Model Checking ω-regular Properties for Quantum Markov Chains*

Yuan Feng[1], Ernst Moritz Hahn[2], Andrea Turrini[3], and Shenggang Ying[4]

1 **Centre for Quantum Software and Information,**
University of Technology Sydney, Sydney, Australia
Yuan.Feng@uts.edu.au

2 **State Key Laboratory of Computer Science, Institute of Software,**
Chinese Academy of Sciences, Beijing, P. R. China; and
Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
hahn@ios.ac.cn

3 **State Key Laboratory of Computer Science, Institute of Software,**
Chinese Academy of Sciences, Beijing, P. R. China
turrini@ios.ac.cn

4 **Centre for Quantum Software and Information,**
University of Technology Sydney, Sydney, Australia
Shenggang.Ying@uts.edu.au

Abstract

Quantum Markov chains are an extension of classical Markov chains which are labelled with super-operators rather than probabilities. They allow to faithfully represent quantum programs and quantum protocols. In this paper, we investigate model checking ω-regular properties, a very general class of properties (including, e.g., LTL properties) of interest, against this model.

For classical Markov chains, such properties are usually checked by building the product of the model with a language automaton. Subsequent analysis is then performed on this product. When doing so, one takes into account its graph structure, and for instance performs different analyses per bottom strongly connected component (BSCC). Unfortunately, for quantum Markov chains such an approach does not work directly, because super-operators behave differently from probabilities. To overcome this problem, we transform the product quantum Markov chain into a single super-operator, which induces a decomposition of the state space (the tensor product of classical state space and the quantum one) into a family of BSCC subspaces. Interestingly, we show that this BSCC decomposition provides a solution to the issue of model checking ω-regular properties for quantum Markov chains.

1998 ACM Subject Classification D.2.4 Software/Program Verification

Keywords and phrases Quantum Markov chains, model checking, ω-regular properties, bottom strongly connected component

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2017.35

* This work was partially supported by the Australian Research Council (Grant Nos. DP130102764 and DP160101652), the Singapore Ministry of Education (Grant No. MOE2015-T2-1-137), the CAS/SAFEA International Partnership Program for Creative Research Teams, the National Natural Science Foundation of China (Grant Nos. 61550110506 and 61650410658), the Chinese Academy of Sciences Fellowship for International Young Scientists, and the CDZ project CAP (GZ 1023).

28th International Conference on Concurrency Theory (CONCUR 2017).
Editors: Roland Meyer and Uwe Nestmann; Article No. 35; pp. 35:1–35:16
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Since its introduction, quantum computing has been considered a really promising technology for solving computationally complex tasks. Some of these tasks, such as factorisation and discrete logarithm computation, are the building blocks of cryptographic protocols developed to ensure security and privacy in communication. Quantum computing, by its own nature, allows for an easy solution to such tasks, so the future construction of a working quantum computer would compromise several important cryptography-based applications such as bank transactions and private communication. This has given rise to a large amount of research for providing a new class of communication protocols based on quantum mechanics so as to get back the desired properties. For instance, protocols such as super-dense coding [7], quantum coin-flipping protocol [6], and quantum key distribution protocols [6, 5] have been proposed as new building blocks for quantum cryptography.

However, as quantum mechanics is counter-intuitive, quantum protocol designers are more likely to make errors than their classical peers. This will become especially serious 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 systems.

This paper explores the possibility of applying model checking [11, 3], one of the dominant techniques for verification which has already a large number of successful industrial applications [8, 10, 21], to the verification of quantum protocols. In particular, we are interested in model checking ω-regular properties, a very general class of properties subsuming those expressible by LTL formulae, against quantum Markov chains (QMCs), an extension of classical Markov chains which allow to faithfully represent quantum programs and quantum protocols. Similar to the classical case, we first take the product of the QMC and a parity automaton representing the ω-regular property of interest. The model checking problem then boils down to calculating the value of the product parity quantum Markov chain (PQMC). However, we show by a counterexample that the traditional BSCC decomposition analysis used for classical model checking does not work in quantum case. To overcome this problem, we transform the product PQMC into a single super-operator on an extended Hilbert space including both the classical and quantum states. We show that due to the special structure of such an extended super-operator, the notion of BSCC *subspaces* for super-operators defined in [32] can be applied to tackle the problem.

1.1 Related works

The main obstacle of model checking quantum systems is that the set of all quantum states, traditionally regarded as the underlying state space of the model 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. [17] considered a special scenario where the initial state is a *stabiliser state*, and the quantum operations allowed all belong to the class of *Clifford group*, so that all the quantum states produced in the evolution are finitely describable. In this way, they proposed an efficient model checker [18] for certain quantum protocols, employing purely classical algorithms. Based on the same simplification, Ardeshir-Larijani et al. developed equivalence checkers for deterministic quantum protocols [1] as well as concurrent quantum protocols that behave *functionally* [2]. However, this approach does not work for general quantum systems. In contrast, the quantum Markov chain model adopted in this paper, which is derived from [16], is capable of describing general quantum programs and protocols, not only those in stabiliser formalism.

The state space of our quantum Markov chain is taken classical and transitions between classical states are labelled by trace-nonincreasing super-operators (thus the corresponding quantum state space is *implicitly* implied). In contrast, there is another notion of quantum Markov chains, which is a pair $(\mathcal{H}, \mathcal{E})$ with $\mathcal{H}$ being a finite dimensional Hilbert space and $\mathcal{E}$ a trace-preserving super-operator on $\mathcal{H}$, investigated in the literature. Model checking techniques for this notion of quantum Markov chains have been extensively investigated in recent years [32, 31, 22]. These two notions of quantum Markov chains turn out to be equivalent in expressive power [22]. However, they are useful in different scenarios. The model in [32] corresponds naturally to generic quantum operations and quantum communication channels, both being popular objects of study in quantum information theory. In contrast, the quantum Markov chain model considered in this paper is more suitable for analysing quantum programs and protocols where classical states such as program counters, program variables, and measurement outcomes are naturally present.

1.2 Relevance of our work

Quantum Markov chains

The notion of quantum Markov chains studied in this paper was introduced in [16] (a similar definition was given in [19] to generalise quantum walks), which has been shown to be expressive enough to describe general quantum systems. The explicit modelling of a quantum **while** program and well-known quantum protocols such as teleportation, superdense coding, quantum key distribution protocol BB84, etc., can be found in [16, 15].

One of the distinct features of this model, for verification purpose, is that it provides a way to check *once for all* in that once a property is checked to hold, it holds for all initial quantum states. This is especially important for the verification of quantum programs. For example, for the reachability problem we calculate the accumulated *super-operator*, say $\mathcal{E}$, along all valid paths. As a result, the reachability *probability* when the program is executed on the initial quantum state ρ is simply the trace $\mathrm{tr}(\mathcal{E}(\rho))$ of $\mathcal{E}(\rho)$.

ω-regular properties for QMCs

It has been shown in [16] how properties in quantum computation tree logic (QCTL), a quantum variant of the probabilistic CTL (PCTL), can be verified. We then provided a tool implementation [15] based on the probabilistic model checker IscasMC [20]. The applicability of this method so far was however hindered by the fact that the expressiveness of QCTL is rather limited. As the logic PCTL by which it was motivated, QCTL basically only allows to describe nested (single-step, bounded, and unbounded) reachability problems. To overcome this issue, in this paper we describe how ω-regular properties, and in particular linear time logic (LTL) properties, can be checked on quantum Markov chains. This allows to express and analyse a wide range of relevant properties, such as repeated reachability, reachability in a restricted order, nested Until properties, or conjunctions of such properties.

Admittedly, up to now we still do not have any quantum communication protocols that have desired properties only describable in ω-regular languages (that is also why we could not have a case study to test the effectiveness of our approach and algorithm in this paper). However, with the rapid development of quantum communication technology, especially quantum cryptographic systems, being able to check these kinds of properties for quantum Markov chains will be necessary, as they allow for instance to verify that the processes in a quantum communication protocol will repeatedly send messages, that messages are sent in the correct order, that the key is exchanged for sure, etc., all of which cannot be expressed in QCTL.

2 Quantum Markov Chains

In this section, we recall the required notions of quantum Markov chains. For a more thorough discussion, we refer the interested reader to [24, 16].

Given a finite dimensional Hilbert space $\mathcal{H}$, let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on it. Let $\mathcal{S}(\mathcal{H})$ be the set of *super-operators*, that is, completely positive linear operators from $\mathcal{L}(\mathcal{H})$ to $\mathcal{L}(\mathcal{H})$. In particular, we denote by $\mathcal{I}_{\mathcal{H}}$ and $0_{\mathcal{H}}$ the identity and null super-operators in $\mathcal{S}(\mathcal{H})$, respectively. For simplicity, we abuse the notation slightly by denoting $\mathcal{E} = \{ E_i \mid i \in I \}$ if $\{ E_i \mid i \in I \}$ is a set of Kraus operators of $\mathcal{E}$; that is, $\mathcal{E}(A) = \sum_{i \in I} E_i A E_i^\dagger$ for all $A \in \mathcal{L}(\mathcal{H})$. For any $\mathcal{E}, \mathcal{F} \in \mathcal{S}(\mathcal{H})$, the composition of $\mathcal{E}$ and $\mathcal{F}$ is defined by $(\mathcal{E} \circ \mathcal{F})(A) = \mathcal{E}(\mathcal{F}(A))$. We sometimes omit the symbol $\circ$ and write $\mathcal{E}\mathcal{F}$ directly for $\mathcal{E} \circ \mathcal{F}$. A (pre-)order is defined in $\mathcal{S}(\mathcal{H})$ by setting $\mathcal{E} \lesssim \mathcal{F}$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\operatorname{tr}(\mathcal{E}(\rho)) \leq \operatorname{tr}(\mathcal{F}(\rho))$. Here $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{L}(\mathcal{H})$, i.e., positive semidefinite operators ρ with the trace $\operatorname{tr}(\rho)$ being no larger than 1. Note that the trace of a partial density operator denotes the probability that the corresponding (normalised) quantum state is reached [28]. Intuitively, $\mathcal{E} \lesssim \mathcal{F}$ means that the success probability of performing $\mathcal{E}$ is always not greater than that of performing $\mathcal{F}$, whatever the initial state is. Let $\eqsim$ be $\lesssim \cap \gtrsim$.

We denote by $\mathcal{S}^{\mathcal{I}}(\mathcal{H})$ the set of trace-nonincreasing super-operators over $\mathcal{H}$; that is, $\mathcal{S}^{\mathcal{I}}(\mathcal{H}) = \{ \mathcal{E} \in \mathcal{S}(\mathcal{H}) \mid 0_{\mathcal{H}} \lesssim \mathcal{E} \lesssim \mathcal{I}_{\mathcal{H}} \}$. Observe that $\mathcal{E} \in \mathcal{S}^{\mathcal{I}}(\mathcal{H})$ if and only if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\operatorname{tr}(\mathcal{E}(\rho)) \in [0, 1]$. Thus it is natural to regard the set $\mathcal{S}^{\mathcal{I}}(\mathcal{H})$ as the quantum counterpart of $[0, 1]$, the domain of traditional probabilities. This is exactly the key to the notion of quantum Markov chains defined in [16], that we use as our basic model.

▶ **Definition 1** (Quantum Markov Chain). A *super-operator weighted Markov chain* over a Hilbert space $\mathcal{H}$, also referred to as *quantum Markov chain (QMC)* for simplicity, is a tuple $(S, \mathbf{Q})$, where

1. S is a finite set of *classical states*;
2. $\mathbf{Q} \colon S \times S \to \mathcal{S}^{\mathcal{I}}(\mathcal{H})$ is called the *transition matrix* where for each $s \in S$, the super-operator $\sum_{s' \in S} \mathbf{Q}(s, s')$ is trace-preserving, that is $\sum_{s' \in S} \mathbf{Q}(s, s') \eqsim \mathcal{I}_{\mathcal{H}}$.

Similar to classical Markov chains, the notions of paths and measures can be defined for QMCs.

▶ **Definition 2** (Paths and measures). Consider a QMC $\mathcal{M} = (S, \mathbf{Q})$. A path σ of $\mathcal{M}$ is a finite or infinite sequence $s_0 s_1 \dots$ of states in S such that for each valid index $i \geq 1$, $\mathbf{Q}(s_{i-1}, s_i) \neq 0_{\mathcal{H}}$. For a valid index i, we let $\sigma[i] \overset{\text{def}}{=} s_i$. We denote the set of finite paths as $\mathrm{Path}^{\mathcal{M}}_{\mathit{fin}}$ and the set of infinite paths as $\mathrm{Path}^{\mathcal{M}}$. We define the *cylinder set* of a finite path $\sigma = s_0 s_1 \dots s_n$ as $\mathit{Cyl}(\sigma) \overset{\text{def}}{=} \{ \sigma' \in \mathrm{Path}^{\mathcal{M}} \mid \forall i, 0 \leq i \leq n.\ \sigma[i] = \sigma'[i] \}$. Let $(\mathrm{Path}^{\mathcal{M}}, \Sigma)$ be a measurable space where Σ is the σ-algebra generated by all the cylinder sets $\mathit{Cyl}(\sigma)$ where $\sigma \in \mathrm{Path}^{\mathcal{M}}_{\mathit{fin}}$. For any $s \in S$, we define $Q^{\mathcal{M}}_s \colon \mathrm{Path}^{\mathcal{M}}_{\mathit{fin}} \to \mathcal{S}(\mathcal{H})$ as

$$Q^{\mathcal{M}}_s(\sigma) \overset{\text{def}}{=} \begin{cases} 0_{\mathcal{H}} & s \neq s_0 \\ \mathcal{I}_{\mathcal{H}} & s = s_0 \wedge n = 0 \\ \mathbf{Q}(s_{n-1}, s_n)\mathbf{Q}(s_{n-2}, s_{n-1}) \cdots \mathbf{Q}(s_0, s_1) & s = s_0 \wedge n > 0. \end{cases}$$

Then $Q^{\mathcal{M}}_s$ induces a (super-operator valued) measure on $(\mathrm{Path}^{\mathcal{M}}, \Sigma)$, denoted by $Q^{\mathcal{M}}_s$ as well for simplicity, by setting $Q^{\mathcal{M}}_s(\mathit{Cyl}(\sigma)) \overset{\text{def}}{=} Q^{\mathcal{M}}_s(\sigma)$.

From [16, Theorem 3.2], this measure is unique up to $\eqsim$.

3 Model checking ω-regular properties for QMCs

LTL and ω-regular properties have been studied extensively for classical Markov chains [13, 12, 9, 3]. To compute the probability $\mathcal{P}(\phi)$ that a certain LTL property ϕ is satisfied in a Markov chain $\mathcal{M}$, the classical automaton-based approach works as follows. At first, ϕ is transformed into a nondeterministic Büchi automaton, which is then transformed into a deterministic automaton $\mathcal{A}$ with a more complex acceptance condition, such as Rabin or Parity acceptance. Such a determinisation step usually exploits a variant of Safra's [26] determinisation construction, such as the techniques presented in [25, 27]. Afterwards, the product $\mathcal{M} \otimes \mathcal{A}$ of $\mathcal{M}$ and $\mathcal{A}$ is constructed, which is a Markov chain equipped with an acceptance condition. Finally, using algorithms operating on the graph structure of the product Markov chain, the states of $\mathcal{M} \otimes \mathcal{A}$ are categorised into those belonging to a *bottom strongly connected component (BSCC)* and *transient states*. According to the acceptance condition, each BSCC is then marked as accepting or rejecting. The probability that ϕ holds in a transient state s can then be obtained by solving an equation system representing the probability that from s an accepting BSCC is reached.

This section is devoted to extending this approach to quantum Markov chains. However, the extension is not trivial: as will be shown by a counterexample in Section 3.2, while the product construction itself does not lead to any problem, its decomposition into BSCCs and transient states cannot be performed as in the classical case. Therefore, in Section 3.3, we provide an alternative approach which does not directly rely on the graph structure of the product. Specifically, we transform $\mathcal{M} \otimes \mathcal{A}$ into a single super-operator, and show that the BSCC decomposition of the classical-quantum Hilbert space (the tensor product of classical state space and the quantum one) induced by this super-operator, instead of the decomposition of the classical state space alone, provides a desired solution to the model checking ω-regular properties for quantum Markov chains.

3.1 Parity automata and parity quantum Markov chains

In order to define properties of QMCs, we consider an extension in which their states are decorated by a labelling function.

▶ **Definition 3** (Labelled Quantum Markov Chain). A *labelled quantum Markov chain* (LQMC) is a tuple $\mathcal{M} = (S, \mathbf{Q}, AP, L)$, where $(S, \mathbf{Q})$ is a QMC and

1. AP is a finite set of *atomic propositions*; and
2. $L\colon S \to 2^{AP}$ is a *labelling function*.

The notions of paths, measures, etc. for LQMCs are as in Definitions 1 and 2. We extend the labelling functions to paths by setting

$$L(s_0 s_1 s_2 \ldots) \overset{\text{def}}{=} L(s_0)L(s_1)L(s_2)\ldots.$$

The properties we are interested in are the ω-regular properties (which include properties definable in LTL).

▶ **Definition 4** (ω-regular Properties). An *ω-regular language* is a subset of $(2^{AP})^\omega$ which can be defined using an ω-regular expression [29]. Consider an LQMC $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ and an ω-regular language $\mathcal{W} \subseteq (2^{AP})^\omega$. We define $Q_s^{\mathcal{M}}(\mathcal{W}) \overset{\text{def}}{=} Q_s^{\mathcal{M}}(\{\, \sigma \in \mathrm{Path}^{\mathcal{M}} \mid L(\sigma) \in \mathcal{W} \,\})$.

We shortly restate a well-known mechanism to decide whether a word is included in a given ω-regular language. For this purpose, an additional definition is needed.

▶ **Definition 5** (Parity Automaton). A *(deterministic) parity automaton* (PA) is a tuple $\mathcal{A} = (A, \overline{a}, AP, t, \mathsf{pri})$, where

1. A is a finite set of automaton states, and $\overline{a} \in A$ is the *initial state*,
2. AP is a finite set of *atomic propositions*,
3. $t \colon A \times 2^{AP} \to A$ is a *transition function*,
4. $\mathsf{pri} \colon A \to \mathbb{N}$ is a *priority function.* Here $\mathbb{N}$ denotes the set of natural numbers.

A *path* of $\mathcal{A}$ is an infinite sequence $\sigma = a_0 L_0 a_1 L_1 \ldots \in (A \times 2^{AP})^\omega$ such that $a_0 = \overline{a}$ and for all $i \geq 0$, $t(a_i, L_i) = a_{i+1}$. We extend the priority function to paths by setting $\mathsf{pri}(\sigma) \overset{\text{def}}{=} \liminf_{i\to\infty} \mathsf{pri}(a_i)$. We use $\mathrm{Path}^{\mathcal{A}}$ to denote the set of all paths of $\mathcal{A}$. The *language* of $\mathcal{A}$ is defined as

$$\mathcal{L}(\mathcal{A}) \overset{\text{def}}{=} \{\, L_0 L_1 \ldots \in (2^{AP})^\omega \mid \exists \sigma = a_0 L_0 a_1 L_1 \ldots \in \mathrm{Path}^{\mathcal{A}}.\ \mathsf{pri}(\sigma) \text{ is even} \,\}.$$

The following result is well known from the literature; see e.g. [23, 14].

▶ **Lemma 6** (PAs represent the ω-regular languages). *A language $\mathcal{W}$ is ω-regular if and only if it is the language of a PA $\mathcal{A}$, i.e., $\mathcal{W} = \mathcal{L}(\mathcal{A})$.*

In particular this means that all properties which can be expressed in LTL can be also expressed as parity automata. Effective means to transform LTL formulas to parity automata exist in, say, [26, 25, 27].

We also need to consider QMCs with parity conditions.

▶ **Definition 7** (Parity Quantum Markov Chain). A parity quantum Markov chain (PQMC) is a tuple $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$, where $(S, \mathbf{Q})$ is a QMC and $\mathsf{pri} \colon S \to \mathbb{N}$ is a *priority function* for the classical states. We define the *value* of $\mathcal{M}$ in $s \in S$ as

$$\mathrm{val}_s^{\mathcal{M}} \overset{\text{def}}{=} Q_s^{\mathcal{M}}(\{\, \sigma \in \mathrm{Path}^{\mathcal{M}} \mid \mathsf{pri}(\sigma) \textit{ is even} \,\}).$$

Here again, we set $\mathsf{pri}(\sigma) \overset{\text{def}}{=} \liminf_{i\to\infty} \mathsf{pri}(s_i)$ provided that $\sigma = s_0 s_1 s_2 \ldots$.

3.2 Product construction

In the following, we describe how to combine an LQMC under consideration with a PA representing the property we are concerned with.

▶ **Definition 8** (LQMC-PA Product). The *product* of an LQMC $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ and a PA $\mathcal{A} = (A, \overline{a}, AP, t, \mathsf{pri})$ with the same set of atomic propositions is a PQMC $\mathcal{M} \otimes \mathcal{A} \overset{\text{def}}{=} (S', \mathbf{Q}', \mathsf{pri}')$ where

1. $S' \overset{\text{def}}{=} S \times A$,
2. $\mathbf{Q}'((s,a),(s',a')) \overset{\text{def}}{=} \mathbf{Q}(s,s')$ if $t(a, L(s)) = a'$, and $0_{\mathcal{H}}$ otherwise,
3. $\mathsf{pri}'((s,a)) \overset{\text{def}}{=} \mathsf{pri}(a)$.

The following lemma shows that the value of this product is trace equivalent to the super-operator corresponding to the property under consideration in the original model.

▶ **Lemma 9.** *Consider the product $\mathcal{M}' \overset{\text{def}}{=} \mathcal{M} \otimes \mathcal{A} = (S', \mathbf{Q}', \mathsf{pri}')$ of an LQMC $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ and a PA $\mathcal{A} = (A, \overline{a}, AP, t, \mathsf{pri})$. We have that for any $s \in S$,*

$$Q_s^{\mathcal{M}}(\mathcal{L}(\mathcal{A})) \eqsim \mathrm{val}_{(s,\overline{a})}^{\mathcal{M}'}.$$

Proof. The proof is standard. ◀

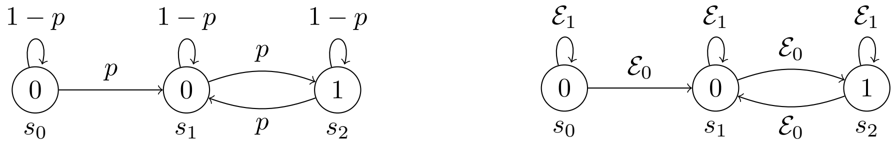

Figure 1 Example showing that BSCC decomposition for the underlying graph does not work for model checking PQMCs.

Up to now, the model checking method works as for classical Markov chains. What would fail is the subsequent part which consists of the evaluation of the PQMC.

The idea for model checking of classical parity Markov chains is quite simple: a path of a PMC is accepted if the lowest priority occurring infinitely often is even. A strongly connected component (SCC) of a classical Markov chain is a maximal set of states B such that any two states in B can reach each other with nonzero probability. A bottom SCC (BSCC) is an SCC B in which no state in B can reach any state outside B with nonzero probability. BSCCs can be computed using only the graph structure of the Markov chain. That is, concrete probabilities are irrelevant; only the information whether the probability of going from one state to another is nonzero matters. In a classical Markov chain, starting from s, the probability that s' is visited infinitely often is 1 if s and s' are in the same BSCC. The probability that a state which is not contained in any BSCC (a transient state) will be visited infinitely often is 0. Thus, model checking for PMCs can be performed as follows:

1. Identify the set of BSCCs using a graph-based algorithm, and let $ACC = \emptyset$.
2. For each BSCC B, check whether the lowest priority occurring on a state of B is even. If yes, add B to ACC, $ACC \leftarrow ACC \cup B$.
3. For any state s, if $s \in ACC$, then $\mathrm{val}_s^{\mathcal{M}} = 1$. Otherwise, $\mathrm{val}_s^{\mathcal{M}}$ is the probability that s reaches any state in ACC. That is, if s is a state of a BSCC $B \not\subseteq ACC$, then $\mathrm{val}_s^{\mathcal{M}} = 0$; and values of transient states can be computed by solving a linear equation system.

Note that a PQMC also has a set of classical states, and the transition super-operators also induce an underlying graph over these states. Thus a natural question is: can we define the notion of BSCCs in terms of the underlying graph structure for a PQMC, just as in the classical case, and employ the above technique to calculate its value? Unfortunately, this idea does not work, as the following example shows. A similar example illustrating this difficulty was also given in [22].

▶ **Example 10.** Consider the two parity Markov models in Figure 1. On the left is a classical one with $0 < p < 1$, while the right is a quantum one with $\mathcal{E}_0, \mathcal{E}_1 \neq 0_{\mathcal{H}}$ and $\mathcal{E}_0 + \mathcal{E}_1 \approx \mathcal{I}_{\mathcal{H}}$. Obviously, both models have the same classical state space, and have exactly the same underlying graph. Thus they have the same set of BSCCs, if we would define BSCCs for PQMCs according to the underlying graphs. However, we will see that this BSCC technique does not help in the evaluation of PQMCs.

In the classical model, s_0 is a transient state which will eventually reach the only BSCC $\{s_1, s_2\}$. Thus, the priority with which s_0 is labelled is irrelevant. From any state of the BSCC, the probability that both states are visited infinitely often is 1. Thus, the probability that from either state the lowest priority 0 is reached infinitely often is 1, and thus the value of the parity Markov chain is also 1.

In contrast, in the quantum model, we assume $\mathcal{E}_0 \overset{\text{def}}{=} \{|0\rangle\langle 0|\}$ and $\mathcal{E}_1 \overset{\text{def}}{=} \{|1\rangle\langle 1|\}$. Note that for $i \in \{0,1\}$ it holds $\mathcal{E}_i\mathcal{E}_i = \mathcal{E}_i$ and $\mathcal{E}_i\mathcal{E}_{1-i} = 0_{\mathcal{H}}$. It is easy to check that if we start from s_0, the infinite path $(s_0)^\omega$, with the corresponding *nonzero* super-operator $\lim_{n\to\infty} \mathcal{E}_1^n = \{|1\rangle\langle 1|\}$, never leaves to the set $\{s_1, s_2\}$. Thus s_0 should not be considered as a transient state at all. Furthermore, as the priority of $(s_0)^\omega$ is 0, this path also contributes to the value of PQMC. On the other hand, if we start from s_1, there are two infinite paths with nonzero super-operator, namely $(s_1)^\omega$ with the corresponding super-operator $\{|1\rangle\langle 1|\}$ and priority 0, and $(s_1 s_2)^\omega$ with the corresponding super-operator $\{|0\rangle\langle 0|\}$ and priority 0. Thus, the value of the PQMC in state s_1 is $\{|0\rangle\langle 0|\} + \{|1\rangle\langle 1|\} \eqsim \mathcal{I}_\mathcal{H}$. However, if we start from s_2 we have $(s_2)^\omega$ with the corresponding super-operator $\{|1\rangle\langle 1|\}$ and priority 1, and $(s_2 s_1)^\omega$ with the corresponding super-operator $\{|0\rangle\langle 0|\}$ and priority 0. Thus, the value in s_2 is $\{|0\rangle\langle 0|\}$, different from the one in s_1.

Thus, algorithms based on BSCC decomposition of the underlying graph do not work for PQMCs: neither are BSCCs reached with certainty, nor do all states of a BSCC have the same value. In addition, the value of a BSCC state might be equivalent to neither $0_\mathcal{H}$ nor $\mathcal{I}_\mathcal{H}$.

3.3 Computing PQMC values

We have seen from Example 10 that the notion of BSCC defined for the underlying graph over *classical states* does not help in evaluation of PQMCs. In this subsection, we show that, rather surprisingly, by encoding the behavior of $\mathcal{M}$ into a single super-operator acting on the *extended Hilbert space* which is the tensor product of the classical state space and the quantum one, the notion of BSCC *subspaces* for super-operators[1] defined in [32] can be used to compute PQMC values.

We first recall some definitions from [32]. For any $\rho \in \mathcal{D}(\mathcal{H})$, the *support* $\mathrm{supp}(\rho)$ is defined to be the space spanned by the eigenvectors of ρ with non-zero eigenvalues. Let $\{X_k\}$ be a family of subspaces of $\mathcal{H}$. The *join* of $\{X_k\}$ is defined as $\bigvee_k X_k = \mathrm{span}(\bigcup_k X_k)$. Let $\mathcal{E}$ be a super-operator acting on $\mathcal{H}$ with $\dim(\mathcal{H}) = d$. A subspace X of $\mathcal{H}$ is said to be *invariant* for $\mathcal{E}$ if $\mathcal{E}(X) \subseteq X$, and it is a BSCC of $\mathcal{E}$ if $\mathcal{R}(|\psi\rangle\langle\psi|) = X$ for any pure state $|\psi\rangle \in X$, where for any $\rho \in \mathcal{D}(\mathcal{H})$,

$$\mathcal{R}(\rho) = \bigvee_{i=0}^{\infty} \mathrm{supp}(\mathcal{E}^i(\rho))$$

is the *reachable subspace* of $\mathcal{E}$ starting in ρ. Apparently, a BSCC is also an invariant subspace. Finally, X is called *transient* if $\lim_{k\to\infty} \mathrm{tr}(P_X \mathcal{E}^k(\rho)) = 0$ for any $\rho \in \mathcal{D}(\mathcal{H})$, where P_X is the projection onto X.

Let $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ be a PQMC on $\mathcal{H}$ with $\mathbf{Q}(s,t) = \{\, E_i^{s,t} \mid i \in I^{s,t} \,\}$. Following [22], we define a super-operator

$$\mathcal{E}_\mathcal{M} \stackrel{\text{def}}{=} \{\, |t\rangle\langle s| \otimes E_i^{s,t} \mid s, t \in S, i \in I^{s,t} \,\} \tag{1}$$

acting on the Hilbert space $\mathcal{H}_c \otimes \mathcal{H}$, where $\mathcal{H}_c$ is a $|S|$-dimensional Hilbert space with an orthonormal basis $\{\, |s\rangle \mid s \in S \,\}$. To see how $\mathcal{E}_\mathcal{M}$ encodes the behavior of $\mathcal{M}$, let for each

[1] We choose not to use the terminology *quantum Markov chain* as in [32], to avoid confusion with the notion of quantum Markov chain defined in this paper. Interestingly, although it has been observed that these two notions of quantum Markov chains have the same expressiveness power [22], this is the first time techniques from one model find applications in the other.

$s \in S$ that $O^s \overset{\text{def}}{=} \{(t,i) \mid t \in S, i \in I^{s,t}\}$, and $M^s \overset{\text{def}}{=} \{\, E_i^{s,t} \mid (t,i) \in O^s \,\}$. Note that for any $\rho \in \mathcal{D}(\mathcal{H})$,

$$\mathrm{tr}\left(\sum_{(t,i)\in O^s} E_i^{s,t}\rho(E_i^{s,t})^\dagger\right) = \mathrm{tr}\left(\sum_{t\in S}\mathbf{Q}(s,t)(\rho)\right) = \mathrm{tr}(\rho)$$

where the second equality comes from the fact that $\sum_{t\in S}\mathbf{Q}(s,t) \eqsim \mathcal{I}_{\mathcal{H}}$ (see Definition 1). That is, M^s is actually a quantum measurement with the outcome set O^s. Furthermore, for any $\sigma \in \mathcal{D}(\mathcal{H}_c)$ and $\rho \in \mathcal{D}(\mathcal{H})$, we calculate that

$$\begin{aligned}\mathcal{E}_{\mathcal{M}}(\sigma \otimes \rho) &= \sum_{s,t\in S}\sum_{i\in I^{s,t}} |t\rangle\langle s|\sigma|s\rangle\langle t| \otimes E_i^{s,t}\rho(E_i^{s,t})^\dagger \\ &= \sum_{s\in S}\langle s|\sigma|s\rangle \sum_{(t,i)\in O^s} |t\rangle\langle t| \otimes E_i^{s,t}\rho(E_i^{s,t})^\dagger.\end{aligned}$$

Thus the behavior of $\mathcal{E}_{\mathcal{M}}$ can be described as the following steps, which exactly captures the intended meaning of $\mathcal{M}$:

1. a projective measurement $M \overset{\text{def}}{=} \{|s\rangle\langle s| : s \in S\}$ is performed on the classical system $\mathcal{H}_c$ to determine the current classical state;
2. if the measurement outcome of M is s, then the quantum measurement M^s is performed on the quantum system $\mathcal{H}$;
3. the classical state is set to be $|t\rangle\langle t|$ if (t,i), for any i, is observed in M^s.

The following lemma shows that for super-operators derived from PQMCs, the classical and quantum systems will remain separable (disentangled) during the evolution, provided that the initial state is in a product form.

▶ **Lemma 11.** *Let $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ be a PQMC on $\mathcal{H}$, $s \in S$, $k \in \mathbb{N}$, and $\rho \in \mathcal{D}(\mathcal{H})$.*

1. *For any $n \geq 0$, $\mathcal{E}^n_{\mathcal{M}}(|s\rangle\langle s| \otimes \rho)$ is block diagonal according to the classical states. Specifically,*

$$\mathcal{E}^n_{\mathcal{M}}(|s\rangle\langle s| \otimes \rho) = \sum_{t\in S}|t\rangle\langle t| \otimes \mathbf{Q}^n(s,t)(\rho).$$

2. *Let $R_s^k = Q_s^{\mathcal{M}}(\{\,\sigma \in \mathrm{Path}^{\mathcal{M}} \mid \mathsf{pri}(\sigma) = k\,\})$. Then for any $n \geq 0$,*

$$\mathrm{tr}(R_s^k(\rho)) = \sum_{t\in S}\mathrm{tr}(R_t^k(\mathbf{Q}^n(s,t)(\rho))).$$

Proof. Statement 1 is easy by induction. For Statement 2, note that for any $n \geq 0$,

$$\begin{aligned}R_s^k &= Q_s^{\mathcal{M}}(\{\,\sigma \in \mathrm{Path}^{\mathcal{M}}(s) \mid \liminf_{i\geq 0}\mathsf{pri}(\sigma[i]) = k\,\}) \\ &\eqsim \sum_{t\in S} Q_t^{\mathcal{M}}(\{\,\sigma \in \mathrm{Path}^{\mathcal{M}}(t) \mid \liminf_{i\geq 0}\mathsf{pri}(\sigma[i]) = k\,\}) \circ \mathbf{Q}^n(s,t) \\ &= \sum_{t\in S} R_t^k \circ \mathbf{Q}^n(s,t).\end{aligned}$$

Then the result follows. ◀

Similar to Lemma 11, it is easy to show that for any fixed point state σ of $\mathcal{E}_{\mathcal{M}}$, i.e. $\mathcal{E}_{\mathcal{M}}(\sigma) = \sigma$, it also has the form $\sigma = \sum_{s\in S}|s\rangle\langle s| \otimes \sigma_s$. Therefore, by [32], any BSCC of $\mathcal{E}_{\mathcal{M}}$

can be spanned by pure states of the form $|s\rangle|\psi\rangle$ where $s \in S$ and $|\psi\rangle \in \mathcal{H}$. For a BSCC B of $\mathcal{E}_{\mathcal{M}}$, let

$$C(B) \stackrel{\text{def}}{=} \{\, s \in S \mid |s\rangle|\psi\rangle \in B \text{ for some } |\psi\rangle \in \mathcal{H} \,\}$$

be the set of classical states supported in B.

Exploiting the *classical-quantum separation* (Lemma 11) of super-operators derived from PQMCs, we are going to show some nice properties of their BSCC decomposition, which are key to our discussion in this paper. First, we prove that two BSCCs X and Y are orthogonal, denoted $X \perp Y$, unless they have the same set of support classical states.

▶ **Lemma 12.** *Let $\mathcal{M}$ be a PQMC. For any two BSCCs X and Y of $\mathcal{E}_{\mathcal{M}}$, if $C(X) \neq C(Y)$ then $X \perp Y$.*

Proof. Suppose $C(X) \neq C(Y)$, and, without loss of generality, let $s \in C(Y) \backslash C(X)$. Let ρ_X and ρ_Y be the fixed point states corresponding to X and Y, respectively. Since $\mathcal{E}_{\mathcal{M}}(\rho_X + \rho_Y) = \rho_X + \rho_Y$, we know that $(\rho_X + \rho_Y)/2$ is a fixed point state corresponding to $Z \stackrel{\text{def}}{=} X \vee Y$. Thus Z can be decomposed into the direct sum of some orthogonal BSCCs: $Z = X \oplus Z_1 \oplus \cdots \oplus Z_n$.

We claim that $n = 1$. Otherwise, for any i, $\dim(Z_i) < \dim(Y)$ (because $\sum_i \dim(Z_i) + \dim(X) = \dim(Z) \leq \dim(X) + \dim(Y)$), and thus $Y \perp Z_i$ by [32, Lemma 2]. This means $Y = X$, a contradiction. Now let $|s\rangle|\psi\rangle \in Y$. Since $s \notin C(X)$, we have $|s\rangle|\psi\rangle \perp X$, and thus $|s\rangle|\psi\rangle \in Z_1$. On the other hand, since both Y and Z_1 are BSCCs, $Y = Z_1 = \mathcal{R}(|s\rangle\langle s| \otimes |\psi\rangle\langle\psi|)$. Thus $X \perp Y$. ◀

Given $k \in \mathbb{N}$, let $\mathcal{BSCC}_k$ be the span of all BSCCs of $\mathcal{E}_{\mathcal{M}}$ with the minimal priority being k; that is,

$$\mathcal{BSCC}_k = \bigvee \{\, B \text{ is a BSCC of } \mathcal{E}_{\mathcal{M}} : \min\{\, \mathsf{pri}(s) \mid s \in C(B) \,\} = k \,\}.$$

Similarly, let $\mathcal{BSCC}_{k^-}$ and $\mathcal{BSCC}_{k^+}$ be the spans of all BSCCs with the minimal priority being less than and larger than k, respectively. Then by Lemma 12, $\mathcal{BSCC}_k$, $\mathcal{BSCC}_{k^-}$, and $\mathcal{BSCC}_{k^+}$ are pairwise orthogonal. From [32], the state space $\mathcal{H}_c \otimes \mathcal{H}$ can be decomposed *uniquely* into

$$\mathcal{H} = T \oplus \mathcal{BSCC}_k \oplus \mathcal{BSCC}_{k^-} \oplus \mathcal{BSCC}_{k^+},$$

where T is the maximum transient subspace of $\mathcal{E}_{\mathcal{M}}$. In the following, we denote by P_T, P_k, P_{k^-} and P_{k^+} the projections onto T, $\mathcal{BSCC}_k$, $\mathcal{BSCC}_{k^-}$ and $\mathcal{BSCC}_{k^+}$, respectively. Then $P_T + P_k + P_{k^-} + P_{k^+} = I_{\mathcal{H}_c \otimes \mathcal{H}}$, the identity operator on $\mathcal{H}_c \otimes \mathcal{H}$.

The following lemma is crucial for our purpose. Note that $\operatorname{tr}(R_t^k(\rho))$ denotes the probability that k is the lowest priority infinitely often reachable from the initial state $|t\rangle\langle t| \otimes \rho$. This lemma essentially says that such a probability will be 1 if starting from $\mathcal{BSCC}_k$ (provided that $\operatorname{tr}(\rho) = 1$; otherwise, the probability is $\operatorname{tr}(\rho)$), and it will be 0 if starting from either $\mathcal{BSCC}_{k^-}$ or $\mathcal{BSCC}_{k^+}$. Thus $\mathcal{BSCC}_k$ for each k acts like the standard BSCCs in classical Markov chains.

▶ **Lemma 13.** *For any $t \in S$ and $\rho \in \mathcal{D}(\mathcal{H})$,*

1. *if* $\operatorname{supp}(|t\rangle\langle t| \otimes \rho) \subseteq \mathcal{BSCC}_k$, *then* $\operatorname{tr}(R_t^k(\rho)) = \operatorname{tr}(\rho)$*;*
2. *if* $\operatorname{supp}(|t\rangle\langle t| \otimes \rho) \subseteq \mathcal{BSCC}_{k^-}$, *then* $\operatorname{tr}(R_t^k(\rho)) = 0$*; and*
3. *if* $\operatorname{supp}(|t\rangle\langle t| \otimes \rho) \subseteq \mathcal{BSCC}_{k^+}$, *then* $\operatorname{tr}(R_t^k(\rho)) = 0$*.*

With the above lemmas, we are now ready to prove the main theorem of this section.

▶ **Theorem 14.** *Given a PQMC $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ and $k \in \mathbb{N}$, for any $s \in S$ and $\rho \in \mathcal{D}(\mathcal{H})$,*

$$\operatorname{tr}(R^k_s(\rho)) = \operatorname{tr}(P_k \mathcal{E}^\infty_{\mathcal{M}}(|s\rangle\langle s| \otimes \rho))$$

where $\mathcal{E}^\infty_{\mathcal{M}} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}^n_{\mathcal{M}}$.

Proof. First we lift the set of super-operators R^k_s on $\mathcal{H}$ to $\mathcal{H}_c \otimes \mathcal{H}$ by defining $\widetilde{R}^k \overset{\text{def}}{=} \sum_{t\in S} \mathcal{E}_t \otimes R^k_t$ where $\mathcal{E}_t = \{|t\rangle\langle t|\}$. Then Lemma 11 says that for any $n \geq 0$, $\operatorname{tr}(R^k_s(\rho)) = \operatorname{tr}(\widetilde{R}^k(\mathcal{E}^n_{\mathcal{M}}(\rho_s)))$ where $\rho_s \overset{\text{def}}{=} |s\rangle\langle s| \otimes \rho$. Thus we have

$$\operatorname{tr}(R^k_s(\rho)) = \operatorname{tr}\left(\widetilde{R}^k\left(\frac{1}{N}\sum_{n=1}^{N} \mathcal{E}^n_{\mathcal{M}}(\rho_s)\right)\right)$$

for any $N \geq 1$, and so $\operatorname{tr}(R^k_s(\rho)) = \operatorname{tr}(\widetilde{R}^k \mathcal{E}^\infty_{\mathcal{M}}(\rho_s))$ by letting N tend to infinity.

On the other side, note that $\rho^\infty_s \overset{\text{def}}{=} \mathcal{E}^\infty_{\mathcal{M}}(\rho_s)$ is a fixed point state of $\mathcal{E}_{\mathcal{M}}$. Then by Lemma 12 and [4, Theorem 6], $P_T \rho^\infty_s P_T = 0$, and ρ^∞_s is block diagonal with respect to $\mathcal{BSCC}_k$, $\mathcal{BSCC}_{k^-}$, and $\mathcal{BSCC}_{k^+}$; that is, $\rho^\infty_s = P_k \rho^\infty_s P_k + P_{k^-} \rho^\infty_s P_{k^-} + P_{k^+} \rho^\infty_s P_{k^+}$. Thus from Lemma 13,

$$\begin{aligned}\operatorname{tr}(R^k_s(\rho)) &= \operatorname{tr}(\widetilde{R}^k(P_k \rho^\infty_s P_k)) + \operatorname{tr}(\widetilde{R}^k(P_{k^-} \rho^\infty_s P_{k^-})) + \operatorname{tr}(\widetilde{R}^k(P_{k^+} \rho^\infty_s P_{k^+}))\\ &= \operatorname{tr}(P_k \rho^\infty_s).\end{aligned}$$ ◀

The following corollary, which is direct from Theorem 14, provides us a neat way to represent the value of a PQMC at a given state using certain super-operators without resorting to quantum states.

▶ **Corollary 15.** *Let $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ be a PQMC. Then for any $s \in S$,*

$$\mathrm{val}^{\mathcal{M}}_s \eqsim \operatorname{tr}_c \circ \mathcal{P}_{even} \circ \mathcal{E}^\infty_{\mathcal{M}} \circ \mathcal{E}_s$$

where tr_c is the partial trace super-operator such that $\operatorname{tr}_c(|s\rangle\langle t| \otimes \rho) = \langle t|s\rangle \cdot \rho$, $\mathcal{P}_{even} = \sum_{\{k\in\mathsf{pri}(S) \mid k \text{ is even}\}} \mathcal{P}_k$ where $\mathcal{P}_k = \{P_k\}$ is the projection super-operator onto $\mathcal{BSCC}_k$, and $\mathcal{E}_s(\rho) = |s\rangle\langle s| \otimes \rho$.

Note that in the above corollary, we do not calculate the value $\mathrm{val}^{\mathcal{M}}_s$ directly. Instead, only a super-operator which is *trace equivalent* to $\mathrm{val}^{\mathcal{M}}_s$ is obtained. Note that from [16, Theorem 3.2], the super-operator valued measure for a QMC (thus PQMC) is well-defined only up to the trace equivalence $\eqsim$. In other words, it does not make sense to talk about the *exact* super-operator associated with a measurable set of paths; only the equivalence class determined by $\eqsim$ is meaningful. Fortunately, this is sufficient for our purpose, as in practice we are interested in the *probability* of satisfying a certain ω-property, starting from an initial quantum state, which depends only on the equivalence class that the super-operator like $\mathrm{val}^{\mathcal{M}}_s$ is in.

▶ **Example 16** (Example 10 revisited)**.** Let $\mathcal{M}$ be the PQMC depicted on the right of Fig. 1 where $\mathcal{E}_0 \overset{\text{def}}{=} \{|0\rangle\langle 0|\}$ and $\mathcal{E}_1 \overset{\text{def}}{=} \{|1\rangle\langle 1|\}$. Then the super-operator encoding $\mathcal{M}$ is

$$\begin{aligned}\mathcal{E}_{\mathcal{M}} = \quad & \{|s_1\rangle\langle s_0|\} \otimes \mathcal{E}_0 + \{|s_0\rangle\langle s_0|\} \otimes \mathcal{E}_1\\ &+ \{|s_1\rangle\langle s_1|\} \otimes \mathcal{E}_1 + \{|s_2\rangle\langle s_1|\} \otimes \mathcal{E}_0\\ &+ \{|s_1\rangle\langle s_2|\} \otimes \mathcal{E}_0 + \{|s_2\rangle\langle s_2|\} \otimes \mathcal{E}_1,\end{aligned}$$

the maximal transient space of $\mathcal{E}_\mathcal{M}$ is $T \overset{\text{def}}{=} \operatorname{span}\{|s_0\rangle|0\rangle\}$, and the BSCCs are

$$B_1 \overset{\text{def}}{=} \operatorname{span}\{|s_0\rangle|1\rangle\}, \qquad B_2 \overset{\text{def}}{=} \operatorname{span}\{|s_1\rangle|1\rangle\},$$
$$B_3 \overset{\text{def}}{=} \operatorname{span}\{|s_1\rangle|0\rangle, |s_2\rangle|0\rangle\}, \qquad B_4 \overset{\text{def}}{=} \operatorname{span}\{|s_2\rangle|1\rangle\}.$$

Thus $\mathcal{BSCC}_0 = \bigvee\{B_1, B_2, B_3\}$, and $P_0 = |s_0\rangle\langle s_0| \otimes |1\rangle\langle 1| + |s_1\rangle\langle s_1| \otimes I + |s_2\rangle\langle s_2| \otimes |0\rangle\langle 0|$. Furthermore, we calculate that for any $n \geq 1$, $\mathcal{E}_\mathcal{M}^{2n-1} = \mathcal{F}_0 \otimes \mathcal{E}_0 + \mathcal{F} \otimes \mathcal{E}_1$ and $\mathcal{E}_\mathcal{M}^{2n} = \mathcal{F}_1 \otimes \mathcal{E}_0 + \mathcal{F} \otimes \mathcal{E}_1$ where $\mathcal{F}_0 \overset{\text{def}}{=} \{|s_1\rangle\langle s_0|, |s_2\rangle\langle s_1|, |s_1\rangle\langle s_2|\}$, $\mathcal{F}_1 \overset{\text{def}}{=} \{|s_2\rangle\langle s_0|, |s_1\rangle\langle s_1|, |s_2\rangle\langle s_2|\}$, and $\mathcal{F} \overset{\text{def}}{=} \{|s_0\rangle\langle s_0|, |s_1\rangle\langle s_1|, |s_2\rangle\langle s_2|\}$. Thus $\mathcal{E}_\mathcal{M}^\infty = \frac{\mathcal{F}_0+\mathcal{F}_1}{2} \otimes \mathcal{E}_0 + \mathcal{F} \otimes \mathcal{E}_1$, and

$$\mathcal{P}_0 \circ \mathcal{E}_\mathcal{M}^\infty = \frac{\mathcal{F}_0 + \mathcal{F}_1}{2} \otimes \mathcal{E}_0 + (\mathcal{P}_{s_0} + \mathcal{P}_{s_1}) \otimes \mathcal{E}_1.$$

Note that $\mathcal{E}_s = \{|s\rangle \otimes I\}$ and $\operatorname{tr}_c = \{\, \langle s_i| \otimes I \mid i = 0, 1, 2\,\}$. It follows that

$$\operatorname{val}_s^\mathcal{M} \eqsim \operatorname{tr}_c \circ \mathcal{P}_0 \circ \mathcal{E}_\mathcal{M}^\infty \circ \mathcal{E}_s = \begin{cases} \mathcal{E}_0 + \mathcal{E}_1 \eqsim \mathcal{I}_\mathcal{H} & \text{if } s = s_0 \vee s = s_1 \\ \mathcal{E}_0 & \text{if } s = s_2, \end{cases}$$

coinciding with the informal discussion given in Example 10.

4 The algorithm

In this section, we propose an algorithm to compute the values of a PQMC. First, we introduce some notations. For a super-operator $\mathcal{E} = \{\, E_i \mid i \in I\,\}$ acting on Hilbert space $\hat{\mathcal{H}}$, let $M_\mathcal{E} = \sum_{i \in I} E_i \otimes E_i^*$ be its matrix representation which is a linear operator on $\hat{\mathcal{H}} \otimes \hat{\mathcal{H}}$. Here the complex conjugate E_i^* is taken according to an orthonormal basis of $\hat{\mathcal{H}}$. It is easy to check that $M_\mathcal{E}$ is independent of the choices of orthonormal basis and Kraus operators E_i of $\mathcal{E}$. Let $M_\mathcal{E} = KJK^{-1}$ be the Jordan decomposition of $M_\mathcal{E}$ where $J = \bigoplus_k J_{\lambda_k}$ and J_{λ_k} is a Jordan block corresponding to the eigenvalue λ_k. Define

$$J^\infty = \bigoplus_{\{\, k | \lambda_k = 1\,\}} J_{\lambda_k} \tag{2}$$

and $M_\mathcal{E}^\infty = KJ^\infty K^{-1}$. Then from [30, Proposition 6.3], $M_\mathcal{E}^\infty$ is the matrix representation of $\mathcal{E}_\infty$.

▶ **Theorem 17.** *Given a PQMC $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ on $\mathcal{H}$ and a classical state $s \in S$, Algorithm 1 computes the matrix representation of a super-operator which is trace equivalent to $\operatorname{val}_s^\mathcal{M}$ in time $O(n^8 d^8)$, where $n = |S|$ and $d = \dim(\mathcal{H})$.*

Proof. Note that for any super-operators $\mathcal{E}$ and $\mathcal{F}$, the matrix representation of $\mathcal{E} \circ \mathcal{F}$ is the product of matrix representations of $\mathcal{E}$ and $\mathcal{F}$; that is, $M_{\mathcal{E}\mathcal{F}} = M_\mathcal{E} \times M_\mathcal{F}$. Then the correctness of Algorithm 1 follows from Corollary 15. The Procedure GetBSCC which, given a super-operator $\mathcal{E}$ and an invariant subspace of $\mathcal{E}$, outputs a complete set of orthogonal BSCCs in that subspace is a revised version of the procedure Decompose from [32].

Note that $\dim(\mathcal{H}_c \otimes \mathcal{H}) = nd$, and the matrix representation of $\mathcal{E}_\mathcal{M}$ has size $n^2d^2 \times n^2d^2$. The complexity of Algorithm 1 can be estimated as follows.

1. The time complexity of computing the matrix representation M of $\mathcal{E}_\mathcal{M}$ is $\sum_{s,t \in S} m_{s,t} d^4 = O(n^2 d^6)$, where $m_{s,t} \overset{\text{def}}{=} |I^{s,t}| \leq d^2$ is the number of Kraus operators in $\mathbf{Q}(s,t)$.
2. Note that the time complexity of Jordan decomposition is $O(m^4)$ for an $m \times m$ matrix. The computation of matrix representation M^∞ of $\mathcal{E}_\mathcal{M}^\infty$ takes time $O(n^8 d^8)$.

Algorithm 1: Compute the values of a PQMC

```
input  : A PQMC $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ on $\mathcal{H}$ and a classical state $s \in S$.
output : (Matrix representation of) a super-operator that is trace equivalent to $\mathrm{val}_s^{\mathcal{M}}$.
begin
    (* Compute the matrix representations of $\mathcal{E}_s$, $\mathrm{tr}_c$, and $\mathcal{E}_{\mathcal{M}}$*)
    $E_s \leftarrow |s\rangle \otimes I_{\mathcal{H}}$; $M_s \leftarrow E_s \otimes E_s^*$;
    $M_c \leftarrow 0$;
    for $t \in S$ do
        $E \leftarrow \langle t| \otimes I_{\mathcal{H}}$; $M_c \leftarrow M_c + E \otimes E^*$;
    end
    $M \leftarrow 0$;
    for $t, t' \in S$ and $i \in I^{t,t'}$ do
        $E \leftarrow |t'\rangle\langle t| \otimes E_i^{t,t'}$; $M \leftarrow M + E \otimes E^*$;        (* $\mathbf{Q}(t,t') = \{ E_i^{t,t'} \mid i \in I^{t,t'} \}$*)
    end
    (* Compute the matrix representation of $\mathcal{E}_{\mathcal{M}}^{\infty}$ *)
    $(K, J) \leftarrow$ Jordan decomposition of $M$;                  (* $M = KJK^{-1}$ *)
    $M^{\infty} \leftarrow KJ^{\infty}K^{-1}$;                          (* $J^{\infty}$ is defined in Eq.(2) *)
    (* Compute the matrix representation of $\mathcal{P}_{even}$ *)
    $M_{even} \leftarrow 0$; $I_c \leftarrow \sum_{t \in S} |t\rangle\langle t|$;
    $\mathcal{B} \leftarrow \mathrm{GetBSCC}(M, I_c \otimes I_{\mathcal{H}})$;
    $EP \leftarrow \{ \mathsf{pri}(t) \mid t \in S \wedge \mathsf{pri}(t) \text{ is even} \}$;
    for $k \in EP$ do
        $P_k \leftarrow 0$;
        for $B \in \mathcal{B}$ with $k = \min\{ \mathsf{pri}(t) \mid t \in C(B) \}$ do
            $P_k \leftarrow P_k + P_B$ where $P_B$ is the projector onto $B$;
        end
        $M_{even} \leftarrow M_{even} + P_k \otimes P_k$;
    end
    return $M_c \times M_{even} \times M^{\infty} \times M_s$;  (* $\times$ denotes normal matrix multiplication *)
end
```

3. For the Procedure $\mathrm{GetBSCC}(M, I_{\hat{\mathcal{H}}})$ where $I_{\hat{\mathcal{H}}} \overset{\text{def}}{=} \mathcal{H}_c \otimes \mathcal{H}$, the most time-consuming step is to compute the null space of the matrix $I_{\hat{\mathcal{H}}} \otimes I_{\hat{\mathcal{H}}} - M$. This can be done by Guassian elimination with complexity being $O((n^2d^2)^3) = O(n^6d^6)$. Note that each recursive call of the procedure decreases the dimension of the subspace by at least one. The complexity of computing $\mathrm{GetBSCC}(M, I_{\hat{\mathcal{H}}})$ is $O(n^7d^7)$. ◀

At the first glance, the time complexity $O(n^8d^8)$ of Algorithm 1 looks very high. However, note that a typical super-operator on a d-dimensional Hilbert space has up to d^2 Kraus operators each of them is a $d \times d$ complex matrix. Thus the input size K of a PQMC $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ is actually of order $O(n^2d^4)$ with $n = |S|$. Thus the time complexity of Algorithm 1 is indeed $O(K^4)$.

Note that the decomposition of M (the matrix representation of $\mathcal{E}_{\mathcal{M}}$) into Jordan blocks in Algorithm 1 is quite expensive. Therefore, for a practical implementation, an approximate approach might be preferable. From $\mathcal{E}_{\mathcal{M}}^{\infty} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}_{\mathcal{M}}^{n}$ (cf. Theorem 14) we can derive its matrix representation $M^{\infty} = \lim_{N\to\infty} M_N$ where $M_N \overset{\text{def}}{=} \frac{1}{N} \sum_{n=1}^{N} M^n$. We then

```
Procedure GetBSCC($M, P$)
input  : The matrix representation $M$ of a super-operator $\mathcal{E}$ acting on $\hat{\mathcal{H}} \overset{\text{def}}{=} \mathcal{H}_c \otimes \mathcal{H}$,
         and a projector $P$ to some invariant subspace $\mathcal{H}' \subseteq \hat{\mathcal{H}}$ of $\mathcal{E}$.
output : A complete set of orthogonal BSCCs of $\mathcal{E}$ in $\mathcal{H}'$.
begin
    $\{ |\psi_i\rangle \mid i \in I \} \leftarrow$ an orthonormal basis of $\hat{\mathcal{H}}$;
    $\mathcal{X} \leftarrow$ a basis of $\{ |x\rangle \in \mathcal{H}' \otimes \mathcal{H}' \mid M|x\rangle = |x\rangle \}$;
    $F \leftarrow \emptyset$;
    for $|x\rangle \in \mathcal{X}$ do
        $X \leftarrow \sum_{i \in I} (I_{\hat{\mathcal{H}}} \otimes \langle\psi_i|) \cdot |x\rangle\langle\psi_i|$;
                (* The matrix $X$ corresponds to $|x\rangle$ in that $X = \sum_{i,j \in I} x_{i,j} |\psi_i\rangle\langle\psi_j|$ iff
         $|x\rangle = \sum_{i,j \in I} x_{i,j} |\psi_i\rangle|\psi_j\rangle$ *)
        $X_R \leftarrow (X + X^\dagger)/2$; $X_I \leftarrow (X - X^\dagger)/2i$ ;
                            (* $X^\dagger$ denotes the transpose and complex conjugate of $X$ *)
        $P_R^+ \leftarrow$ the projector onto eigenspace of $X_R$ with positive eigenvalues;
        $P_I^+ \leftarrow$ the projector onto eigenspace of $X_I$ with positive eigenvalues;
        $X_R^+ = P_R^+ X_R P_R^+$; $X_R^- = X_R^+ - X_R$;
        $X_I^+ = P_I^+ X_I P_I^+$; $X_I^- = X_I^+ - X_I$;
        (* All of them are positive semidefinite, and $X = X_R^+ - X_R^- + i(X_I^+ - X_I^-)$ *)
        for $Y \in \{X_R^+, X_R^-, X_I^+, X_I^-\} \wedge Y \neq 0$ do
            $F \leftarrow F \cup \{Y/\mathrm{tr}(Y)\}$;                (* Fixed point states of $\mathcal{E}$ *)
        end
    end
    if $|F| = 1$ then
        return $\{\mathrm{supp}(Y)\}$;                        (* $Y$ is the only element of $F$ *)
    else
        $Y_1, Y_2 \leftarrow$ two arbitrary different elements of $F$;
        $P^+ \leftarrow$ the projector onto eigenspace of $Y_1 - Y_2$ with positive eigenvalues;
        $P^- \leftarrow P - P^+$;
        $M^+ \leftarrow (P^+ \otimes I_{\hat{\mathcal{H}}}) M (I_{\hat{\mathcal{H}}} \otimes P^+)$;
        $M^- \leftarrow (P^- \otimes I_{\hat{\mathcal{H}}}) M (I_{\hat{\mathcal{H}}} \otimes P^-)$;
        return GetBSCC($M^+, P^+$) $\cup$ GetBSCC($M^-, P^-$);
    end
end
```

compute $M_0, M_1, M_2, \ldots$ until we have reached an N for which $\|M_N - M_{N-1}\|_{\max} < \varepsilon$ for a predefined precision ε, so as to obtain an approximation of M^∞. Note that M_N can be computed using a dynamic programming approach by means of the equality

$$M_N = \begin{cases} M & \text{if } N = 1, \\ \frac{1}{N}((N-1)M_{N-1} + M^N) & \text{if } N > 1. \end{cases}$$

In stochastic model checking, such value iteration based approaches are commonly used, and in [15], we have successfully applied a similar method for model checking QCTL Until formulas.

5 Conclusion

In this paper, we have investigated model checking ω-regular and in particular LTL properties against super-operator weighted quantum Markov chains, which can be used to faithfully model a practically relevant class of quantum processes. As future work, we would like to implement our model checking algorithm in IscasMC [20] and apply it on case studies from the area of quantum communication protocols and evaluate the actual performance of our approach.

References

1 Ebrahim Ardeshir-Larijani, Simon J. Gay, and Rajagopal Nagarajan. Equivalence checking of quantum protocols. In *TACAS*, volume 7795 of *LNCS*, pages 478–492, 2013.

2 Ebrahim Ardeshir-Larijani, Simon J. Gay, and Rajagopal Nagarajan. Verification of concurrent quantum protocols by equivalence checking. In *TACAS*, volume 8413 of *LNCS*, pages 500–514, 2014.

3 Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. The MIT Press, 2008.

4 Bernhard Baumgartner and Heide Narnhofer. The structures of state space concerning Quantum Dynamical Semigroups. *Reviews in Mathematical Physics*, 24(02):1250001, 2012.

5 Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68:3121, 1992.

6 Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing*, pages 175–179, 1984.

7 Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

8 Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Panagiotis Katsaros, Konstantinos Mokos, Viet Yen Nguyen, Thomas Noll, Bart Postma, and Marco Roveri. Spacecraft early design validation using formal methods. *Reliability Engineering and System Safety*, 132:20–35, 2014.

9 Doron Bustan, Sasha Rubin, and Moshe Y Vardi. Verifying omega-regular properties of Markov chains. In *CAV*, volume 4, pages 189–201, 2004.

10 Taolue Chen, Marco Diciolla, Marta Kwiatkowska, and Alexandru Mereacre. Quantitative verification of implantable cardiac pacemakers. In *Real-Time Systems Symposium*, pages 263–272, 2012.

11 Edmund M Clarke, Orna Grumberg, and Doron Peled. *Model checking*. MIT press, 1999.

12 Costas Courcoubetis and Mihalis Yannakakis. The complexity of probabilistic verification. *JACM*, 42(4):857–907, 1995.

13 Luca de Alfaro. *Formal Verification of Probabilistic Systems*. PhD thesis, Stanford University, 1997.

14 E. Allen Emerson and Charanjit S. Jutla. Tree automata, mu-calculus and determinacy. In *FOCS*, SFCS, pages 368–377. IEEE CS, 1991.

15 Yuan Feng, Ernst Moritz Hahn, Andrea Turrini, and Lijun Zhang. QPMC: A model checker for quantum programs and protocols. In *FM'15*, volume 9109 of *Lecture Notes in Computer Science*, pages 265–272. Springer, 2015.

16 Yuan Feng, Nengkun Yu, and Mingsheng Ying. Model checking quantum Markov chains. *Journal of Computer and System Sciences*, 79(7):1181–1198, 2013.

17 Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. Probabilistic model-checking of quantum protocols. In *Proceedings of the 2nd International Workshop on Developments in Computational Models*, 2006.

18 Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. QMC: A model checker for quantum systems. In *CAV 08*, pages 543–547. Springer, 2008.

19 Stanley Gudder. Quantum Markov chains. *Journal of Mathematical Physics*, 49(7):072105, 14, 2008.

20 Ernst Moritz Hahn, Yi Li, Sven Schewe, Andrea Turrini, and Lijun Zhang. IscasMC: A web-based probabilistic model checker. In *FM'14*, volume 8442 of *Lecture Notes in Computer Science*, pages 312–317. Springer, 2014.

21 Khaza Anuarul Hoque, Otmane Aït Mohamed, and Yvon Savaria. Towards an accurate reliability, availability and maintainability analysis approach for satellite systems based on probabilistic model checking. In *Design, Automation & Test in Europe*, pages 1635–1640, 2015.

22 Lvzhou Li and Yuan Feng. Quantum markov chains: description of hybrid systems, decidability of equivalence, and model checking linear-time properties. *Information and Computation*, 244:229–244, 2015.

23 Andrzej Wlodzimierz Mostowski. Regular expressions for infinite trees and a standard form of automata. In *Computation Theory*, volume 208 of *LNCS*, pages 157–168. Springer, 1984.

24 Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2000.

25 Nir Piterman. From nondeterministic Büchi and Streett automata to deterministic parity automata. *JLMCS*, 3(3:5), 2007.

26 Shmuel Safra. On the complexity of ω-automata. In *FOCS*, pages 319–327, 1988.

27 Sven Schewe. Tighter bounds for the determinisation of Büchi automata. In *FoSSaCS*, volume 5504 of *LNCS*, pages 167–181, 2009.

28 Peter Selinger. A brief survey of quantum programming languages. *Functional and Logic Programming*, 2998:1–6, 2004.

29 Wolfgang Thomas. Automata on infinite objects. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science (Vol. B)*, pages 133–191. MIT Press, Cambridge, MA, USA, 1990.

30 Michael M Wolf. Quantum channels & operations: Guided tour. *https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf*, 2012.

31 Mingsheng Ying, Yangjia Li, Nengkun Yu, and Yuan Feng. Model-checking linear-time properties of quantum systems. *ACM Transactions on Computational Logic (TOCL)*, 15(3):22, 2014.

32 Shenggang Ying, Yuan Feng, Nengkun Yu, and Mingsheng Ying. Reachability probabilities of quantum markov chains. In *CONCUR'13*, pages 334–348. Springer, 2013.