Journal of Computer and System Sciences 79 (2013) 1181–1198

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Model checking quantum Markov chains

Yuan Feng [a,b,*], Nengkun Yu [a,b], Mingsheng Ying [a,b]

[a] University of Technology, Sydney, Australia
[b] Tsinghua University, China

ARTICLE INFO

Article history:
Received 10 May 2012
Received in revised form 28 November 2012
Accepted 22 April 2013
Available online 25 April 2013

Keywords:
Quantum Markov chains
Quantum protocols
Model checking

ABSTRACT

Although security of quantum cryptography is provable based on principles of quantum mechanics, it can be compromised by flaws in the design of quantum protocols. So, it is indispensable to develop techniques for 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*, especially suited for modelling quantum cryptographic protocols, in which quantum effects are encoded as 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.

1. Introduction

Quantum cryptography, which uses 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, MagiQ Technologies, QuintessenceLabs, and NEC [26]. 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 principles of quantum mechanics. In practice, however, errors which comprise this *absolute* security may still creep in the protocol design level: As quantum mechanics is counter-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. 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 [22]. 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 started to explore the possibility of applying model-checking in the verification of quantum cryptographic protocols. The main obstacle for model checking quantum systems 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.

* Corresponding author at: University of Technology, Sydney, Australia.
E-mail address: Yuan.Feng@uts.edu.au (Y. Feng).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2013.04.002

[13,25] 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. [18,19] to synthesise quantum circuits. By formulating quantum logic synthesis problem via 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. We propose 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. In this way, the state spaces of quantum Markov chains become countable, and often finite. 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 [29] introduced such a measure by letting the σ-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 σ-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 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. In particular, a large part of classical techniques are 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 Appendix A for the convenience of the readers. For more details, we refer to [24].

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 [27]. Prior to our work, there were quite a few different notions of quantum Markov chains [1,8,12,30], 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.

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.

An exogenous quantum computation tree logic has already been proposed in [3], which is very powerful and can express quantum states in a Hilbert space as well as quantum operations performed on them. As a result, it can be used for reasoning about evolution of quantum (software as well as hardware) systems. The QCTL presented in this paper, however, only consider *classical* properties as its atomic propositions. This is in accordance with our notion of quantum Markov chains where the state space is classical. Thus our approach is suitable for model checking the classical aspect of quantum *software* systems. Note that a large part of quantum communication protocols, such as superdense coding [6], BB84 quantum key distribution [4], quantum leader election [28] etc., all aim at achieving some classical tasks. This is not a very serious limitation.

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 $\mathcal{S}(\mathcal{H})$ be the set of super-operators on $\mathcal{H}$, ranged over by $\mathcal{E}, \mathcal{F}, \ldots$. Obviously, both $(\mathcal{S}(\mathcal{H}), 0_{\mathcal{H}}, +)$ and $(\mathcal{S}(\mathcal{H}), \mathcal{I}_{\mathcal{H}}, \circ)$ are monoids, where $\mathcal{I}_{\mathcal{H}}$ and $0_{\mathcal{H}}$ are the identity and null super-operators on $\mathcal{H}$, respectively, and $\circ$ is the composition of super-operators defined by $(\mathcal{E} \circ \mathcal{F})(\rho) = \mathcal{E}(\mathcal{F}(\rho))$ for any $\rho \in \mathcal{D}(\mathcal{H})$ where $\mathcal{D}(\mathcal{H})$ is the set of density

operators on $\mathcal{H}$. We always omit the symbol $\circ$ and write $\mathcal{E}\mathcal{F}$ directly for $\mathcal{E}\circ\mathcal{F}$. Furthermore, the operation $\circ$ is (both left and right) distributive with respect to $+$:

$$\mathcal{E}(\mathcal{F}_1+\mathcal{F}_2)=\mathcal{E}\mathcal{F}_1+\mathcal{E}\mathcal{F}_2,\qquad (\mathcal{F}_1+\mathcal{F}_2)\mathcal{E}=\mathcal{F}_1\mathcal{E}+\mathcal{F}_2\mathcal{E}.$$

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

Definition 2.1. Let $\mathcal{E},\mathcal{F}\in\mathcal{S}(\mathcal{H})$.

(1) $\mathcal{E}\sqsubseteq\mathcal{F}$ if for any $\rho\in\mathcal{D}(\mathcal{H})$, $\mathcal{F}(\rho)-\mathcal{E}(\rho)$ is positive semi-definite;
(2) $\mathcal{E}\lesssim\mathcal{F}$ if for any $\rho\in\mathcal{D}(\mathcal{H})$, $\mathrm{tr}(\mathcal{E}(\rho))\leqslant\mathrm{tr}(\mathcal{F}(\rho))$.

The first order is lifted from Löwner partial order on density operators, whereas the second one is used to compare the ability of 'trace preservation'. Note that the trace of a (unnormalised) quantum state is exactly the probability that the (normalised) state is reached [27]. Intuitively, $\mathcal{E}\lesssim\mathcal{F}$ if and only if the success probability of performing $\mathcal{E}$ is always not greater than that of performing $\mathcal{F}$, whatever the initial state is.

Note that $\sqsubseteq$ is a partial order while $\lesssim$ is a pre-order. Let $\eqsim$ be $\lesssim\cap\gtrsim$; it is obviously an equivalence relation.

Lemma 2.2. *Let $\mathcal{E},\mathcal{F}\in\mathcal{S}(\mathcal{H})$. Then*

(1) *$\mathcal{E}\sqsubseteq\mathcal{F}$ implies $\mathcal{E}\lesssim\mathcal{F}$, while the reverse is not true in general.*
(2) *$\mathcal{E}\lesssim\mathcal{F}$ implies $\mathcal{E}\sqsubseteq\mathcal{F}'$ for some $\mathcal{F}'\eqsim\mathcal{F}$.*

Proof. (1) is obvious. To prove (2), let $\mathcal{E}=\{E_i\colon\ i\in I\}$ and $\mathcal{F}=\{F_j\colon\ j\in J\}$ be the Kraus representation of $\mathcal{E}$ and $\mathcal{F}$, respectively. Then $\mathcal{E}\lesssim\mathcal{F}$ 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 $G=E^\dagger E$ and define the super-operator $\mathcal{G}=\{E\}$. Let $\mathcal{F}'=\mathcal{E}+\mathcal{G}$. Then it is easy to check $\mathcal{F}'\eqsim\mathcal{F}$ and $\mathcal{E}\sqsubseteq\mathcal{F}'$. □

The next lemma shows that the two orders $\lesssim$ and $\sqsubseteq$ are preserved by the right application of composition.

Lemma 2.3. *Let $\mathcal{E},\mathcal{F},\mathcal{G}\in\mathcal{S}(\mathcal{H})$. If $\mathcal{E}\lesssim\mathcal{F}$, then $\mathcal{E}\mathcal{G}\lesssim\mathcal{F}\mathcal{G}$, and if $\mathcal{E}\sqsubseteq\mathcal{F}$, then $\mathcal{E}\mathcal{G}\sqsubseteq\mathcal{F}\mathcal{G}$.*

Let

$$\mathcal{S}^1(\mathcal{H})=\big\{\mathcal{E}\in\mathcal{S}(\mathcal{H})\colon\ \mathcal{E}\lesssim\mathcal{I}_{\mathcal{H}}\big\}.$$

Let $\mathcal{S}^1(\mathcal{H})^n$ be the set of n-size row vectors over $\mathcal{S}^1(\mathcal{H})$, and extend the partial order $\sqsubseteq$ componentwise to it. Then we have

Lemma 2.4. *The set $(\mathcal{S}^1(\mathcal{H})^n,\sqsubseteq)$ is a complete partial order set with the least element $(0_{\mathcal{H}},\ldots,0_{\mathcal{H}})$.*

Proof. The case when $n=1$ is from [27], 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. To make the paper more readable, we present the proof in Appendix A.3.

Theorem 2.5. *Let $\mathcal{T}$ and $\widetilde{\mathcal{G}}$ be two matrices of super-operators with sizes $n\times n$ and $1\times n$, respectively, and for each j, $\sum_i\mathcal{T}_{i,j}+\widetilde{\mathcal{G}}_j\lesssim\mathcal{I}_{\mathcal{H}}$. Let*

$$f(X)=X\mathcal{T}+\widetilde{\mathcal{G}}\tag{1}$$

be a function from $\mathcal{S}(\mathcal{H})^n$ to $\mathcal{S}(\mathcal{H})^n$. Then

(1) *$f(X)$ has the least fixed point, denoted by $\widetilde{\mathcal{E}}$, in $\mathcal{S}^1(\mathcal{H})^n$ with respect to the order $\sqsubseteq$;*
(2) *Given any $\mathcal{E}\in\mathcal{S}^1(\mathcal{H})$ and $1\leqslant i\leqslant n$, it can be decided whether $\mathcal{E}\sim\widetilde{\mathcal{E}}_i$, $\sim\in\{\lesssim,\gtrsim\}$, in time $O(n^2d^4)$ where $d=\dim(\mathcal{H})$ is the dimension of $\mathcal{H}$.*

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 2.6. Let (Ω,Σ) be a measurable space; that is, Ω is a non-empty set and Σ a σ-algebra over Ω. A function $\Delta:\Sigma\to\mathcal{S}^1(\mathcal{H})$ is said to be a super-operator valued measure (SVM for short) if Δ satisfies the following properties:

(1) $\Delta(\Omega) \eqsim \mathcal{I}_{\mathcal{H}}$;
(2) $\Delta(\biguplus_i A_i) \eqsim \sum_i \Delta(A_i)$ for any pairwise disjoint and countable sequence $A_1, A_2, \ldots$ in Ω.

We call the triple (Ω, Σ, Δ) a (super-operator valued) measure space.

We write $A = \biguplus_i A_i$ if $A = \bigcup_i A_i$ and A_is 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 2.7. *Let (Ω, Σ, Δ) be a measure space. Then*

(1) $\Delta(\emptyset) = 0_{\mathcal{H}}$;
(2) $\Delta(A^c) + \Delta(A) \eqsim \mathcal{I}_{\mathcal{H}}$ *where A^c is the complement set of A in Ω*;
(3) (*monotonicity*) *for any $A, A' \in \Sigma$, if $A \subseteq A'$ then $\Delta(A) \lesssim \Delta(A')$*;
(4) (*continuity*) *for any sequence $A_1, A_2, \ldots$ in Σ,*
- *if $A_1 \subseteq A_2 \subseteq \cdots$, then there exists a sequence $\mathcal{E}_1 \sqsubseteq \mathcal{E}_2 \sqsubseteq \cdots$ in $\mathcal{S}^1(\mathcal{H})$ such that for any i, $\Delta(A_i) \eqsim \mathcal{E}_i$, and $\Delta(\bigcup_{i\geqslant 1} A_i) \eqsim \lim_{i\to\infty} \mathcal{E}_i$;*
- *if $A_1 \supseteq A_2 \supseteq \cdots$, then there exists a sequence $\mathcal{E}_1 \sqsupseteq \mathcal{E}_2 \sqsupseteq \cdots$ in $\mathcal{S}^1(\mathcal{H})$ such that for any i, $\Delta(A_i) \eqsim \mathcal{E}_i$, and $\Delta(\bigcap_{i\geqslant 1} A_i) \eqsim \lim_{i\to\infty} \mathcal{E}_i$.*

Proof. We only prove the first item of (4). Suppose $A_1 \subseteq A_2 \subseteq \cdots$. Let $B_n = A_n \setminus \bigcup_{i<n} A_i$, $n = 1, 2, \ldots$. Then each pair B_i and B_j is disjoint provided that $i \neq j$, and for each n, $A_n = \biguplus_{i\leqslant n} B_i$. Let $\mathcal{E}_n = \sum_{i\leqslant n} \Delta(B_i)$. Then $\mathcal{E}_1 \sqsubseteq \mathcal{E}_2 \sqsubseteq \cdots$, and by the additivity of Δ we have $\Delta(A_n) \eqsim \mathcal{E}_n$. Finally,

$$\Delta\left(\bigcup_{i\geqslant 1} A_i\right) = \Delta\left(\biguplus_{i\geqslant 1} B_i\right) \eqsim \sum_{i\geqslant 1} \Delta(B_i) = \lim_{n\to\infty} \mathcal{E}_n.$$

Here the existence of the limit is guaranteed by Lemma 2.4. □

3. Super-operator weighted Markov chains

We now extend classical Markov chains to super-operator weighted ones.

Definition 3.1. A super-operator weighted Markov chain, or quantum Markov chain (qMC), is a tuple $(S, \mathbf{Q}, AP, L)$, where

(1) S is a countable (typically finite) set of states;
(2) $\mathbf{Q}: S \times S \to \mathcal{S}^1(\mathcal{H})$ is called the transition matrix where for each $s \in S$, $\sum_{t\in S} \mathbf{Q}(s,t) \eqsim \mathcal{I}_{\mathcal{H}}$;
(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 in the transition matrix have the form $p\mathcal{I}_{\mathcal{H}}$ for some $0 \leqslant p \leqslant 1$. Let $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ be a quantum Markov chain. A path π of $\mathcal{M}$ is an infinite sequence of states $s_0 s_1 \ldots$ where for all $i \geqslant 0$, $s_i \in S$ and $\mathbf{Q}(s_i, s_{i+1}) \neq 0_{\mathcal{H}}$. A finite path $\hat{\pi}$ is a finite-length prefix of a path, and its length, denoted $|\hat{\pi}|$, is defined to be the number of states in it. We denote by $\pi(i)$ the ith state of a path π, and $\hat{\pi}(i)$ the ith state of a finite path $\hat{\pi}$ if $i < |\hat{\pi}|$. Note that we index the states in a path or finite path from 0. The sets of all infinite and finite paths of $\mathcal{M}$ starting in state s are denoted $Path^{\mathcal{M}}(s)$ and $Path^{\mathcal{M}}_{fin}(s)$, respectively.

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 SVM Q_s for each $s \in S$ as follows. For any finite path $\hat{\pi} = s_0 \ldots s_n \in Path^{\mathcal{M}}_{fin}(s)$, we define the super-operator

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

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

$$Cyl(\hat{\pi}) = \left\{\pi \in Path^{\mathcal{M}}(s) \colon \hat{\pi} \text{ is a prefix of } \pi\right\};$$

that is, the set of all infinite paths with prefix $\hat{\pi}$. It is easy to check that the set

$$\mathcal{S}^{\mathcal{M}}(s) = \left\{Cyl(\hat{\pi}) \colon \hat{\pi} \in Path^{\mathcal{M}}_{fin}(s)\right\} \cup \{\emptyset\}$$

is a semi-algebra on $Path^{\mathcal{M}}(s)$. Let a mapping Q_s from $\mathcal{S}^{\mathcal{M}}(s)$ to $\mathcal{S}^1(\mathcal{H})$ be defined by letting $Q_s(\emptyset) = 0_{\mathcal{H}}$ and

$$Q_s\big(Cyl(\hat{\pi})\big) = \mathbf{Q}(\hat{\pi}). \tag{2}$$

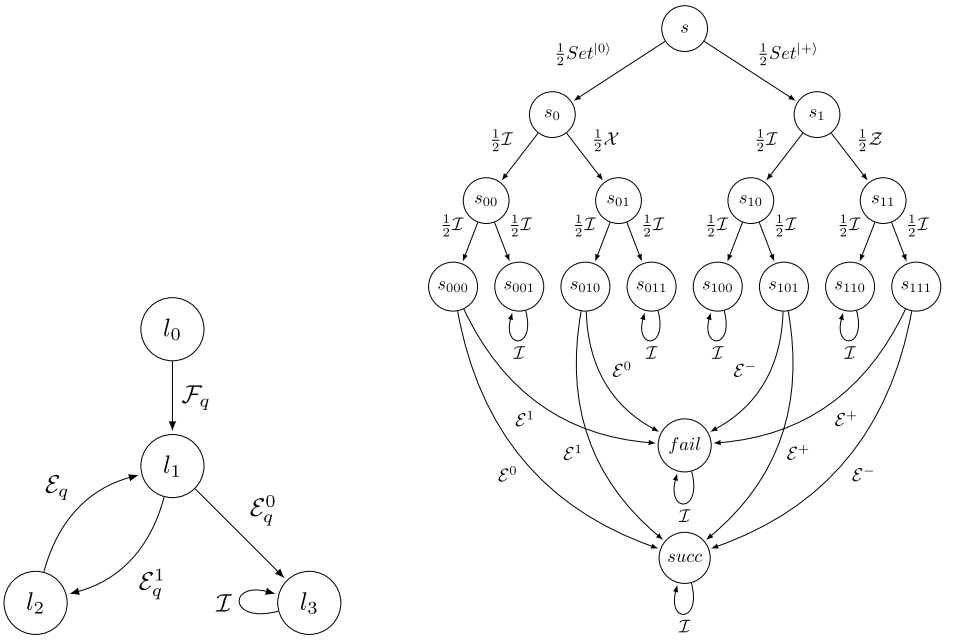

Fig. 1. qMCs for a quantum loop program (left) and BB84 protocol when $n = 1$ (right).

The following theorem states that we can extend the mapping Q_s defined above to a super-operator valued measure on the σ-algebra of infinite paths generated by cylinder extensions of finite paths, similar to Vardi's work for classical Markov chains [29]. The main tool we use here is Kluvanek's generalisation of the Carathéodory–Hahn extension theorem from vector measure theory [10]. We defer the detailed proof to Appendix A.4 for the sake of readability.

Theorem 3.2. *The mapping Q_s defined above can be extended to a SVM, denoted by Q_s again, on the σ-algebra generated by $\mathcal{S}^{\mathcal{M}}(s)$. Furthermore, this extension is unique up to the equivalence relation $\approx$.*

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

Example 3.3 *(Quantum loop programs).* A simple quantum loop program goes as follows:

l_0: $q := \mathcal{F}(q)$

l_1: **while** $M[q]$ **do**

l_2: $q := \mathcal{E}(q)$

l_3: **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 λ_0 is observed, then the program terminates at line l_3; 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 $S = \{l_i\colon\ 0 \leqslant i \leqslant 3\}$, $AP = S$, $L(l_i) = \{l_i\}$ for each i, and $\mathbf{Q}$ be defined as $\mathbf{Q}(l_0, l_1) = \mathcal{F}_q$, $\mathbf{Q}(l_1, l_3) = \mathcal{E}_q^0 = \{|0\rangle_q\langle 0|\}$, $\mathbf{Q}(l_1, l_2) = \mathcal{E}_q^1 = \{|1\rangle_q\langle 1|\}$, $\mathbf{Q}(l_2, l_1) = \mathcal{E}_q$, and $\mathbf{Q}(l_3, l_3) = \mathcal{I}_{\mathcal{H}}$. The qMC is depicted in Fig. 1 (left). Let $\hat{\pi} = l_0 l_1 l_2 l_1 l_2 l_1 l_3$ be a finite path from l_0. Then

$$\mathbf{Q}(\hat{\pi}) = \mathbf{Q}(l_1, l_3)\mathbf{Q}(l_2, l_1)\mathbf{Q}(l_1, l_2)\mathbf{Q}(l_2, l_1)\mathbf{Q}(l_1, l_2)\mathbf{Q}(l_0, l_1) = \mathcal{E}_q^0\mathcal{E}_q\mathcal{E}_q^1\mathcal{E}_q\mathcal{E}_q^1\mathcal{F}_q.$$

Example 3.4 *(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 $\widetilde{B}_a$ and $\widetilde{K}_a$, each with size n.
(2) Alice prepares a string of qubits $\tilde{q}$, with size n, such that the ith qubit of $\tilde{q}$ is $|x_y\rangle$ where x and y are the ith bits of $\widetilde{B}_a$ and $\widetilde{K}_a$, respectively, and $|0_0\rangle = |0\rangle$, $|0_1\rangle = |1\rangle$, $|1_0\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|1_1\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

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

After the execution of the basic BB84 protocol above, the remaining bits of $\widetilde{K}_a$ and $\widetilde{K}_b$ 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 (right), where $Set^{|\psi\rangle}$ 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-Z 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 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_0, $B_a = 0$; in s_{01}, $B_a = 0$ and $K_a = 1$; and in s_{101}, $B_a = B_b = 1$ and $K_a = 0$. Let $AP = S \cup \{abort\}$ and $L(s) = \{abort\}$ if $s \in \{s_{001}, s_{011}, s_{100}, s_{110}\}$, meaning that at these states Alice and Bob's bases differ, so the protocol will be aborted without generating any key. For other states s, we let $L(s) = \{s\}$ naturally.

We use the states *succ* and *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 $\{|+\rangle, |-\rangle\}$ at s_{101}, they will regard the key bit 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 $\mathbf{Q}(s_{101}, succ) = \mathcal{E}^+$ while $\mathbf{Q}(s_{101}, fail) = \mathcal{E}^-$.

4. Quantum computation tree logic (QCTL)

This section is devoted to a quantum extension of the probabilistic computation tree logic (PCTL) [16], which in turn is an extension of the classical computation tree logic (CTL) [11].

Definition 4.1. The syntax of quantum computation tree logic (QCTL) is as follows:

$$\Phi ::= a \mid \neg\Phi \mid \Phi \wedge \Phi \mid \mathbb{Q}_{\sim\mathcal{E}}[\phi],$$
$$\phi ::= \mathbf{X}\Phi \mid \Phi\mathbf{U}^{\leqslant k}\Phi \mid \Phi\mathbf{U}\Phi$$

where $a \in AP$ is an atomic proposition, $\sim \in \{\lesssim, \gtrsim\}$, $\mathcal{E} \in \mathcal{S}^1(\mathcal{H})$, and $k \in \mathbb{N}$. We call Φ a *state formula* and ϕ 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 $\mathbb{P}_{\sim p}[\phi]$ in PCTL, which asserts that the probability of paths from a certain state satisfying the path formula ϕ is constrained by $\sim p$ where $0 \leqslant p \leqslant 1$, is replaced in QCTL by $\mathbb{Q}_{\sim\mathcal{E}}[\phi]$, which asserts that the accumulated super-operators corresponding to paths from a certain state satisfying the formula ϕ is constrained by $\sim\mathcal{E}$ where $0_{\mathcal{H}} \lesssim \mathcal{E} \lesssim \mathcal{I}_{\mathcal{H}}$. Note that $\mathbb{P}_{\sim p}[\phi]$ is a special case of $\mathbb{Q}_{\sim\mathcal{E}}[\phi]$ by taking $\mathcal{E} = p\mathcal{I}_{\mathcal{H}}$.

Definition 4.2. Let $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ be a quantum Markov chain. For any state $s \in S$, the satisfaction relation $\models$ is defined inductively by

$$\begin{aligned}
&s \models a && \text{if } a \in L(s),\\
&s \models \neg\Phi && \text{if } s \not\models \Phi,\\
&s \models \Phi \wedge \Psi && \text{if } s \models \Phi \text{ and } s \models \Psi,\\
&s \models \mathbb{Q}_{\sim\mathcal{E}}[\phi] && \text{if } Q^{\mathcal{M}}(s, \phi) \sim \mathcal{E}
\end{aligned}$$

where

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

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

$$\pi \models \mathbf{X}\Phi \qquad \text{if } \pi(1) \models \Phi,$$
$$\pi \models \Phi \mathbf{U}^{\leqslant k} \Psi \quad \text{if } \exists i \in \mathbb{N}.\big(i \leqslant k \wedge \pi(i) \models \Psi \wedge \forall j < i.\big(\pi(j) \models \Phi\big)\big),$$
$$\pi \models \Phi \mathbf{U} \Psi \qquad \text{if } \exists i \in \mathbb{N}.\big(\pi(i) \models \Psi \wedge \forall j < i.\big(\pi(j) \models \Phi\big)\big).$$

Similarly to PCTL, we can check that for each path formula ϕ and each state s in a qMC $\mathcal{M}$, the set $\{\pi \in Path^{\mathcal{M}}(s) \mid \pi \models \phi\}$ is in the σ-algebra generated by $\mathcal{S}^{\mathcal{M}}(s)$. As usual, we introduce some syntactic sugars to simplify notations: the disjunction $\Psi_1 \vee \Psi_2 \equiv \neg(\neg\Psi_1 \wedge \neg\Psi_2)$, the tautology $\mathtt{tt} \equiv a \vee \neg a$, the eventually operator $\Diamond\Psi \equiv \mathtt{tt}\mathbf{U}\Psi$, and the step-bounded eventually operator $\Diamond^{\leqslant k}\Psi \equiv \mathtt{tt}\mathbf{U}^{\leqslant k}\Psi$.

Example 4.3. We revisit the examples in the previous section, to show the expressive power of QCTL.

(1) Example 3.3. The QCTL formula $\mathbb{Q}_{\gtrsim \mathcal{E}}[\Diamond^{\leqslant k} l_3]$ asserts that the probability that the loop program in Example 3.3 terminates within k iterations is lower bounded by $\mathcal{E}$. That is, for any initial quantum state ρ, the termination probability is not less than $\mathrm{tr}(\mathcal{E}(\rho))$. In particular, the property that it terminates everywhere can be described as $\mathbb{Q}_{\gtrsim \mathcal{I}_{\mathcal{H}}}[\Diamond l_3]$.

(2) Example 3.4. The correctness of basic BB84 protocol can be stated as

$$s \models \mathbb{Q}_{\lesssim 0_{\mathcal{H}}}[\Diamond \mathit{fail}] \wedge \mathbb{Q}_{\gtrsim \frac{1}{2}\mathcal{I}}\big[\Diamond^{\leqslant 4}\, \mathit{succ}\big],$$

which asserts that the protocol never (with probability 0) fails, and with probability at least one half, it will successfully terminate at a shared key within 4 steps. As there is only a half chance for Bob to correctly guess Alice's basis, the probability of successfully establishing a key cannot exceed 1/2.

5. Model checking quantum Markov chains

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

$$Sat(a) = \big\{s \in S\colon\ a \in L(s)\big\},$$
$$Sat(\neg\Psi) = S \backslash Sat(\Psi),$$
$$Sat(\Psi \wedge \Phi) = Sat(\Psi) \cap Sat(\Phi),$$
$$Sat\big(\mathbb{Q}_{\sim\mathcal{E}}[\phi]\big) = \big\{s \in S\colon\ Q^{\mathcal{M}}(s,\phi) \sim \mathcal{E}\big\}.$$

Most of the formulae above are the same as in probabilistic model checking. The only difference is $Sat(\mathbb{Q}_{\sim\mathcal{E}}[\phi])$. In the following, we will elaborate how to employ the results presented in the previous sections to calculate the satisfaction sets for such a kind of formulae. To this end, we need to compute $Q^{\mathcal{M}}(s,\phi)$ for the following three cases.[1]

Case 1: $\phi = \mathbf{X}\Phi$. By Definition 4.2, $\{\pi \in Path^{\mathcal{M}}(s)\colon\ \pi \models \mathbf{X}\Phi\} = \biguplus_{t \in Sat(\Phi)} Cyl(st)$. Thus

$$Q^{\mathcal{M}}(s, \mathbf{X}\Phi) = Q_s\Big(\biguplus_{t \in Sat(\Phi)} Cyl(st)\Big) \eqsim \sum_{t \in Sat(\Phi)} Q_s\big(Cyl(st)\big) = \sum_{t \in Sat(\Phi)} \mathbf{Q}(s,t).$$

This can be calculated easily since by the recursive nature of the definition, we can assume that $Sat(\Phi)$ is already known.

Case 2: $\phi = \Phi\mathbf{U}^{\leqslant k}\Psi$. For any $s \in S$ and $k \geqslant 0$, we let $\Pi_s^k = \{\pi \in Path^{\mathcal{M}}(s)\colon\ \pi \models \Phi\mathbf{U}^{\leqslant k}\Psi\}$. Then

$$\Pi_s^k = \begin{cases} Cyl(s), & \text{if } s \in Sat(\Psi); \\ \emptyset, & \text{if } s \notin Sat(\Phi) \cup Sat(\Psi) \vee (k = 0 \wedge s \notin Sat(\Psi)); \\ \biguplus_{t \in post(s)} s^\frown \Pi_t^{k-1}, & \text{if } s \in Sat(\Phi) \backslash Sat(\Psi) \wedge k \geqslant 1, \end{cases}$$

where $post(s) = \{t \in S\colon\ \mathbf{Q}(s,t) \neq 0_{\mathcal{H}}\}$, and $s^\frown \Pi_t^{k-1}$ denotes the set of strings obtained by prepending s to strings in Π_t^{k-1}. By induction on k, we can show that for each k and s, $\Pi_s^k = \emptyset$ or it is the disjoint union of some cylinder sets; specifically, we have $\Pi_s^k = \biguplus_{\hat{\pi} \in A_s^k} Cyl(\hat{\pi})$ where

$$A_s^k = \begin{cases} \{s\}, & \text{if } s \in Sat(\Psi); \\ \emptyset, & \text{if } s \notin Sat(\Phi) \cup Sat(\Psi) \vee (k = 0 \wedge s \notin Sat(\Psi)); \\ \biguplus_{t \in post(s)} s^\frown A_t^{k-1}, & \text{if } s \in Sat(\Phi) \backslash Sat(\Psi) \wedge k \geqslant 1. \end{cases}$$

[1] Strictly speaking, we are computing a super-operator which is $\eqsim$-equivalent to $Q^{\mathcal{M}}(s,\phi)$. But this is sufficient for our purpose, as only whether or not $Q^{\mathcal{M}}(s,\phi) \sim \mathcal{E}$ matters here.

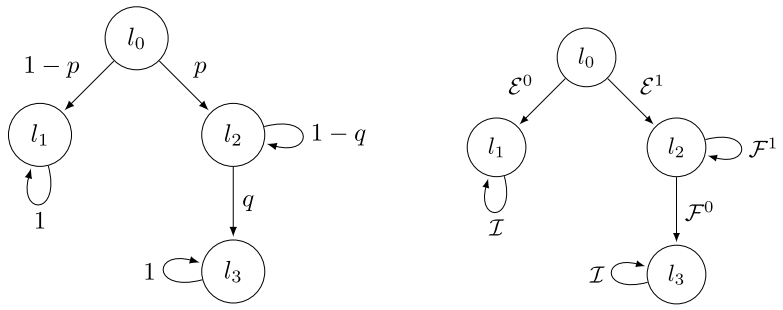

Fig. 2. Difference between pMC and qMC.

Thus if $s \in Sat(\Phi)\backslash Sat(\Psi)$ and $k \geqslant 1$, we have

$$\begin{aligned} Q_s\big(\Pi_s^k\big) &= Q_s\Big(\biguplus_{\hat{\pi}\in A_s^k} Cyl(\hat{\pi})\Big) \eqsim \sum_{\hat{\pi}\in A_s^k} Q_s\big(Cyl(\hat{\pi})\big) \\ &= \sum_{t\in post(s)} \sum_{\hat{\pi}'\in A_t^{k-1}} \mathbf{Q}\big(s^\frown \hat{\pi}'\big) = \sum_{t\in post(s)} \sum_{\hat{\pi}'\in A_t^{k-1}} \mathbf{Q}\big(\hat{\pi}'\big)\mathbf{Q}(s,t) \\ &= \sum_{t\in S} \sum_{\hat{\pi}'\in A_t^{k-1}} Q_t\big(Cyl\big(\hat{\pi}'\big)\big)\mathbf{Q}(s,t) \eqsim \sum_{t\in S} Q_t\big(\Pi_t^{k-1}\big)\mathbf{Q}(s,t). \end{aligned}$$

Adding the other two cases together, we finally have

$$Q^{\mathcal{M}}\big(s, \Phi\mathbf{U}^{\leqslant k}\Psi\big) \eqsim \begin{cases} \mathcal{I}_{\mathcal{H}}, & \text{if } s \in Sat(\Psi); \\ 0_{\mathcal{H}}, & \text{if } s \notin Sat(\Phi)\cup Sat(\Psi) \vee (k=0 \wedge s \notin Sat(\Psi)); \\ \sum_{t\in S} Q^{\mathcal{M}}(t, \Phi\mathbf{U}^{\leqslant k-1}\Psi)\mathbf{Q}(s,t), & \text{if } s \in Sat(\Phi)\backslash Sat(\Psi) \wedge k \geqslant 1. \end{cases}$$

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

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

$$Q^{\mathcal{M}}(s, \Phi\mathbf{U}\Psi) \eqsim \begin{cases} \mathcal{I}_{\mathcal{H}}, & \text{if } s \in Sat(\Psi); \\ 0_{\mathcal{H}}, & \text{if } s \notin Sat(\Phi)\cup Sat(\Psi); \\ \sum_{t\in S} Q^{\mathcal{M}}(t, \Phi\mathbf{U}\Psi)\mathbf{Q}(s,t), & \text{if } s \in Sat(\Phi)\backslash Sat(\Psi). \end{cases}$$

Recall that in probabilistic model checking, to simplify the computation and translate 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 $Sat(\Psi)$ without leaving states in $Sat(\Phi)$ is exactly 0 or 1. However, it is impossible in quantum case to calculate the *exact* set of states s for which $Q^{\mathcal{M}}(s, \Phi\mathbf{U}\Psi)$ is equivalent to $0_{\mathcal{H}}$ or $\mathcal{I}_{\mathcal{H}}$ 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 $Sat(\Psi) = \{l_3\}$ and $Sat(\Phi) = \{l_0, l_2\}$. In the pMC, $P(l_0, \Phi\mathbf{U}\Psi) = 0$ if and only if $p = 0$ or $q = 0$, as $pq = 0$ if and only if $p(1-q)^n q = 0$ for any $n \geqslant 0$. However, in the qMC, things are complicated. First, we cannot claim $Q^{\mathcal{M}}(l_0, \Phi\mathbf{U}\Psi) \neq 0_{\mathcal{H}}$ by only checking that neither $\mathcal{F}^0$ nor $\mathcal{E}^1$ is $0_{\mathcal{H}}$; they can be orthogonal with each other: let $\mathcal{F}^0 = \mathcal{E}^0 = \{|0\rangle\langle 0|\}$, $\mathcal{E}^1 = \mathcal{F}^1 = \{|1\rangle\langle 1|\}$. Then we have $Q^{\mathcal{M}}(l_0, \Phi\mathbf{U}\Psi) \eqsim 0_{\mathcal{H}}$. Conversely, we cannot claim $Q^{\mathcal{M}}(l_0, \Phi\mathbf{U}\Psi) \eqsim 0_{\mathcal{H}}$ by only checking $\mathcal{F}^0\mathcal{E}^1 = 0_{\mathcal{H}}$ either. Let $\mathcal{E}^0$ and $\mathcal{E}^1$ be defined as above but let $\mathcal{F}^0 = \{\frac{1}{\sqrt{2}}|0\rangle\langle 0|\}$ and $\mathcal{F}^1 = \{\frac{1}{\sqrt{2}}|1\rangle\langle 1|, \frac{1}{\sqrt{2}}X\}$ where X is the Pauli-X operator. Then $\mathcal{F}^0\mathcal{F}^1\mathcal{E}^1 \neq 0_{\mathcal{H}}$, thus $Q^{\mathcal{M}}(l_0, \Phi\mathbf{U}\Psi) \neq 0_{\mathcal{H}}$. To sum up, to check if $Q^{\mathcal{M}}(s, \Phi\mathbf{U}\Psi) \eqsim 0_{\mathcal{H}}$, the accumulated super-operators along all possible paths from s to $Sat(\Psi)$ through $Sat(\Phi)$, including all cycles and self-loops, must be considered. This is essentially as difficult as solving the original super-operator equation system in which the state s is involved. Similar argument applies to determining if $Q^{\mathcal{M}}(s, \Phi\mathbf{U}\Psi) \eqsim \mathcal{I}_{\mathcal{H}}$.

We have shown that in general it is not practical to pre-compute the two sets $Sat(\mathbb{Q}_{\lesssim 0_{\mathcal{H}}}[\Phi\mathbf{U}\Psi])$ and $Sat(\mathbb{Q}_{\gtrsim \mathcal{I}_{\mathcal{H}}}[\Phi\mathbf{U}\Psi])$. Nevertheless, we can still simplify the calculation by identifying *some* S^0 and $S^{\mathcal{I}}$ such that

$$S\backslash\big(Sat(\Psi)\cup Sat(\Phi)\big) \subseteq S^0 \subseteq Sat\big(\mathbb{Q}_{\lesssim 0_{\mathcal{H}}}[\Phi\mathbf{U}\Psi]\big)$$

and

$$Sat(\Psi) \subseteq S^{\mathcal{I}} \subseteq Sat\big(\mathbb{Q}_{\gtrsim \mathcal{I}_{\mathcal{H}}}[\Phi\mathbf{U}\Psi]\big),$$

Table 1
Algorithms to calculate S^0 and $S^{\mathcal{I}}$.

Input: $Sat(\Phi)$ and $Sat(\Psi)$ Output: A subset S^0 of S such that $S\backslash Sat(\Psi)\backslash Sat(\Phi) \subseteq S^0 \subseteq Sat(\mathbb{Q}_{\lesssim 0_{\mathcal{H}}}[\Phi \mathbf{U} \Psi])$	Input: $Sat(\Phi)$ and $Sat(\Psi)$ Output: A subset $S^{\mathcal{I}}$ of S such that $Sat(\Psi) \subseteq S^{\mathcal{I}} \subseteq Sat(\mathbb{Q}_{\gtrsim \mathcal{I}_{\mathcal{H}}}[\Phi \mathbf{U} \Psi])$
$R := \{s$: no direct path from s to states in $Sat(\Psi)\}$ $R := R \cup (S\backslash Sat(\Phi)\backslash Sat(\Psi))$ $done :=$ **false** **while** ($done =$ **false**) **do** $R' := R \cup \{s \in S\backslash R$: $\sum_{t \in R} \mathbf{Q}(s,t) + \mathbf{Q}(s,s) \eqsim \mathcal{I}\}$ **if** ($R' = R$) **then** $done :=$ **true** $R := R'$ **od** return R	$R := Sat(\Psi)$ $done :=$ **false** **while** ($done =$ **false**) **do** $R' := R \cup \{s \in Sat(\Phi)\backslash R$: $\sum_{t \in R} \mathbf{Q}(s,t) \eqsim \mathcal{I}\}$ **if** ($R' = R$) **then** $done :=$ **true** $R := R'$ **od** return R

which are calculated by the algorithms presented in Table 1, motivated by [21]. Now let $S^? = S\backslash(S^0 \cup S^{\mathcal{I}})$. Then for each $s \in S^?$, the argument for the bounded-until case indeed shows for $k \geqslant 0$,

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U}^{\leqslant k+1} \Psi) \lesssim \sum_{t \in S^?} Q^{\mathcal{M}}(t, \Phi \mathbf{U}^{\leqslant k} \Psi) \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) \tag{3}$$

and for unbounded-until case,

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \eqsim \sum_{t \in S^?} Q^{\mathcal{M}}(t, \Phi \mathbf{U} \Psi) \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t). \tag{4}$$

Let $\mathcal{T} = (\mathbf{Q}(t,s))_{s,t \in S^?}$ and $\widetilde{\mathcal{G}} = (\sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t))_{s \in S^?}$ be two state-indexed matrices of super-operators.

Theorem 5.1. *Let $f(X) = X\mathcal{T} + \widetilde{\mathcal{G}}$, and $\widetilde{\mathcal{E}}$ be the least fixed point of f. Then for any $s \in S^?$,*

$$\widetilde{\mathcal{E}}_s \eqsim Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi).$$

Proof. First, we check that for each $s \in S^?$,

$$\sum_{t \in S^?} \mathcal{T}_{t,s} + \widetilde{\mathcal{G}}_s = \sum_{t \in S^?} \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) = \sum_{t \in S^{\mathcal{I}} \uplus S^?} \mathbf{Q}(s,t) \lesssim \mathcal{I}_{\mathcal{H}}.$$

The existence of the least fixed point $\widetilde{\mathcal{E}}$ in $\mathcal{S}^1(\mathcal{H})^{|S^?|}$ follows from Theorem 2.5. Let $\widetilde{\mathcal{E}}^{(0)} = (\widetilde{\mathcal{E}}_s^{(0)})_{s \in S^?}$ where $\widetilde{\mathcal{E}}_s^{(0)} = 0_{\mathcal{H}}$ for each $s \in S^?$, and $\widetilde{\mathcal{E}}^{(k+1)} = \widetilde{\mathcal{E}}^{(k)}\mathcal{T} + \widetilde{\mathcal{G}}$. As f is Scott continuous with respect to $\sqsubseteq$, we have $\widetilde{\mathcal{E}}^{(0)} \sqsubseteq \widetilde{\mathcal{E}}^{(1)} \sqsubseteq \cdots$, and $\widetilde{\mathcal{E}} = \lim_k \widetilde{\mathcal{E}}^{(k)}$. On the other hand, by Lemma 2.7(4), for any $s \in S^?$ there exists a nondecreasing sequence $(\mathcal{F}_s^k)_{k \geqslant 0}$ of super-operators such that $Q^{\mathcal{M}}(s, \Phi \mathbf{U}^{\leqslant k} \Psi) \eqsim \mathcal{F}_s^k$ and $Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \eqsim \lim_k \mathcal{F}_s^k$. Thus to prove the theorem, it suffices to show that for any $k \geqslant 0$ and $s \in S^?$,

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U}^{\leqslant k} \Psi) \lesssim \widetilde{\mathcal{E}}_s^{(k)} \lesssim Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi). \tag{5}$$

In the following, we prove Eq. (5) by induction. Fix arbitrarily $s \in S^?$. When $k = 0$, we have $\widetilde{\mathcal{E}}_s^{(0)} = Q^{\mathcal{M}}(s, \Phi \mathbf{U}^{\leqslant 0} \Psi) = 0_{\mathcal{H}} \lesssim Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi)$ as $s \notin Sat(\Psi)$. Now suppose Eq. (5) holds for k. Then

$$\begin{aligned} Q^{\mathcal{M}}(s, \Phi \mathbf{U}^{\leqslant k+1} \Psi) &\lesssim \sum_{t \in S^?} Q^{\mathcal{M}}(t, \Phi \mathbf{U}^{\leqslant k} \Psi) \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) \quad \text{by Eq. (3)} \\ &\lesssim \sum_{t \in S^?} \widetilde{\mathcal{E}}_t^{(k)} \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) \quad \text{by induction and Lemma 2.3} \\ &= \widetilde{\mathcal{E}}_s^{(k+1)} \end{aligned}$$

and

$$\begin{aligned} \widetilde{\mathcal{E}}_s^{(k+1)} &= \sum_{t \in S^?} \widetilde{\mathcal{E}}_t^{(k)} \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) \\ &\lesssim \sum_{t \in S^?} Q^{\mathcal{M}}(t, \Phi \mathbf{U} \Psi) \mathbf{Q}(s,t) + \sum_{t \in S^{\mathcal{I}}} \mathbf{Q}(s,t) \quad \text{by induction and Lemma 2.3} \\ &\eqsim Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \quad \text{by Eq. (4).} \end{aligned}$$

□

From Theorems 5.1 and 2.5, whether or not $Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \sim \mathcal{E}$ can be determined efficiently.

Table 2
Table for $Q^{\mathcal{M}}(t, \diamond^{\leqslant k}\, succ)$, $0 \leqslant k \leqslant 4$, in Example 3.4.

k \ t	s	s_0	s_1	s_{00}	s_{01}	s_{10}	s_{11}	s_{000}	s_{010}	s_{101}	s_{111}	$succ$
0	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$\mathcal{I}_{\mathcal{H}}$
1	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$\mathcal{E}^0$	$\mathcal{E}^1$	$\mathcal{E}^+$	$\mathcal{E}^-$	$\mathcal{I}_{\mathcal{H}}$
2	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^+$	$\frac{1}{2}\mathcal{E}^-$	$\mathcal{E}^0$	$\mathcal{E}^1$	$\mathcal{E}^+$	$\mathcal{E}^-$	$\mathcal{I}_{\mathcal{H}}$
3	$0_{\mathcal{H}}$	$\frac{1}{4}(\mathcal{E}^0 + \mathcal{E}^1\mathcal{X})$	$\frac{1}{4}(\mathcal{E}^+ + \mathcal{E}^-\mathcal{Z})$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^+$	$\frac{1}{2}\mathcal{E}^-$	$\mathcal{E}^0$	$\mathcal{E}^1$	$\mathcal{E}^+$	$\mathcal{E}^-$	$\mathcal{I}_{\mathcal{H}}$
4	$\frac{1}{8}\sum_{i\in\{0,1,+,-\}} Set^{\lvert i\rangle}$	$\frac{1}{4}(\mathcal{E}^0 + \mathcal{E}^1\mathcal{X})$	$\frac{1}{4}(\mathcal{E}^+ + \mathcal{E}^-\mathcal{Z})$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^+$	$\frac{1}{2}\mathcal{E}^-$	$\mathcal{E}^0$	$\mathcal{E}^1$	$\mathcal{E}^+$	$\mathcal{E}^-$	$\mathcal{I}_{\mathcal{H}}$

Example 5.2. This example is devoted to model checking the properties listed in Example 4.3 against the qMCs of Examples 3.3 and 3.4.

(1) Quantum loop program. We only check the property $\mathbb{Q}_{\gtrsim\mathcal{E}}[\diamond\, l_3]$. Let $\mathcal{F} = \{|+\rangle\langle i|\colon\ i = 0, 1\}$ be the super-operator which sets the target qubit to $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $\mathcal{E}^i = \{|i\rangle\langle i|\}$, $i = 0, 1$, and $\mathcal{E} = \mathcal{X}$ the Pauli-X super-operator. We first calculate that $Sat(l_3) = \{l_3\}$ and $Sat(\mathtt{tt}) = \{l_0, l_1, l_2, l_3\}$. Then from the algorithm in Table 1 we have $S^0 = \emptyset$, and $S^{\mathcal{I}} = \{l_3\}$. So $S^? = \{l_0, l_1, l_2\}$. We proceed as follows:

$$
\begin{aligned}
&Q^{\mathcal{M}}(l_0, \diamond\, l_3) = Q^{\mathcal{M}}(l_1, \diamond\, l_3)\mathcal{F},\\
&Q^{\mathcal{M}}(l_1, \diamond\, l_3) = Q^{\mathcal{M}}(l_2, \diamond\, l_3)\mathcal{E}^1 + \mathcal{E}^0,\\
&Q^{\mathcal{M}}(l_2, \diamond\, l_3) = Q^{\mathcal{M}}(l_1, \diamond\, l_3)\mathcal{E}.
\end{aligned}
$$

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

$$
\mathcal{T} = \begin{pmatrix} 0_{\mathcal{H}} & 0_{\mathcal{H}} & 0_{\mathcal{H}} \\ \mathcal{F} & 0_{\mathcal{H}} & \mathcal{E} \\ 0_{\mathcal{H}} & \mathcal{E}^1 & 0_{\mathcal{H}} \end{pmatrix} \quad \text{with } M_{\mathcal{T}} = \begin{pmatrix} 0_{4\times 4} & 0_{4\times 4} & 0_{4\times 4} \\ M_{\mathcal{F}} & 0_{4\times 4} & M_{\mathcal{E}} \\ 0_{4\times 4} & M_{\mathcal{E}^1} & 0_{4\times 4} \end{pmatrix},
$$

where

$$
M_{\mathcal{E}^0} = |0\rangle\langle 0| \otimes |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad M_{\mathcal{E}^1} = |1\rangle\langle 1| \otimes |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},
$$

$$
M_{\mathcal{E}} = X \otimes X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad M_{\mathcal{F}} = \sum_{i=0}^{1} |+\rangle\langle i| \otimes |+\rangle\langle i| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.
$$

Using Matlab, we find that all eigenvalues of the matrix $M_{\mathcal{T}}$ have the absolute value strictly less than 1, and $M_{\widetilde{\mathcal{G}}}(I - M_{\mathcal{T}})^{-1} = [M, M, M]$ 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 $i = 0, 1, 2$, $Q^{\mathcal{M}}(l_i, \diamond\, l_3) = Set^0$ where $Set^0 = \{|0\rangle\langle 0|, |0\rangle\langle 1|\} \eqsim \mathcal{I}$, and so $l_i \models \mathbb{Q}_{\gtrsim\mathcal{E}}[\diamond\, l_3]$ for any $\mathcal{E} \lesssim \mathcal{I}$.

(2) BB84 protocol. We will compute $Q^{\mathcal{M}}(s, \diamond^{\leqslant 4}\, succ)$ and $Q^{\mathcal{M}}(s, \diamond\, fail)$ separately. For $Q^{\mathcal{M}}(s, \diamond^{\leqslant 4}\, succ)$, we first obtain from the algorithm in Table 1 that $S^0 = \{s_{001}, s_{011}, s_{100}, s_{110}, fail\}$, and $S^{\mathcal{I}} = \{succ\}$. Then Table 2 calculates $Q^{\mathcal{M}}(t, \diamond^{\leqslant k}\, succ)$ for each $t \in S^? = S\backslash S^0\backslash S^{\mathcal{I}}$ and $0 \leqslant k \leqslant 4$. The item $Q^{\mathcal{M}}(s, \diamond^{\leqslant 4}\, succ)$ is calculated as follows:

$$
\begin{aligned}
Q^{\mathcal{M}}\big(s, \diamond^{\leqslant 4}\, succ\big) &= \sum_{t\in S^?} Q^{\mathcal{M}}\big(t, \diamond^{\leqslant 3}\, succ\big)\mathbf{Q}(s, t)\\
&= \frac{1}{8}\big(\mathcal{E}^0 + \mathcal{E}^1\mathcal{X}\big)Set^{|0\rangle} + \frac{1}{8}\big(\mathcal{E}^+ + \mathcal{E}^-\mathcal{Z}\big)Set^{|+\rangle}\\
&= \frac{1}{8}\big(Set^{|0\rangle} + Set^{|1\rangle} + Set^{|+\rangle} + Set^{|-\rangle}\big) \eqsim \frac{1}{2}\mathcal{I}_{\mathcal{H}}.
\end{aligned}
$$

Similarly, for $Q^{\mathcal{M}}(t, \diamond\, fail)$ we have $S^0 = \{s_{001}, s_{011}, s_{100}, s_{110}, succ\}$ and $S^{\mathcal{I}} = \{fail\}$. Table 3 computes $Q^{\mathcal{M}}(t, \diamond^{\leqslant 4}\, fail)$ for each $t \in S^? = S\backslash S^0\backslash S^{\mathcal{I}}$ and $0 \leqslant k \leqslant 4$ where

Table 3
Table for $Q^{\mathcal{M}}(t, \diamond^{\leqslant k}\, fail)$, $0 \leqslant k \leqslant 4$, in Example 3.4.

k \ t	s	s_0	s_1	s_{00}	s_{01}	s_{10}	s_{11}	s_{000}	s_{010}	s_{101}	s_{111}
0	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$
1	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$\mathcal{E}^1$	$\mathcal{E}^0$	$\mathcal{E}^-$	$\mathcal{E}^+$
2	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$0_{\mathcal{H}}$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^-$	$\frac{1}{2}\mathcal{E}^+$	$\mathcal{E}^1$	$\mathcal{E}^0$	$\mathcal{E}^-$	$\mathcal{E}^+$
3	$0_{\mathcal{H}}$	$\frac{1}{4}(\mathcal{E}^1+\mathcal{E}^0\mathcal{X})$	$\frac{1}{4}(\mathcal{E}^-+\mathcal{E}^+\mathcal{Z})$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^-$	$\frac{1}{2}\mathcal{E}^+$	$\mathcal{E}^1$	$\mathcal{E}^0$	$\mathcal{E}^-$	$\mathcal{E}^+$
4	$0_{\mathcal{H}}$	$\frac{1}{4}(\mathcal{E}^1+\mathcal{E}^0\mathcal{X})$	$\frac{1}{4}(\mathcal{E}^-+\mathcal{E}^+\mathcal{Z})$	$\frac{1}{2}\mathcal{E}^1$	$\frac{1}{2}\mathcal{E}^0$	$\frac{1}{2}\mathcal{E}^-$	$\frac{1}{2}\mathcal{E}^+$	$\mathcal{E}^1$	$\mathcal{E}^0$	$\mathcal{E}^-$	$\mathcal{E}^+$

$$Q^{\mathcal{M}}(s, \diamond^{\leqslant 4}\, fail) = \sum_{t\in S} Q^{\mathcal{M}}(t, \diamond^{\leqslant 3}\, fail)\mathbf{Q}(s,t)$$
$$= \frac{1}{8}(\mathcal{E}^1+\mathcal{E}^0\mathcal{X})Set^{|0\rangle} + \frac{1}{8}(\mathcal{E}^- + \mathcal{E}^+\mathcal{Z})Set^{|+\rangle} = 0_{\mathcal{H}}.$$

Note that $Q^{\mathcal{M}}(t, \diamond^{\leqslant k}\, fail) = Q^{\mathcal{M}}(t, \diamond^{\leqslant 4}\, fail)$ for any $t \in S$ and $k > 4$. We have

$$s \models \mathbb{Q}_{\lesssim 0_{\mathcal{H}}}[\diamond\, fail] \wedge \mathbb{Q}_{\gtrsim \frac{1}{2}\mathcal{I}}\left[\diamond^{\leqslant 4}\, succ\right]$$

as expected.

5.1. Complexity

Recall that the overall time complexity for model checking a PCTL formula Φ 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 [21]. Let $d = \dim(\mathcal{H})$. The greatest extra cost of our algorithm is the until operator but from Theorem 2.5 it is of the order n^2d^4. Thus the complexity for model checking a QCTL formula Φ against a qMC is again linear in $|\Phi|$ and polynomial in n and d.

6. Conclusion and future work

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. By employing 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 examples of model-checking the correctness of a simple quantum loop program as well as the basic BB84 protocol. The properties checked in these examples are essentially classical in the sense that we are interested only in 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 final location is proportional to the identity super-operator. This treatment resorts to the ability to calculate the accumulated super-operators when constructing the model. We will further explore this issue in our future work.

The BB84 protocol is verified in this paper with the implicit assumption that no noise occurs at all. However, 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.

Acknowledgments

This work was supported by Australian Research Council grants DP110103473, DP130102764, and FT100100218. The authors are also partially supported by the Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Sciences.

Appendix A

A.1. Basic linear algebra

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

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

such that

(1) $\langle\psi|\psi\rangle \geqslant 0$ 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 $\mathbf{C}$ is the set of complex numbers, and for each $c\in\mathbf{C}$, c^* stands for the complex conjugate of c. For any vector $|\psi\rangle\in\mathcal{H}$, its length $\||\psi\rangle\|$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$, and it is said to be *normalised* if $\||\psi\rangle\| = 1$. 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 is 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 a set of normalised eigenvectors of a Hermitian operator in $\mathcal{L}(\mathcal{H})$ constitutes an orthonormal basis for $\mathcal{H}$. That is, there exists the so-called spectral decomposition for each Hermitian A such that

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

where the set $\{|i\rangle\}$ constitute an orthonormal basis of $\mathcal{H}$, $spec(A)$ denotes the set of eigenvalues of A, and E_i is the projector to the corresponding eigenspace of λ_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 $\mathrm{tr}(A) = \sum_i\langle i|A|i\rangle$ 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 $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ 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 $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle\otimes|\psi_2\rangle$ 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 respected to $\mathcal{H}_1$ is defined as $\mathrm{tr}_{\mathcal{H}_1}(A) = \sum_i\langle i|A|i\rangle$ where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}_1$. Similarly, we can define the partial trace of A with respected to $\mathcal{H}_2$. Partial trace functions are also independent of the orthonormal basis selected.

Traditionally, a linear operator $\mathcal{E}$ 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 $\mathcal{I}_{\mathcal{H}'}\otimes\mathcal{E}$ also maps positive operators in $\mathcal{L}(\mathcal{H}'\otimes\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H}'\otimes\mathcal{H})$. Here $\mathcal{I}_{\mathcal{H}'}$ is the identity operator on $\mathcal{L}(\mathcal{H}')$. We always assume complete positivity for super-operators in this paper. The elegant and powerful *Kraus representation theorem* [20] of completely positive super-operators states that a super-operator $\mathcal{E}$ is completely positive if and only if there is some set of operators $\{E_i:\ i\in I\}$ with appropriate dimension such that

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

for any $A\in\mathcal{L}(\mathcal{H})$. The operators E_i are called Kraus operators of $\mathcal{E}$. We abuse the notation slightly by denoting $\mathcal{E} = \{E_i: i\in I\}$. 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 $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ 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 $\mathcal{X} = \{X\}$, $\mathcal{Z} = \{Z\}$, and $\mathcal{Y} = \{Y\}$ where

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

A.2. Basic quantum mechanics

According to von Neumann's formalism of quantum mechanics [23], 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 ρ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\mathrm{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geqslant 0$, $\sum_i p_i = 1$, 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 ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, partial traces of ρ have explicit physical meanings: the density operators $\mathrm{tr}_{\mathcal{H}_1}\rho$ and $\mathrm{tr}_{\mathcal{H}_2}\rho$ are exactly the reduced quantum states of ρ 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

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big).$$

This kind of state is called *entangled state*. To see the strangeness of entanglement, suppose a measurement $M = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ 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 λ_0 or λ_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 ρ_1 and ρ_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 $\sum_m M_m^\dagger M_m = I_{\mathcal{H}}$. If the system is in state ρ, then the probability that measurement result m occurs is given by

$$p(m) = \mathrm{tr}\big(M_m^\dagger M_m \rho\big),$$

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

$$M = \sum_{m \in spec(M)} m E_m \tag{6}$$

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

$$\mathcal{E}_m(\rho) = E_m \rho E_m$$

is again a super-operator by Kraus Theorem.

A.3. Proof of Theorem 2.5

This section is devoted to the proof of Theorem 2.5. 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,

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

and each $J_{n_i}(\lambda_i)$ is an $n_i \times n_i$-Jordan block with the eigenvalue λ_i. Let $\widetilde{M} = S\widetilde{J}S^{-1}$ where $\widetilde{J}$ 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 $\widetilde{J} = diag(J^1, J^2, \ldots, J^k)$ where

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

Lemma A.1. *If $\sum_{m=0}^{\infty} NM^m$ exists, then for each $m \geqslant 0$, $NM^m = N\widetilde{M}^m$.*

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

$$NSJ^m = \left(K_1 J_{n_1}^m(\lambda_1), \ldots, K_k J_{n_k}^m(\lambda_k)\right),$$

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

$$\begin{aligned} 0 &= \lim_{m\to\infty} \left\| K_i J_{n_i}^m(\lambda_i) \right\| \\ &= \lim_{m\to\infty} \|K_i\| \cdot \left\| J_{n_i}(\lambda_i) \right\|^m \\ &\geqslant \lim_{m\to\infty} \|K_i\| \cdot |\lambda_i|^m \end{aligned}$$

where the last inequality is from Theorem 5.6.9 of [17]. From this we deduce that $K_i = 0$ for each i whenever $|\lambda_i| \geqslant 1$. Thus $NSJ^m = NS\widetilde{J}^m$, and $NM^m = N\widetilde{M}^m$. □

Corollary A.2. *For any matrices N and M,*

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

provided that the limit exists.

Proof. Observe that by definition, the spectral radius of $\widetilde{M}$ is strictly less than 1. Then from Corollary 5.6.16 of [17], $I - \widetilde{M}$ is invertible, and $(I - \widetilde{M})^{-1} = \sum_{m=0}^{\infty} \widetilde{M}^m$. The result thus follows from Lemma A.1. □

We also need a notion of matrix representation for super-operators, which was investigated in [30]. To do this, we fix an orthonormal basis $\{|k\rangle\colon\ k \in K\}$ of $\mathcal{H}$.

Definition A.3. Let $\mathcal{E} = \{E_i\colon\ i \in I\} \in \mathcal{S}(\mathcal{H})$ 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 $\{|k\rangle\colon\ k \in K\}$.

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 $\mathcal{T} = (\mathcal{E}_{i,j})$ be an $m \times n$-matrix of super-operators. Then the matrix representation of $\mathcal{T}$, denoted $M_{\mathcal{T}}$, is defined as the block matrix

$$M_{\mathcal{T}} = \begin{pmatrix} M_{\mathcal{E}_{1,1}} & \ldots & M_{\mathcal{E}_{1,n}} \\ \vdots & \ddots & \vdots \\ M_{\mathcal{E}_{m,1}} & \ldots & M_{\mathcal{E}_{m,n}} \end{pmatrix}$$

where for each i and j, $M_{\mathcal{E}_{i,j}}$ is the matrix representation of $\mathcal{E}_{i,j}$. In particular, let $\widetilde{\mathcal{E}} = (\mathcal{E}_1, \ldots, \mathcal{E}_n)$ be a (row) vector of super-operators. Then $M_{\widetilde{\mathcal{E}}} = (M_{\mathcal{E}_1}, \ldots, M_{\mathcal{E}_n})$. 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 [30].

Lemma A.4. *Let $M_{\mathcal{E}}$ be the matrix representation of $\mathcal{E} \in \mathcal{S}(\mathcal{H})$. Then for any $E \in \mathcal{L}(\mathcal{H})$, we have*

$$\left(\mathcal{E}(E) \otimes I_{\mathcal{H}}\right)|\Psi\rangle = M_{\mathcal{E}}(E \otimes I_{\mathcal{H}})|\Psi\rangle.$$

Table 4
Algorithm for Theorem 2.5.

Input: (1) An $n \times n$ matrix $\mathcal{T} = (\mathcal{T}_{i,j})$ and a $1 \times n$ vector $\widetilde{\mathcal{G}}$ of super-operators such that for each j, $\sum_i \mathcal{T}_{i,j} + \widetilde{\mathcal{G}}_j \lesssim \mathcal{I}_{\mathcal{H}}$. (2) A super-operator $\mathcal{E} \in \mathcal{S}^1(\mathcal{H})$ and i such that $1 \leqslant i \leqslant n$.
Output: 'yes' if $\mathcal{E} \sim \widetilde{\mathcal{E}}_i$ and 'no' otherwise, where $\widetilde{\mathcal{E}}$ is the least fixed point of Eq. (1).
(1) Construct $M_{\widetilde{\mathcal{G}}}$ and $M_{\mathcal{T}}$ from $\widetilde{\mathcal{G}}$ and $\mathcal{T}$, respectively; (2) Calculate the Jordan decomposition $M_{\mathcal{T}} = SJS^{-1}$; (3) Compute $M_{\widetilde{\mathcal{E}}} = M_{\widetilde{\mathcal{G}}} S(I - \widetilde{J})^{-1} S^{-1}$; (4) Use the method described in Eq. (7) to determine if $\widetilde{\mathcal{E}} \sim \widetilde{\mathcal{E}}_i$, and output the result.

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

$$\begin{aligned}\langle k|\Big(\sum_{i\in I} E_i^\dagger E_i\Big)|l\rangle &= \operatorname{tr}\sum_{i\in I} E_i|l\rangle\langle k|E_i^\dagger \\ &= \operatorname{tr}\big[\mathcal{E}\big(|l\rangle\langle k|\big)\big] \\ &= \langle\Psi|\mathcal{E}\big(|l\rangle\langle k|\big)\otimes I_{\mathcal{H}}|\Psi\rangle \\ &= \langle\Psi|M_{\mathcal{E}}\big(|l\rangle\langle k|\otimes I_{\mathcal{H}}\big)|\Psi\rangle \\ &= \langle\Psi|M_{\mathcal{E}}|lk\rangle. \end{aligned} \tag{7}$$

Note that for an operator $E \in \mathcal{L}(\mathcal{H})$, $\langle k|E|l\rangle$ is exactly the (k,l)th element of the matrix representation of E under the basis $\{|k\rangle\colon\ k \in K\}$. Lemma A.4 indeed provides us an efficient way to determine whether or not $\mathcal{E} \lesssim \mathcal{F}$ when the matrix representations of $\mathcal{E}$ and $\mathcal{F}$ are given.

A.3.1. Proof of Theorem 2.5

We now turn to the proof of Theorem 2.5. For the first part, we check that $f(X)$ indeed maps $\mathcal{S}^1(\mathcal{H})^n$ into $\mathcal{S}^1(\mathcal{H})^n$. Let $\widetilde{\mathcal{F}} \in \mathcal{S}^1(\mathcal{H})^n$. Then for each j,

$$f(\widetilde{\mathcal{F}})_j = \sum_{i=1}^n \widetilde{\mathcal{F}}_i \mathcal{T}_{i,j} + \widetilde{\mathcal{G}}_j \lesssim \sum_{i=1}^n \mathcal{T}_{i,j} + \widetilde{\mathcal{G}}_j \lesssim \mathcal{I}_{\mathcal{H}}$$

where the first inequality is from Lemma 2.3 and the fact that $\widetilde{\mathcal{F}}_i \lesssim \mathcal{I}_{\mathcal{H}}$. Note that the function f defined in Eq. (1) is Scott continuous with respect to the partial order $\sqsubseteq$. Then by Lemma 2.4 and Kleene fixed point theorem, $f(X)$ has a (unique) least fixed point which can be written as

$$\widetilde{\mathcal{E}} = \sum_{m=0}^{\infty} \widetilde{\mathcal{G}}\mathcal{T}^m.$$

For the second part of Theorem 2.5, we first prove that the matrix representation of $\widetilde{\mathcal{E}}$ is

$$M_{\widetilde{\mathcal{E}}} = M_{\widetilde{\mathcal{G}}}(I - \widetilde{M}_{\mathcal{T}})^{-1}. \tag{8}$$

For any $1 \leqslant i \leqslant n$ and $E_i \in \mathcal{L}(\mathcal{H})$, we calculate from Lemma A.4 that

$$\begin{aligned} M_{\widetilde{\mathcal{E}}_i}(E_i \otimes I_{\mathcal{H}})|\Psi\rangle &= \widetilde{\mathcal{E}}_i(E_i)\otimes I_{\mathcal{H}}|\Psi\rangle \\ &= \sum_{m=0}^{\infty}\sum_{k_1,\ldots,k_m=1}^{n} \widetilde{\mathcal{G}}_{k_1}\mathcal{T}_{k_1,k_2}\cdots\mathcal{T}_{k_m,i}(E_i)\otimes I_{\mathcal{H}}|\Psi\rangle \\ &= \sum_{m=0}^{\infty}\sum_{k_1,\ldots,k_m=1}^{n} (M_{\widetilde{\mathcal{G}}_{k_1}} M_{\mathcal{T}_{k_1,k_2}}\cdots M_{\mathcal{T}_{k_m,i}})(E_i\otimes I_{\mathcal{H}})|\Psi\rangle \\ &= \sum_{m=0}^{\infty}\big(M_{\widetilde{\mathcal{G}}}M_{\mathcal{T}}^m\big)_i(E_i\otimes I_{\mathcal{H}})|\Psi\rangle \end{aligned}$$

where $(M_{\widetilde{\mathcal{G}}}M_{\mathcal{T}}^m)_i$ is the ith block of $M_{\widetilde{\mathcal{G}}}M_{\mathcal{T}}^m$ at the corresponding position of $M_{\widetilde{\mathcal{E}}_i}$ in $M_{\widetilde{\mathcal{E}}}$. 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 $M_{\widetilde{\mathcal{E}}_i} = \sum_{m=0}^{\infty}(M_{\widetilde{\mathcal{G}}}M_{\mathcal{T}}^m)_i$, and thus $M_{\widetilde{\mathcal{E}}} = \sum_{m=0}^{\infty} M_{\widetilde{\mathcal{G}}}M_{\mathcal{T}}^m$. Then Eq. (8) follows from Corollary A.2.

An algorithm which determines for any $\mathcal{E} \in \mathcal{S}^1(\mathcal{H})$ and $1 \leqslant i \leqslant n$ if $\mathcal{E} \sim \widetilde{\mathcal{E}}_i$ is sketched in Table 4. It is easy to see that the time complexity is cn^2, where the constant c is of the order d^4, and d is the dimension of the Hilbert space $\mathcal{H}$. □

A.4. Proof of Theorem 3.2

A.4.1. Basic results for vector measures

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

Let Ω be a non-empty set. A semi-algebra $\mathcal{S}$ on Ω is a subset of the power set 2^{Ω} with the following properties:

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

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

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

Definition A.5. Let $T \subseteq 2^{\Omega}$, and Δ be a function from T to a Banach space $\mathcal{B}$. We call Δ a countably additive vector measure, or vector measure for simplicity, if for any sequence $(A_i)_{i \geqslant 1}$ of pairwise disjoint members of T such that $\biguplus_{i=1}^{\infty} A_i \in T$, it holds that

$$\Delta\left(\biguplus_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \Delta(A_i).$$

Definition A.6. Let $\mathcal{R}$ be an algebra on Ω and $\Delta : \mathcal{R} \to \mathcal{B}$ a vector measure. Let μ be a finite nonnegative real-valued measure on $\mathcal{R}$. Then Δ is said to be μ-continuous if

$$\lim_{\mu(A) \to 0} \Delta(A) = 0.$$

The next theorem from [10] is the key to prove Theorem 3.2.

Theorem A.7 *(Carathéodory–Hahn–Kluvanek Extension Theorem). Let $\mathcal{R}$ be an algebra on Ω and $\Delta : \mathcal{R} \to \mathcal{B}$ a bounded vector measure. If there exists a finite and nonnegative real-valued measure μ on $\mathcal{R}$ such that Δ is μ-continuous, then Δ can be uniquely extended to a vector measure $\Delta' : \sigma(\mathcal{R}) \to \mathcal{B}$ on the σ-algebra generated by $\mathcal{R}$ such that*

$$\Delta'(A) = \Delta(A) \quad \textit{for any } A \in \mathcal{R}.$$

A.4.2. 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 operators on $\mathcal{L}(\mathcal{H})$; that is

$$\mathcal{HP}(\mathcal{H}) = \left\{\mathcal{E} \in \mathcal{L}\big(\mathcal{L}(\mathcal{H})\big) \;\middle|\; \mathcal{E}(E) \text{ is Hermitian provided that } E \text{ is Hermitian}\right\}.$$

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, $\mathcal{S}(\mathcal{H}) \subseteq \mathcal{HP}(\mathcal{H})$, and the orders $\sqsubseteq$ and $\lesssim$ defined in Definition 2.1 can be lifted to $\mathcal{HP}(\mathcal{H})$. We denote by $\mathcal{HP}_{\eqsim}(\mathcal{H})$ the quotient set of $\mathcal{HP}(\mathcal{H})$ by $\eqsim$, and $[\mathcal{E}] \in \mathcal{HP}_{\eqsim}(\mathcal{H})$ the equivalent class of $\mathcal{E} \in \mathcal{HP}(\mathcal{H})$. Note that although the quotient set $\mathcal{HP}_{\eqsim}(\mathcal{H})$ 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 $\mathcal{HP}_{\eqsim}(\mathcal{H})$: Let $\mathcal{E} = \{X\}$ be the Pauli-X super-operator, and $\mathcal{G} = \{|0\rangle\langle 0|\}$. Then $[\mathcal{E}] = [\mathcal{I}_{\mathcal{H}}]$, but $\mathcal{G}\mathcal{E} \neq \mathcal{G}\mathcal{I}_{\mathcal{H}}$ since $\mathrm{tr}(\mathcal{G}\mathcal{E}(|0\rangle\langle 0|)) = 0$ while $\mathrm{tr}(\mathcal{G}\mathcal{I}_{\mathcal{H}}(|0\rangle\langle 0|)) = 1$.

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

Lemma A.8. *Let $\|\cdot\|$ be an arbitrary operator norm. Then the quotient set $(\mathcal{HP}_{\eqsim}(\mathcal{H}), \|\cdot\|_{\eqsim})$ is again a Banach space, where the norm $\|\cdot\|_{\eqsim}$ is defined by*

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

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 $(\mathcal{HP}_{\eqsim}(\mathcal{H}), \|\cdot\|_{\eqsim})$. □

A.4.3. Proof of Theorem 3.2

We are now ready to prove Theorem 3.2. To do this, we first regard the mapping Q_s defined in Eq. (2) as from $\mathcal{S}^{\mathcal{M}}(s)$ to $\mathcal{HP}(\mathcal{H})$. Let Q'_s be a mapping from $\mathcal{S}^{\mathcal{M}}(s)$ to $\mathcal{HP}_{\eqsim}(\mathcal{H})$ such that for any $A \in \mathcal{S}^{\mathcal{M}}(s)$,

$$Q'_s(A) = \big[Q_s(A)\big].$$

Then we have the following lemmas.

Lemma A.9. *The mapping Q'_s defined above is a bounded vector measure over $\mathcal{S}^{\mathcal{M}}(s)$.*

Proof. We only need to check that Q'_s is countably additive. Let $\emptyset \neq A = \biguplus_{i\geqslant 1} A_i$ for a disjoint sequence $(A_i)_{i\geqslant 1}$ in $\mathcal{S}^{\mathcal{M}}(s)$ and $A \in \mathcal{S}^{\mathcal{M}}(s)$. We need to show

$$Q'_s(A) = \sum_{i\geqslant 1} Q'_s(A_i). \tag{9}$$

Without loss of generality, we assume that the sequence $(A_i)_{i\geqslant 1}$ 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 $i \leqslant n$.

We claim that there are only finitely many non-empty sets in the sequence; that is, there exists n such that $A_i \neq \emptyset$ if and only if $i \leqslant n$. We prove this claim by contradiction. Suppose $A = Cyl(\hat{\pi}_0)$, and for each $i \geqslant 1$, $A_i = Cyl(\hat{\pi}_i)$ where all $\hat{\pi}_i$s are in $Path^{\mathcal{M}}_{fin}(s)$ and $\hat{\pi}_0$ is a prefix of each $\hat{\pi}_i$ for $i \geqslant 1$. By the fact that A_is are disjoint, $\hat{\pi}_i$ cannot be a prefix of $\hat{\pi}_j$ for distinct $i, j \geqslant 1$. Let $\Pi = \{\hat{\pi}_i\colon\ i \geqslant 1\}$. For any $\hat{\pi} \in Path^{\mathcal{M}}_{fin}(s)$, let $Ind_{\hat{\pi}} = \{i \geqslant 1\colon\ \hat{\pi}$ is a prefix of $\hat{\pi}_i\}$, and

$$K = \big\{\hat{\pi} \in Path^{\mathcal{M}}_{fin}(s)\colon\ Ind_{\hat{\pi}} \text{ is infinite}\big\}.$$

Obviously, $K \cap \Pi = \emptyset$. Note that $\hat{\pi}_0 \in K$, and for any $\hat{\pi} \in K$, since

$$Ind_{\hat{\pi}} = \biguplus_{t\in S} Ind_{\hat{\pi}^\frown t},$$

there exists $t_{\hat{\pi}} \in S$ such that $\hat{\pi}^\frown t_{\hat{\pi}} \in K$ again. Thus we can extend $\hat{\pi}_0$ to an (infinite) path $\pi \in Path^{\mathcal{M}}(s)$ such that any finite-length prefix $\hat{\pi}$ of π with $|\hat{\pi}| \geqslant |\hat{\pi}_0|$ is not included in Π. Thus for any i, $\pi \notin A_i$, contradicting the fact that $\pi \in A$.

With the claim in hand, we let $N = \max\{|\hat{\pi}_i|\colon\ 1 \leqslant i \leqslant n\}$ and $\Pi_N = \{\hat{\pi} \in \Pi\colon\ |\hat{\pi}| = N\}$. Obviously, we can partition Π_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 $\{\hat{\pi}'_1, \ldots, \hat{\pi}'_{I_N}\}$ such that for each $1 \leqslant i \leqslant I_N$, $|\hat{\pi}'_i| = N-1$, and

$$\Pi_N = \biguplus_{i=1}^{I_N} \Pi^i_N \quad \text{where } \Pi^i_N = \big\{\hat{\pi}'^\frown_i t\colon\ t \in S\big\}.$$

We delete Π_N from Π and add $\hat{\pi}'_i$, $1 \leqslant i \leqslant I_N$, into it. Denote by $\Pi_{\leqslant N-1}$ the resultant set. Then each element in $\Pi_{\leqslant N-1}$ has length less than N, and it is easy to check that

$$\sum_{\hat{\pi}\in\Pi_N} \mathbf{Q}(\hat{\pi}) \eqsim \sum_{i=1}^{I_N} \mathbf{Q}\big(\hat{\pi}'_i\big), \quad \text{thus} \quad \sum_{\hat{\pi}\in\Pi} \mathbf{Q}(\hat{\pi}) \eqsim \sum_{\hat{\pi}\in\Pi_{\leqslant N-1}} \mathbf{Q}(\hat{\pi}).$$

Proceeding in this way, we can construct a sequence of sets Π_i, $|\hat{\pi}_0| + 1 \leqslant i \leqslant N$, such that for any i, $\sum_{\hat{\pi}\in\Pi_{\leqslant i}} \mathbf{Q}(\hat{\pi}) \eqsim \sum_{\hat{\pi}\in\Pi_{\leqslant i-1}} \mathbf{Q}(\hat{\pi})$ where $\Pi_{\leqslant N} = \Pi$. Note that $\Pi_{\leqslant|\hat{\pi}_0|} = \{\hat{\pi}_0\}$. We finally have

$$\sum_{i\geqslant 1} Q'_s(A_i) = \sum_{\hat{\pi}\in\Pi} \big[\mathbf{Q}(\hat{\pi})\big] = \big[\mathbf{Q}(\hat{\pi}_0)\big] = Q'_s(A).$$

That completes the proof of the lemma. □

Lemma A.10. *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 $\mathcal{HP}_{\eqsim}(\mathcal{H})$. Furthermore, for any $A \in \sigma(\mathcal{S}^{\mathcal{M}}(s))$,*

$$[0_{\mathcal{H}}] \lesssim Q'_s(A) \lesssim [\mathcal{I}_{\mathcal{H}}]. \tag{10}$$

Proof. Let $\mathcal{R} = \mathcal{R}(\mathcal{S}^{\mathcal{M}}(s))$ be the algebra generated by $\mathcal{S}^{\mathcal{M}}(s)$. Obviously, we have

$$\mathcal{R} = \left\{A\colon\ A = \biguplus_{i=1}^{n} A_i \text{ for some } n \geqslant 0,\ A_i \in \mathcal{S}^{\mathcal{M}}(s)\right\}.$$

We extend the mapping Q'_s to $\mathcal{R}$ by defining $Q'_s(\biguplus_{i=1}^n A_i) = \sum_{i=1}^n Q'_s(A_i)$, which turns out to be a bounded vector measure from $\mathcal{R}$ to $\mathcal{HP}_{\eqsim}(\mathcal{H})$. Let μ_s be a mapping defined as follows:

- $\mu_s(\emptyset) = 0$, and for any $A = Cyl(\hat{\pi}) \in \mathcal{S}^{\mathcal{M}}(s)$, $\mu_s(A) = \mathrm{tr}(\mathbf{Q}(\hat{\pi})(\rho_m))$ where $\rho_m = I_{\dim(\mathcal{H})}/\dim(\mathcal{H})$ is the maximally mixed state in $\mathcal{D}(\mathcal{H})$;
- for any disjoint sets $A_1, \ldots, A_n$ in $\mathcal{S}^{\mathcal{M}}(s)$, $\mu_s(\biguplus_{i=1}^n A_i) = \sum_{i=1}^n \mu_s(A_i)$.

Then μ_s is indeed a finite and nonnegative real-valued measure on $\mathcal{R}$, since $\mu_s(Path^{\mathcal{M}}(s)) = \mu_s(Cyl(s)) = \mathrm{tr}(\mathcal{I}_{\mathcal{H}}(\rho_m)) = 1$. Note that for any super-operator $\mathcal{E} = \{E_i\colon\ i \in I\}$, $\mathrm{tr}(\mathcal{E}(\rho_m)) = \sum_{i\in I} \|E_i\|_2^2/\dim(\mathcal{H})$ where $\|\cdot\|_2$ is the Euclidean norm. It follows that if $\lim_{i\to\infty} \mathrm{tr}(\mathcal{E}_i(\rho_m)) = 0$, where $(\mathcal{E}_i)_{i\geqslant 1}$ is a sequence of super-operators, then $\lim_{i\to\infty}[\mathcal{E}_i] = [0_{\mathcal{H}}]$. So we have $\lim_{\mu_s(A)\to 0} Q'_s(A) = [0_{\mathcal{H}}]$, which means that Q'_s is μ_s-continuous.

Now using Theorem A.7, we can extend Q'_s uniquely to a vector measure $Q'_s : \sigma(\mathcal{S}^{\mathcal{M}}(s)) \to \mathcal{HP}_{\eqsim}(\mathcal{H})$. In the following, we show that the extension satisfies Eq. (10). By the additivity of Q'_s, it suffices to show that for any $A \in \sigma(\mathcal{S}^{\mathcal{M}}(s))$, $[0_{\mathcal{H}}] \lesssim Q'_s(A)$; that is, for any $\rho \in \mathcal{D}(\mathcal{H})$, $\mathrm{tr}(Q'_s(A)(\rho)) \geqslant 0$. Let $\mu_\rho : \sigma(\mathcal{S}^{\mathcal{M}}(s)) \to \mathbb{R}$ be defined as

$$\forall A \in \sigma\big(\mathcal{S}^{\mathcal{M}}(s)\big)\colon\ \mu_\rho(A) = \mathrm{tr}\big(Q'_s(A)(\rho)\big).$$

Then obviously, μ_ρ is an (ordinary) real-valued measure over $\sigma(\mathcal{S}^{\mathcal{M}}(s))$ and its restriction on $\mathcal{S}^{\mathcal{M}}(s)$, denoted $\mu_\rho|_{\mathcal{S}^{\mathcal{M}}(s)}$, is a probabilistic measure. Now from Carathéodory Theorem for probabilistic measures [7], $\mu_\rho|_{\mathcal{S}^{\mathcal{M}}(s)}$ can be uniquely extended to a probabilistic measure μ'_ρ over $\sigma(\mathcal{S}^{\mathcal{M}}(s))$. Then we have $\mathrm{tr}(Q'_s(A)(\rho)) = \mu_\rho(A) = \mu'_\rho(A) \geqslant 0$ by the uniqueness of such extension. □

With the two lemmas above, we can easily prove Theorem 3.2. For any $A \in \sigma(\mathcal{S}^{\mathcal{M}}(s))$, let $Q_s(A)$ be any super-operator in the equivalent class $Q'_s(A)$. It is obvious that such an extension is indeed a SVM, and it is unique up to the equivalence relation $\eqsim$. □

References

[1] L. Accardi, Nonrelativistic quantum mechanics as a noncommutative Markov process, Adv. Math. 20 (1976) 329.
[2] C. Baier, J.P. Katoen, Principles of Model Checking, MIT Press, 2008.
[3] P. Baltazar, R. Chadha, P. Mateus, Quantum computation tree logic – model checking and complete calculus, Int. J. Quantum Inform. 6 (2008) 219–236.
[4] C.H. Bennett, G. Brassard, Quantum cryptography: Public-key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing, 1984, pp. 175–179.
[5] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. Wootters, Teleporting an unknown quantum state via dual classical and EPR channels, Phys. Rev. Lett. 70 (1993) 1895–1899.
[6] C.H. Bennett, S.J. Wiesner, Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states, Phys. Rev. Lett. 69 (20) (1992) 2881–2884.
[7] P. Billingsley, Probability and Measure, Wiley–India, 2008.
[8] H.P. Breuer, F. Petruccione, The Theory of Open Quantum Systems, Oxford University Press, Oxford, 2002.
[9] E.M. Clarke, O. Grumberg, D. Peled, Model Checking, MIT Press, 1999.
[10] J. Diestel, J.J. Uhl, Vector Measures, Amer. Math. Soc., 1977.
[11] E. Emerson, Temporal and modal logic, in: Handbook of Theoretical Computer Science, vol. 2, 1990, pp. 995–1072.
[12] U. Faigle, A. Schönhuth, Discrete quantum Markov chains, arXiv:1011.1295, 2010.
[13] S. Gay, R. Nagarajan, N. Papanikolaou, Probabilistic model-checking of quantum protocols, in: Proceedings of the 2nd International Workshop on Developments in Computational Models, 2006.
[14] S. Gay, R. Nagarajan, N. Papanikolaou, QMC: A model checker for quantum systems, in: CAV '08, Springer, 2008, pp. 543–547.
[15] S. Gudder, Quantum Markov chains, J. Math. Phys. 49 (7) (2008) 072105.
[16] H. Hansson, B. Jonsson, A logic for reasoning about time and reliability, Formal Aspects Comput. 6 (5) (September 1994) 512–535.
[17] R.A. Horn, C.R. Johnson, Matrix Analysis, Cambridge University Press, 1990.
[18] W.N.N. Hung, X. Song, G. Yang, J. Yang, M. Perkowski, Quantum logic synthesis by symbolic reachability analysis, in: Proceedings of the 41st Design Automation Conference, July 2004, pp. 838–841.
[19] W.N.N. Hung, X. Song, G. Yang, J. Yang, M. Perkowski, Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reachability analysis, IEEE Trans. Comput. Aided Design Integrated Circuits Syst. 25 (9) (2006) 1652–1663.
[20] K. Kraus, States, Effects and Operations: Fundamental Notions of Quantum Theory, Springer, Berlin, 1983.
[21] M. Kwiatkowska, G. Norman, D. Parker, Stochastic model checking, in: Formal Methods for Performance Evaluation, 2007, pp. 220–270.
[22] G. Lowe, Breaking and fixing the Needham–Schroeder public-key protocol using FDR, in: Tools and Algorithms for the Construction and Analysis of Systems, 1996, pp. 147–166.
[23] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton University Press, Princeton, NJ, 1955.
[24] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[25] N.K. Papanikolaou, Model checking quantum protocols, PhD thesis, 2008.
[26] Id Quantique: http://www.idquantique.com;
MagiQ Technologies: http://magiqtech.com/MagiQ;
QuintessenceLabs: http://qlabsusa.com;
NEC: http://www.nec.com/en/global/rd/research/gr/quantum.html.
[27] P. Selinger, Towards a quantum programming language, Math. Structures Comput. Sci. 14 (4) (2004) 527–586.
[28] S. Tani, H. Kobayashi, K. Matsumoto, Exact quantum algorithms for the leader election problem, ACM Trans. Comput. Theory 4 (1) (March 2012).
[29] M.Y. Vardi, Automatic verification of probabilistic concurrent finite state programs, in: Proceedings of the 26th IEEE FOCS, 1985, pp. 327–338.
[30] M.S. Ying, N.K. Yu, Y. Feng, R.Y. Duan, Verification of quantum programs, Manuscript. Available online at: arXiv:1106.4063, 2011.