Even when the security has been proved for ideal quantum cryptographic protocols, the security of physically implemented cryptographic systems is highly difficult to guarantee, as any physical
implementation is imperfect and attackers can disguise themselves as environmental noise. In fact, the commercial system implementing BB84 quantum key distribution protocol [4] made by ID Quantique has been found insecure, by taking advantage of the synchronisation signals that pass between Alice and Bob [27].

Therefore, it is indispensable to develop methodologies and techniques for the verification of quantum cryptographic systems.

Over the last four decades, model-checking [9, 2] has become one of the dominant techniques for verification of classical hardware as well as software systems, and has proved mature as witnessed by a large number of successful industrial applications. Model-checking techniques have also been widely used in the verification of security protocols [21]. One of the advantages of model checking is that it is usually automatic and provides counter-examples, which are indispensable in debugging, in case the property is violated.

Given its advantage stated above, people reasonably started to explore the possibility of applying model-checking in the verification of quantum cryptographic protocols. The main obstacle for model checking quantum system is that the set of all quantum states, traditionally regarded as the underlying state space of the models to be checked, is a continuum. Hence the techniques of classical model checking, which normally work only for a finite state space, cannot be applied directly. Gay et al. [13, 23] provided a clever solution for this problem by restricting the state space to a set of finitely describable states called stabiliser states, and restricting the quantum operations applied on them to the class of Clifford group. By doing this, they were able to obtain an efficient model checker for quantum protocols, employing purely classical algorithms. They even developed an automatic tool QMC (Quantum Model-Checker) for model-checking quantum communication protocols [14]. However, the limitation of their approach is also obvious: it can only check the (partial) behaviours of a protocol on stabiliser states, and does not work for more general protocols. A similar idea was independently introduced by Hung et al. [17, 18] to synthesise quantum circuits. By formulating quantum logic synthesis problem vis symbolic reachability analysis, they were able to reduce the original problem to multiple-valued logic synthesis, thus simplifying the search space and algorithm complexity.

This paper presents another solution to the problem, which applies to general quantum protocols. After a thorough examination of almost all existing quantum protocols, we observe that quantum operations in these protocols can always be dealt with in a high-level way without resorting to the underlying quantum states. This leads to a novel notion of quantum Markov chain where quantum effects are entirely encoded into super-operators labelling transitions, and the nodes of its transition graph carry only classical information and thus they are discrete. Therefore, we circumvent the obstacle of continuous state spaces in model-checking quantum systems. However, the following new difficulty has to be overcome, namely,
A prerequisite for defining probabilistic temporal logic is a suitable probability measure on the set of infinite paths of a Markov chain. Vardi [25] introduced such a measure by letting the $\sigma$-algebra be generated by cylinder extensions of finite paths and proved that the events of infinite paths specified by various temporal logical formulas are measurable. The probabilities of these cylinder sets are given in a natural way. Then the probability measure on the cylinder sets can be extended to Vardi’s $\sigma$-algebra by the Carathéodory-Hahn extension theorem. For a quantum Markov chain, however, a super-operator valued measure instead of a numerical measure must be introduced because its transitions are labelled by super-operators instead of numerical probabilities. How can we apply Vardi’s procedure to this new kind of measures?

This paper solves the above problem by employing the Kluvanek’s generalisation of the Carathéodory-Hahn extension theorem from vector measure theory [10]. Furthermore, we define a quantum extension of PCTL and develop an algorithm for model-checking quantum Markov chains. Compared to the quantum computation tree logic presented in [3], our logic is much simpler and more like PCTL. Consequently, a large part of classical techniques can be easily adapted to verify properties of quantum systems expressed in this logic.

We assume the readers are familiar with the basic notions of linear algebra and quantum theory. We put a brief introduction into the appendix for the convenience of the readers. For more details, we refer to [22].

1.1 Related work

The mathematical structure employed in this paper to model quantum systems is a super-operator weighted quantum Markov chain. The idea of defining the denotational semantics of a quantum program as a super-operator was first proposed by Selinger [24]. Prior to our work, there were quite a few different notions of quantum Markov chains [1, 8, 11], introduced by authors from different research communities. The major difference is that in their models transitions are considered between quantum states which always form a continuum, whereas in our model transitions are considered between different points in an execution path, and quantum operations are treated as labels of the transitions. Consequently, the state spaces of our quantum Markov chains are typically finite, and classical model checking techniques can be easily adapted to verify quantum systems.

Thanks to one of the reviewers of CAV’12, we are aware of that a quantum Markov model similar to that used in this paper was introduced by Gudder [15] where the transition between different vertices is characterised by an operation matrix whose entries are super-operators and the sum of each column is trace-preserving. However, the motivations are very different: Gudder [15] aimed at defining a pure mathematical generalisation of quantum walks, whereas our model is extracted from semantics of quantum protocols and quantum programs.
2 Super-operators and super-operator valued measures

For the sake of simplicity, in the following we use the term super-operator to denote a completely positive super-operator. Let $SO(H)$ be the set of super-operators on $H$, ranged over by $E, F, \cdots$. Obviously, both $(SO(H), 0_H, +)$ and $(SO(H), I_H, \circ)$ are monoids, where $I_H$ and $0_H$ are the identity and null super-operators on $H$, respectively, and $\circ$ is the composition of super-operators defined by $(E \circ F)(\rho) = E(F(\rho))$ for any $\rho \in D(H)$ where $D(H)$ is the set of density operators on $H$. We always omit the symbol $\circ$ and write $EF$ directly for $E \circ F$.

Furthermore, the operation $\circ$ is (both left and right) distributive with respect to $+$:

$$E(F_1 + F_2) = EF_1 + EF_2, \quad (F_1 + F_2)E = F_1E + F_2E.$$ 

Thus $(SO(H), +, \circ)$ forms a semiring. We will use two different orders:

Definition 1. Let $E, F \in SO(H)$.

(1) $E \preceq F$ if for any $\rho \in D(H)$, $F(\rho) - E(\rho)$ is positive semi-definite;

(2) $E \mathbin{\asymp} F$ if for any $\rho \in D(H)$, $tr(E(\rho)) \leq tr(F(\rho))$.

The first order is lifted from Löwner partial order on density operators, whereas the second one is used to compare the ability of ‘preserving trace’. Note that the trace of a (unnormalised) quantum state is exactly the probability that the (normalised) state is reached [24]. Intuitively, $E \mathbin{\asymp} F$ if and only if the success probability of performing $E$ is always not greater than that of performing $F$, whatever the initial state is.

Let $\preceq$ be $\mathbin{\asymp} \cap \gtrsim$; it is obviously an equivalence relation. Note that $\preceq$ is a partial order while $\mathbin{\asymp}$ is merely a pre-order.

Lemma 1. Let $E, F \in SO(H)$. Then

(1) $E \subseteq F$ if for any $\rho \in D(H)$, $F(\rho) - E(\rho)$ is positive semi-definite;

(2) $E \mathbin{\subseteq} F$ if for any $\rho \in D(H)$, $tr(E(\rho)) \leq tr(F(\rho))$.

Proof. (1) is obvious. To prove (2), let $E = \{E_i : i \in I\}$ and $F = \{F_j : j \in J\}$ be the Kraus representation of $E$ and $F$, respectively. Then $E \mathbin{\subseteq} F$ if and only if $G = \sum_{j \in J} F_j^\dagger F_j - \sum_{i \in I} E_i^\dagger E_i$ is positive semi-definite. Let $G = F^\dagger F$ and define the super-operator $G = \{E\}$. Let $F' = E + G$. Then it is easy to check $F' \approx F$ and $E \subseteq F'$.

The next lemma shows that the two orders $\mathbin{\subseteq}$ and $\preceq$ are preserved by the right application of composition.

Lemma 2. Let $E, F, G \in SO(H)$. If $E \mathbin{\subseteq} F$, then $EG \subseteq FG$, and if $E \preceq F$, then $EG \preceq FG$.

Let $SI(H) = \{E \in SO(H) : E \preceq I_H\}$.

Let $SI(H)^n$ be the set of $n$-size row vectors over $SI(H)$, and extend the partial order $\preceq$ component-wisely to it. Then we have
Lemma 3. The set \((SI(H)^n, \sqsubseteq)\) is a complete partial order set with the least element \((0_H, \ldots, 0_H)\).

Proof. The case when \(n = 1\) is from [24], while the extension to \(n > 1\) is obvious.

With the notations and properties presented above, we can prove the main result of this section, which is the key to verifying the long-run properties of quantum Markov chains. Due to lack of space, we put the proof to the Appendix.

Theorem 1. Let \(T\) and \(\tilde{G}\) be two matrices of super-operators with sizes \(n \times n\) and \(1 \times n\), respectively, and for each \(j\), \(\sum_i T_{i,j} + \tilde{G}_{j} \subseteq I_H\). Let

\[
f(X) = XT + \tilde{G}
\]

be a function from \(SO(H)^n\) to \(SO(H)^n\). Then

1. \(f(X)\) has the least fixed point, denoted by \(\tilde{E}^0\), in \(SI(H)^n\) under the order \(\sqsubseteq\);
2. Given any \(E \in SI(H)\) and \(1 \leq i \leq n\), it can be decided whether \(E \sim \tilde{E}^0\), \(\sim \in \{\leq, \geq\}\), in time \(O(n^2d^4)\) where \(d = \dim(H)\) is the dimension of \(H\).

To conclude this section, we introduce the notion of super-operator valued measures, which will play a role similar to probability measures for probabilistic model checking.

Definition 2. Let \((\Omega, \Sigma)\) be a measurable space; that is, \(\Omega\) is a non-empty set and \(\Sigma\) a \(\sigma\)-algebra over \(\Omega\). A function \(\Delta : \Sigma \rightarrow SI(H)\) is said to be a super-operator valued measure (SVM for short) if \(\Delta\) satisfies the following properties:

1. \(\Delta(\Omega) \supseteq I_H\);
2. \(\Delta(\bigcup_{i} A_i) \approx \sum_i \Delta(A_i)\) for all pairwise disjoint and countable sequence \(A_1, A_2, \ldots\) in \(\Omega\).

We call the triple \((\Omega, \Sigma, \Delta)\) a (super-operator valued) measure space.

Here and in the following of this paper, we always write \(A = \bigcup_{i} A_i\) if \(A = \bigcup_{i} A_i\) and \(A_i\)'s are pairwise disjoint; that is, for any \(i \neq j\), \(A_i \cap A_j = \emptyset\). SVMs enjoy some similar properties satisfied by probabilistic measures, which are collected as follows.

Lemma 4. Let \((\Omega, \Sigma, \Delta)\) be a measure space. Then

1. \(\Delta(\emptyset) = 0_H\);
2. \(\Delta(A^c) + \Delta(A) \approx I_H\) where \(A^c\) is the complement set of \(A\) in \(\Omega\);
3. (monotonic) for any \(A, A' \in \Sigma\), if \(A \subseteq A'\) then \(\Delta(A) \lesssim \Delta(A')\);
4. for any sequence \(A_1, A_2, \ldots\) in \(\Sigma\),
   - if \(A_1 \subseteq A_2 \subseteq \ldots\), then there exists a sequence \(E_1 \sqsubseteq E_2 \sqsubseteq \ldots\) in \(SI(H)\) such that for any \(i\), \(\Delta(A_i) \approx E_i\), and \(\Delta(\bigcup_{i \geq 1} A_i) = \lim_{i \to \infty} E_i\).
   - if \(A_1 \supseteq A_2 \supseteq \ldots\), then there exists a sequence \(E_1 \supseteq E_2 \supseteq \ldots\) in \(SI(H)\) such that for any \(i\), \(\Delta(A_i) \approx E_i\), and \(\Delta(\bigcap_{i \geq 1} A_i) = \lim_{i \to \infty} E_i\).
We now extend the ordinary notion of Markov chains to super-operator weighted ones.

**Definition 3.** A super-operator weighted Markov chain, or quantum Markov chain (qMC), is a tuple $(S, Q, AP, L)$, where

1. $S$ is a countable (typically finite) set of states;
2. $Q : S \times S \rightarrow SI(H)$ is called the transition matrix where for each $s \in S$, $\sum_{t \in S} Q(s, t) \approx I_H$;
3. $AP$ is a finite set of atomic propositions;
4. $L$ is a mapping from $S$ to $2^{AP}$.

A classical Markov chain may be viewed as a degenerate quantum Markov chain in which all super-operators appear in the transition matrix have the form $pI_H$ for some $0 \leq p \leq 1$. Let $M = (S, Q, AP, L)$ be a quantum Markov chain. A path \(\pi\) of $M$ is an infinite sequence of states $s_0, s_1, \ldots$ where for all $i \geq 0$, $s_i \in S$ and $Q(s_i, s_{i+1}) \neq 0_H$. A finite path $\tilde{\pi}$ is a finite-length prefix of a path, and its length, denoted $|\tilde{\pi}|$, is defined to be the number of states in it. We denote by $\pi(i)$ the $i$th state of a path $\pi$, and $\tilde{\pi}(i)$ the $i$th state of a finite path $\tilde{\pi}$ if $i < |\tilde{\pi}|$.

In order to reason about the behaviour of a qMC, we need to determine the accumulated super-operator along certain paths. To this end, we construct a $\mathrm{SVM}_Q$ for each $s \in S$ as follows. For any finite path $\hat{\pi} = s_0 \ldots s_n \in \mathrm{Path}^M_{\text{fin}}(s)$, we define the super-operator

$$Q(\hat{\pi}) = \begin{cases} I_H, & \text{if } n = 0; \\ Q(s_{n-1}, s_n) \cdots Q(s_0, s_1), & \text{otherwise.} \end{cases}$$

Next we define the cylinder set $Cyl(\tilde{\pi}) \subseteq \mathrm{Path}^M(s)$ as

$$Cyl(\tilde{\pi}) = \{ \pi \in \mathrm{Path}^M(s) : \tilde{\pi} \text{ is a prefix of } \pi \};$$

that is, the set of all infinite paths with prefix $\tilde{\pi}$. It is easy to check that the set $\mathcal{S}^M(s) = \{ Cyl(\tilde{\pi}) : \tilde{\pi} \in \mathrm{Path}^M_{\text{fin}}(s) \} \cup \{ \emptyset \}$ is a semi-algebra on $\mathrm{Path}^M(s)$. Let a mapping $Q_s$ from $\mathcal{S}^M(s)$ to $SI(H)$ be defined by letting $Q_s(\emptyset) = 0_H$ and

$$Q_s(Cyl(\tilde{\pi})) = Q(\tilde{\pi}).$$

The following theorem states that we can extend the mapping $Q_s$ defined above to a super-operator valued measure on the $\sigma$-algebra of infinite paths generated by cylinder extensions of finite paths, similar to Vardi’s work for classical Markov chains [25]. The main tool we use here is the Kluvanek’s generalisation of the Carathéodory-Hahn extension theorem from vector measure theory [10]. We defer the detailed proof to the appendix for the sake of space limit.
Theorem 2. The mapping $Q_s$ defined above can be extended to a SVM, denoted by $Q_s$, again, on the $\sigma$-algebra generated by $S^M(s)$. Furthermore, this extension is unique up to the equivalence relation $\sim$.

To show the expressive power of quantum Markov chains, we present some examples.

Example 1. (quantum loop programs) A simple quantum loop program, whose termination has been investigated extensively in [12] and [28], goes as follows:

$$l_0 : q := \mathcal{F}(q)$$
$$l_1 : \text{while } M[q] \text{ do}$$
$$l_2 : \quad q := \mathcal{E}(q)$$
$$l_3 : \text{od}$$

where $M = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$. The intuitive meaning of this program is as follows. We first initialise the state of the quantum system $q$ at line $l_0$, by a trace-preserving super-operator $\mathcal{F}$. At line $l_1$, the two-outcome projective measurement $M$ is applied to $q$. If the outcome $\lambda_0$ is observed, then the program terminates at line $l_1$; otherwise it proceeds to $l_2$ where a trace-preserving super-operator $\mathcal{E}$ is performed at $q$, and then the program returns to line $l_1$ and another iteration continues.

We now construct a qMC to describe the program. Let $S = \{l_i : 0 \leq i \leq 3\}$, $AP = S$, $L(l_i) = \{l_i\}$ for each $i$, and $Q$ be defined as $Q(l_0, l_1) = \mathcal{F}_q$, $Q(l_1, l_2) = \mathcal{E}^0_q = \{|0\rangle_q\langle 0|\}$, $Q(l_1, l_2) = \mathcal{E}^1_q = \{|1\rangle_q\langle 1|\}$, $Q(l_2, l_1) = \mathcal{E}^1_q$, and $Q(l_3, l_3) = I_H$. The qMC is depicted in Figure 1 (the left one). Let $\hat{\pi} = l_0l_1l_2l_3l_4$ be a finite path from $l_0$. Then

$$Q(\hat{\pi}) = Q(l_1, l_4)Q(l_2, l_1)Q(l_1, l_2)Q(l_2, l_1)Q(l_1, l_2)Q(l_0, l_1) = \mathcal{E}^{0}_{q}\mathcal{E}^{1}_{q}\mathcal{E}^{1}_{q}\mathcal{E}^{1}_{q}\mathcal{E}^{0}_{q}\mathcal{F}_q.$$

Example 2. [Quantum key-distribution] BB84, the first quantum key distribution protocol developed by Bennett and Brassard in 1984 [4], provides a provably secure way to create a private key between two parties, say, Alice and Bob. The basic BB84 protocol goes as follows:

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

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

The qMC for the basic BB84 protocol in the simplest case of $n = 1$ is depicted in Fig. 1 (the right one), where $\text{Set}_{\psi}$ is the 1-qubit super-operator which sets the target qubit to $|\psi\rangle$, $\mathcal{X} = \{X\}$ and $\mathcal{Z} = \{Z\}$ are respectively the Pauli-X and Pauli-Y super-operators, and $\mathcal{E}^i = \{|i\rangle\langle i|\}$, $i = 0, 1, +, -$. As all the super-operators are applied on the same quantum qubit, we omit the subscripts of them for simplicity. We use the subscripts for the $s$-states to denote the choices of the basis $B_a$ of Alice, the key $K_a$ generated by Alice, and the basis $B_b$ guessed by Bob. For example, in $s_{101}$, $B_a = B_b = 1$ and $K_a = 0$. The atomic proposition set $AP$ is the same as $S$, and $L(s) = \{s\}$ for each $s \in S$.

We use the states $\text{succ}$ and $\text{fail}$ to denote the successful and unsuccessful termination of BB84 protocol, respectively. We take the state $s_{101}$ as an example to illustrate the basic idea. As the bases of Alice and Bob are both $\{|+, -\}$ at $s_{101}$, they will regard the key bits as the final key generated by the protocol. Thus if the outcome of Bob’s measurement is 0, which corresponds to the super-operator $\mathcal{E}^+$, then the protocol succeeds since Alice and Bob indeed share the
same key bit 0; otherwise the protocol fails as they end up with different bits: Alice with 0 while Bob with 1. That explains why we have $Q(s_{101}, \text{succ}) = \mathcal{E}^+$ while $Q(s_{101}, \text{fail}) = \mathcal{E}^-$. Note also that at states $s_{001}, s_{011}, s_{100}$ and $s_{110}$ Alice and Bob’s bases differ, so the protocol will be aborted without generating any key. In these cases, the protocol should also be regarded as being successful.

4 Quantum Computation Tree Logic (QCTL)

This section is devoted to a quantum extension of classical computation tree logic (CTL) and probabilistic computation tree logic (PCTL).

Definition 4. The syntax of quantum computation tree logic (QCTL) is as follows:

$$
\Phi ::= a \mid \neg \Phi \mid \Phi \land \Phi \mid Q_{\sim E}[\phi]
$$

$$
\phi ::= X\Phi \mid \Phi \leq_k \Phi \mid \Phi U \Phi
$$

where $a$ is an atomic proposition, $\sim \in \{\leq, \geq\}$, $E \in \mathcal{SI}(\mathcal{H})$, and $k \in \mathbb{N}$. We call $\Phi$ a state formula and $\phi$ a path formula.

Compared to the logic presented in [3], our QCTL here is simpler and more like PCTL: the only difference is that the formula $P_{\sim p}[\phi]$ in PCTL, which asserts that the probability of paths from a certain state satisfying the path formula $\phi$ is constrained by $\sim p$ where $0 \leq p \leq 1$, is replaced in QCTL by $Q_{\sim E}[\phi]$, which asserts that the accumulated super-operators corresponding to paths from a certain state satisfying the formula $\phi$ is constrained by $\sim E$ where $0_{\mathcal{H}} \leq E \leq I_{\mathcal{H}}$. Note that $P_{\sim p}[\phi]$ is merely a special case of $Q_{\sim E}[\phi]$ by taking $E = pI_{\mathcal{H}}$.

Definition 5. Let $\mathcal{M} = (S, Q, AP, L)$ be a quantum Markov chain. For any state $s \in S$, the satisfaction relation $\models$ is defined inductively by

$$
\begin{align*}
s \models a & \text{ if } a \in L(s) \\
s \models \neg \Phi & \text{ if } s \not\models \Phi \\
s \models \Phi \land \Psi & \text{ if } s \models \Phi \text{ and } s \models \Psi \\
s \models Q_{\sim E}[\phi] & \text{ if } Q^\mathcal{M}(s, \phi) \sim E
\end{align*}
$$

where

$$Q^\mathcal{M}(s, \phi) = Q_s(\{\pi \in \text{Path}^\mathcal{M}(s) \mid \pi \models \phi\}),$$

and for any path $\pi \in \text{Path}^\mathcal{M}(s)$,

$$
\begin{align*}
\pi \models X\Phi & \text{ if } \pi(1) \models \Phi \\
\pi \models \Phi \leq_k \Psi & \text{ if } \exists i \in \mathbb{N}.(i < k \land \pi(i) \models \Psi \land \forall j < i.(\pi(j) \models \Phi)) \\
\pi \models \Phi U \Psi & \text{ if } \exists i \in \mathbb{N}.(\pi(i) \models \Psi \land \forall j < i.(\pi(j) \models \Phi)).
\end{align*}
$$
Similar to PCTL, we can check that for each path formula $\phi$ and each state $s$ in a qMC $M$, the set $\{ \pi \in \text{Path}^M(s) \mid \pi \models \phi \}$ is in the $\sigma$-algebra generated by $S^M(s)$. As usual, we introduce some syntactic sugars to simplify notations: the disjunction $\Psi_1 \lor \Psi_2 \equiv \neg(\neg \Psi_1 \land \neg \Psi_2)$, the tautology $tt \equiv a \lor \neg a$, the eventually operator $\Diamond \Psi \equiv tt \mathcal{U} \Psi$, and the step-bounded eventually operator $\Diamond \leq k \Psi \equiv tt \mathcal{U} \leq k \Psi$.

Example 3. We revisit the examples in the previous section, to show the expressive power of QCTL.

(1) Example 1. The QCTL formula $Q \triangleright E [\Diamond \leq k 3]$ asserts that the probability that the loop program in Example 1 terminates within $k$ iterations is lower bounded by $E$. That is, for any initial quantum state $\rho$, the termination probability is not less than $\text{tr}(E(\rho))$. In particular, the property that it terminates everywhere can be described as $Q \triangleright I H [\Diamond l 3]$.

(2) Example 2. To check the correctness of the basic BB84 protocol, we need to modify the atomic propositions and the labelling function such that $AP = S \cup \{\text{retry}\}$, and for each $t \in S$, $L(t) = \{t\}$ except that $L(s_{001}) = L(s_{011}) = L(s_{100}) = L(s_{110}) = \{\text{retry}\}$. The intuition behind this modification is, when the bases of Alice and Bob do not coincide, the generated key will be abandoned, and another run of the protocol will be made. The correctness of basic BB84 protocol can be stated as $s |\models Q \preceq 0 H [\Diamond \text{fail}] \land Q \succeq 1/2 I [\Diamond \leq 4 \text{succ}]$.

5 Model checking quantum Markov chains

As in the classical case, given a state $s$ in a qMC $M = (S, Q, AP, L)$ and a state formula $\Phi$ expressed in QCTL, model checking if $s$ satisfies $\Phi$ is essentially to determine whether $s$ belongs to the satisfaction set $\text{Sat}(\Phi) = \{s \in S : s |\models \Phi \}$ which is defined inductively as follows:

$$\begin{align*}
\text{Sat}(a) &= \{s \in S : a \in L(s)\} \\
\text{Sat}(\neg \Psi) &= S \setminus \text{Sat}(\Psi) \\
\text{Sat}(\Psi \land \Phi) &= \text{Sat}(\Psi) \cap \text{Sat}(\Phi) \\
\text{Sat}(Q_{\preceq E}[\phi]) &= \{s \in S : Q^M(s, \phi) \sim E\}.
\end{align*}$$

Most of the formulae above are the same as in probabilistic model checking. The only difference is $\text{Sat}(Q_{\preceq E}[\phi])$. In the following, we will elaborate how to employ the results presented in previous sections to calculate the satisfaction sets for such kind of formulae. To this end, we need to compute $Q^M(s, \phi)$ for the following three cases.

Case 1: $\phi = X \Phi$. By definition, $\{\pi \in \text{Path}^M(s) : \pi \models X \Phi\} = \text{sat}(s) \cup_{t \in \text{Sat}(\Phi)} \text{Cyl}(st)$. Thus

$$Q^M(s, X \Phi) = Q_s \left( \bigcup_{t \in \text{Sat}(\Phi)} \text{Cyl}(st) \right) \approx \sum_{t \in \text{Sat}(\Phi)} Q_s(\text{Cyl}(st)) = \sum_{t \in \text{Sat}(\Phi)} Q(s, t).$$
This can be calculated easily since by the recursive nature of the definition, we can assume that \( \text{Sat}(\Phi) \) is already known.

Case 2: \( \phi = \Phi U \leq^k \Psi \). For any \( s \in S \) and \( k \geq 0 \), we let \( \Pi^k_s = \{ \pi \in \text{Path}^M(s) : \pi \models \Phi U \leq^k \Psi \} \). Then

\[
\Pi^k_s = \begin{cases} 
Cyl(s), & \text{if } s \in \text{Sat}(\Psi); \\
\emptyset, & \text{if } s \not\in \text{Sat}(\Phi) \cup \text{Sat}(\Psi) \vee (k = 0 \land s \not\in \text{Sat}(\Psi)); \\
\bigcup_{t \in \text{post}(s)} s^- \Pi^{k-1}_t, & \text{if } s \in \text{Sat}(\Phi) \setminus \text{Sat}(\Psi) \land k \geq 1.
\end{cases}
\]

where \( \text{post}(s) = \{ t \in S : \text{Q}(s, t) \neq 0 \} \), and \( s^- \Pi^{k-1}_t \) denotes the set of strings obtained by appending \( s \) to strings of \( \Pi^{k-1}_t \) from the beginning. By induction on \( k \), we can show that for each \( k \) and \( s \), \( \Pi^k_s = \emptyset \) or it is the disjoint union of some cylinder sets; to be specific, we have \( \Pi^k_s = \bigcup_{\pi \in A^k_s} \text{Cyl}(\pi) \) where

\[
A^k_s = \begin{cases} 
\{ s \}, & \text{if } s \in \text{Sat}(\Psi); \\
\emptyset, & \text{if } s \not\in \text{Sat}(\Phi) \cup \text{Sat}(\Psi) \vee (k = 0 \land s \not\in \text{Sat}(\Psi)); \\
\bigcup_{t \in \text{post}(s)} s^- A^{k-1}_t, & \text{if } s \in \text{Sat}(\Phi) \setminus \text{Sat}(\Psi) \land k \geq 1.
\end{cases}
\]

Thus if \( s \in \text{Sat}(\Phi) \setminus \text{Sat}(\Psi) \) and \( k \geq 1 \), we have

\[
Q_s(\Pi^k_s) = Q_s \left( \bigcup_{\pi \in A^k_s} \text{Cyl}(\pi) \right) = \sum_{\pi \in A^k_s} Q_s(Cyl(\pi))
\]

\[
= \sum_{t \in \text{post}(s)} \sum_{\pi' \in A^{k-1}_t} Q(s^- \pi') = \sum_{t \in \text{post}(s)} \sum_{\pi' \in A^{k-1}_t} Q(\pi') Q(s, t)
\]

\[
= \sum_{t \in S} \sum_{\pi' \in A^{k-1}_t} Q_t(Cyl(\pi')) Q(s, t) = \sum_{t \in S} Q_t(\Pi^{k-1}_t) Q(s, t).
\]

Adding the other two cases together, we finally have

\[
Q^M(s, \Phi U \leq^k \Psi) = \begin{cases} 
I_H, & \text{if } s \in \text{Sat}(\Psi); \\
0_H, & \text{if } s \not\in \text{Sat}(\Phi) \cup \text{Sat}(\Psi) \vee (k = 0 \land s \not\in \text{Sat}(\Psi)); \\
\sum_{t \in S} Q^M(t, \Phi U \leq^{k-1} \Psi) Q(s, t), & \text{if } s \in \text{Sat}(\Phi) \setminus \text{Sat}(\Psi) \land k \geq 1.
\end{cases}
\]

Again, this can be calculated easily since by the recursive nature of the definition, we can assume that both \( \text{Sat}(\Phi) \) and \( \text{Sat}(\Psi) \) are already known.

Case 3: \( \phi = \Phi U \Psi \). In this case, we define for any \( s \in S \) that \( \Pi_s = \{ \pi \in \text{Path}^M(s) : \pi \models \Phi U \Psi \} \). Similar to the bounded-until case, we get the equation system

\[
Q^M(s, \Phi U \Psi) = \begin{cases} 
I_H, & \text{if } s \in \text{Sat}(\Psi); \\
0_H, & \text{if } s \not\in \text{Sat}(\Phi) \cup \text{Sat}(\Psi); \\
\sum_{t \in S} Q^M(t, \Phi U \Psi) Q(s, t), & \text{if } s \in \text{Sat}(\Phi) \setminus \text{Sat}(\Psi).
\end{cases}
\]

We are interested in the least solution of this equation system, which can be calculated directly using Theorem 1.
Recall that in probabilistic model checking, to simplify the computation and transfer the equation system into one with a unique solution, a pre-computation process is usually employed to compute all the states from which the probability of eventually reaching $\text{Sat}(\Psi)$ without leaving states in $\text{Sat}(\Phi)$ is exactly 0 or 1. However, it is impossible in quantum case to calculate the exact set of states $s$ for which $Q^M(s, \Phi U \Psi)$ is equivalent to 0 or $I_H$ without solving an equation system of super-operators. This can be best explained by an example. In Fig. 2 we have a pMC and a qMC with the same graph structure. Let $\text{Sat}(\Psi) = \{l_3\}$ and $\text{Sat}(\Phi) = \{l_0, l_2\}$. In the pMC, $P(l_0, \Phi U \Psi) = 0$ if and only if $p = 0$ or $q = 0$, as $pq = 0$ if and only if $p(1 - q)nq = 0$ for any $n \geq 0$. However, in the qMC, things are complicated. First, we can not claim $Q^M(l_0, \Phi U \Psi) \not\equiv 0_H$ by only checking that neither $E^0$ nor $E^1$ is $0_H$; they can be orthogonal with each other: let $E^0 = \text{Set}|0\rangle$, $E^1 = \text{Set}|1\rangle$, and $E = I$. Then we have $Q^M(l_0, \Phi U \Psi) \approx 0_H$. Conversely, we can not claim $Q^M(l_0, \Phi U \Psi) \equiv 0_H$ by only checking $E^0 E^1 \not\equiv 0_H$ either. Let $E^0$ and $E^1$ be defined as above but let $E = X$ be the Pauli-X superoperator. Then $E^0 X E^1 \not\equiv 0_H$, thus $Q^M(l_0, \Phi U \Psi) \not\equiv 0_H$. To sum up, to check if $Q^M(s, \Phi U \Psi) \equiv 0_H$ or $I_H$, the accumulated super-operators along all possible paths from $s$ to $\text{Sat}(\Psi)$ through $\text{Sat}(\Phi)$, including all cycles and self-loops, must be considered. This is essentially as difficult as to solve the original super-operator equation system in which the state $s$ is involved. Similar argument applies to determining if $Q^M(s, \Phi U \Psi) \approx I_H$.

We have shown that in general it is not practical to pre-compute the two sets $\text{Sat}(Q_{\leq 0_H} [\Phi U \Psi])$ and $\text{Sat}(Q_{\geq I_H} [\Phi U \Psi])$. Nevertheless, we can still simplify the calculation by identifying some $S^0$ and $S^2$ such that

$$S \setminus (\text{Sat}(\Psi) \cup \text{Sat}(\Phi)) \subseteq S^0 \subseteq \text{Sat}(Q_{\leq 0_H} [\Phi U \Psi])$$

and

$$\text{Sat}(\Psi) \subseteq S^2 \subseteq \text{Sat}(Q_{\geq I_H} [\Phi U \Psi]),$$

which are calculated by the algorithms presented in Table 1, motivated by [20]. Now let $S^* = S \setminus (S^0 \cup S^2)$. Then for each $s \in S^*$,
Quantum loop program. We only check the property \( \Phi \). Then from Theorem 1, we can determine whether or not \( Q \subseteq \mathbb{R} \) for each \( s \in S \).

**Example 4.** This example is devoted to model checking the properties listed in Example 3 against the qMCs of Examples 1 and 2.

(1) Quantum loop program. We only check the property \( Q \subseteq \mathbb{R} \). Let \( \mathcal{T} = (Q(t, s))_{s,t \in S} \) and \( \mathcal{G} = (\sum_{t \in S} Q(s, t))_{s \in S} \) be two state-indexed matrices of super-operators. Then the required row vector \( (Q_M(s, \Phi \mathcal{U} \Psi))_{s \in S} \) is indeed the least fixed point of the function \( f(X) = X \mathcal{T} + \mathcal{G} \) in \( \mathcal{S} \mathcal{T}(\mathcal{H})^{S} \).

Let \( \sum_{t \in S} \mathcal{T}_{s,t} + \mathcal{G}_{s} = \sum_{t \in S} Q(s, t) + \sum_{t \in S} Q(s, t) = \sum_{t \in S \cup S} Q(s, t) \). Then from Theorem 1, we can determine whether or not \( Q_M(s, \Phi \mathcal{U} \Psi) \) efficiently.

**Table 1.** Algorithm to calculate \( S^0 \) and \( S^\mathcal{T} \).

\[
Q_M(s, \Phi \mathcal{U} \Psi) = \sum_{t \in S} Q_M(t, \Phi \mathcal{U} \Psi)Q(s, t) + \sum_{t \in S} Q(s, t).
\]

Let \( \mathcal{T} = (Q(t, s))_{s,t \in S} \) and \( \mathcal{G} = (\sum_{t \in S} Q(s, t))_{s \in S} \) be two state-indexed matrices of super-operators. Then the required row vector \( (Q_M(s, \Phi \mathcal{U} \Psi))_{s \in S} \) is indeed the least fixed point of the function \( f(X) = X \mathcal{T} + \mathcal{G} \) in \( \mathcal{S} \mathcal{T}(\mathcal{H})^{S} \).

Let \( \mathcal{G} = [0_{\mathcal{H}}, \mathcal{E}^0, 0_{\mathcal{H}}] \) with its matrix representation being \( M_{\mathcal{G}} = [0_{4 \times 4}, M_{\mathcal{E}^0}, 0_{4 \times 4}] \), and

\[
\mathcal{T} = \begin{pmatrix}
0_{\mathcal{H}} & 0_{\mathcal{H}} & 0_{\mathcal{H}} \\
\mathcal{F} & 0_{\mathcal{H}} & \mathcal{E} \\
0_{\mathcal{H}} & \mathcal{E}^1 & 0_{\mathcal{H}}
\end{pmatrix}
\]

with \( M_{\mathcal{T}} = \begin{pmatrix}
0_{4 \times 4} & 0_{4 \times 4} & 0_{4 \times 4} \\
M_{\mathcal{F}} & 0_{4 \times 4} & M_{\mathcal{E}} \\
0_{4 \times 4} & M_{\mathcal{E}^0} & 0_{4 \times 4}
\end{pmatrix} \).
\[ M_{E^0} = |0\rangle\langle 0| \otimes |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_{E^1} = |1\rangle\langle 1| \otimes |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \]

\[ M_E = X \otimes X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad M_F = \sum_{s=0}^{1} |i\rangle \otimes |i\rangle = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \]

Using Matlab, we find that all eigenvalues of the matrix \( M_T \) have the absolute value strictly less than 1, and \( M_T(I - M_T)^{-1} = [M, M, M] \) where

\[ M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1|. \]

Thus for \( i = 0, 1, 2 \), \( Q^M(l_i, \Diamond l_3) = Set^0 \) where \( Set^0 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} \cong \mathcal{I} \), and so \( l_i \models Q_{\geq \varepsilon}[\Diamond l_3] \) for any \( \varepsilon \leq \mathcal{I} \).

(2) BB84 protocol. We will compute \( Q^M(s, \Diamond \text{fail}) \) and \( Q^M(s, \Diamond \leq \varepsilon \text{ succ}) \) separately. Table 2 calculates \( Q^M(t, \Diamond \leq k \text{ succ}) \) for each \( t \in S \setminus S^0 \) and \( 0 \leq k \leq 4 \), where \( S^0 = \{s_{001}, s_{011}, s_{100}, s_{110}, \text{fail}\} \). The item \( Q^M(s, \Diamond \leq \varepsilon \text{ succ}) \) is calculated as follows:

\[
Q^M(s, \Diamond \leq \varepsilon \text{ succ}) = \sum_{t \in S} Q^M(t, \Diamond \leq \varepsilon \text{ succ})Q(s, t) \\
= \frac{1}{8}(E^0 + E^1 X)Set^{(0)} + \frac{1}{8}(E^+ + E^- Z)Set^{(+)} \\
= \frac{1}{8}(Set^{(0)} + Set^{(1)} + Set^{(+)} + Set^{(-)}) \cong \frac{1}{2} I_H.
\]

To compute \( Q^M(t, \Diamond \text{ fail}) \), we first obtain from the algorithm in Table 1 that \( \mathcal{S}^0 = \{s_{001}, s_{011}, s_{100}, s_{110}, \text{succ}\} \), and \( \mathcal{S}^T = \{\text{fail}\} \). Then Table 3 computes \( Q^M(t, \Diamond \text{ fail}) \) for each \( t \in S \setminus S^0 \setminus \mathcal{S}^T \) and \( 0 \leq k \leq 4 \). The item \( Q^M(s, \Diamond \leq k \text{ fail}) \) is calculated as follows:

\[
Q^M(s, \Diamond \leq k \text{ fail}) = \sum_{t \in S} Q^M(t, \Diamond \leq k \text{ fail})Q(s, t) \\
= \frac{1}{8}(E^1 + E^0 X)Set^{(0)} + \frac{1}{8}(E^- + E^+ Z)Set^{(+)} = 0_H.
\]

Note that \( Q^M(t, \Diamond \leq k \text{ fail}) = Q^M(t, \Diamond \leq k \text{ fail}) \) for any \( t \in S \) and \( k > 4 \). We have \( s \models Q_{\leq \varepsilon \text{ succ}}[\Diamond \text{ fail}] \land Q_{\geq \varepsilon \text{ succ}}[\Diamond \leq \varepsilon \text{ succ}] \) as expected.
Theorem 1 this cost is of the order $n$.

Based on this result, we introduce a novel notion of quantum Markov chains, which is specially suited for modelling quantum cryptographic protocols. By employing the results of this paper, we can model the behaviour of quantum systems in a more natural way, while leaving the location information being classical. This model is successfully applied to the development of quantum protocols for secure communication.

The main contribution of this paper is the introduction of a novel notion of quantum Markov chains, which is well suited for modelling quantum cryptographic protocols. By employing this model, we can model the behaviour of quantum systems in a more natural way, while leaving the location information being classical. This model is successfully applied to the development of quantum protocols for secure communication.

5.1 Complexity

Recall that the overall time complexity for model checking a PCTL formula $\Phi$ against a classical Markov chain with $n$ states is linear in $|\Phi|$ and polynomial in $n$, where the size $|\Phi|$ of a formula is defined to be the number of logical connectives and temporal operators in the formula plus the sum of the sizes of the temporal operators [20]. The complexity of our algorithm for model checking a QCTL formula $\Phi$ against a qMC with $n$ states is again linear in $|\Phi|$ and polynomial in $n$ and $d = \text{dim}(\mathcal{H})$ as the greatest extra cost is the until operator but from Theorem 1 this cost is of the order $n^2d^4$.

6 Conclusion and future works

The main contribution of this paper is a novel notion of quantum Markov chains where quantum effects are entirely encoded into super-operators labelling transitions, while leaving the location information being classical. This model is specially suited for modelling quantum cryptographic protocols. By employing the Kluvanek’s generalisation of Carathéodory-Hahn extension theorem from vector measure theory, we are able to define an appropriate super-operator valued measure on events of infinite paths in a quantum Markov chain. Based on this, we propose a quantum extension of PCTL and develop an algorithm for model-checking quantum Markov chains.

We demonstrate the utility of the techniques developed in this paper by an example of model-checking the correctness of basic BB84 protocol. The proper-
ties checked in this example are essentially classical in the sense that what we are really concerned with is the probabilities of certain events, not the quantum states themselves. However, there are also quantum protocols, such as teleportation which can make use of a maximally entangled state shared between the sender and the receiver to teleport an unknown quantum state by sending only classical information [5], where the properties we need to check are related to the resultant quantum states directly. One possible way of verifying such properties is to extend the atomic propositions, say, in the case of teleportation, to specify whether or not the accumulated super-operator from the initial location to the current location is proportional to the identity super-operator. This treatment, however, resorts to the ability to calculate the accumulated super-operators when constructing the model. Note that this can be done by the model-checking algorithm presented in this paper. We will further explore the possibility of this idea in our future work.

The BB84 protocol is checked in this paper with the implicit assumption that no noise occurs at all. As pointed out in the Introduction, the security of quantum cryptography is always compromised by the inevitable noise in physical implementations. A natural question then arises: can the techniques in the current paper be used to check security of physically implemented quantum cryptographic systems? This is also one of the future directions we are pursuing. It seems that the quantum Markov chain proposed in this paper is inclusive enough for this purpose because noisy implementation of unitary operators used in quantum communication can always be modelled by super-operators.

Acknowledgement

This work was partially supported by Australian ARC grants FT100100218 and DP110103473.

References

7 Appendix

7.1 Basic linear algebra

A Hilbert space $\mathcal{H}$ is a complete vector space equipped with an inner product

$$\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

such that

1. $\langle \psi | \psi \rangle \geq 0$ for any $|\psi\rangle \in \mathcal{H}$, with equality if and only if $|\psi\rangle = 0$;
2. $\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^*$;
3. $\langle \phi \sum_i c_i |\psi_i\rangle = \sum_i c_i \langle \phi |\psi_i\rangle$,

where $\mathbb{C}$ is the set of complex numbers, and for each $c \in \mathbb{C}$, $c^*$ stands for the complex conjugate of $c$. For any vector $|\psi\rangle \in \mathcal{H}$, its length $||\psi||$ is defined to be $\sqrt{\langle \psi | \psi \rangle}$, and it is said to be normalised if $||\psi|| = 1$. Two vectors $|\psi\rangle$ and $|\phi\rangle$ are orthogonal if $\langle \psi | \phi \rangle = 0$. An orthonormal basis of a Hilbert space $\mathcal{H}$ is a basis $\{|i\rangle\}$ where each $|i\rangle$ is normalised and any pair of them are orthogonal.

Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. For any $A \in \mathcal{L}(\mathcal{H})$, $A$ is Hermitian if $A^\dagger = A$ where $A^\dagger$ is the adjoint operator of $A$ such that $\langle \psi | A^\dagger | \phi \rangle = \langle \phi | A | \psi \rangle^*$ for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. The fundamental spectral theorem states that the set of all normalised eigenvectors of a Hermitian operator in $\mathcal{L}(\mathcal{H})$ constitutes an orthonormal basis for $\mathcal{H}$. That is, there exists a so-called spectral decomposition for each Hermitian $A$ such that

$$A = \sum_i \lambda_i |i\rangle \langle i| = \sum_{\lambda_i \in \text{spec}(A)} \lambda_i E_i$$

where the set $\{|i\rangle\}$ constitute an orthonormal basis of $\mathcal{H}$, $\text{spec}(A)$ denotes the set of eigenvalues of $A$, and $E_i$ is the projector to the corresponding eigenspace of $\lambda_i$. A linear operator $A \in \mathcal{L}(\mathcal{H})$ is unitary if $A^\dagger A = AA^\dagger = I_{\mathcal{H}}$ where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$. The trace of $A$ is defined as $\text{tr}(A) = \sum_i \langle i | A | i \rangle$ for some given orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$. It is worth noting that trace function is actually independent of the orthonormal basis selected. It is also easy to check that trace function is linear and $\text{tr}(AB) = \text{tr}(BA)$ for any operators $A, B \in \mathcal{L}(\mathcal{H})$.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Their tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as a vector space consisting of linear combinations of the vectors $|\psi_1 \psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. Here the tensor product of two vectors is defined by a new vector such that

$$\left( \sum_i \lambda_i |\psi_i\rangle \right) \otimes \left( \sum_j \mu_j |\phi_j\rangle \right) = \sum_{i,j} \lambda_i \mu_j |\psi_i\rangle \otimes |\phi_j\rangle.$$

Then $\mathcal{H}_1 \otimes \mathcal{H}_2$ is also a Hilbert space where the inner product is defined as the following: for any $|\psi_1\rangle, |\phi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle, |\phi_2\rangle \in \mathcal{H}_2$,

$$\langle \psi_1 \otimes \psi_2 | \phi_1 \otimes \phi_2 \rangle = \langle \psi_1 | \phi_1 \rangle_{\mathcal{H}_1} \langle \psi_2 | \phi_2 \rangle_{\mathcal{H}_2}.$$
where $\langle \cdot | \cdot \rangle_{\mathcal{H}_i}$ is the inner product of $\mathcal{H}_i$. For any $A_1 \in \mathcal{L}(\mathcal{H}_1)$ and $A_2 \in \mathcal{L}(\mathcal{H}_2)$, $A_1 \otimes A_2$ is defined as a linear operator in $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that for each $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$,

$$(A_1 \otimes A_2)|\psi_1\psi_2\rangle = A_1|\psi_1\rangle \otimes A_2|\psi_2\rangle.$$  

The partial trace of $A \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ with respect to $\mathcal{H}_1$ is defined as $\text{tr}_{\mathcal{H}_1}(A) = \sum_i (i|A|i)$ where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}_1$. Similarly, we can define the partial trace of $A$ with respect to $\mathcal{H}_2$. Partial trace functions are also independent of the orthonormal basis selected.

Traditionally, a linear operator $E$ on $\mathcal{L}(\mathcal{H})$ is called a super-operator on $\mathcal{H}$. A super-operator is said to be completely positive if it maps positive operators in $\mathcal{L}(\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H})$, and for any auxiliary Hilbert space $\mathcal{H}'$, the trivially extended operator $I_{\mathcal{H}'} \otimes E$ also maps positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$. Here $I_{\mathcal{H}'}$ is the identity operator on $\mathcal{L}(\mathcal{H}')$. The elegant and powerful Kraus representation theorem [19] of completely positive super-operators states that a super-operator $E$ is completely positive if and only if there are some set of operators $\{E_i : i \in I\}$ with appropriate dimension such that

$$E(A) = \sum_{i \in I} E_i A E_i^\dagger$$

for any $A \in \mathcal{L}(\mathcal{H})$. The operators $E_i$ are called Kraus operators of $E$. We abuse the notation slightly by denoting $E = \{E_i : i \in I\}$. It is worth noting that the set of Kraus operators is not unique and we can always take one such that the number of Kraus operators does not exceed $d^2$ where $d$ is the dimension of the Hilbert space. A super-operator is said to be trace-preserving if $\text{tr}(E(A)) = \text{tr}(A)$ for any positive $A \in \mathcal{L}(\mathcal{H})$; equivalently, its Kraus operators $E_i$ satisfy $\sum_i E_i^\dagger E_i = I$. In this paper, we will use the well-known (unitary) Pauli super-operators $X = \{X\}, Z = \{Z\}$, and $Y = \{Y\}$ where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$  

### 7.2 Basic quantum mechanics

According to von Neumann’s formalism of quantum mechanics [26], an isolated physical system is associated with a Hilbert space which is called the state space of the system. A pure state of a quantum system is a normalised vector in its state space, and a mixed state is represented by a density operator on the state space. Here a density operator $\rho$ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\text{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geq 0$, $\sum_i p_i = 1$, and $|\psi_i\rangle$ are pure states, then $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ is a density operator. Conversely, each density operator can be generated by an ensemble of pure states in this way. Let $\mathcal{D}(\mathcal{H})$ denote the set of density operators on $\mathcal{H}$. 
The state space of a composite system (for example, a quantum system consisting of many qubits) is the tensor product of the state spaces of its components. For a mixed state \( \rho \) on \( \mathcal{H}_1 \otimes \mathcal{H}_2 \), partial traces of \( \rho \) have explicit physical meanings: the density operators \( \text{tr}_{\mathcal{H}_1} \rho \) and \( \text{tr}_{\mathcal{H}_2} \rho \) are exactly the reduced quantum states of \( \rho \) on the second and the first component system, respectively. Note that in general, the state of a composite system cannot be decomposed into tensor product of the reduced states on its component systems. A well-known example is the 2-qubit state

\[
|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)
\]

which appears repeatedly in our examples of this paper. This kind of state is called **entangled state**. To see the strangeness of entanglement, suppose a measurement \( M = \lambda_0 |0\rangle \langle 0| + \lambda_1 |1\rangle \langle 1| \) is applied on the first qubit of \( |\Psi\rangle \) (see the following for the definition of quantum measurements). Then after the measurement, the second qubit will definitely collapse into state \(|0\rangle\) or \(|1\rangle\) depending on whether the outcome \( \lambda_0 \) or \( \lambda_1 \) is observed. In other words, the measurement on the first qubit changes the state of the second qubit in some way. This is an outstanding feature of quantum mechanics which has no counterpart in classical world, and is the key to many quantum information processing tasks such as teleportation [5] and superdense coding [6].

The evolution of a closed quantum system is described by a unitary operator on its state space: if the states of the system at times \( t_1 \) and \( t_2 \) are \( \rho_1 \) and \( \rho_2 \), respectively, then \( \rho_2 = U \rho_1 U^\dagger \) for some unitary operator \( U \) which depends only on \( t_1 \) and \( t_2 \). In contrast, the general dynamics which can occur in a physical system is described by a trace-preserving super-operator on its state space. Note that the unitary transformation \( U(\rho) = U \rho U^\dagger \) is a super-operator.

A quantum **measurement** is described by a collection \( \{M_m\} \) of measurement operators, where the indices \( m \) refer to the measurement outcomes. It is required that the measurement operators satisfy the completeness equation \( \sum_m M_m^\dagger M_m = 1_H \). If the system is in state \( \rho \), then the probability that measurement result \( m \) occurs is given by

\[
p(m) = \text{tr}(M_m^\dagger M_m \rho),
\]

and the state of the post-measurement system is \( M_m \rho M_m^\dagger / p(m) \).

A particular case of measurement is **projective measurement** which is usually represented by a Hermitian operator. Let \( M \) be a Hermitian operator and

\[
M = \sum_{m \in \text{spec}(M)} m E_m
\]

its spectral decomposition. Obviously, the projectors \( \{E_m : m \in \text{spec}(M)\} \) form a quantum measurement. If the state of a quantum system is \( \rho \), then the probability that result \( m \) occurs when measuring \( M \) on the system is \( p(m) = \text{tr}(E_m \rho) \), and the post-measurement state of the system is \( E_m \rho E_m / p(m) \). Note that for each outcome \( m \), the map

\[
E_m(\rho) = E_m \rho E_m
\]
is again a super-operator by Kraus Theorem.

7.3 Proof of Theorem 1

This section is devoted to the proof of Theorem 1. We first recall some basic results from linear algebra. Let $M$ be a squared matrix and $M = SJS^{-1}$ its Jordan decomposition where $S$ is a nonsingular matrix,

$$J = \text{diag}(J_{n_1}(\lambda_1), J_{n_2}(\lambda_2), \ldots, J_{n_k}(\lambda_k)),$$

and each $J_{n_i}(\lambda_i)$ is a $n_i \times n_i$-Jordan block with the eigenvalue $\lambda_i$. Let $\tilde{M} = S\tilde{J}S^{-1}$ where $\tilde{J}$ is obtained from $J$ by replacing each Jordan block whose associated eigenvalue has absolute value greater than or equal to 1 with the zero block of the same size; that is $\tilde{J} = \text{diag}(J^1, J^2, \ldots, J^k)$ where

$$J^i = \begin{cases} 0_{n_i \times n_i}, & \text{if } |\lambda_i| \geq 1; \\ J_{n_i}(\lambda_i), & \text{otherwise.} \end{cases}$$

Lemma 5. If $\sum_{m=0}^{\infty} NM^m$ exists, then for each $m \geq 0$, $NM^m = N\tilde{M}^m$.

Proof. Suppose $\sum_{m=0}^{\infty} NM^m$ exists. Then $\lim_{m \to \infty} NM^m = 0$. Since $M^m = S\tilde{J}^m S^{-1}$, we have $\lim_{m \to \infty} NS\tilde{J}^m = 0$. Decompose the columns of $NS$ according to the blocks of $J$ as $NS = (K_1, \ldots, K_k)$. Then

$$NS\tilde{J}^m = (K_1 J_{n_1}^m(\lambda_1), \ldots, K_k J_{n_k}^m(\lambda_k)),$$

which implies that for each $i$, $\lim_{m \to \infty} K_i J_{n_i}^m(\lambda_i) = 0$. Let $\| \cdot \|$ be an (arbitrary) matrix norm. We have

$$0 = \lim_{m \to \infty} \| K_i J_{n_i}^m(\lambda_i) \| \\
= \lim_{m \to \infty} \| K_i \| \cdot \| J_{n_i}(\lambda_i) \|^m \\
\geq \lim_{m \to \infty} \| K_i \| \cdot |\lambda_i|^m$$

where the last inequality is from Theorem 5.6.9 of [16]. From this we deduce that $K_i = 0$ for each $i$ whenever $|\lambda_i| \geq 1$. Thus $NS\tilde{J}^m = NSJ^m$, and $NM^m = N\tilde{M}^m$.

Corollary 1. For any matrices $N$ and $M$,

$$\sum_{m=0}^{\infty} NM^m = N(I - M)^{-1}$$

provided that the limit exists.

Proof. Observe that by definition, the spectral radius of $\tilde{M}$ is strictly less than 1. Then from Corollary 5.6.16 of [16], $I - M = 0.5$ is invertible, and $(I - M)^{-1} = \sum_{m=0}^{\infty} M^m$. The result thus follows from Lemma 5.
We also need a notion of matrix representation for super-operators, which was first introduced in [29]. To do this, we fix an orthonormal basis \( \{ |k\rangle : k \in K \} \) of \( \mathcal{H} \).

**Definition 6.** Let \( \mathcal{E} = \{ E_i : i \in I \} \in SO(\mathcal{H}) \) be a super-operator. The matrix representation of \( \mathcal{E} \) is defined as

\[
M_{\mathcal{E}} = \sum_{i \in I} E_i \otimes E_i^*.
\]

Here the complex conjugate is taken according to the orthonormal basis \( \{ |k\rangle : k \in K \} \).

It is easy to check that \( M_{\mathcal{E}} \) is independent of the choice of orthonormal basis and the Kraus operators \( E_i \).

Furthermore, we can define the matrix representation for a matrix of super-operators. Let \( T = (E_{i,j}) \) be an \( m \times n \)-matrix of super-operators. Then the matrix representation of \( T \), denoted \( M_T \), is defined as the block matrix

\[
M_T = \begin{pmatrix}
M_{E_{1,1}} & \cdots & M_{E_{1,n}} \\
\vdots & \ddots & \vdots \\
M_{E_{m,1}} & \cdots & M_{E_{m,n}}
\end{pmatrix}
\]

where for each \( i \) and \( j \), \( M_{E_{i,j}} \) is the matrix representation of \( E_{i,j} \). In particular, let \( \mathcal{E} = (E_1, \ldots, E_n) \) be a (row) vector of super-operators. Then \( M_\mathcal{E} = (M_{E_1}, \ldots, M_{E_n}) \). We always denote by \( M_X \) the matrix representation of \( X \), whenever \( X \) is a super-operator, a vector of super-operators, or a matrix of super-operators.

Let \( |\Psi\rangle = \sum_{k \in K} |kk\rangle \) be a (un-normalised) maximally entangled state in \( \mathcal{H} \otimes \mathcal{H} \). The next lemma is from [29].

**Lemma 6.** Let \( M_\mathcal{E} \) be the matrix representation of \( \mathcal{E} \in SO(\mathcal{H}) \). Then for any \( E \in L(\mathcal{H}) \), we have

\[
(E(\mathcal{H} \otimes I_\mathcal{H})|\Psi\rangle = M_\mathcal{E}(E \otimes I_\mathcal{H})|\Psi\rangle.
\]

Let \( \mathcal{E} = \{ E_i : i \in I \} \) be a super-operator on \( \mathcal{H} \). Then for any \( k, l \in K \),

\[
\langle k | \left( \sum_{i \in I} E_i^\dagger E_i \right) | l \rangle = \text{tr} \left( \sum_{i \in I} E_i |l\rangle \langle k| E_i^\dagger \right) = \text{tr}[\mathcal{E}(|l\rangle \langle k|)] = \langle \Psi | \mathcal{E}(|l\rangle \langle k|) \otimes I_\mathcal{H} |\Psi\rangle = \langle \Psi | M_\mathcal{E}(|l\rangle \langle k|) \otimes I_\mathcal{H} |\Psi\rangle = \langle \Psi | M_\mathcal{E} |l\rangle \langle k|).
\]

Note that for an operator \( E \in L(\mathcal{H}) \), \( \langle k|E|l\rangle \) is exactly the \((k,l)-th\) element of the matrix representation of \( E \) under the basis \( \{ |k\rangle : k \in K \} \). Lemma 6 indeed provides us an efficient way to determine whether or not \( \mathcal{E} \preceq \mathcal{F} \) when the matrix representations of \( \mathcal{E} \) and \( \mathcal{F} \) are given.
Input: (1) An \( n \times n \) matrix \( T = (T_{i,j}) \) and a \( 1 \times n \) vector \( \tilde{G} \) of super-operators such that for each \( j \), \( \sum_i T_{i,j} + \tilde{G}_j \lesssim I_H \).
(2) A super-operator \( E \in S\mathcal{I}(H) \) and \( i \) such that \( 1 \leq i \leq n \).

Output: ‘yes’ if \( E \sim \tilde{E}^0_i \) and ‘no’ otherwise, where \( \tilde{E}^0 \) is the least fixed point of Eq.(1).

1. Construct \( M_{\tilde{G}} \) and \( M_T \) from \( \tilde{G} \) and \( T \), respectively;
2. Calculate the Jordan decomposition \( M_T = SJS^{-1} \);
3. Compute \( M_{\tilde{E}} = M_{\tilde{G}}S(I - \tilde{J})^{-1}S^{-1} \);
4. Use the method described in Eq.(4) to determine if \( \tilde{E} \sim \tilde{E}^0_i \), and output the result.

**Table 4. Algorithm for Theorem 1.**

**Proof of Theorem 1.** We now turn to the proof of Theorem 1. For the first part, we check that \( f(X) \) indeed maps \( SI(H)^n \) into \( SI(H)^n \). Let \( \tilde{E} \in SI(H)^n \) and \( \tilde{F} = f(\tilde{E}) \). Then for each \( j \),
\[
\tilde{F}_j = \sum_{i=1}^n \tilde{E}_i T_{i,j} + \tilde{G}_j \lesssim \sum_{i=1}^n T_{i,j} + \tilde{G}_j \lesssim I_H
\]
where the first inequality is from Lemma 2 and the fact that \( \tilde{E}_i \lesssim I_H \). Note that the function \( f \) defined in Eq.(1) is Scott continuous with respect to the partial order \( \sqsubseteq \). Then by Lemma 3 and Kleene fixed point theorem, \( f(X) \) has a (unique) least fixed point which can be written as
\[
\tilde{E}^0 = \sum_{m=0}^{\infty} \tilde{G}T^m.
\]

For the second part of Theorem 1, we first prove that the matrix representation of \( \tilde{E}^0 \) is
\[
M_{\tilde{F}} = M_{\tilde{G}}(I - \tilde{M}_T)^{-1}.
\] (5)
For any \( 1 \leq i \leq n \) and \( E_i \in \mathcal{L}(H) \), we calculate from Lemma 6 that
\[
M_{\tilde{F}}(E_i \otimes I_H)|\Psi\rangle = \tilde{E}^0_i(E_i \otimes I_H)|\Psi\rangle
= \sum_{m=0}^{\infty} \sum_{k_1, \ldots, k_m=1} \tilde{G}_{k_1} T_{k_1,k_2} \cdots T_{k_m,i}(E_i \otimes I_H)|\Psi\rangle
= \sum_{m=0}^{\infty} \sum_{k_1, \ldots, k_m=1} (M_{\tilde{G}_{k_1}} M_{T_{k_1,k_2}} \cdots M_{T_{k_m,i}})(E_i \otimes I_H)|\Psi\rangle
= \sum_{m=0}^{\infty} (M_{\tilde{G}M_{T}^m})_i(E_i \otimes I_H)|\Psi\rangle
\]
where \((M_2M^n_m)_i\) is the \(i\)th block of \(M_2M^n_m\) at the corresponding position of \(M_\tilde{E}_0^i\) in \(\tilde{M}_E\). Note that when \(E_i\) ranges over \(\mathcal{L}(\mathcal{H})\), the state \((E_i \otimes I_\mathcal{H})|\Psi\rangle\) ranges over all pure state in \(\mathcal{H} \otimes \mathcal{H}\). The above equations indeed imply that 
\[M_\tilde{E}_0^i = \sum_{m=0}^{\infty} (M_2M^n_m)_i,\]
and thus \(M_\tilde{E}_0 = \sum_{m=0}^{\infty} M_2M^n_m\). Then Eq.(5) follows from Corollary 1.

An algorithm which determines for any \(\tilde{E} \in SI(\mathcal{H})\) and \(1 \leq i \leq n\) if \(\tilde{E} \sim \tilde{E}_i^0\) can be sketched as in Table 4. It is easy to see that the time complexity of steps (1) through (4) is \(cn^2\), where the constant \(c\) is of the order \(d^4\), and \(d\) is the dimension of the Hilbert space \(\mathcal{H}\).

7.4 Proof of Theorem 2

Basic results for vector measures. We review some necessary definitions and results of vector measures. For more details, please refer to [10].

Let \(\Omega\) be a non-empty set. Recall that a semi-algebra \(S\) on \(\Omega\) is a subset of the power set \(2^\Omega\) with the following properties:

1. \(\emptyset \in S\);
2. \(A, B \in S\) implies \(A \cap B \in S\);
3. \(A, B \in S\) implies that \(A \setminus B = \bigsqcup_{i=1}^n A_i\) for some disjoint \(A_1, \ldots, A_n \in S\).

An algebra is a semi-algebra which is further closed under union and subtraction; a \(\sigma\)-algebra is an algebra which is also closed under complement and countably union. Given a semi-algebra \(S\), we denote by \(R(S)\) (resp. \(\sigma(S)\)) the algebra (resp. \(\sigma\)-algebra) generated by \(S\); that is, the intersection of all algebras (resp. \(\sigma\)-algebras) which contain \(S\) as a subset. Obviously, \(\sigma(S) = \sigma(R(S))\).

Recall also that a Banach space is a complete normed vector space.

**Definition 7.** Let \(T \subseteq 2^\Omega\), and \(\Delta\) a function from \(T\) to a Banach space \(B\). We call \(\Delta\) a countably additive vector measure, or vector measure for simplicity, if for any sequence \((A_i)_{i \geq 1}\) of pairwise disjoint members of \(T\) such that \(\bigsqcup_{i=1}^\infty A_i \in T\), it holds that
\[\Delta\left(\bigsqcup_{i=1}^\infty A_i\right) = \sum_{i=1}^\infty \Delta(A_i).\]

**Definition 8.** Let \(\mathcal{R}\) be an algebra on \(\Omega\) and \(\Delta : \mathcal{R} \rightarrow B\) a vector measure. Let \(\mu\) be a finite nonnegative real-valued measure on \(\mathcal{R}\). Then \(\Delta\) is said to be \(\mu\)-continuous if
\[\lim_{\mu(A) \rightarrow 0} \Delta(A) = 0.\]

The next theorem from [10] is the key to prove Theorem 2.

**Theorem 3.** [Carathéodory-Hahn-Kluvanek Extension Theorem] Let \(\mathcal{R}\) be an algebra on \(\Omega\) and \(\Delta : \mathcal{R} \rightarrow B\) a bounded vector measure. If there exists a finite and nonnegative real-valued measure \(\mu\) on \(\mathcal{R}\) such that \(\Delta\) is \(\mu\)-continuous, then \(\Delta\) can be uniquely extended to a vector measure \(\Delta' : \sigma(\mathcal{R}) \rightarrow B\) on the \(\sigma\)-algebra generated by \(\mathcal{R}\) such that
\[\Delta'(A) = \Delta(A)\] for any \(A \in \mathcal{R}\).
Banach space of Hermitian-preserving mappings. Suppose $\mathcal{H}$ is a Hilbert space. Let $\mathcal{HP}(\mathcal{H})$ be the set of Hermitian-preserving linear mapping on $\mathcal{L}(\mathcal{H})$; that is

$$\mathcal{HP}(\mathcal{H}) = \{ \mathcal{E} \in \mathcal{L}(\mathcal{L}(\mathcal{H})) \mid \mathcal{E}(E) \text{ is Hermitian provided that } E \text{ is Hermitian} \}.$$  

It is easy to show that $\mathcal{E}$ is Hermitian-preserving if and only if for any $E \in \mathcal{L}(\mathcal{H})$, $\mathcal{E}(E^\dagger) = \mathcal{E}(E)^\dagger$. Obviously, $(\mathcal{HP}(\mathcal{H}), +, \circ)$ forms a ring, and the orders $\subseteq$ and $\subseteq$ defined in Definition 1 can be lifted to $\mathcal{HP}(\mathcal{H})$. We denote by $\mathcal{HP}_0(\mathcal{H})$ the quotient set of $\mathcal{HP}(\mathcal{H})$ by $\sim$, and $[\mathcal{E}] \in \mathcal{HP}_0(\mathcal{H})$ the equivalent class of $\mathcal{E} \in \mathcal{HP}(\mathcal{H})$. Note that although the quotient set $\mathcal{HP}_0(\mathcal{H})$ is again an Abelian group with respect to the addition $+$, by defining $[\mathcal{E}] + [\mathcal{F}] = [\mathcal{E} + \mathcal{F}]$, the composition $\circ$ is not even well defined in $\mathcal{HP}_0(\mathcal{H})$: Let $\mathcal{E} = \{\sigma_i\}$ be the Pauli-X super-operator, and $\mathcal{G} = [(0)(0)]$. Then $[\mathcal{E}] = [\mathcal{I}_\mathcal{H}]$, but $\mathcal{GE} \neq \mathcal{GI}_\mathcal{H}$ since $\text{tr}(\mathcal{GE}(0)(0)]) = 0$ while $\text{tr}(\mathcal{G}\mathcal{I}_\mathcal{H}(0)(0)]) = 1$.

We further extend the pre-order $\lessgtr$ to the quotient set $\mathcal{HP}_0(\mathcal{H})$ by letting $[\mathcal{E}] \lessgtr [\mathcal{F}]$ if $\mathcal{E} \lesssim \mathcal{F}$. It is easy to check that this definition is well defined, and $\lesssim$ becomes a partial order in $\mathcal{HP}_0(\mathcal{H})$.

Lemma 7. Let $\| \cdot \|$ be an arbitrary operator norm. Then the quotient set $(\mathcal{HP}_0(\mathcal{H}), \| \cdot \|)$ is again a Banach space, where the norm $\| \cdot \|$ is defined by

$$\| [\mathcal{E}] \| = \inf_{\mathcal{F} \in [\mathcal{E}]} \| \mathcal{F} \|.$$  

Proof. Note that $\mathcal{HP}(\mathcal{H})$ is a finite dimensional vector space over the field of real numbers. Thus $(\mathcal{HP}, \| \cdot \|)$ is a Banach space, and so is the quotient space $(\mathcal{HP}_0(\mathcal{H}), \| \cdot \|)$.

Proof of Theorem 2. We are now ready to prove Theorem 2. To do this, we first note that any super-operator is a Hermitian-preserving mapping; that is $\mathcal{SO}(\mathcal{H}) \subseteq \mathcal{HP}(\mathcal{H})$. So we can regard the mapping $Q_\star$ defined in Eq.(2) as from $\mathcal{SM}(s)$ to $\mathcal{HP}(\mathcal{H})$. Let $Q_\star'$ be a mapping from $\mathcal{SM}(s)$ to $\mathcal{HP}_0(\mathcal{H})$ such that for any $A \in \mathcal{SM}(s)$,

$$Q_\star'(A) = [Q_\star(A)].$$  

Then we have the following lemmas.

Lemma 8. The mapping $Q_\star'$ defined above is a bounded vector measure over $\mathcal{SM}(s)$.

Proof. We only need to check that $Q_\star'$ is countably additive. Let $\emptyset \neq A = \bigsqcup_{i \geq 1} A_i$ for a disjoint sequence $(A_i)_{i \geq 1}$ in $\mathcal{SM}(s)$ and $A \in \mathcal{SM}(s)$. We need to show that

$$Q_\star'(A) = \sum_{i \geq 1} Q_\star'(A_i).$$  

(6)

Without loss of generality, we assume that the sequence $(A_i)$ has been arranged such that all empty sets, if there are any, are put at the tail of the sequence; that is, whenever $A_n \neq \emptyset$ then $A_i \neq \emptyset$ for any $i \leq n$.
We claim that there are only finitely many nonempty sets in the sequence; that is, there exists \( n \) such that \( A_i \neq \emptyset \) if and only if \( i \leq n \). We prove this claim by contradiction. Suppose \( A = \text{Cyl}(\bar{\pi}_0) \), and for each \( i \geq 1 \), \( A_i = \text{Cyl}(\bar{\pi}_i) \) where all \( \bar{\pi}_i \)s are in \( \text{Path}_{fin}^\mathcal{M}(s) \). By the fact that \( (A_i) \) are disjoint, we know that \( \bar{\pi}_i \) cannot be a prefix of \( \bar{\pi}_j \) whenever \( i \neq j \). Let \( \Pi = \{ \bar{\pi}_i : i \geq 1 \} \). For any \( \bar{\pi} \in \text{Path}_{fin}^\mathcal{M}(s) \), let \( \text{Ind}_{\bar{\pi}} = \{ i \geq 1 : \bar{\pi} \text{ is a prefix of } \bar{\pi}_i \} \), and
\[
K = \{ \bar{\pi} \in \text{Path}_{fin}^\mathcal{M}(s) : \text{Ind}_{\bar{\pi}} \text{ is infinite} \}.
\]
Obviously, \( K \cap \Pi = \emptyset \). Note that \( \bar{\pi}_0 \in K \), and for any \( \bar{\pi} \in K \), since
\[
\text{Ind}_{\bar{\pi}} = \bigcup_{t \in S} \text{Ind}_{\bar{\pi} \triangle t},
\]
there exists \( t_{\bar{\pi}} \in S \) such that \( \bar{\pi} \triangle t_{\bar{\pi}} \in K \) again. Thus we can extend \( \bar{\pi}_0 \) to a (infinite) path \( \pi \in \text{Path}^\mathcal{M}(s) \) such that any finite-length prefix \( \bar{\pi} \) of \( \pi \) with \( |\bar{\pi}| \geq |\bar{\pi}_0| \) is not included in \( \Pi \). Thus for any \( i, \pi \notin A_i \), contradicting the fact that \( \pi \in A \).

With the claim in hand, we let \( N = \max\{|\bar{\pi}_i| : 1 \leq i \leq n\} \) and \( \Pi_N = \{ \bar{\pi} \in \Pi : |\bar{\pi}| = N \} \). Obviously, we can partition \( \Pi_N \) into several disjoint subsets such that each one contains exactly \( |S| \) elements with the same \( N - 1 \)-length prefix; that is, there exists a set \( \{ \bar{\pi}_1, \ldots, \bar{\pi}_{I_N} \} \) such that for each \( 1 \leq i \leq I_N \), \( |\bar{\pi}_i| = N - 1 \), and
\[
\Pi_N = \bigcup_{i=1}^{I_N} \Pi^i_N \text{ where } \Pi^i_N = \{ \bar{\pi} \triangle t : t \in S \}.
\]
We delete \( \Pi_N \) from \( \Pi \) and add \( \bar{\pi}_i \), \( 1 \leq i \leq I_N \), into it. Denote by \( \Pi_{\leq N-1} \) the resultant set. Then each element in \( \Pi_{\leq N-1} \) has length less than \( N \), and it is easy to check that
\[
\sum_{\bar{\pi} \in \Pi^i_N} Q(\bar{\pi}) \asymp \sum_{i=1}^{I_N} Q(\bar{\pi}_i), \text{ thus } \sum_{\bar{\pi} \in \Pi} Q(\bar{\pi}) \asymp \sum_{\bar{\pi} \in \Pi_{\leq N-1}} Q(\bar{\pi}).
\]
Proceeding in this way, we can construct a sequence of sets \( \Pi_i, |\bar{\pi}_0| \leq i \leq N \), such that for any \( i, \sum_{\bar{\pi} \in \Pi_i} Q(\bar{\pi}) \approx \sum_{\bar{\pi} \in \Pi_{\leq i-1}} Q(\bar{\pi}) \) where \( \Pi_{\leq N} = \Pi \). Note that \( \Pi_{\leq |\bar{\pi}_0|} = \{ \bar{\pi}_0 \} \). We finally have
\[
\sum_{i \geq 1} Q'_s(A_i) = \sum_{\bar{\pi} \in \Pi} [Q(\bar{\pi})] = [Q(\bar{\pi}_0)] = Q'_s(A).
\]
That completes the proof of the lemma.

**Lemma 9.** The mapping \( Q'_s \) defined above can be extended uniquely to a vector measure, denoted by \( Q'_s \) again, from \( \sigma(\mathcal{S}^\mathcal{M}(s)) \) to \( \mathcal{H}_\infty(\mathcal{H}) \). Furthermore, for any \( A \in \sigma(\mathcal{S}^\mathcal{M}(s)) \),
\[
[0_{\mathcal{H}}] \preceq Q'_s(A) \preceq [\mathcal{I}_{\mathcal{H}}]. \tag{7}
\]
Proof. Let \( \mathcal{R} = \mathcal{R}(\mathcal{M}(s)) \) be the algebra generated by \( \mathcal{M}(s) \). Obviously, we have
\[
\mathcal{R} = \{ A : A = \bigoplus_{i=1}^{n} A_i \text{ for some } n \geq 0, A_i \in \mathcal{M}(s) \}.
\]
We extend the mapping \( Q'_s \) to \( \mathcal{R} \) by defining \( Q'_s(\{A_i\}) = \sum_{i=1}^{n} Q'_s(A_i) \), which turns out to be a bounded vector measure from \( \mathcal{R} \) to \( \mathcal{H} \). Let \( \mu_s \) be a mapping defined as follows:
\[
\begin{align*}
\mu_s(\emptyset) &= 0, \quad \text{and for any } A \in \mathcal{M}(s), \quad \mu_s(A) = \text{tr}(Q(\tilde{\sigma})(\rho_m)) \text{ where } \\
\rho_m &= I_{\dim(\mathcal{H})/\dim(\mathcal{H})} \text{ is the maximally mixed state in } \mathcal{D}(\mathcal{H}); \\
\text{for any disjoint sets } A_1, \ldots, A_n \in \mathcal{M}(s), \quad \mu_s(\{A_i\}) = \sum_{i=1}^{n} \mu_s(A_i).
\end{align*}
\]
Then \( \mu_s \) is indeed a finite and nonnegative real-valued measure on \( \mathcal{R} \), since \( \mu_s(\text{Path}^{M}(s)) = \mu_s(Cyl(\tilde{\sigma})) = \text{tr}(I_{\mathcal{H}}(\rho_m)) = 1 \). Note that for any super-operator \( \mathcal{E} = \{ \mathcal{E}_i : i \in I \} \), \( \text{tr}(\mathcal{E}(\rho_m)) = \sum_{i \in I} \| \mathcal{E}_i \|_2^2 \) where \( \| \cdot \|_2 \) is the Euclidean norm. It follows that if \( \lim_{i \to \infty} \text{tr}(\mathcal{E}_i(\rho_m)) = 0 \), where \( (\mathcal{E}_i)_{i \geq 1} \) is a sequence of super-operators, then \( \lim_{i \to \infty} [\mathcal{E}_i] = [0_H] \). So we have \( \lim_{\mu(A) \to 0} Q'_s(A) = [0_H] \), which means that \( Q'_s \) is \( \mu_s \)-continuous.

Now using Theorem 3, we can extend \( Q'_s \) uniquely to a vector measure \( Q'_s : \sigma(\mathcal{M}(s)) \to \mathcal{H} \). In the following, we show that the extension satisfies Eq.(7). By the additivity of \( Q'_s \), it suffices to show that for any \( A \in \sigma(\mathcal{M}(s)) \), \( [0_H] \preceq Q'_s(A) \); that is, for any \( \rho \in \mathcal{D}(\mathcal{H}) \), \( \text{tr}(Q'_s(A)(\rho)) \geq 0 \). Let \( \mu' : \sigma(\mathcal{M}(s)) \to \mathcal{R} \) be defined as
\[
\forall A \in \sigma(\mathcal{M}(s)) : \mu'_p(A) = \text{tr}(Q'_s(A)(\rho)).
\]
Then obviously, \( \mu'_p \) is an (ordinary) real-valued measure over \( \sigma(\mathcal{M}(s)) \) and its restriction on \( \mathcal{M}(s) \), denoted \( \mu'_p|\mathcal{M}(s) \), is a probabilistic measure. Now from Carathéodory Theorem for probabilistic measures [7], \( \mu'_p|\mathcal{M}(s) \) can be uniquely extended to a probabilistic measure \( \mu'_p \) over \( \sigma(\mathcal{M}(s)) \). Then we have \( \text{tr}(Q'_s(A)(\rho)) = \mu_p(A) = \mu'_p(A) \geq 0 \) by the uniqueness of such extension.

With the two lemmas above, we can easily prove Theorem 2. For any \( A \in \sigma(\mathcal{M}(s)) \), let \( Q_s(A) \) be any super-operator in the equivalent class \( Q'_s(A) \). It is easy to check that such an extension is indeed a SVM, and it is unique up to the equivalence relation \( \approx \).