Measurement-Based Verification of Quantum Markov Chains

Ji Guan[1(✉)], Yuan Feng[2], Andrea Turrini[1,3(✉)], and Mingsheng Ying[4]

[1] Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
{guanj,turrini}@ios.ac.cn
[2] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[3] Institute of Intelligent Software, Guangzhou 511458, China
[4] Centre for Quantum Software and Information, University of Technology Sydney, Sydney, NSW 2007, Australia

Abstract. Model-checking techniques have been extended to analyze quantum programs and communication protocols represented as quantum Markov chains, an extension of classical Markov chains. To specify qualitative temporal properties, a subspace-based quantum temporal logic is used, which is built on Birkhoff-von Neumann atomic propositions. These propositions determine whether a quantum state is within a subspace of the entire state space. In this paper, we propose the measurement-based linear-time temporal logic MLTL to check quantitative properties. MLTL builds upon classical linear-time temporal logic (LTL) but introduces quantum atomic propositions that reason about the probability distribution after measuring a quantum state. To facilitate verification, we extend the symbolic dynamics-based techniques for stochastic matrices described by Agrawal et al. (JACM 2015) to handle more general quantum linear operators (super-operators) through eigenvalue analysis. This extension enables the development of an efficient algorithm for approximately model checking a quantum Markov chain against an MLTL formula. To demonstrate the utility of our model-checking algorithm, we use it to simultaneously verify linear-time properties of both quantum and classical random walks. Through this verification, we confirm the previously established advantages discovered by Ambainis et al. (STOC 2001) of quantum walks over classical random walks and discover new phenomena unique to quantum walks.

1 Introduction

Model checking is a formal verification technique that is used to ensure the correctness of a system based on a given specification [1]. In recent years, model checking has been applied to quantum systems and has become a powerful tool for verifying the behaviors and properties of quantum programs or communication protocols [2,3]. Similar to the classical case, the main components of model

A. Gurfinkel and V. Ganesh (Eds.): CAV 2024, LNCS 14683, pp. 533–554, 2024.
https://doi.org/10.1007/978-3-031-65633-0_24

checking quantum systems are the system model and the temporal logic, which are used to mathematically describe the evolution of the system and specify its temporal properties, respectively.

System Model. Quantum Markov Chains (QMCs), which are the quantum extension of classical *Markov chains* (MCs), provide an exceptional paradigm for modeling the evolution of quantum systems in various scenarios, including quantum control [4], quantum information theory [5], quantum programming [6], and quantum communication systems [7]. Notably, quantum walks, which are a special class of QMCs, have been successfully employed in the design of quantum algorithms (for a survey of this research line, see [8,9]). A QMC $\mathcal{Q}$ is defined as a triple $\mathcal{Q} = (\mathcal{H}, \mathcal{E}, \rho_0)$ that corresponds to a classical Markov chain (S, P, s_0), where $\mathcal{H}$ is a finite-dimensional Hilbert (linear) state space instead of the finite state set S, $\mathcal{E}$ is a *super-operator* on $\mathcal{H}$ instead of the transition stochastic matrix P on S, and ρ_0, which is a *density matrix*, represents the initial state instead of s_0. Intuitively, the super-operator $\mathcal{E}(\cdot)$, which is a linear mapping, models the dynamics of the system and transforms a state (density matrix) ρ into another state $\mathcal{E}(\rho)$. Some special cases of QMCs have emerged, such as open quantum walks [10] and classical-quantum (super-operator valued) Markov chains [11], where the latter resemble classical Markov chains but with the transition stochastic matrix $P = \{p_{i,j}\}_{i,j \in S}$ being replaced by a transition set $\{\mathcal{E}_{i,j}\}_{i,j \in S}$ of super-operators, while still maintaining the finite state set S.

Temporal Logics. The dynamic extension of Birkhoff-von Neumann quantum logic [12] was proposed to specify a wide range of temporal properties of quantum systems. In this approach, atomic propositions are used to describe qualitative properties of a quantum system, represented as closed subspaces of the system's state Hilbert space (whether or not a quantum state ρ is in a subspace $\mathcal{X}$ of $\mathcal{H}$). Furthermore, QMCs are abstracted as subspace transition systems, and the temporal properties of interest are represented by infinite sequences of sets of atomic propositions (subspaces) [3]. This subspace-based temporal logic allows for the specification of linear-time properties, such as invariants and safety properties, for quantum automata (a simplified form of QMCs) [13]. Model-checking algorithms have been developed for the subspace-based temporal logic in [14], and the (un)decidability of model checking quantum automata has been studied in [15]. However, a limitation of model checking QMCs against subspace-based temporal logics is that it can only handle qualitative properties, which means that only simple examples can be checked. Given that the power of quantum systems lies in their probabilistic nature, it is crucial to be able to check probabilistic (quantitative) properties.

To address this issue, in this paper, we propose a measurement-based linear-time temporal logic to capture these properties and develop a model-checking algorithm to check the quantitative properties of QMCs. More specifically, we observe that the properties of the quantum systems in question can be described using quantum measurements, which extract classical (probabilistic) information from quantum states. Building on this observation, we introduce measurement-based atomic propositions to describe static quantitative properties, namely, the

measurement outcome probability of a quantum state under a measurement. This can be seen as a generalization of the subspace-based atomic propositions of the Birkhoff-von Neumann quantum logic [12], where a quantum state ρ in a subspace $\mathcal{X} \subseteq \mathcal{H}$ can be regarded as having a measurement outcome probability of 1 under the measurement onto $\mathcal{X}$. By combining with standard linear-time temporal logic (LTL) [1,16], we obtain MLTL, the measurement-based LTL, to specify the temporal quantitative properties of quantum systems.

In order to develop an algorithm for model checking QMCs against MLTL formulas, we extend the Thiagarajan's approximate verification [17] of a stochastic transition matrix P to encompass more general linear operators in quantum systems, e.g., the super-operators. The key technique for this generalization is based on the eigenvalue analysis of QMCs, which simplifies the previous work based on the *Bottom Strongly Connected Component (BSCC) decomposition* [1] of the state space of classical Markov chains [17]. Subsequently, we provide an effective procedure for the approximate model checking of QMCs against MLTL formulas. In Sect. 6, we provide several case studies to illustrate how our model and algorithm can be applied in a quantum walk. These case studies help to verify the previously established advantages of quantum walks over classical random walks, as discovered by Ambainis et al. [18]. Additionally, we explore new phenomena unique to quantum walks when we verify the same MLTL formulas on both types of walks.

In summary, this paper makes the following main contributions:

1. *Introducing* a quantum temporal logic, called measurement-based linear-time logic (MLTL), which allows for specifying quantitative properties of QMCs.
2. *Generalizing* symbolic dynamics-based verification techniques of the transition stochastic matrix given in [17] to more general quantum linear operators (super-operators) by *eigenvalue analysis*; based on this, a model-checking algorithm for QMCs against MLTL is developed.
3. *Verifying* numerous quantitative properties of quantum walks through our model-checking algorithm as case studies. This serves to validate the established advantages of quantum walks over their classical counterparts and discover new phenomena unique to quantum walks.

1.1 Related Works and Challenges

To provide a suitable context for our work, let us delve deeper into the discussion of related works and the challenges we encounter in this paper.

Hybrid vs. Quantum Temporal Logic. In a previous study [11,19], a specialized type of quantum Markov chain known as super-operator-valued quantum Markov chain was proposed. This model was designed for the purpose of modeling quantum programs and quantum cryptographic protocols. Additionally, a quantum extension of the probabilistic computation tree logic (PCTL) called quantum computation tree logic (QCTL) was introduced, along with a

model-checking algorithm specifically tailored for this Markov model. In a subsequent development, algorithms for verifying ω-regular properties were also introduced [20].

However, these hybrid temporal logic approaches heavily rely on the classical state graph and are not applicable to quantum systems. This is because quantum systems have a continuous state space and an infinite number of states, making it impossible to obtain a connection graph. In order to address this limitation and specify the properties of quantum Markov chains, we propose a measurement-based linear-time temporal logic (MLTL) approach that does not require a connection graph. This allows us to directly reason about the transitions of measurement outcome probability distributions. Our MLTL approach adopts classical LTL with quantum physical interpretation, providing the advantage of utilizing existing classical techniques and facilitating contributions from the classical model-checking community to the field of quantum computing.

Classical vs. Quantum Markov Chains. The main technique used for model checking classical Markov chains in [17] involves studying the periodicity of states in sub-chains obtained through BSCC decomposition [1], a widely-used method in the field of model checking Markov chains. However, when it comes to the quantum extension of this decomposition, as described in [21], the BSCC decomposition of QMCs is not unique but there are infinitely many decompositions due to the continuous state space, unlike the classical case. Consequently, we cannot directly generalize Thiagarajan's *approximate verification* [17]. To overcome this unique challenge posed by quantum mechanics, we propose a method based on eigenvalue analysis to directly explore the periodic properties of QMCs. As a result, QMCs are not always periodically stable like classical Markov chains. We provide a way to determine the periodic stability depending on the initial states of QMCs. With these efforts, we successfully extend the idea of approximate model checking to work for QMCs, pushing the application boundary of such model-checking techniques to more general linear systems.

Model Checking Quantum Walks. As a result of the phenomenon known as *quantum interference* [22], quantum walks can propagate at significantly faster or slower rates compared to their classical counterparts [18]. Quantum walks have gained attention due to their potential application in the development of randomized algorithms, with various quantum algorithms incorporating this concept [8,9]. Notably, in certain search problems, quantum walks can offer quadratic or exponential speedups compared to classical algorithms.

Previously, researchers have conducted case-by-case studies on the dynamic properties of quantum walks, requiring the introduction of various techniques depending on the specific property and underlying topological structure of the walks. In this paper, we introduce a model-checking method that overcomes this limitation by allowing for the automatic verification of a wide range of properties of the walks. To model quantum walks, we utilize QMCs, and to specify the relevant dynamical properties, we employ MLTL formulas. By simultaneously verifying classical and quantum walks using our model-checking algorithm, we can confirm the advantages of quantum walks that have already been estab-

lished in [18], as well as discover new phenomena that are distinct from classical random walks. We anticipate that these new phenomena, discovered by our model-checking algorithm, will contribute to the development of more efficient quantum walk-based algorithms with enhanced speedup capabilities.

2 Preliminaries

In this section, we aim to explain the three components that appear in a QMC $\mathcal{Q} = (\mathcal{H}, \mathcal{E}, \rho_0)$, as well as quantum measurements, an essential part of our MLTL.

Quantum State Space. $\mathcal{H}$. The *state space* of a quantum system is a finite-dimensional linear space $\mathcal{H}$, which is commonly known as the *Hilbert space* in the field of quantum computing. A *quantum pure state* is represented by a unit complex column vector ψ in $\mathcal{H}$. In the field of quantum computing, the *bra-ket notation* is widely used to represent quantum states, making it easier to perform calculations that frequently arise in quantum mechanics. This notation uses angle brackets, $\langle$ and $\rangle$, along with a vertical bar $|$, to construct "bras" and "kets" that represent row and column vectors, respectively. The following list provides the notation used in this paper to represent linear algebra concepts:

1. $|\psi\rangle$ represents a unit complex column vector (quantum pure state) in $\mathcal{H}$, labeled with ψ;
2. $\langle\psi| := |\psi\rangle^\dagger$ denotes the complex conjugate and transpose of $|\psi\rangle$;
3. $\langle\psi_1|\psi_2\rangle := \langle\psi_1||\psi_2\rangle$ represents the inner product of $|\psi_1\rangle$ and $|\psi_2\rangle$;
4. $|\psi_1\rangle\langle\psi_2| := |\psi_1\rangle \cdot \langle\psi_2|$ denotes the outer product of $|\psi_1\rangle$ and $|\psi_2\rangle$.

It is important to note that any vector in $\mathcal{H}$ can be linearly represented by a *computational basis*, which is a set of mutually orthogonal unit vectors. In order to compare with classical Markov chains denoted as (S, P, μ_0), we use the finite state set $S = \{s_0, \ldots, s_{d-1}\}$ to label the computational basis of $\mathcal{H}$, with dimension d, as $\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$. Here, $|s_k\rangle$ is a unit column vector with the k-th element being 1 and the remaining elements being 0 (the index starts from 0). Then $\mathcal{H}$ is denoted as $\mathcal{H} = \text{span}\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$.

Using this basis, any quantum state $|\psi\rangle$ in $\mathcal{H}$ can be expressed as a linear combination of $\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$ with complex coefficients a_k: $|\psi\rangle = \sum_{k=0}^{d-1} a_k|s_k\rangle$ with the normalization condition $\langle\psi|\psi\rangle = \sum_{k=0}^{d-1} a_k a_k^* = 1$, where a_k^* is the complex conjugate of a_k. In the case of a 2-dimensional space, we have:

$$|s_0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |s_1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix}a_0\\a_1\end{pmatrix} \qquad \langle\psi| = \begin{pmatrix}a_0^*, a_1^*\end{pmatrix}.$$

It is evident that a quantum pure state has the capability to depict a *superposition* of state set $S = \{s_0, \ldots, s_{d-1}\}$ as $|\psi\rangle = \sum_{k=0}^{d-1} a_k|s_k\rangle$. The superposition is a unique feature of quantum systems and the main reason for the advantages of quantum algorithms over their classical counterparts [23].

Quantum Mixed State ρ. In quantum mechanics, uncertainty is a common characteristic of quantum systems, arising from quantum noise and measurements. To describe the uncertainty of possible quantum pure states, the concept of *quantum mixed state* ρ on $\mathcal{H}$ is introduced. It can be represented as

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|. \tag{1}$$

Here, $\{(p_k, |\psi_k\rangle)\}_k$ represents an ensemble, indicating that the quantum state is at $|\psi_k\rangle$ with probability p_k. This concept can also be used to describe the uncertainty of a classical probability distribution, where each $|\psi_k\rangle$ represents s_k by $|\psi_k\rangle = |s_k\rangle$. Specifically, a (row) probability distribution $\mu = (p_0, \ldots, p_{d-1})$ over the state set $S = \{s_0, \ldots, s_{d-1}\}$ can be represented by a quantum mixed state. This representation involves a diagonal matrix on $\mathcal{H}$, where the diagonal elements correspond to the probabilities p_k as follows.

$$\rho_\mu = \sum_k p_k |s_k\rangle\langle s_k| = \mathrm{diag}(p_0, \ldots, p_{d-1}). \tag{2}$$

Hence, a quantum mixed state ρ is an extension of a probability distribution μ. Generally, the quantum uncertainty is more complex because the ensemble decomposition in Eq. (1) of a quantum state ρ can have infinitely many variants. This means that ρ can represent multiple ensembles $\{(p_k, |\psi_k\rangle)\}_k$ simultaneously.

From a mathematical perspective, a quantum mixed state $\rho \in \mathcal{L}(\mathcal{H})$ is a linear operator (d-by-d matrix) on $\mathcal{H}$ that satisfies three conditions: 1) *Hermitian* $\rho^\dagger = \rho$; 2) *positive semi-definite* $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$; and 3) *unit trace* $\mathrm{tr}(\rho) = \sum_k \langle s_k|\rho|s_k\rangle = 1$, where $\mathrm{tr}(\rho)$ is the trace of ρ and represents the sum of the diagonal elements of ρ. Here, $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators on $\mathcal{H}$. Let $\mathcal{D}(\mathcal{H}) \subseteq \mathcal{L}(\mathcal{H})$ be the set of all quantum mixed states on $\mathcal{H}$. To avoid any ambiguity, in the subsequent discussion, the term "quantum states" will specifically refer to quantum mixed states, given that we are considering the broader scenario.

Quantum Evolution $\mathcal{E}$. In the realm of quantum computing, the evolution of a quantum system is commonly represented by the equation

$$\rho' = \mathcal{E}(\rho). \tag{3}$$

Here, $\mathcal{E}$ is referred to as a *super-operator*. Mathematically, $\mathcal{E}(\,\cdot\,)$ is a linear mapping from $\mathcal{L}(\mathcal{H})$ to $\mathcal{L}(\mathcal{H})$, allowing for the transformation of one quantum state ρ into another ρ'. As stated by the *Kraus representation theorem* [24], $\mathcal{E}$ can be characterized by a finite set of d-by-d matrices $\{ E_k : 0 \leq k \leq m-1 \} \subseteq \mathcal{L}(\mathcal{H})$, where $m \leq d^2$. The expression is given by $\mathcal{E}(\rho) = \sum_{k=0}^{m-1} E_k \rho E_k^\dagger$ for all $\rho \in \mathcal{D}(\mathcal{H})$.

This representation also satisfies the trace-preserving condition $\sum_k E_k^\dagger E_k = I$, where I is the identity matrix on $\mathcal{H}$ and $\dagger$ denotes the complex conjugate and transpose of matrices. In other words, for all $\rho \in \mathcal{D}(\mathcal{H})$, we have $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\rho)$ by $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\sum_k E_k \rho E_k^\dagger) = \mathrm{tr}(\sum_k E_k^\dagger E_k \rho) = \mathrm{tr}(\rho)$.

An example of the use of super-operators can be found in Sect. 3.1, where a super-operator is employed to represent the evolution of quantum walks. In the degenerate scenario, the Kraus operator is simplified to only include a *unitary matrix* U on $\mathcal{H}$ (where $U^\dagger U = U^\dagger U = I$), and $\mathcal{E}(\rho) = U\rho U^\dagger$.

Quantum Measurement. To extract information from a quantum state, a *quantum measurement* is performed. This measurement yields a classical outcome which is represented as a probability distribution over the possible results. Mathematically, a quantum measurement is described by a set $\{M_k\}_{k\in\mathcal{O}}$ of positive semi-definite matrices on the state (Hilbert) space $\mathcal{H}$, where $\mathcal{O}$ is a finite set of possible outcomes. The measurement process is probabilistic: if the quantum system is in a state ρ before the measurement, the probability of obtaining the outcome k is given as follows.

$$p_k = \mathrm{tr}(M_k\rho).$$

Note that the measurement $\{M_k\}_{k\in\mathcal{O}}$ satisfies the *unity condition* $\sum_k M_k = I$, which guarantees that the total probability of all outcomes is equal to 1. In other words, $\sum_k \mathrm{tr}(M_k\rho) = \mathrm{tr}(\sum_k M_k\rho) = \mathrm{tr}(\rho) = 1$.

In the case where we want to extract the classical probability distribution μ encoded in the quantum state ρ_μ as shown in Eq. (2), we can choose the measurement $\{M_k = |s_k\rangle\langle s_k|\}_{s_k\in S}$. In this scenario, the measurement probability of obtaining outcome s_k is given by

$$\mathrm{tr}(|s_k\rangle\langle s_k|\rho_\mu) = \sum_l \langle s_l||s_k\rangle\langle s_k|\rho_\mu|s_l\rangle = \langle s_k|\rho_\mu|s_k\rangle = \langle s_k|(\sum_j p_j|s_j\rangle\langle s_j|)|s_k\rangle = p_k.$$

The above equations rely on the mutual orthogonality of the computational basis $\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$, meaning that $\langle s_j|s_l\rangle = 0$ for $j \neq l$, and also the fact that each $|s_k\rangle$ is normalized, represented by $\langle s_k|s_k\rangle = 1$.

It should be noted that after the measurement, the state will collapse or be altered, depending on the measurement outcome k, which distinguishes quantum computation from classical computation. For instance, in the case of a *projection measurement* denoted as $\{P_k\}_{k\in\mathcal{O}}$, the state after obtaining outcome k is given by $P_k\rho P_k/p_k$ with $p_k = \mathrm{tr}(P_k\rho)$. Here, each positive semi-definite matrix P_k represents a projection operator ($P_k^2 = P_k$), and a specific example of a projection measurement is the above measurement $\{|s_k\rangle\langle s_k|\}_{s_k\in S}$. Another concrete example is provided in Example 2 for the case of quantum walks. For other scenarios involving post-measurement states that are not encountered in this paper, please refer to [23, Section 2.2.3].

3 Quantum Markov Chains

In this section, we present the formal definition of QMCs. For a more detailed discussion, we refer the interested readers to [3].

Definition 1. *A QMC is a tuple $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$, where $\mathcal{H}$ is a finite-dimensional Hilbert space, $\mathcal{E}$ is a super-operator on $\mathcal{H}$, and $\rho_0 \in \mathcal{D}(\mathcal{H})$ is an initial state.*

The execution of $\mathcal{G}$ is naturally described by the trajectory of quantum states:

$$\sigma(\mathcal{G}) := \rho_0, \mathcal{E}(\rho_0), \mathcal{E}^2(\rho_0), \ldots. \tag{4}$$

QMCs are a direct extension of classical Markov chains and can simulate their execution; see the following example.

Example 1 (Classical Markov chains as QMCs). Not surprisingly, any classical Markov chain (S, P, μ_0) can be effectively encoded as a QMC. We can use $\mathcal{H} = \text{span}\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$ to encode S, and $\mathcal{E}$ can be a super-operator with Kraus operators $\{E_{k,l} = \sqrt{p_{k,l}}|s_l\rangle\langle s_k|\}_{s_k, s_l \in S}$ that encode the probabilities $p_{k,l}$ of P.

It can be easily verified that $\mathcal{E}$ is a valid super-operator, i.e., $\sum_{k,l} E_{k,l}^\dagger E_{k,l} = I$. Furthermore, let $\rho_0 = \sum_{s \in S} \mu_0(s)|s\rangle\langle s|$ encode the initial probability distribution μ_0. Then, the QMC $(\mathcal{H}, \mathcal{E}, \rho_0)$ can fully simulate the behavior of (S, P, μ_0) in the sense that for all $n \geq 0$:

$$\mathcal{E}^n(\rho_0) = \sum_{k=0}^{d-1} \mu_n(s_k)|s_k\rangle\langle s_k| = (\mu_n(s_0), \ldots, \mu_n(s_{d-1})).$$

Here, $\mu_n = \mu_0 P^n$, $\mu_n(s_k)$ represents the k-th entry of μ_n, and $\mathcal{E}^0 = \text{id}_{\mathcal{H}}$, which is the *identity super-operator* with only one Kraus operator $\{I\}$. The proof follows a straightforward induction on n.

3.1 Quantum Walks

The case study of this paper is to explore the new and advanced properties of quantum walks compared to classical random walks by model checking QMCs. This exploration begins with modeling quantum walks using QMCs. Before presenting this, we introduce one-dimensional quantum walks with absorbing boundaries in the following example. Furthermore, we also need the bra-ket notation $|\psi_1\rangle|\psi_2\rangle := |\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, which represents the composition (tensor product) of $|\psi_1\rangle$ and $|\psi_2\rangle$ in the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively.

Example 2 (Quantum walk with absorbing boundaries). We consider an unbiased quantum walk on a one-dimensional lattice indexed from s_0 to s_d, with the boundaries s_0 and s_d being absorbing.

State Space. Let $\mathcal{H}_p = \text{span}\{|s_0\rangle, \ldots, |s_d\rangle\}$ be a $(d+1)$-dimensional Hilbert space, where the pure state (unit vector) $|s_k\rangle$ represents the position s_k for each $0 \leq k \leq d$. In order to facilitate the evolution of the quantum walk, an additional coin space is required. Let $\mathcal{H}_c$ be the coin (direction) space, which is a 2-dimensional Hilbert space with orthonormal basis states $|L\rangle$ and $|R\rangle$, indicating the directions left and right, respectively. Therefore, the state space of the quantum walk is $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$.

Initial State. The initial state is $\rho_0 = |\psi_0\rangle\langle\psi_0|$ with $|\psi_0\rangle = |s_k\rangle|X\rangle$, indicating the initial position s_k and direction X, where $0 \leq k \leq d$ and $X \in \{L, R\}$.

Evolution. Each step of the walk consists of three operations:

First, measure the current position of the system to determine whether it is absorbing positions s_0 or s_d. If the position is s_0 or s_d, then the walk terminates. The measurement is described by

$$\{M_{yes} = (|s_0\rangle\langle s_0| + |s_n\rangle\langle s_n|) \otimes I_c, M_{no} = I - M_{yes}\}.$$

Here, I_c and I are the identity operators on $\mathcal{H}_c$ and $\mathcal{H}$, respectively. According to the principles of measurements, from the current state ρ, the walk terminates at state ρ_{yes} with probability p_{yes}, and it continues with state ρ_{no}, with probability p_{no}, where

$$p_x = \mathrm{tr}(M_x\rho) \quad \text{and} \quad \rho_x = M_x\rho M_x^\dagger/p_x \quad \text{for} \quad x = yes, no.$$

Second, apply an unbiased "coin-tossing" (unitary) operator on the coin space $\mathcal{H}_c$. This operator, denoted as U_H, is given by:

$$U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = |+\rangle\langle L| + |-\rangle\langle R|.$$

Here, $|\pm\rangle = \frac{1}{\sqrt{2}}(|L\rangle \pm |R\rangle)$. The operator U_H represents the *Hadamard operator* on $\mathcal{H}_c$, where the probabilities of going left and right are both equal to 0.5.

Third, perform a shift (unitary) operator on the space $\mathcal{H}$. The shift operator, denoted as U_S, is given by:

$$U_S = \sum_{k=0}^{d} |s_{k\ominus 1}\rangle\langle s_k| \otimes |L\rangle\langle L| + |s_{k\oplus 1}\rangle\langle s_k| \otimes |R\rangle\langle R|.$$

The intuitive meaning of the operator U_S is that the system walks one step left or right based on the coin state on $\mathcal{H}_c$. Here, $\oplus$ and $\ominus$ represent addition and subtraction modulo $d+1$, respectively.

In summary, in each step, given the current state ρ as the input, the quantum walk transforms ρ into $\rho' = U\rho_{no}U^\dagger$ with a probability p_{no}, where $U = U_S(I_p \otimes U_H)$ and I_p is the identity operator on $\mathcal{H}_p$. Additionally, the walk terminates at state ρ_{yes} with a probability p_{yes}. The resulting state ρ' then serves as the input state for the subsequent step of the quantum walk.

For a better understanding, Appendix A in the full version of our paper [25] provides a visual representation (Fig. 1) that showcases the evolution of the quantum walk in Example 2 from a physical perspective.

Now, we demonstrate how to represent the quantum walk given in Example 2 using a QMC. To begin, we introduce the super-operator $\mathcal{E}$, which incorporates the unitary operator U representing the combined evolution of the second and third operations of the quantum walk. For any given $\rho \in \mathcal{D}(\mathcal{H})$, we let $\mathcal{E}(\rho)$ be

$$\mathcal{E}(\rho) = UM_{no}\rho M_{no}^\dagger U^\dagger + M_{yes}\rho M_{yes}^\dagger.$$

It is worth noting that $M_{no}M_{yes} = 0$ and $M_{yes}^2 = M_{yes}$, indicating that once the QMC terminates, its state remains unchanged. By using induction on the number of steps, we can easily verify that the evolution of the quantum walk can be modeled by the QMC $(\mathcal{H}_p \otimes \mathcal{H}_c, \mathcal{E}, \rho_0 = |\psi_0\rangle\langle\psi_0|)$.

4 Measurement-Based Linear-Time Temporal Logic

In this section, we introduce a specification language called *Measurement-based Linear-time Temporal Logic* (MLTL) for describing the properties of quantum systems. MLTL is similar to ordinary LTL, but its atomic propositions are interpreted in the context of quantum computing. It also expands on the subspace-based atomic propositions introduced by Birkhoff and von Neumann [12].

4.1 Measurement-Based Atomic Propositions

As mentioned in Sect. 2, a quantum measurement is the process of extracting classical information from quantum states. A quantum measurement can be represented by a finite set $\{M_k\}_{k\in\mathcal{O}}$ of positive semi-definite matrices with the unity condition $\sum_k M_k = I$. Each matrix M_k is called a *measurement operator* and it is associated with the probability $\mathrm{tr}(M_k\rho)$ of obtaining the outcome k when measuring the quantum state ρ. Mathematically, a measurement operator M is positive semi-definite and satisfies $M \leq I$, which means that $I - M$ is also positive semi-definite.

In the following discussion, our main focus is on the measurement operator M_k and its associated probability $\mathrm{tr}(M_k\rho)$. Therefore, we will often disregard the specific outcome value k and simply refer to the measurement operator as M. Additionally, we will not explicitly mention the measurement consisting of M, as a binary quantum measurement $\{M, I - M\}$ can be determined based on M itself (as seen in Example 2 with the measurement operators M_{yes} and M_{no}).

Our atomic propositions are designed to estimate the probability of the outcome $\mathrm{tr}(M\rho)$ after measuring the quantum state ρ, given the measurement operator M.

Definition 2. *Given a Hilbert space $\mathcal{H}$,*

1. *an atomic proposition in $\mathcal{H}$ is a pair $\langle M, \mathcal{I}\rangle$, where M represents a measurement operator on $\mathcal{H}$ and $\mathcal{I} \subseteq [0, 1]$ is an interval;*
2. *a state $\rho \in \mathcal{D}(\mathcal{H})$ satisfies $\langle M, \mathcal{I}\rangle$, written $\rho \models \langle M, \mathcal{I}\rangle$, if the outcome probability of the measurement operator M applied to ρ falls within the interval $\mathcal{I}$, that is, $\mathrm{tr}(M\rho) \in \mathcal{I}$.*

In terms of the expressive power of our measurement-based atomic propositions, it is worth noting that they extend the existing atomic propositions in both the classical and quantum domains.

Classical: the atomic proposition $\langle M, \mathcal{I} \rangle$ of ρ expands upon the proposition $\langle s_k, \mathcal{I} \rangle$ of μ in interval linear-time temporal logic. This classical logic has been used to specify (static) properties of classical Markov chains [17] and continuous-time Markov chains [26]. The proposition asserts that the probability of state $s_k \in S$ in distribution μ over S falls within the interval $\mathcal{I}$. The extension is achieved by utilizing $\rho_\mu = \sum_k \mu(s_k)|s_k\rangle\langle s_k|$ in Eq. (2) and $M = |s_k\rangle\langle s_k|$, resulting in $\mathrm{tr}(M\rho_\mu) = \mu(s_k)$. Consequently, $\mathrm{tr}(M\rho_\mu) \in \mathcal{I}$ if and only if $\mu(s_k) \in \mathcal{I}$.

Quantum: furthermore, an atomic proposition $\langle M, \mathcal{I} \rangle$ of a mixed state ρ can encode the subspace-based proposition $\mathcal{X} \subseteq \mathcal{H}$ of a pure state $|\psi\rangle$ in the Birkhoff-von Neumann quantum logic. This proposition asserts that $|\psi\rangle \in \mathcal{X}$. This observation is made by setting $M = P_\mathcal{X}$, which represents the projection onto $\mathcal{X}$, $\mathcal{I} = [1, 1]$, and $\rho = |\psi\rangle\langle\psi|$. As a result, we can conclude that $\rho = |\psi\rangle\langle\psi| \models \langle P_\mathcal{X}, [1, 1] \rangle$ (i.e., $\mathrm{tr}(P_\mathcal{X}\rho) = 1$) is equivalent to $|\psi\rangle \in \mathcal{X}$.

To demonstrate the practicality of our atomic propositions, we will present a series of specific instances in Example 3 later. These examples will effectively illustrate the characteristics and properties of quantum walks.

From an algorithmic perspective, we gather a finite number of pairs $\langle M, \mathcal{I} \rangle$ as the set of atomic propositions that are based on quantum measurements. This set is denoted as AP.

4.2 Quantum Linear-Time Temporal Logic

In this section, we enhance the linear-time temporal logic [1,16] by incorporating the newly introduced measurement-based atomic propositions. This will result in the formation of our measurement-based linear-time temporal logic MLTL.

The MLTL formulas, which involve the use of measurement-based AP, are defined according to the following syntax:

$$\varphi ::= \mathbf{true} \mid a \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 U \varphi_2,$$

where $a = \langle M, \mathcal{I} \rangle \in AP$. We can also derive additional standard Boolean operators and temporal modalities such as $\Diamond$ (*eventually*) and $\Box$ (*always*) using conventional methods.

The semantics of MLTL is also defined in a familiar manner. For any infinite word ξ over 2^{AP} and any MLTL formula φ over AP, the satisfaction relation $\xi \models \varphi$ is defined by induction on the structure of φ:

- $\xi \models \mathbf{true}$ always holds;
- $\xi \models a$ iff $a \in \xi[0]$;
- $\xi \models \neg\varphi$ iff it is not the case that $\xi \models \varphi$ (written $\xi \not\models \varphi$);
- $\xi \models \varphi_1 \vee \varphi_2$ iff $\xi \models \varphi_1$ or $\xi \models \varphi_2$;
- $\xi \models \bigcirc\varphi$ iff $\xi[1+] \models \varphi$; and
- $\xi \models \varphi_1 U \varphi_2$ iff there exists $k \geq 0$ such that $\xi[k+] \models \varphi_2$ and for each $0 \leq j < k$, $\xi[j+] \models \varphi_1$,

where $\xi[k]$ and $\xi[k+]$ denote the $(k+1)$-th element and the $(k+1)$-th suffix of ξ, respectively. The indexes start from zero so that, say, $\xi = \xi[0+]$. In addition, the *semantics* $\mathcal{L}_\omega(\varphi)$ of φ is defined as the language containing all infinite words over 2^{AP} that satisfy φ: $\mathcal{L}_\omega(\varphi) = \{\, \xi \in (2^{AP})^\omega : \xi \models \varphi \,\}$.

Now, let us extend the satisfaction relation $\rho \models a$ to $\mathcal{G} \models \varphi$ between a QMC $\mathcal{G}$ and an MLTL formula φ. To this end, we introduce the labeling function:

$$L\colon \mathcal{D}(\mathcal{H}) \to 2^{AP}, \qquad L(\rho) = \{\, a \in AP : \rho \models a \,\} \tag{5}$$

which assigns to each quantum state ρ the set of atomic propositions in AP satisfied by ρ. We further extend the labeling function to sequences of quantum states by setting $L(\rho_0, \rho_1, \ldots) = L(\rho_0), L(\rho_1), \ldots$ as usual. Then we define:

$$\mathcal{G} \models \varphi \text{ if and only if } L(\sigma(\mathcal{G})) \in \mathcal{L}_\omega(\varphi)$$

where $\sigma(\mathcal{G})$ is the state trajectory of $\mathcal{G}$ as defined in Eq. (4).

We now exhibit realistic settings where our approach leads to valuable insights for the quantum walk presented in Example 2.

Example 3 (Quantum walk with absorbing boundaries, continued). Given a finite set of intervals $\{\mathcal{I}_l \subseteq [0,1]\}_{l=0}^{L}$, let

$$AP = \{\, \langle M_{s_k}, \mathcal{I}_l \rangle : M_{s_k} = |s_k\rangle\langle s_k| \otimes I_c, 0 \le k \le d, 0 \le l \le L \,\}$$

with the atomic proposition $\langle M_{s_k}, \mathcal{I}_l \rangle$ asserting that $\mathrm{tr}(M_{s_k}\rho) \in \mathcal{I}_l$ for $0 \le k \le d$ and $0 \le l \le L$. This allows us to trace the probability distribution on all positions (including boundaries) of the quantum walk.

First, we can discuss the advantages of quantum walks over their classical counterparts, as discovered by Ambainis et al. in [18]. When given the initial state $|s_1\rangle|R\rangle$, the absorbing probability at position 0 tends to $1/\sqrt{2}$ in the limit as $d \to \infty$, whereas in the classical case, the value is 1. This property can be expressed as the MLTL formula $\varphi_0 = \Diamond\Box\langle M_{s_0}, \mathcal{I}_0 \rangle$, where $\mathcal{I}_0 = [1/\sqrt{2} - \gamma, 1/\sqrt{2} + \gamma]$ and $\gamma > 0$ is a given precision parameter.

Next, we examine two properties of interest that demonstrate significant differences between quantum walks and their classical counterparts. To the best of our knowledge, these findings are new.

1. In the classical case, the absorbing probability at position d is always smaller than 0.5 if the walk starts from the middle position and d is even. However, this does not necessarily hold for quantum walks. Let $\varphi_1 = \Box\langle M_{s_d}, \mathcal{I}_1 \rangle$, where $\mathcal{I}_1 = [0, 0.5)$, be the MLTL formula that expresses this property. Assuming the initial state is $|s_{d/2}\rangle|R\rangle$, we will see in Sect. 6 that φ_1 is false when $d = 20$.
2. Let $\mathcal{I}_2 = (0.4, 1]$ and $\varphi_2 = \Box(\langle M_{s_{d-1}}, \mathcal{I}_2 \rangle \implies \langle M_{s_1}, \mathcal{I}_2 \rangle)$, which states that at any given time point, if the probability at position $d-1$ is larger than 0.4, then the probability at position 1 is also larger than 0.4. In the classical case, φ_2 is true due to the symmetry of the distribution over positions. However, as shown in Sect. 6, φ_2 does not hold in the quantum case. Therefore, the distribution of the unbiased quantum walk over positions is asymmetric even when the walk starts from the middle position.

5 Model Checking Algorithm

In this section, we present an algorithm that can be used to approximately verify the satisfaction of $\mathcal{G} \models \varphi$. For the convenience of the reader, we put all proofs of theoretical results in the appendix.

Using the notations in Eq. (5), we can formally define the model checking problem for $\sigma(\mathcal{G})$ against MLTL formulas as follows.

Problem 1. Given a QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$, a labeling function L, and an MLTL formula φ, the task is to decide whether $\mathcal{G} \models \varphi$, which means determining whether $L(\sigma(\mathcal{G})) \in \mathcal{L}_\omega(\varphi)$.

Although MLTL extends LTL with quantum atomic propositions, the traditional model-checking techniques for LTL cannot be directly applied to solve Problem 1. This is because the state space of a QMC is continuous and uncountably infinite, even in the case where the state space is finite-dimensional. In contrast, classical LTL model checking deals with a discrete and finite state set. However, QMCs can simulate Markov chains as seen in Example 1, and interval LTL formulas in [17] can be represented by MLTL formulas as discussed in Sect. 4. Despite this, the counter-example presented in [17] shows that the language $\{L(\sigma(\mathcal{G}))\}$ is generally not ω-regular. Therefore, the standard approach [27] of model checking ω-regular languages cannot directly solve Problem 1 either.

To address this, we turn to the problem of approximate verification for QMCs, following the techniques introduced in [17]. The main idea in [17] involves studying the periodicity of states in *finitely many* sub-chains obtained through BSCC decomposition [1], and a key property of Markov chains known as *periodic stability*, which ensures their stability. However, extending this idea to the quantum setting is not straightforward. It has been proven that the BSCC decomposition of QMCs is not unique, but rather has *infinitely many* possibilities [21,28,29] due to the continuous state space. Additionally, we will demonstrate below that QMCs do not exhibit periodic stability.

Definition 3. *A QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ is called* periodically stable *if there exists an integer $\theta > 0$ such that $\lim_{n\to\infty} \mathcal{E}^{n\theta}(\rho_0) = \rho^*$ for some limiting quantum state ρ^*. The smallest value of θ, if it exists, is referred to as the* period *of $\mathcal{G}$ and is denoted as $p(\mathcal{G})$. Moreover, $\{\, \mathcal{E}^k(\rho^*) : 0 \le k < p(\mathcal{G}) \,\}$ are called the* periodically stable states *of $\mathcal{G}$ as $\lim_{n\to\infty} \mathcal{E}^{n\theta}(\mathcal{E}^k(\rho_0)) = \mathcal{E}^k(\rho^*)$.*

In the classical case, any Markov chain (S, P, μ_0) is periodically stable [30]. This means that there exists an integer $\theta > 0$ such that $\lim_{n\to\infty} \mu_0 P^{n\theta} = \mu^*$ for some limiting distribution μ^*. Furthermore, θ is independent of μ_0. However, this property does not hold for QMCs, as demonstrated by the following example.

Example 4. Let $\mathcal{H} = \mathrm{span}\{|s_0\rangle, |s_1\rangle\}$ and $U = |s_0\rangle\langle s_0| + e^{i2\pi\psi}|s_1\rangle\langle s_1|$ be a unitary operator on $\mathcal{H}$, where ψ is an irrational number. It can be proven that the

QMC $(\mathcal{H}, \mathcal{E}_U, \rho_0)$, where $\mathcal{E}_U(\rho) = U\rho U^\dagger$, is not periodically stable for any generic initial state ρ_0. In fact, a simple calculation reveals that

$$\mathcal{E}_U^{n\theta}(\rho_0) = \rho_{00} \cdot |s_0\rangle\langle s_0| + \rho_{11} \cdot |s_1\rangle\langle s_1| + e^{-i2\pi\psi n\theta}\rho_{01} \cdot |s_0\rangle\langle s_1| + e^{i2\pi\psi n\theta}\rho_{10} \cdot |s_1\rangle\langle s_0|$$

where $\rho_{ij} = \langle s_i|\rho|s_j\rangle$. It is worth noting that since ψ is irrational, the set $\{ e^{i2\pi\psi m} : m \in \mathbb{N} \}$ is dense in the unit circle [31]. Therefore, for any integer $\theta > 0$, the limit $\lim_{n\to\infty} \mathcal{E}_U^{n\theta}(\rho_0)$ cannot exist, except when $\rho_{01} = \rho_{10} = 0$.

Note that the operator $\mathcal{E}_U$ in Example 4 has four eigenvalues (with multiplicity taken into account): 1, 1, $e^{-i2\pi\psi}$, and $e^{i2\pi\psi}$. The corresponding eigenvectors are $|s_0\rangle\langle s_0|$, $|s_1\rangle\langle s_1|$, $|s_0\rangle\langle s_1|$, and $|s_1\rangle\langle s_0|$, respectively. We have proven that the system $(\mathcal{H}, \mathcal{E}_U, \rho_0)$ is periodically stable if and only if the initial state ρ_0 does not have any components in the directions of $|s_0\rangle\langle s_1|$ and $|s_1\rangle\langle s_0|$. Interestingly, this is precisely why a QMC cannot be periodically stable (see Appendix B of the full version of our paper [25]). To put it in another way, a QMC is periodically stable only if the initial quantum state does not contain any components in the directions defined by the eigenvectors of the relevant super-operator (linear operator) corresponding to eigenvalues of the form $e^{i2\pi\psi}$ where ψ is an irrational number. This result also offers an efficient method to verify the periodic stability of a given QMC $\mathcal{G}$ (and determine the period $p(\mathcal{G})$). Specifically, symbolic computation can be used to check whether the eigenvalues of QMCs are irrational by analyzing their algebraic representations and mathematical properties. Such a method can be utilized to confirm the periodic stability of the quantum walk in Example 2. Therefore, the approximate verification technique described in this paper can be applied to the quantum walk.

Proposition 1. *Given a QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ with $\dim(\mathcal{H}) = d$, there is a way to check whether $\mathcal{G}$ is periodically stable with computational complexity $\mathcal{O}(d^8)$. If it is indeed stable, we can compute the period $p(\mathcal{G})$ with a complexity of $\mathcal{O}(d^8)$.*

The evaluation process for periodic stability, as described in Proposition 1, involves examining the eigenvalues and eigenvectors of the super-operator $\mathcal{E}$. To calculate these eigenvalues and eigenvectors of $\mathcal{E}$ with Kraus operators $\{E_k\}_k$, we can use the matrix representation $\mathcal{M}_\mathcal{E}$ [32] of $\mathcal{E}$, given by $\mathcal{M}_\mathcal{E} = \sum_k E_k \otimes E_k^*$. Here, E_k^* represents the entry-wise complex conjugate of E_k. The linear operator (matrix) $\mathcal{M}_\mathcal{E}$ acts on $\mathcal{H} \otimes \mathcal{H}$. Based on this, we can derive the following lemma:

Lemma 1. *For a non-zero $A \in \mathcal{L}(\mathcal{H})$, A is an eigenvector of $\mathcal{E}$ corresponding to the eigenvalue λ if and only if $|A\rangle$ is an eigenvector of $\mathcal{M}_\mathcal{E}$ corresponding to the eigenvalue λ. In other words, $\mathcal{E}(A) = \lambda A$ if and only if $\mathcal{M}_\mathcal{E}|A\rangle = \lambda|A\rangle$.*

In this context, $|A\rangle \in \mathcal{H} \otimes \mathcal{H}$ represents the vectorization of A, denoted by $|A\rangle := (A \otimes I)|\Omega\rangle$. Here, $|\Omega\rangle$ denotes the (unnormalized) maximally entangled state on $\mathcal{H} \otimes \mathcal{H}$ [23]. Assuming $\mathcal{H} = \text{span}\{|s_0\rangle, \ldots, |s_{d-1}\rangle\}$, the maximally entangled state can be expressed as $|\Omega\rangle = \sum_{k=0}^{d-1} |s_k\rangle|s_k\rangle$. In particular, for a quantum state $\rho \in \mathcal{D}(\mathcal{H})$, we write $|\rho\rangle = (\rho \otimes I)|\Omega\rangle$.

Now, our attention can be directed towards approximately model checking the QMC $\mathcal{G}$ that is periodically stable. To achieve this with a desired level of accuracy ε, we can adopt the following approach. First and foremost, we need to identify the states of the chain that are periodically stable as defined in Definition 3. After a sufficient number of steps, any state on the trajectory $\sigma(\mathcal{G})$ will be close to one of the periodically stable states. This approach can also be applied to the labeled trajectory $L(\sigma(\mathcal{G}))$. By doing so, we can obtain an ω-regular language. Following that, we can utilize the standard Büchi automata approach of model checking ω-regular languages to analyze the obtained language. Therefore, in the following subsections, we will outline the step-by-step process for handling this.

5.1 Periodically Stable States

Given a periodically stable QMC $(\mathcal{H}, \mathcal{E}, \rho_0)$, we can obtain the periodically stable states by employing a specific super-operator called the *stabilizer* of $\mathcal{G}$, denoted by $\mathcal{E}_\phi$. This stabilizer is generated by the super-operator $\mathcal{E}$.

Lemma 2. *If a QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ is periodically stable with period $p(\mathcal{G})$, then the set $\{\mathcal{E}_\phi(\mathcal{E}^k(\rho_0))\}_{0\le k<p(\mathcal{G})}$ consists of the periodically stable states of $\mathcal{G}$. The computational complexity of obtaining such a set is $\mathcal{O}(d^8)$, where $d = \dim(\mathcal{H})$.*

The super-operator $\mathcal{E}_\phi$ is constructed from $\mathcal{E}$ by retaining the eigenvectors corresponding to eigenvalues with a magnitude of one, which do not vanish in the evolution $\mathcal{E}^n(\rho)$ as n tends to infinity. Specifically, let $\mathcal{M}_\mathcal{E}$ be the matrix representation of $\mathcal{E}$ with Jordan decomposition $\mathcal{M}_\mathcal{E} = SJS^{-1}$, where $J = \bigoplus_{k=0}^{K} J_k(\lambda_k) = \bigoplus_{k=0}^{K} \lambda_k P_k + N_k$. Here, λ_k represents the eigenvalues of $\mathcal{M}_\mathcal{E}$, P_k is a projector onto the corresponding (generalized) eigenvector space, and N_k is the corresponding nilpotent part. Furthermore, according to [7, Proposition 6.2], the geometric multiplicity of any λ_k with a magnitude of one (i.e., $|\lambda_k| = 1$) is equal to its algebraic multiplicity, i.e., $N_k = 0$. Then we define $J_\phi := \bigoplus_{k:|\lambda_k|=1} P_k$ as the projector onto the eigenspace corresponding to eigenvalues with a magnitude of one. By [7, Proposition 6.3], it is confirmed that $\mathcal{M}_{\mathcal{E}_\phi} = SJ_\phi S^{-1}$ is indeed the matrix representation of some super-operator $\mathcal{E}_\phi$.

5.2 Neighborhood of Quantum States

Now we proceed to introduce the concepts of (symbolic) neighborhoods for (sequences of) quantum states using the labeling function L.

Definition 4. *Let $\rho \in \mathcal{D}(\mathcal{H})$ be a quantum state and $\varepsilon > 0$. The (symbolic) ε-neighborhood $\mathcal{N}_\varepsilon(\rho)$ of ρ is the subset of 2^{AP} defined as*

$$\mathcal{N}_\varepsilon(\rho) := \{\, L(\rho') : \rho' \in \mathcal{D}(\mathcal{H}), \|\rho - \rho'\| < \varepsilon \,\},$$

where $\|A\| := \sqrt{\mathrm{tr}(A^\dagger A)}$ represents the Schatten 2-norm (also known as the Hilbert-Schmidt norm) for the linear operator $A \in \mathcal{L}(\mathcal{H})$.

Now we show that, after a certain number of steps, the symbols $L(\mathcal{E}^n(\rho_0))$ will be enclosed within the ε-neighborhood of one of the periodically stable states.

Lemma 3. *Consider a periodically stable QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ with period $p(\mathcal{G})$. Let $\eta_k = \mathcal{E}_\phi(\mathcal{E}^k(\rho_0))$, for each $0 \leq k < p(\mathcal{G})$, as the periodically stable states of $\mathcal{G}$. Then for any $\varepsilon > 0$, there exists an integer $K^\varepsilon > 0$ such that for any $n \geq K^\varepsilon$,*

$$L(\mathcal{E}^n(\rho_0)) \in \mathcal{N}_\varepsilon(\eta_{n \bmod p(\mathcal{G})}).$$

Moreover, the time complexity of computing K^ε is in $\mathcal{O}(d^8)$, where $d = \dim(\mathcal{H})$.

With Lemma 3, we can define the concept of the (symbolic) neighborhood of trajectories for periodically stable QMCs.

Definition 5. *Given a periodically stable QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ and $\varepsilon > 0$, the (symbolic) ε-neighborhood of the trajectory $\sigma(\mathcal{G})$ of $\mathcal{G}$ is defined to be the language $\mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ over $(2^{AP})^\omega$ such that $\xi \in \mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ if and only if*

- *$\xi[n] = L(\mathcal{E}^n(\rho_0))$ for all $0 \leq n \leq K^\varepsilon - 1$ and*
- *$\xi[n] \in \mathcal{N}_\varepsilon(\eta_{n \bmod p(\mathcal{G})})$ for all $n \geq K^\varepsilon$,*

where the states $\{\, \eta_k : 0 \leq k < p(\mathcal{G}) \,\}$ and K^ε are as given in Lemma 3.

5.3 Approximate Verification of Quantum Markov Chains

Using Definition 5, we can formulate and address the problem of approximate model checking for QMCs against MLTL formulas in the following manner.

Problem 2. Given a periodically stable QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$, a labeling function L, an MLTL formula φ, and $\varepsilon > 0$, decide whether

1. *$\mathcal{G}$ ε-approximately satisfies φ from below*, denoted $\mathcal{G} \models_\varepsilon \varphi$; that is, whether $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \cap \mathcal{L}_\omega(\varphi) \neq \emptyset$;
2. *$\mathcal{G}$ ε-approximately satisfies φ from above*, denoted $\mathcal{G} \models^\varepsilon \varphi$; that is, whether $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \subseteq \mathcal{L}_\omega(\varphi)$.

To justify that Problem 2 is indeed an approximate version of Problem 1, we first note that $L(\sigma(\mathcal{G})) \in \mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$. Then we have three cases:

1. if $\mathcal{G} \not\models_\varepsilon \varphi$, then $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \cap \mathcal{L}_\omega(\varphi) = \emptyset$, and hence $L(\sigma(\mathcal{G})) \notin \mathcal{L}_\omega(\varphi)$ ($\mathcal{G} \not\models \varphi$);
2. if $\mathcal{G} \models^\varepsilon \varphi$, then $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \subseteq \mathcal{L}_\omega(\varphi)$, and hence $L(\sigma(\mathcal{G})) \in \mathcal{L}_\omega(\varphi)$ ($\mathcal{G} \models \varphi$);
3. if neither $\mathcal{G} \not\models_\varepsilon \varphi$ nor $\mathcal{G} \models^\varepsilon \varphi$, then whether or not $\mathcal{G} \models \varphi$ is unknown.

If we find ourselves in the third scenario (the unknown case), we have the option to decrease the value of ε by half and then repeat the approximate model-checking process described in the previous scenarios. We can continue this process until we reach either of the first two cases, which will provide us with either a negative or affirmative answer to Problem 1. In exceptional cases, diminishing ε may not lead to termination. To prevent this, a predetermined number

Algorithm 1. ModelCheck$(\mathcal{G}, AP, L, \varphi, \varepsilon)$

Require: A periodically stable QMC $\mathcal{G} = (\mathcal{H}, \mathcal{E}, \rho_0)$ with Kraus operators $\{E_k\}_k$, a finite set of (measurement-based) atomic propositions AP, a labeling function L, an MLTL formula φ, and $\varepsilon > 0$.

Ensure: **true**, **false**, or **unknown**, where **true** indicates $\mathcal{G} \models \varphi$, **false** indicates $\mathcal{G} \not\models \varphi$, and **unknown** stands for an inconclusive answer.

1: Put $\mathcal{M}_{\mathcal{E}} = \sum_k E_k \otimes E_k^*$
2: Get $p(\mathcal{G})$ and $M_{\mathcal{E}_\phi} = SJ_\phi S^{-1}$ by the Jordan decomposition form $\mathcal{M}_{\mathcal{E}} = SJS^{-1}$
3: Put $|\rho_0\rangle = (\rho_0 \otimes \mathcal{I})|\Omega\rangle$
4: **for each** $k \in \{0, 1, \ldots, p(\mathcal{G}) - 1\}$ **do**
5: Set $|\eta_k\rangle$ to be $M_{\mathcal{E}_\phi} M_{\mathcal{E}}^k |\rho_0\rangle$
6: Compute $\mathcal{N}_\varepsilon(\eta_k)$ by semi-definite programming
7: **end for**
8: Get K^ε by solving some inequalities
9: **for each** $k \in \{0, 1, \ldots, K^\varepsilon - 1\}$ **do**
10: Put $\rho_k = \mathcal{E}^k(\rho_0)$ and compute $L(\rho_k)$
11: **end for**
12: Put $\zeta_k = \eta_{(K^\varepsilon + k) \bmod p(\mathcal{G})}$ for $0 \le k < p(\mathcal{G})$
13: Let $\mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ be the ω-regular language
$$\{L(\rho_0)\}\{L(\rho_1)\}\cdots\{L(\rho_{K^\varepsilon-1})\} \cdot (\mathcal{N}_\varepsilon(\zeta_0)\mathcal{N}_\varepsilon(\zeta_1)\cdots\mathcal{N}_\varepsilon(\zeta_{p(\mathcal{G})-1}))^\omega$$
14: Construct the NBA A_φ for φ *// standard construction*
15: Construct the NBA $A_{\mathcal{G}}$ accepting $\mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ *// standard lasso-shaped construction*
16: **if** $\mathcal{L}(A_{\mathcal{G}}) \cap \mathcal{L}(A_\varphi) = \emptyset$ **then** *// standard Büchi automata operation*
17: **return false**
18: **else if** $\mathcal{L}(A_{\mathcal{G}}) \subseteq \mathcal{L}(A_\varphi)$ **then** *// standard Büchi automata operation*
19: **return true**
20: **else**
21: **return unknown**
22: **end if**

of iterations can be set for reducing epsilon. Determining when the procedure terminates seems difficult, and we would like to leave it as future work.

Finally, to solve Problem 2, we represent $\mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ in Definition 5 as the ω-regular expression

$$\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) = \{L(\rho_0)\} \cdot \{L(\mathcal{E}(\rho_0))\} \cdots \{L(\mathcal{E}^{K^\varepsilon - 1}(\rho_0))\} \cdot \big(\mathcal{N}_\varepsilon(\zeta_0) \cdots \mathcal{N}_\varepsilon(\zeta_{p(\mathcal{G})-1})\big)^\omega$$

where $\zeta_k = \eta_{(K^\varepsilon + k) \bmod p(\mathcal{G})}$, $0 \le k < p(\mathcal{G})$, and for any two sets X and Y, $X \cdot Y = \{\, xy : x \in X, y \in Y \,\}$. Thus $\mathcal{N}_\varepsilon(\sigma(\mathcal{G}))$ is ω-regular and standard techniques [1,33] can be employed to check $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \cap \mathcal{L}_\omega(\varphi) = \emptyset$ and $\mathcal{N}_\varepsilon(\sigma(\mathcal{G})) \subseteq \mathcal{L}_\omega(\varphi)$.

Theorem 1. *The verification problem outlined in Problem 2 can be addressed using Algorithm 1 within a time complexity of* $\mathcal{O}(2^{\mathcal{O}(|\varphi|)} \cdot (K^\varepsilon + p(\mathcal{G})) + d^8)$. *Here,* $d = \dim(\mathcal{H})$, $|\varphi|$ *represents the size of MLTL formula* φ, *and* $p(\mathcal{G})$ *and* K^ε *are as given in Proposition 1 and Lemma 3, respectively.*

Algorithm 1 summarizes our techniques proposed above to answer Problem 2. Starting from lines 1 to 7, we make use of the Jordan decomposition of the matrix

representation $\mathcal{M}_{\mathcal{E}}$ of $\mathcal{E}$ to determine the period $p(\mathcal{G})$ and the stabilizer $\mathcal{E}_{\phi}$. These computations allow us to obtain the periodically stable states $\{\eta_k\}_{k=0}^{p(\mathcal{G})-1}$ of $\mathcal{G}$ and their corresponding symbolic ε-neighborhood $\{\mathcal{N}_{\varepsilon}(\eta_k)\}_{k=0}^{p(\mathcal{G})-1}$ based on the given approximation level ε. The steps involved in these computations utilize Proposition 1 and Lemma 2. Afterwards, in line 8, we determine the truncation number K^{ε} using Lemma 3. Subsequently, we compute $\{L(\rho_k)\}_{k=0}^{K^{\varepsilon}-1}$, which represents the symbols in AP of the first K^{ε} quantum states in the trajectory $\sigma(\mathcal{G})$, from lines 9 to 11. Finally, in lines 12 and 13, we obtain an ω-regular language $\mathcal{N}_{\varepsilon}(\sigma(\mathcal{G}))$ that represents the symbolic neighborhoods of the evolution $\sigma(\mathcal{G})$. The Büchi automaton A_{φ} for the MLTL formula φ is constructed at line 14 by means of a standard construction for an LTL formula φ (see, e.g., [33]) while the Büchi automaton $A_{\mathcal{G}}$ at line 15 is obtained by an ordinary lasso-shaped construction: it is enough to insert a new state between each letter, make the state joining the stem and the lasso part accepting, and use the accepting state as the target of the last action in the lasso. The two operations on Büchi automata at lines 16 and 18 are standard: intersection and emptiness reduce to automata product and strongly connected components decomposition, respectively, which require quadratic time (cf. [33]). Language inclusion, however, in general, requires exponential time and is PSPACE-complete (cf. [33]); in our case, however, we can remain in quadratic time by replacing the check $\mathcal{L}(A_{\mathcal{G}}) \subseteq \mathcal{L}(A_{\varphi})$ with $\mathcal{L}(A_{\mathcal{G}}) \cap \mathcal{L}(A_{\neg\varphi}) = \emptyset$, since constructing the Büchi automata A_{φ} and $A_{\neg\varphi}$ requires the same asymptotic effort (cf. [33, Section 4.6.1]).

Remark 1. The complexity of approximately verifying MCs against interval LTL formulas in the work of Agrawal et al. [17] is challenging to analyze and remains unknown. This is because the BSCC decomposition analysis, which is relied upon, is not an analytical method. Our model-checking algorithm, however, overcomes this by utilizing the Jordan normal form to create a linear-algebraic representation of the graph-theoretic (BSCC-based) model-checking algorithm mentioned in [17]. Consequently, our model-checking algorithm (Algorithm 1) can effectively verify MC models against interval LTL formulas. This capability stems from the ability of QMCs to emulate MCs, as illustrated in Example 1, and the greater expressiveness of our MLTL compared to interval LTL in [17], as discussed in Sect. 4. Notably, MCs are inherently periodically stable, which extends to the modeled QMCs, making our model-checking algorithm suitable for this context. Additionally, while Agrawal et al. [17] did not offer a complexity analysis for their algorithm, our method establishes the first upper bound on the computational complexity of approximate model-checking for MCs against interval LTL specifications from their work. Specifically, when using our algorithm for model checking MCs, the complexity is reduced to $\mathcal{O}(2^{\mathcal{O}(|\varphi|)} \cdot (K^{\varepsilon} + p(\mathcal{G})) + d^4)$, where d represents the number of states in the MC. This reduction is due to the fact that the complexity of computing the Jordan decomposition of the d-by-d stochastic matrix P in MCs is $\mathcal{O}(d^4)$. As a result, the time complexity of calculating K^{ε} and $p(\mathcal{G})$ is also reduced to $\mathcal{O}(d^4)$.

6 Case Studies

To demonstrate the utility of the model-checking techniques proposed in this paper, we conducted case studies on quantum walks to investigate their temporal linear-time properties. We completed a prototype for implementing our model-checking algorithm and used it to automatically model check all MLTL formulas provided in Example 3. The prototype was built using Python for the quantum part to generate an ω-regular language and Java for the classical part to model check the language against LTL formulas by calling Spot, a platform for LTL and ω-automata manipulation [34].

Before conducting the verification process, it is crucial to ensure the periodic stability of the QMC model for the quantum walk in Example 2. By Proposition 1, this can be achieved by computing the eigenvalues of the model and confirming that they only have 1 as the eigenvalue with a magnitude of one. Armed with this information, we can then employ Algorithm 1 to verify the properties outlined in Example 3. The experimental results for these verifications can be found in Table 1.

The first experiment in Table 1 confirms the advantages of quantum walks over classical random walks, which was previously established by Ambainis et al. in [18]. The remaining two experiments aim to uncover new properties of quantum walks. Moreover, we also utilized Algorithm 1 to verify these same properties for one-dimensional unbiased classical random walks with absorbing boundaries, which yielded contrasting results (**false** for the first experiment and **true** for the last two experiments in Table 1). This confirms that these properties are unique phenomena specific to quantum walks.

Table 1. The experimental result for position number $d = 20$ and different initial states $\rho_0 = |\psi_0\rangle\langle\psi_0|$.

$\|\phi_0\rangle$	Formula φ	Parameter ε		
		0.5	0.25	0.125
$\|s_1\rangle\|R\rangle$	$\Diamond\Box\langle M_{s_0}, [1/\sqrt{2}-0.1, 1/\sqrt{2}+0.1]\rangle$	**unknown**	**unknown**	**true**
$\|s_{10}\rangle\|R\rangle$	$\Box\langle M_{s_{20}}, [0, 0.5)\rangle$	**unknown**	**unknown**	**false**
	$\Box(\langle M_{s_{19}}, (0.4, 1]\rangle \implies \langle M_{s_1}, (0.4, 1]\rangle)$	**unknown**	**unknown**	**false**

7 Conclusion

In this paper, we proposed a new quantum logic called measurement-based linear-time temporal logic (MLTL) to specify the quantitative properties of quantum Markov chains (QMCs). For model checking MLTL formulas, an algorithm was developed. The measurement-based atomic propositions of MLTL build upon the subspace-based quantum atomic propositions introduced by Birkhoff and von Neumann [12]. Furthermore, we demonstrated the practical applicability of our model-checking algorithm in quantum walks. This not only confirms

the previously established advantages discovered by Ambainis et al. [18] of quantum walks over classical random walks, but also uncovers new phenomena that are unique to quantum walks.

As future work, we note that the quantum walk in Example 2 can also be written as a while-loop quantum program [32], and the absorbing probabilities are exactly the termination probabilities of the program. Indeed, any quantum program written in the While language can be modeled by a QMC [6]. So our model-checking approach can be naturally applied in the verification of quantum program properties specified as MLTL formulas. Therefore, we plan to apply our model-checking algorithms to verify quantum programs. Moreover, it would be intriguing to broaden the application of the methods presented in this paper to verify the behavior of non-periodically stable QMCs. One possible approach is that any non-periodically stable QMC will be close to a periodically stable one with arbitrary precision, as any irrational number (eigenvalue) will be close to a rational number (eigenvalue) with the same precision.

Acknowledgments. We would like to thank the anonymous reviewers for their valuable suggestions. This work was partly supported by the Youth Innovation Promotion Association, Chinese Academy of Sciences (Grant No. 2023116), the Key Research Program of the Chinese Academy of Sciences (Grant No. ZDRW-XX-2022-1), and the Australian Research Council (Grant No: DP220102059).

This work is part of the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant no. 101008233.

References

1. Baier, C., Katoen, J.-P.: Principles of model checking. MIT press (2008)
2. Ying, M., Feng, Y.: Model-checking quantum systems. Nat. Sci. Rev. **6**(1), 28–31 (2019)
3. Ying, M., Feng, Y.: Model Checking Quantum Systems: Principles and Algorithms. Cambridge University Press (2021)
4. Ticozzi, F., Viola, L.: Quantum Markovian subsystems: Invariance, attractivity, and control. IEEE Trans. Autom. Control **53**(9), 2048–2063 (2008)
5. Guan, J., Feng, Y., Ying, M.: The structure of decoherence-free subsystems. arXiv preprint arXiv:1802.04904 (2018)
6. Ying, M.: Foundations of Quantum Programming. Morgan Kaufmann (2016)
7. Wolf, M.M.: Quantum channels & operations: Guided tour. Lecture notes available at. https://mediatum.ub.tum.de/doc/1701036/document.pdf (2012)
8. Ambainis, A.: Quantum walks and their algorithmic applications. Inter. J. Quantum Inform. **1**, 507–518 (2003)
9. Kempe, J.: Quantum random walks: an introductory overview. Contemp. Phys. **44**(4), 307–327 (2003)
10. Attal, S., Petruccione, F., Sabot, C., Sinayskiy, I.: Open quantum random walks. J. Stat. Phys. **147**(4), 832–852 (2012)
11. Feng, Y., Nengkun, Yu., Ying, M.: Model checking quantum Markov chains. J. Comput. Syst. Sci. **79**(7), 1181–1198 (2013)
12. Birkhoff, G., von Neumann, J.: The logic of quantum mechanics. Annals Math., 823–843 (1936)

13. Moore, C., Crutchfield, J.P.: Quantum automata and quantum grammars. Theoretical Comput. Sci. **237**(1–2), 275–306 (2000)
14. Ying, M., Li, Y., Nengkun, Yu., Feng, Y.: Model-checking linear-time properties of quantum systems. ACM Trans. Comput. Logic (TOCL) **15**(3), 22 (2014)
15. Li, Y., Ying, M.: (Un)decidable problems about reachability of quantum systems. In: Baldan, P., Gorla, D. (eds.) CONCUR 2014. LNCS, vol. 8704, pp. 482–496. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44584-6_33
16. Pnueli, A.: The temporal logic of programs. In : 18th Annual Symposium on Foundations of Computer Science, Providence, Rhode Island, USA, 31 October - 1 November 1977, pp. 46–57. IEEE Computer Society (1977)
17. Agrawal, M., Akshay, S., Genest, B., Thiagarajan, P.S.: Approximate verification of the symbolic dynamics of Markov chains. J. ACM (JACM) **62**(1), 2 (2015)
18. Ambainis, A., Bach, E., Nayak, A., Vishwanath, A., Watrous, J.: One-dimensional quantum walks. In: Proceedings of the thirty-third annual ACM symposium on Theory of computing (STOC), pp 37–49. ACM (2001)
19. Feng, Y., Hahn, E.M., Turrini, A., Zhang, L.: QPMC: a model checker for quantum programs and protocols. In: Bj$\mathcal{O}$rner, N., de Boer, F. (eds.) FM 2015. LNCS, vol. 9109, pp. 265–272. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19249-9_17
20. Feng, Y., Hahn, E.M., Turrini, A., Ying, S.: Model checking omega-regular properties for quantum Markov chains. In: LIPIcs-Leibniz International Proceedings in Informatics, vol. 85. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2017)
21. Ying, S., Feng, Y., Yu, N., Ying, M.: Reachability probabilities of quantum markov chains. In: D'Argenio, P.R., Melgratti, H. (eds.) CONCUR 2013. LNCS, vol. 8052, pp. 334–348. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40184-8_24
22. Venegas-Andraca, S.E.: Quantum walks: a comprehensive review. Quantum Inf. Process. **11**(5), 1015–1106 (2012)
23. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press (2010)
24. Choi, M.-D.: Completely positive linear maps on complex matrices. Linear Algebra Appl. **10**(3), 285–290 (1975)
25. Guan, J., Feng, Y., Turrini, A., Ying, M.: Measurement-based verification of quantum markov chains. arXiv preprint arXiv:2405.05825 (2024)
26. Guan, J., Yu, N.: A probabilistic logic for verifying continuous-time markov chains. In: TACAS 2022. LNCS, vol. 13244, pp. 3–21. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-99527-0_1
27. Vardi, M.Y.: Probabilistic linear-time model checking: an overview of the automata-theoretic approach. In: Katoen, J.-P. (ed.) ARTS 1999. LNCS, vol. 1601, pp. 265–276. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48778-6_16
28. Baumgartner, B., Narnhofer, H.: The structures of state space concerning quantum dynamical semigroups. Rev. Math. Phys. **24**(02), 1250001 (2012)
29. Guan, J., Feng, Y., Ying, M.: Decomposition of quantum Markov chains and its applications. J. Comput. Syst. Sci. (2018)
30. Gallager, R.G.: Discrete stochastic processes, vol. 321. Springer Science & Business Media (2012)
31. Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. Oxford university press (1979)
32. Ying, M., Nengkun, Yu., Feng, Y., Duan, R.: Verification of quantum programs. Sci. Comput. Program. **78**, 1679–1700 (2013)

33. Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R. (eds.) Handbook of Model Checking. Springer (2018). https://doi.org/10.1007/978-3-319-10575-8
34. Duret-Lutz, A., et al.: From Spot 2.0 to Spot 2.10: What's new? In: Proceedings of the 34th International Conference on Computer Aided Verification (CAV 2022), vol. 13372 LNCS. pp. 174–187. Springer (2022). https://doi.org/10.1007/978-3-031-13188-2_9