An Algebraic Method to Fidelity-based Model Checking over Quantum Markov Chains

Ming Xu, Jianling Fu, Jingyi Mei, Yuxin Deng

Shanghai Key Laboratory of Trustworthy Computing, & MoE Engineering Research Center of Software/Hardware Co-design Technology and Application, East China Normal University, Shanghai, 200062, China

Abstract

Fidelity is one of the most widely used quantities in quantum information that measures the distance of two quantum states through a noisy channel, a kind of quantum operations. In this paper, we consider the model of quantum Markov chain (QMC), in which transitions are weighted by super-operators to characterize quantum operations and the initial quantum state is left parametric. A quantum analogy of probabilistic computation tree logic, called QCTL, is introduced to take into account fidelity, instead of probability measure, over QMC. The key to the model checking problem lies in computing the fidelity of the super-operator valued measure specified by a path formula in QCTL. It is minimized over all initial quantum states, which is intended for analyzing the system performance in the worst case. We achieve it by a reduction to quantifier elimination in the existential theory of the reals. The method is absolutely exact, so that model checking QCTL formulas against QMCs is proved to be decidable in exponential time.

Keywords: Model Checking, Formal Logic, Quantum Computing, Computer Algebra

1. Introduction

Markov chains (MCs) have attracted a lot of attention in the field of formal verification [6, 2]. In 1989, Hansson and Jonsson introduced probabilistic computation tree logic (PCTL) to specify quantitative properties over MCs, and presented an algorithm to check whether a property ϕ holds over an MC $\mathfrak{M}$ or not [19]. The time complexity is polynomial w. r. t. the size of both ϕ and $\mathfrak{M}$. Later, more efficient approximation algorithms were presented and implemented in various model checkers, such as PRISM [22], Storm [8], and EPMC [12], to solve numerous practical problems. Such model checkers provide a Boolean answer to the decision problem: Does $\mathfrak{M}$ satisfy ϕ? In case of a negative answer, a counter-example can be provided [18] to locate the potential bug. Thereby, the model checking technology has achieved great success in both academic and industrial communities.

Quantum hardware has been rapidly developed in the last decades, particularly in very recent years. For example, in December 2020, the quantum computer Jiuzhang implemented a type of Boson sampling on 76 photonic qubits, in which case the quantum computer spent less than 20

Email addresses: mxu@cs.ecnu.edu.cn (Ming Xu), scsse_fjl2015@126.com (Jianling Fu), mjyecnu@163.com (Jingyi Mei), yxdeng@sei.ecnu.edu.cn (Yuxin Deng)

seconds while a classical supercomputer would require 600 million years [30]. One year later, IBM's latest quantum-computing chip established a milestone of sorts: it packed in 127 qubits, and several hundred qubits are expected within the next few years [3]. In the meantime, quantum software will be crucial in harnessing the power of quantum computers, such as the BB84 protocol for quantum key distribution [5], Shor's algorithm for integer factorization [25], Grover's algorithm for unstructured search [16], and the HHL algorithm for solving linear equations [20]. To ensure the reliability of quantum software, verification technologies are urgent to be developed for quantum systems and protocols. Due to the features in quantum mechanics, three major challenges in verification are:

1. the state space is a continuum, where quantum states are represented by *density operators* that are positive semi-definite matrices with trace (the sum of diagonal entries) being unit,
2. quantum operations, which are mappings from density operators to themselves, are much complicated to be described, and
3. to get classical information from quantum states, one has to exploit the quantum measurement that destroys the original quantum states.

To tackle them effectively, researchers imposed some restrictions on the quantum model and the properties to be checked. Gay *et al.* [14, 15] restricted the quantum operations to the Clifford group gates (including Hadamard, CNOT and phase gates), restricted the state space to a set of finitely describable states called stabilizers that is closed under those Clifford group gates, and applied PRISM to check the quantum protocols — superdense coding, quantum teleportation, and quantum error correction. Whereas, Feng *et al.* proposed the model of super-operator weighted Markov chain [11], in which super-operators are used to characterize the general quantum operations. It gave rise to an alternative way to finitely describe states. The model was shown to be able to describe a kind of hybrid systems [23], whose state space has both discrete and continuous components although the evolution is discrete-time. Under the model, the authors considered the reachability probability [29], the repeated reachability probability [10], and the model checking of linear time properties [23] and a quantum analogy of computation tree logic (QCTL) [11]. A key step in their work is decomposing the state space (known as a Hilbert space) into a direct-sum of some bottom strongly connected component (BSCC) subspaces plus a maximal transient subspace. Here the BSCC subspaces are the state sets in which any two states can reach each other almost surely under the given quantum operation. After decomposition, all the aforementioned problems were shown to be computable/decidable in polynomial time.

The above works focus only on the probability measure of quantitative properties, where the probabilities are taken from the traces of density operators. For example, let us consider a quantum particle in state

$$\rho_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

After travelling through a noisy channel $\mathcal{E}$, the state ρ_0 is changed into $\rho_1 = \mathcal{E}(\rho_0)$ as follows,

$$\rho_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \xrightarrow{\mathcal{E}} \rho_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

The two states ρ_0 and ρ_1 are obviously different states, but distinguishing them relies on a perfect measurement, which cannot be achieved in general. Direct comparison with the probability measure tells nothing, as ρ_0 and ρ_1 have the same probability measure 1. Some key information concerning the quantum states has been lost when we only focus on their probability measure. To address this issue, we resort to fidelity.

Fidelity is a basic concept in quantum information that prescribes the quantification of the similarity degree of two quantum states. For a fixed quantum channel $\mathcal{E}$, the fidelity between quantum states ρ and $\mathcal{E}(\rho)$ characterizes precisely how well the channel could preserve the quantum information. Qualitatively, the fidelity, ranging over the unit interval $[0, 1]$, attains its minimum if and only if the column space of ρ and $\mathcal{E}(\rho)$ are mutually orthogonal, and attains its maximum value 1 if and only if $\rho = \mathcal{E}(\rho)$. It decreases as two states become more distinguishable, where the distinguishability reflects the effect of a quantum channel. In the aforementioned example, the fidelity between ρ_0 and ρ_1 attains the minimum 0 as expected although the probability measures of ρ_0 and ρ_1 are both 1. Hence the probability measure does not suffice to recognize general quantum states in the situation where the preservation of quantum information is viewed as an important indicator, but the fidelity does!

In this paper, we consider the fidelity-based property over (super-operator weighted) quantum Markov chains (QMCs). This property is specified by another quantum analogy of computation tree logic (QCTL), including a novel kind of fidelity-quantifier formula instead of the trace-quantifier formula in [11]. Since the state formulas and the path formulas in QCTL are mutually inductive, we perform the model checking in three steps: i) decide the basic state formulas, ii) synthesize the super-operators of path formulas, and iii) decide the fidelity-quantifier formulas. The last step plays a central role in the model checking, and depends on the second step. To effectively synthesize the super-operators, we first remove the BSCC subspaces that cover all fixed-points of a super-operator in consideration. By Brouwer's fixed-point theorem, the direct-sum of all these BSCC subspaces are easily obtained. We explicitly express the super-operators using matrix representation, thus complete the synthesizing. Finally, the fidelity-quantifier formula over QMC is decided by a reduction to quantifier elimination in the existential theory of the reals. The complexity of our method is shown to i) be exponential time for the QMC with a *parametric* initial quantum state; and ii) (as an immediate corollary) be polynomial time for the QMC with a *concrete* initial quantum state.

Finally, we summarize the contributions of the paper as follows:

1. a useful fidelity-based QCTL is presented;
2. all BSCC subspaces are removed by a simple approach, which is more efficient than the existing approach in [10];
3. the complexity is compatible/competitive when the QMC is provided with an initial quantum state, e. g. in [28].

Organization of the paper. Section 2 gives the basic notions and notations from quantum computing. Sections 3 and 4 introduce the model of QMC and the logic — QCTL, respectively. Section 5 presents the model checking algorithm, incorporating with an algebraic approach to the fidelity computation. Section 6 is the conclusion.

2. Preliminaries

Here we recall some basic notions and notations in quantum computing. Interested readers can refer to [24, 11] for more details. Let $[n]$ ($n \in \mathbb{Z}^+$) denote the finite set $\{1, 2, \ldots, n\}$, and $\mathcal{H}$ a Hilbert space with dimension $d := \dim(\mathcal{H})$ throughout this paper. We will adopt the Dirac notations that are standard in quantum computing:

- $|\psi\rangle$ stands for a unit column vector in $\mathcal{H}$ labelled with ψ;
- $\langle\psi| := |\psi\rangle^\dagger$ is the Hermitian adjoin (i. e., complex conjugate and transpose) of $|\psi\rangle$;
- $\langle\psi_1|\psi_2\rangle := \langle\psi_1|\,|\psi_2\rangle$ is the inner product of $|\psi_1\rangle$ and $|\psi_2\rangle$;
- $|\psi_1\rangle\langle\psi_2|$ is the outer product.

Specifically, $|i\rangle$ with $i \in [d]$ denotes the vector, in which the ith entry is 1 and others are 0. Thus, $\langle i|i\rangle = 1$ and $\langle i|j\rangle = 0$ hold for any positive integer $j \neq i$ by orthonormality.

Linear operators. One of the most popular ways to describe quantum states and operations is employing linear operators. Before describing quantum information, we give the definitions of several classes of linear operators. Let $\mathcal{L}_{\mathcal{H}}$ be the set of linear operators on $\mathcal{H}$. Such a subscript $\mathcal{H}$ will be omitted for conciseness if it is clear from the context. A linear operator γ is *Hermitian* if $\gamma = \gamma^\dagger$; it is *positive* if $\langle\psi|\,\gamma\,|\psi\rangle \geq 0$ holds for any $|\psi\rangle \in \mathcal{H}$. The *trace* of a linear operator γ is given by $\mathrm{tr}(\gamma) := \sum_{i\in[d]} \langle\psi_i|\,\gamma\,|\psi_i\rangle$ for any orthonormal basis $\{|\psi_i\rangle : i \in [d]\}$ of $\mathcal{H}$. The trace is defined to be linear in its input. A *density operator* (resp. *partial density operator*) ρ is a positive operator with trace 1 (resp. ≤ 1), which will be used to express quantum states later. Let $\mathcal{D}$ be the set of partial density operators on $\mathcal{H}$, and $\mathcal{D}^1$ the set of density operators.

Extension to a composite system. Sometimes, we need to consider a system composed of two subsystems, say, whose Hilbert spaces are $\mathcal{H}$ and $\mathcal{H}'$, respectively. Then the elements of the composite system $\mathcal{H} \otimes \mathcal{H}'$ are of the form $|\psi, \psi'\rangle$, a shorthand of $|\psi\rangle\,|\psi'\rangle := |\psi\rangle \otimes |\psi'\rangle$, where $\otimes$ denotes tensor product, for $|\psi\rangle \in \mathcal{H}$ and $|\psi'\rangle \in \mathcal{H}'$. It is easy to validate that $\langle\psi_1, \psi'_1\,|\,\psi_2, \psi'_2\rangle = \langle\psi_1|\psi_2\rangle\,\langle\psi'_1\,|\,\psi'_2\rangle$ holds for any $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ and $|\psi'_1\rangle, |\psi'_2\rangle \in \mathcal{H}'$. For any linear operators $\gamma \in \mathcal{L}_{\mathcal{H}}$ and $\gamma' \in \mathcal{L}_{\mathcal{H}'}$, the product operator $\gamma \otimes \gamma'$ has the partial traces $\mathrm{tr}_{\mathcal{H}'}(\gamma \otimes \gamma') := \mathrm{tr}(\gamma')\gamma$ and $\mathrm{tr}_{\mathcal{H}}(\gamma \otimes \gamma') := \mathrm{tr}(\gamma)\gamma'$, which result in linear operators on $\mathcal{H}$ and $\mathcal{H}'$, respectively.

Linear subspaces. There are two important subspaces of a Hilbert space related to particular linear operators. The *support* $\mathrm{supp}(\gamma)$ of a Hermitian operator γ is the subspace of $\mathcal{H}$ spanned by all eigenvectors of γ associated with nonzero eigenvalues. It can be computed in such a way: let the spectral decomposition [24, Box 2.2] of γ be

$$\gamma = \sum_{i\in[d]} \lambda_i\,|\psi_i\rangle\langle\psi_i|\,, \tag{1}$$

where $\lambda_i \in \mathbb{R}$ ($i \in [d]$) are all eigenvalues of γ and $|\psi_i\rangle$ are the corresponding eigenvectors; then $\mathrm{supp}(\gamma)$ is $\mathrm{span}(\{|\psi_i\rangle : i \in [d] \wedge \lambda_i \neq 0\})$. A projection subspace is given by a *projector* $\mathbf{P}$, which is a positive operator of the form $\sum_{i\in[m]} |\psi_i\rangle\langle\psi_i|$ for some orthonormal $|\psi_i\rangle$ ($i \in [m]$) with $m \leq d$. Obviously, there is a bijective map between projectors $\mathbf{P} = \sum_{i\in[m]} |\psi_i\rangle\langle\psi_i|$ on $\mathcal{H}$ and projection subspaces of $\mathcal{H}$ that are spanned by $\{|\psi_i\rangle : i \in [m]\}$.

Quantum states. According to the postulate of quantum mechanics [24, Subsection 2.2.1], quantum operations take place in the Hilbert space $\mathcal{H}$ whose elements are expressed by some orthonormal basis $\{|i\rangle : i \in [d]\}$, where each basis element $|i\rangle$ represents a state vector. Then any unit element $|\psi\rangle = \sum_{i\in[d]} c_i\,|i\rangle$ of $\mathcal{H}$ represents a quantum state, which is entirely determined by those coefficients $c_i \in \mathbb{C}$ ($i \in [d]$), satisfying $\sum_{i\in[d]} |c_i|^2 = 1$, under that basis. General quantum states are represented by the probabilistic ensembles $\{(p_i, |\psi_i\rangle)\colon 1 \leq i \leq k\}$ for some $p_i > 0$ with

$\sum_{i=1}^{k} p_i = 1$, which means we are in $|\psi_i\rangle$ with probability p_i. An alternative representation is using density operators $\rho = \sum_{i=1}^{k} p_i\, |\psi_i\rangle\langle\psi_i|$. Here those $|\psi_i\rangle$ are not necessary to be orthonormal. To be more explicit, thanks to the spectral decomposition [24, Box 2.2], we have $\rho = \sum_{i=1}^{d} \lambda_i\, |\lambda_i\rangle\langle\lambda_i|$, where $|\lambda_i\rangle$ are eigenvectors interpreted as the *eigenstates* of ρ and λ_i are eigenvalues interpreted as the *probabilities* of taking the eigenstates $|\lambda_i\rangle$. It is worth noting that the spectral decomposition of ρ is not unique, but the number of nonzero eigenvalues is unique since it is exactly the rank of ρ. When there is only one eigenstate with unit probability, ρ is said to be a *pure* state, i.e. $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$, in this case, we can also use the vector $|\psi\rangle$ to express the pure state; otherwise it is a *mixed* state. In other words, a pure state indicates the system state which we completely know; a mixed state gives all possible system states with a total probability of one.

Quantum operations. To characterize the change between the general quantum states expressed by density operators, we employ the notion of *super-operator* $\mathcal{E}$ on $\mathcal{H}$ that is a linear operator on $\mathcal{L}_{\mathcal{H}}$. A super-operator is *completely positive* if for any Hilbert space $\mathcal{H}'$, the trivially extended operator $\mathcal{E} \otimes \mathcal{I}_{\mathcal{H}'}$ maps the set of positive operators on $\mathcal{L}_{\mathcal{H}\otimes\mathcal{H}'}$ to itself, where $\mathcal{I}_{\mathcal{H}'}$ is the identity super-operator on $\mathcal{H}'$. Let $\mathcal{S}$ be the set of completely positive super-operators on $\mathcal{H}$. A more detailed description of super-operator is given below.

By Kraus representation [24, Theorem 8.3], a super-operator $\mathcal{E}$ is completely positive on $\mathcal{H}$ if and only if there are m linear operators $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_m \in \mathcal{L}$ (called *Kraus* operators) with $m \le d^2$, such that for any $\gamma \in \mathcal{L}$, we have

$$\mathcal{E}(\gamma) = \sum_{\ell\in[m]} \mathbf{E}_\ell\, \gamma\, \mathbf{E}_\ell^\dagger. \tag{2}$$

Here, each term $\mathbf{E}_\ell\, \gamma\, \mathbf{E}_\ell^\dagger$ ensures that the map is from Hermitian operators γ to Hermitian operators $\mathbf{E}_\ell\, \gamma\, \mathbf{E}_\ell^\dagger$, and further from positive operators to positive operators, as well as their sum. The description of $\mathcal{E}$ is entirely determined by those Kraus operators $\{\mathbf{E}_\ell : \ell \in [m]\}$ (with the brace notation). Thus, we have:

- the sum $\mathcal{E}_1 + \mathcal{E}_2$ of super-operators $\mathcal{E}_1 = \{\mathbf{E}_{1,\ell} : \ell \in [m_1]\}$ and $\mathcal{E}_2 = \{\mathbf{E}_{2,\ell} : \ell \in [m_2]\}$ is given by the union $\{\mathbf{E}_{1,\ell} : \ell \in [m_1]\} \cup \{\mathbf{E}_{2,\ell} : \ell \in [m_2]\}$;
- the composition $\mathcal{E}_2 \circ \mathcal{E}_1$ is given by $\{\mathbf{E}_{2,\ell_2}\mathbf{E}_{1,\ell_1} : \ell_1 \in [m_1] \wedge \ell_2 \in [m_2]\}$;
- the product super-operator $\mathcal{E}_1 \otimes \mathcal{E}_2$ is given by $\{\mathbf{E}_{1,\ell_1} : \ell_1 \in [m_1]\} \otimes \{\mathbf{E}_{2,\ell_2} : \ell_2 \in [m_2]\} = \{\mathbf{E}_{1,\ell_1} \otimes \mathbf{E}_{2,\ell_2} : \ell_1 \in [m_1] \wedge \ell_2 \in [m_2]\}$.

It is easy to validate that $\mathcal{E} \otimes \mathcal{E}'(\gamma \otimes \gamma') = \mathcal{E}(\gamma) \otimes \mathcal{E}'(\gamma')$ holds for any $\gamma \in \mathcal{L}_{\mathcal{H}}$ and $\gamma' \in \mathcal{L}_{\mathcal{H}'}$.

An operation in a probabilistic system is required to preserve the probability; it is required to preserve the trace in a quantum system, which could be realized as follows. A trace pre-order $\lesssim$ is defined on $\mathcal{S}$ as: $\mathcal{E}_1 \lesssim \mathcal{E}_2$ if and only if $\mathrm{tr}(\mathcal{E}_1(\rho)) \le \mathrm{tr}(\mathcal{E}_2(\rho))$ holds for any $\rho \in \mathcal{D}$. The equivalence $\mathcal{E}_1 \eqsim \mathcal{E}_2$ means $\mathcal{E}_1 \lesssim \mathcal{E}_2$ and $\mathcal{E}_1 \gtrsim \mathcal{E}_2$. For a super-operator $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\}$, the completeness $\mathcal{E} \eqsim \mathcal{I}$ holds if and only if $\sum_{\ell\in[m]} \mathbf{E}_\ell^\dagger \mathbf{E}_\ell = \mathbf{I}$ where $\mathbf{I}$ is the identity operator. Here the completeness means the trace-preserving, as

$$\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}\left(\sum_{\ell\in[m]} \mathbf{E}_\ell\, \rho\, \mathbf{E}_\ell^\dagger\right) = \mathrm{tr}\left(\sum_{\ell\in[m]} \mathbf{E}_\ell^\dagger \mathbf{E}_\ell\, \rho\right) = \mathrm{tr}(\mathbf{I}\rho) = \mathrm{tr}(\rho). \tag{3}$$

Let $\mathcal{S}^{\lesssim\mathcal{I}}$ be the set of *trace-nonincreasing* super-operators $\mathcal{E}$, i. e., $\mathcal{S}^{\lesssim\mathcal{I}} = \{\mathcal{E} \in \mathcal{S} : \mathcal{E} \lesssim \mathcal{I}\}$. Later on, we would characterize quantum operations by these super-operators $\mathcal{E} \in \mathcal{S}^{\lesssim\mathcal{I}}$.

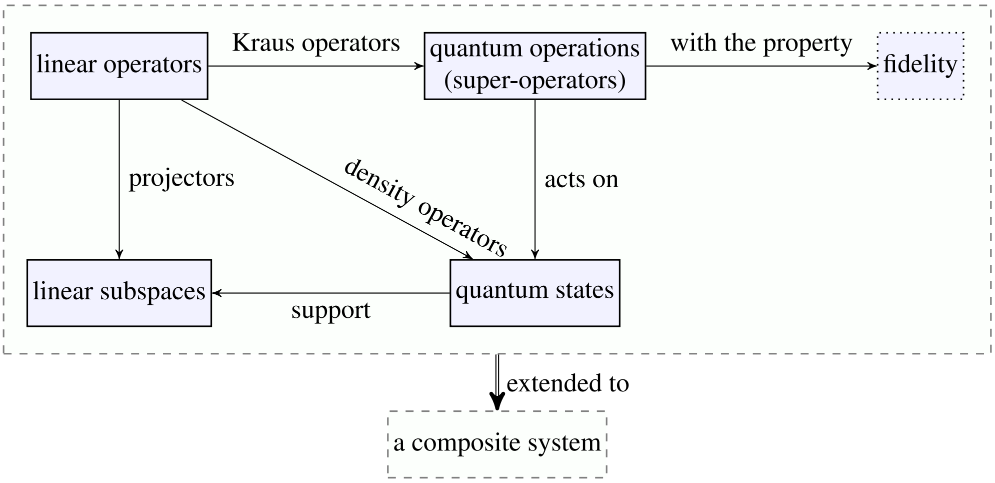

Figure 1: The organization of basic notions

Summarizing the notations, we would like to use letters in bold font, e. g. $\mathbf{E}, \mathbf{F}, \mathbf{I}, \mathbf{P}$, for linear operators with two exceptional Greek letters — γ intended for Hermitian operators and ρ for density operators, and use letters in calligraphic font, e. g. $\mathcal{E}, \mathcal{F}, \mathcal{I}, \mathcal{P}$, for super-operators. All the above categories of notions are organized as Figure 1, where the exceptional category of fidelity will be delivered in Section 4.

3. Quantum Markov Chain

Here we introduce the model of quantum Markov chain, and then establish the measurable space over its paths for formally reasoning about quantitative properties. Let AP be a set of atomic propositions throughout this paper.

Definition 3.1 ([11, Definition 3.1]). *A labelled* quantum Markov chain *(QMC for short)* $\mathfrak{C}$ *over Hilbert space* $\mathcal{H}$ *is a triple* (S, Q, L)*, in which*

- S *is a finite set of classical states,*
- $Q \colon S \times S \to \mathcal{S}_{\mathcal{H}}^{\lesssim \mathcal{I}}$ *is a transition super-operator matrix, satisfying* $\sum_{t \in S} Q(s,t) \eqsim \mathcal{I}_{\mathcal{H}}$ *for each* $s \in S$*, and*
- $L \colon S \to 2^{AP}$ *is a labelling function.*

The QMC $\mathfrak{C}$ is a composite system of two components: a classical subsystem S and a quantum one $\mathcal{H}$. We employ the following Dirac notations to encode the classical component, so that the two components can be unified into a composite quantum system. Let $|s\rangle$ $(s \in S)$ be the quantisation of each classical state s that is the unit vector in which the entry corresponding to s is 1 and others are 0, and $\{|s\rangle : s \in S\}$ a set of orthonormal states serving as the quantisation of S. Then the classical subsystem S induces a Hilbert space $C := \mathrm{span}(\{|s\rangle : s \in S\})$, and the composite classical–quantum system is defined on the enlarged Hilbert space $\mathcal{H}_{\mathrm{cq}} := C \otimes \mathcal{H}$. The dimension of $\mathcal{H}_{\mathrm{cq}}$ is $N := nd$ where $n = |S|$, which will be used to reflect the size of the input model $\mathfrak{C}$. The instantaneous descriptions (IDs) of $\mathfrak{C}$ are uniformly represented by the density operator $\varrho = \sum_{s \in S} |s\rangle\langle s| \otimes \rho_s$ on $\mathcal{H}_{\mathrm{cq}}$ with partial density operators $\rho_s \in \mathcal{D}_{\mathcal{H}}$ distributed over classical states $s \in S$, satisfying $\sum_{s \in S} \mathrm{tr}(\rho_s) = 1$. The initial ID is left *parametric* in the model, particularly suitable for the uncertainty in quantum system.

For a classical state $s \in S$, the super-operators $Q(s,t)$ $(t \in S)$ characterize the changes from state s with partial density operator ρ_s to state t with ρ_t. Summarizing over all successors $t \in S$, they are required to preserve the trace, i. e., meeting the completeness $\sum_{t \in S} Q(s,t) \eqsim \mathcal{I}$. All single transition super-operators $Q(s,t)$ $(s,t \in S)$ on $\mathcal{H}$ can be extended to $\{|t\rangle\langle s|\} \otimes Q(s,t)$ on $\mathcal{H}_{\mathrm{cq}}$. After $\{|t\rangle\langle s|\} \otimes Q(s,t)$ acts on an ID, the super-operator $\{|t\rangle\langle s|\}$ changes the classical state from s to t, while $Q(s,t)$ changes the quantum state from ρ_s to $Q(s,t)(\rho_s)$.

Example 3.2. *Let us consider the QMC* $\mathfrak{C}_1 = (S, Q, L)$ *over a* 2*-qubit (*4*-dimensional) Hilbert space* $\mathcal{H} = \mathrm{span}(\{|1,1\rangle, |1,2\rangle, |2,1\rangle, |2,2\rangle\})$ *as shown in Figure 2. The classical state set* S *is* $\{s_0, s_1, s_2, s_3, s_4, s_5\}$*, where* $L(s_5) = \{\mathtt{ok}\}$*,* $L(s_4) = \{\mathtt{error}\}$*, and other states are labelled with* $\emptyset$*. If the ID of* $\mathfrak{C}_1$ *is* $\varrho_1 = |s_1\rangle\langle s_1| \otimes \rho_1 + |s_2\rangle\langle s_2| \otimes \rho_2$ *for some partial density operators* $\rho_1, \rho_2 \in \mathcal{D}_{\mathcal{H}}$ *satisfying* $\mathrm{tr}(\rho_1) + \mathrm{tr}(\rho_2) = 1$*, it means that we are in classical state* s_1 *carrying unit quantum information* $\rho_1/\mathrm{tr}(\rho_1)$ *with probability* $\mathrm{tr}(\rho_1)$ *and in classical state* s_2 *carrying unit quantum information* $\rho_2/\mathrm{tr}(\rho_2)$ *with probability* $\mathrm{tr}(\rho_2)$*.*

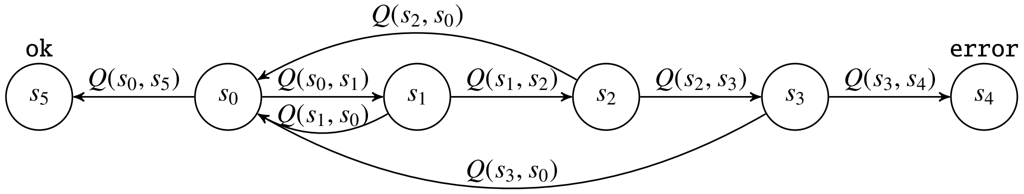

Figure 2: A sample QMC

The transition super-operator matrix Q *is given by the following nonzero entries in Kraus representation:*

$$\begin{aligned} Q(s_0, s_1) &= \{|1,+\rangle\langle 1,1|, \tfrac{4}{5}\,|1,-\rangle\langle 1,2|\}, & Q(s_0, s_5) &= \{\tfrac{3}{5}\,|1,2\rangle\langle 1,2|, |2\rangle\langle 2| \otimes \mathbf{I}\}, \\ Q(s_1, s_0) &= \{|1,1\rangle\langle 1,+|, \tfrac{4}{5}\,|1,2\rangle\langle 1,-|\}, & Q(s_1, s_2) &= \{\tfrac{3}{5}\,|1,2\rangle\langle 1,-|, |2\rangle\langle 2| \otimes \mathbf{I}\}, \\ Q(s_2, s_0) &= \{\tfrac{12}{25}\,\mathbf{X} \otimes \mathbf{I}, \tfrac{9}{25}\,\mathbf{X} \otimes \mathbf{X}\}, & Q(s_2, s_3) &= \{\tfrac{16}{25}\,\mathbf{I} \otimes \mathbf{I}, \tfrac{12}{25}\,\mathbf{I} \otimes \mathbf{X}\}, \\ Q(s_3, s_0) &= \{\tfrac{12}{25}\,\mathbf{I} \otimes \mathbf{Z}, \tfrac{12}{25}\,\mathbf{Z} \otimes \mathbf{I}\}, & Q(s_3, s_4) &= \{\tfrac{16}{25}\,\mathbf{I} \otimes \mathbf{I}, \tfrac{9}{25}\,\mathbf{Z} \otimes \mathbf{Z}\}, \\ Q(s_4, s_4) &= \{\mathbf{I} \otimes \mathbf{I}\}, & Q(s_5, s_5) &= \{\mathbf{I} \otimes \mathbf{I}\}, \end{aligned}$$

where $|\pm\rangle = (|1\rangle \pm |2\rangle)/\sqrt{2}$*,* $\mathbf{I} = |1\rangle\langle 1| + |2\rangle\langle 2|$ *is the identity operator,* $\mathbf{X} = |1\rangle\langle 2| + |2\rangle\langle 1|$ *is the bit flip and* $\mathbf{Z} = |1\rangle\langle 1| - |2\rangle\langle 2|$ *is the phase flip. In a super-operator* $Q(s,t)$*, each Kraus operator makes a part of change moving* ρ_s *to* ρ_t*. For instance,* $\frac{3}{5}\,|1,2\rangle\langle 1,-|$ *in* $Q(s_1, s_2)$ *moves* $\frac{9}{25}\,|1,2\rangle\langle 1,-|\rho_{s_1}|1,-\rangle\langle 1,2|$ *from classical state* s_1 *to* s_2*. After* $Q(s_1, s_2)$ *acts on* ρ_{s_1}*, the resulting partial density operator* $Q(s_1, s_2)(\rho_{s_1})$ *would constitute the quantum information* ρ_{s_2} *at classical state* s_2*. It is easy to validate that the completeness* $\sum_{t \in S} Q(s,t) \eqsim \mathcal{I}$ *holds for each* $s \in S$[1]*.*

[1] The intention of those super-operators is to characterize the computation through a noisy channel with trace-

Actually, the model of QMC is more expressive than that of the ordinary Markov chain (MC). It can be seen from the following lemma:

Lemma 3.3. *Given an MC $\mathcal{M} = (S, \mathbf{Q}, L)$, it can be modelled by a QMC $\mathfrak{C} = (S, Q, L)$ over $\mathcal{H}$, even when $\mathcal{H}$ is one-dimensional.*

Proof. The state set S and the labelling function L of the QMC $\mathfrak{C}$ are directly taken from the MC $\mathcal{M} = (S, \mathbf{Q}, L)$. In $\mathcal{M}$, the ID is given by some probability distribution that is in state s with probability p_s, satisfying $\sum_{s \in S} p_s = 1$, while the transition from s to t is given by the transition probability $\mathbf{Q}(s,t)$. We are to encode them in $\mathfrak{C}$ as follows. Let $|\psi\rangle$ be a fixed element of $\mathcal{H}$. The ID of $\mathfrak{C}$ is correspondingly given by the density operator $\sum_{s \in S} p_s \, |s\rangle\langle s| \otimes |\psi\rangle\langle\psi|$ on $\mathcal{H}_{\mathrm{cq}}$. We choose $Q(s,t)$ as the singleton $\{\mathbf{Q}(s,t)^{1/2}\,\mathbf{I}\}$, so that

$$Q(s,t)(p_s\,|\psi\rangle\langle\psi|) = [\mathbf{Q}(s,t)^{1/2}\,\mathbf{I}]p_s\,|\psi\rangle\langle\psi|\,[\mathbf{Q}(s,t)^{1/2}\,\mathbf{I}] = \mathbf{Q}(s,t)p_s\,|\psi\rangle\langle\psi|$$
$$\{|t\rangle\langle s|\} \otimes Q(s,t)(p_s\,|s\rangle\langle s| \otimes |\psi\rangle\langle\psi|) = \mathbf{Q}(s,t)p_s\,|t\rangle\langle t| \otimes |\psi\rangle\langle\psi|\,.$$

Thus the transition probability matrix $\mathbf{Q}$ is imitated by the transition super-operator matrix Q. When $\dim(\mathcal{H}) = 1$, the same imitation follows with the linear operators $\mathbf{I}$ and $|\psi\rangle\langle\psi|$ both being degenerated to the constant 1. □

Sometimes, it is convenient to combine all the transition super-operator matrix $Q(s,t)$ $(s, t \in S)$ on $\mathcal{H}$ together to form a large single super-operator, namely $\mathcal{F} := \sum_{s,t \in S} \{|t\rangle\langle s|\} \otimes Q(s,t)$, on the enlarged Hilbert space $\mathcal{H}_{\mathrm{cq}}$. The enlarged transition super-operator $\mathcal{F}$ is functionally analogous to the transition probability matrix in the MC.

Example 3.4. *All the super-operators on $\mathcal{H}$ appeared in the QMC $\mathfrak{C}_1$ in Example 3.2 could be combined as a single super-operator on $\mathcal{H}_{\mathrm{cq}}$:*

$$\begin{aligned}\mathcal{F} = {} & \{|s_1\rangle\langle s_0|\} \otimes Q(s_0, s_1) + \{|s_5\rangle\langle s_0|\} \otimes Q(s_0, s_5) + \{|s_0\rangle\langle s_1|\} \otimes Q(s_1, s_0) + \\ & \{|s_2\rangle\langle s_1|\} \otimes Q(s_1, s_2) + \{|s_0\rangle\langle s_2|\} \otimes Q(s_2, s_0) + \{|s_3\rangle\langle s_2|\} \otimes Q(s_2, s_3) + \\ & \{|s_0\rangle\langle s_3|\} \otimes Q(s_3, s_0) + \{|s_4\rangle\langle s_3|\} \otimes Q(s_3, s_4) + \{|s_4\rangle\langle s_4|\} \otimes \mathcal{I} + \{|s_5\rangle\langle s_5|\} \otimes \mathcal{I},\end{aligned}$$

in which the left operand of the tensor product in a term is a super-operator on C and the right operand is a super-operator on $\mathcal{H}$. Applying $\mathcal{F}$ to the ID ϱ_1, we get a new ID

$$\begin{aligned}\varrho_1' = {} & (\{|s_0\rangle\langle s_1|\} \otimes Q(s_1, s_0))(|s_1\rangle\langle s_1| \otimes \rho_1) + (\{|s_2\rangle\langle s_1|\} \otimes Q(s_1, s_2))(p\,|s_1\rangle\langle s_1| \otimes \rho_1) + \\ & (\{|s_0\rangle\langle s_2|\} \otimes Q(s_2, s_0))(|s_2\rangle\langle s_2| \otimes \rho_2) \;+ (\{|s_3\rangle\langle s_2|\} \otimes Q(s_2, s_3))(|s_2\rangle\langle s_2| \otimes \rho_2) \\ = {} & |s_0\rangle\langle s_0| \otimes Q(s_1, s_0)(\rho_1) + |s_2\rangle\langle s_2| \otimes Q(s_1, s_2)(\rho_1) + \\ & |s_0\rangle\langle s_0| \otimes Q(s_2, s_0)(\rho_2) + |s_3\rangle\langle s_3| \otimes Q(s_2, s_3)(\rho_2),\end{aligned}$$

which is easily calculated by the orthonormality $\langle s_i|s_i\rangle = 1$ and $\langle s_i|s_j\rangle = 0$ for $i \neq j$.

allocation of quantum information. In practice, the trace-allocation of quantum information has a large proportion of being the identity operator **I** and a small proportion of being noise operators, e. g. the bit flip **X** and the phase flip **Z**, which would change density operators. However, to present our method precisely, we focus more on the situation where severe noises appear and choose an underlying graph with several cycles. Thus we set super-operator entries simply by those noise operators.

A path ω in the QMC $\mathfrak{C}$ is an infinite state sequence in the form $s_0\, s_1\, s_2 \cdots$, where $s_i \in S$ and $Q(s_i, s_{i+1}) \neq 0$ for $i \geq 0$. Let $\omega(i)$ be the $(i+1)$-th state of ω for $i \geq 0$, e. g. $\omega(0) = s_0$ and $\omega(1) = s_1$ for $\omega = s_0\, s_1\, s_2 \cdots$. We denote by $\mathit{Path}(s)$ the set of all paths starting in s, and by $\mathit{Path}_{\mathrm{fin}}(s)$ the set of all finite paths starting in s, i. e., $\mathit{Path}_{\mathrm{fin}}(s) := \{\hat{\omega} : \hat{\omega}$ is a finite prefix of some $\omega \in \mathit{Path}(s)\}$.

Example 3.5. *In the QMC $\mathfrak{C}_1$ shown in Example 3.2, $\omega_1 = s_3\, s_0\, s_1\, s_0\, s_5\, s_5 \cdots$ is a path starting in s_3, where $\omega_1(0) = s_3$, $\omega_1(1) = \omega_1(3) = s_0$, $\omega_1(2) = s_1$, and $\omega_1(i) = s_5$ for $i \geq 4$; while $\hat{\omega}_1 = s_3\, s_0\, s_1\, s_0\, s_5$ is a finite prefix of ω_1. Therefore, we have $\omega_1 \in \mathit{Path}(s_3)$ and $\hat{\omega}_1 \in \mathit{Path}_{\mathrm{fin}}(s_3)$.*

Since the initial ID of the QMC in Definition 3.1 is parametric, it is necessary to develop some measurement over paths, independent from concrete initial IDs, for reasoning about quantitative properties. We resort to the notion of super-operator valued measure (SOVM) that is a function from $\mathcal{D}$ to itself, and establish the SOVM space as follows. Recall that:

Definition 3.6. *A* measurable space *is a pair (Ω, Σ), where Ω is a nonempty set and Σ is a σ-algebra on Ω that is a collection of subsets of Ω, satisfying:*

- $\Omega \in \Sigma$, *and*
- Σ *is closed under countable union and complement.*

In addition, an SOVM space *is a triple (Ω, Σ, Δ), where (Ω, Σ) is a measurable space and $\Delta\colon \Sigma \to \mathcal{S}^{\lesssim \mathcal{I}}$ is an SOVM, satisfying:*

- $\Delta(\Omega) \eqsim \mathcal{I}$, *and*
- $\Delta(\biguplus_i A_i) \eqsim \sum_i \Delta(A_i)$ *for any pairwise disjoint $A_i \in \Sigma$.*

From the definition, we can see that an event A is (Ω, Σ)-measurable if A belongs to Σ, and its SOVM is given by the Δ defined on that Σ.

For a given finite path $\hat{\omega} \in \mathit{Path}_{\mathrm{fin}}(s)$, we define the cylinder set as

$$\mathit{Cyl}(\hat{\omega}) := \{\omega \in \mathit{Path}(s) : \omega \text{ has the prefix } \hat{\omega}\}; \tag{4}$$

and for $B \subseteq \mathit{Path}_{\mathrm{fin}}(s)$, we extend (4) by $\mathit{Cyl}(B) := \bigcup_{\hat{\omega} \in B} \mathit{Cyl}(\hat{\omega})$. In particular, we have $\mathit{Cyl}(s) = \mathit{Path}(s)$. Let $\Omega = \mathit{Path}(s)$ for a given $s \in S$, and $\Pi \subseteq 2^{\Omega}$ be the countable set of all cylinder sets $\{\mathit{Cyl}(\hat{\omega}) : \hat{\omega} \in \mathit{Path}_{\mathrm{fin}}(s)\}$ plus the empty set $\emptyset$. By [2, Chapter 10], there is a smallest σ-algebra Σ of Π that contains Π and is closed under countable union and complement. It is clear that the pair (Ω, Σ) forms a measurable space.

Next, for a given finite path $\hat{\omega} = s_0\, s_1 \cdots s_n$, we define the composed super-operator along with $\hat{\omega}$ as

$$\Delta(\mathit{Cyl}(\hat{\omega})) := \begin{cases} \mathcal{I} & \text{if } n = 0, \\ Q(s_{n-1}, s_n) \circ \cdots \circ Q(s_0, s_1) & \text{otherwise.} \end{cases} \tag{5}$$

By [11, Theorem 3.2], the domain of Δ can be extended to Σ, i. e., $\Delta\colon \Sigma \to \mathcal{S}^{\lesssim \mathcal{I}}$, which is unique under the countable union $\bigcup_i A_i$ for any $A_i \in \Pi$ and is an equivalence class of super-operators in terms of the equivalence $\eqsim$ under the complement A^{c} for some $A \in \Pi$. Hence the triple (Ω, Σ, Δ) forms an SOVM space.

Example 3.7. *For each $s \in S$, we can establish an SOVM space (Ω, Σ, Δ) over the path set Path(s) of $\mathfrak{C}_1$ in Example 3.4. To demonstrate the generality of the method, we choose $\Omega =$ Path(s_3). Then, for the finite path $\hat{\omega}_1 = s_3\, s_0\, s_1\, s_0\, s_5$, the SOVM could be calculated as*

$$\begin{aligned}\Delta(Cyl(\hat{\omega}_1)) &= Q(s_0, s_5) \circ Q(s_1, s_0) \circ Q(s_0, s_1) \circ Q(s_3, s_0) \\ &= Q(s_0, s_5) \circ Q(s_1, s_0) \circ Q(s_0, s_1) \circ \{\tfrac{12}{25}\, \mathbf{I} \otimes \mathbf{Z}, \tfrac{12}{25}\, \mathbf{Z} \otimes \mathbf{I}\} \\ &= Q(s_0, s_5) \circ Q(s_1, s_0) \circ \{\tfrac{12\sqrt{2}}{25}\, |1, +\rangle\langle 1, 1|\,, \tfrac{48\sqrt{2}}{125}\, |1, -\rangle\langle 1, 2|\} \\ &= Q(s_0, s_5) \circ \{\tfrac{12\sqrt{2}}{25}\, |1, 1\rangle\langle 1, 1|\,, \tfrac{192\sqrt{2}}{625}\, |1, 2\rangle\langle 1, 2|\} \\ &= \{\tfrac{576\sqrt{2}}{3125}\, |1, 2\rangle\langle 1, 2|\}.\end{aligned}$$

In details, we calculate the composition of super-operators using right associativity, e. g.

$$\begin{aligned}& Q(s_0, s_1) \circ Q(s_3, s_0) \\ &= \{|1, +\rangle\langle 1, 1|\,, \tfrac{4}{5}\, |1, -\rangle\langle 1, 2|\} \circ \{\tfrac{12}{25}\, \mathbf{I} \otimes \mathbf{Z}, \tfrac{12}{25}\, \mathbf{Z} \otimes \mathbf{I}\} \\ &= \{\tfrac{12}{25}\, |1, +\rangle\langle 1, 1|\, (\mathbf{I} \otimes \mathbf{Z}), \tfrac{12}{25}\, |1, +\rangle\langle 1, 1|\, (\mathbf{Z} \otimes \mathbf{I}), \tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\, (\mathbf{I} \otimes \mathbf{Z}), \tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\, (\mathbf{Z} \otimes \mathbf{I})\} \\ &= \{\tfrac{12}{25}\, |1, +\rangle\langle 1, 1|\,, \tfrac{12}{25}\, |1, +\rangle\langle 1, 1|\,, -\tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\,, \tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\} \\ &= \{\tfrac{12\sqrt{2}}{25}\, |1, +\rangle\langle 1, 1|\,, \tfrac{48\sqrt{2}}{125}\, |1, -\rangle\langle 1, 2|\},\end{aligned}$$

where the last equation follows from a combination of Kraus operators, saying

$$\begin{aligned}& \{-\tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\,, \tfrac{48}{125}\, |1, -\rangle\langle 1, 2|\}(\rho) \\ &= (-\tfrac{48}{125}\, |1, -\rangle\langle 1, 2|)\rho(-\tfrac{48}{125}\, |1, 2\rangle\langle 1, -|) + (\tfrac{48}{125}\, |1, -\rangle\langle 1, 2|)\rho(\tfrac{48}{125}\, |1, 2\rangle\langle 1, -|) \\ &= (\tfrac{48\sqrt{2}}{125}\, |1, -\rangle\langle 1, 2|)\rho(\tfrac{48\sqrt{2}}{125}\, |1, 2\rangle\langle 1, -|) \\ &= \{\tfrac{48\sqrt{2}}{125}\, |1, -\rangle\langle 1, 2|\}(\rho).\end{aligned}$$

4. Quantum Computation Tree Logic

In practice, the transition of quantum information suffers from all kinds of noises. It is worth considering how close the output state is to the input one through a noisy channel. As we mentioned in the introduction, fidelity is a useful tool in comparing quantum states, and in many occasions, fidelity can detect the effect of a noisy channel but probability measure cannot. So we introduce a quantum extension of computation tree logic (QCTL) based on fidelity. The main ingredient is to replace the trace (probability) measure in the existing logic of [11] with fidelity.

We first recall the notion of fidelity.

Definition 4.1. *For a super-operator $\mathcal{E} \in \mathcal{S}^{\lesssim I}$ and a density operator $\rho \in \mathcal{D}^1$, the* fidelity *is defined as*

$$\mathrm{Fid}(\mathcal{E}, \rho) := \mathrm{tr}\left(\sqrt{\rho^{1/2}\mathcal{E}(\rho)\rho^{1/2}}\right), \tag{6a}$$

where $\rho^{1/2} = \sum_{i \in [d]} \lambda_i^{1/2}\, |\psi_i\rangle\langle\psi_i|$ is obtained from some spectral decomposition $\sum_{i \in [d]} \lambda_i\, |\psi_i\rangle\langle\psi_i|$ of ρ. In particular, when ρ is a pure state $|\psi\rangle\langle\psi|$, it is simply

$$\mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) := \sqrt{\langle\psi|\, \mathcal{E}(|\psi\rangle\langle\psi|)\, |\psi\rangle}. \tag{6b}$$

The fidelity reflects how well the quantum operation $\mathcal{E}$ has preserved the quantum state ρ. The better a quantum state is preserved, the larger the fidelity would be. It can be seen from a simple case: assuming $\rho = |\psi\rangle\langle\psi|$ and $\mathcal{E}(|\psi\rangle\langle\psi|) = |\varphi\rangle\langle\varphi|$, the fidelity $\mathrm{Fid}(\mathcal{E}, \rho)$ is just $\sqrt{\langle\psi|\varphi\rangle\,\langle\varphi|\psi\rangle}$, measuring the angle between the two vectors $|\psi\rangle$ and $|\varphi\rangle$. Generally speaking, the fidelity measures the average angle between the vectors in $\mathrm{supp}(\rho)$ and those in $\mathrm{supp}(\mathcal{E}(\rho))$, which implies that $\arccos \mathrm{Fid}(\mathcal{E}, \rho)$ would be a standard metric between ρ and $\mathcal{E}(\rho)$.

For a fixed trace-preserving super-operator $\mathcal{E}$, we can see that the fidelity $\mathrm{Fid}(\mathcal{E}, \rho)$, ranging over $[0, 1]$, varies with the density operator ρ. It attains the minimum if and only if the supports of ρ and $\mathcal{E}(\rho)$ are orthogonal, and attains the maximum if and only if $\rho = \mathcal{E}(\rho)$. For the sake of conservation, we would like to study the system performance in the worst case. That is based on the minimum fidelity of $\mathcal{E}$ defined by

$$\underline{\mathrm{Fid}}(\mathcal{E}) := \min_{\rho\in\mathcal{D}^1} \mathrm{Fid}(\mathcal{E}, \rho) = \min_{|\psi\rangle\in\mathcal{H}} \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|), \tag{7}$$

where the last equation comes from the joint concavity [24, Exercise 9.19].

In the following, we present the syntax and semantics of the new logic, then compare it with probabilistic CTL (PCTL) presented in [19] and with the QCTL in [11].

Definition 4.2. *The syntax of QCTL consists of state formulas Φ and path formulas ϕ:*

$$\Phi := \mathrm{a} \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \mathfrak{F}_{\sim\tau}[\phi]$$
$$\phi := \mathrm{X}\,\Phi \mid \Phi_1 \mathrm{U}^{\leq k}\Phi_2 \mid \Phi_1 \mathrm{U}\,\Phi_2$$

where a $\in$ *AP is an atomic proposition, $\sim \in \{<, \leq, =, \geq, >, \neq\}$ is a comparison operator, $\tau \in \mathbb{Q} \cap [0, 1]$ is a threshold, and $k \geq 0$ is a step bound.*

The state formula $\mathfrak{F}_{\sim\tau}[\phi]$ in QCTL is called the *fidelity-quantifier* formula, and other state formulas are *basic* ones. The three kinds of path formulas $\mathrm{X}\,\Phi$, $\Phi_1 \mathrm{U}^{\leq k}\Phi_2$ and $\Phi_1 \mathrm{U}\,\Phi_2$ are the *next*, the *bounded-until* and the *unbounded-until* formulas, respectively.

Definition 4.3. *The semantics of QCTL interpreted over a QMC $\mathfrak{C} = (S, Q, L)$ is given by the satisfaction relation $\models$:*

$$\begin{aligned}
s &\models \mathrm{a} && \text{if } s \text{ has the label a in } \mathfrak{C}, \text{ i.e., a} \in L(s),\\
s &\models \neg\Phi && \text{if } s \not\models \Phi,\\
s &\models \Phi_1 \wedge \Phi_2 && \text{if } s \models \Phi_1 \wedge s \models \Phi_2,\\
s &\models \mathfrak{F}_{\sim\tau}[\phi] && \text{if } \underline{\mathrm{Fid}}(\Delta(\{\omega \in \mathit{Path}(s) : \omega \models \phi\})) \sim \tau,\\
\omega &\models \mathrm{X}\,\Phi && \text{if } \omega(1) \models \Phi,\\
\omega &\models \Phi_1 \mathrm{U}^{\leq k}\Phi_2 && \text{if } \exists\, i \leq k : (\omega(i) \models \Phi_2 \wedge \forall\, j < i : \omega(j) \models \Phi_1),\\
\omega &\models \Phi_1 \mathrm{U}\,\Phi_2 && \text{if } \exists\, i : (\omega(i) \models \Phi_2 \wedge \forall\, j < i : \omega(j) \models \Phi_1).
\end{aligned}$$

Other logic connectives $\vee$, $\rightarrow$ and $\leftrightarrow$ can be easily derived by $\neg$ and $\wedge$ as usual.

Here, the next formula $\mathrm{X}\,\Phi$ requires that the second state $\omega(1)$ of the path $\omega = \omega(0)\,\omega(1)\,\omega(2)\cdots$ should satisfy Φ; the bounded-until formula $\Phi_1 \mathrm{U}^{\leq k}\Phi_2$ requires that there is a state $\omega(i)$ within the step bound $i \leq k$ satisfying Φ_2 and all proper predecessors $\omega(j)$ satisfy Φ_1; the unbounded-until formula $\Phi_1 \mathrm{U}\,\Phi_2$ drops the step bound $\leq k$; letting Δ be the SOVM of all paths in $\mathit{Path}(s)$ that satisfy ϕ, the fidelity-quantifier formula $\mathfrak{F}_{\sim\tau}[\phi]$ requires that the minimum fidelity of Δ should meet the threshold $\sim \tau$. In details, the trace-nonincreasing super-operator Δ is a function mapping from an initial quantum state $\rho_s \in \mathcal{D}^1$ to a new quantum state $\rho' \in \mathcal{D}$, and $\mathfrak{F}_{\sim\tau}[\phi]$ is the quantitative property asking whether the minimum of the fidelity $\mathrm{Fid}(\rho_s, \rho')$, with ρ_s ranging over $\mathcal{D}^1$, meets the threshold $\sim \tau$. For example, suppose the super-operator Δ induced by ϕ is determined by the Kraus representation $\{\frac{4}{5}\,|-\rangle\langle 2|\,, |+\rangle\langle 1|\}$. Given an initial density operator $\rho_s = |1\rangle\langle 1|$ (resp. $\rho_s = |2\rangle\langle 2|$), the final quantum state after applying Δ involves into $\rho' = |+\rangle\langle +|$ (resp. $\rho' = \frac{16}{25}\,|-\rangle\langle -|$), and the fidelity between the pair of states is $1/\sqrt{2}$ (resp. $2\sqrt{2}/5$). With the initial quantum state varying, $\mathfrak{F}_{\sim\tau}[\phi]$ is used to compare the minimum fidelity $\underline{\mathrm{Fid}}(\Delta)$ among such pairs of quantum states with the threshold τ.

For any path formula ϕ, the path set $A = \{\omega \in \mathit{Path}(s) : \omega \models \phi\}$ belongs to the σ-algebra Σ that contains all cylinder sets of $\Omega = \mathit{Path}(s)$, since

- if $\phi = \mathrm{X}\,\Phi$, A is the finite union of those cylinder sets $\mathit{Cyl}(s\,t)$ that satisfy $t \models \Phi$;
- if $\phi = \Phi_1 \mathrm{U}^{\leq k} \Phi_2$, A is the finite union of $\mathit{Cyl}(s_0 \cdots s_i)$ for some $i \leq k$, that satisfy $s_0 = s$, $s_i \models \Phi_2$, and $s_j \models \Phi_1$ for each $j < i$;
- if $\phi = \Phi_1 \mathrm{U}\, \Phi_2$, A is the countable union of $\mathit{Cyl}(s_0 \cdots s_i)$ for some $i \geq 0$, that satisfy $s_0 = s$, $s_i \models \Phi_2$, and $s_j \models \Phi_1$ for each $j < i$.

Thereby, the set A is (Ω, Σ)-measurable, and the SOVM $\Delta(A)$ is uniquely defined. For conciseness, we will write $\Delta(\hat{\omega})$ for $\Delta(\mathit{Cyl}(\hat{\omega}))$ and $\Delta(\phi)$ for $\Delta(\{\omega \in \mathit{Path}(s) : \omega \models \phi\})$ afterwards.

Example 4.4. *Consider the path $\omega_1 = s_3\, s_0\, s_1\, s_0\, s_5\, s_5 \cdots$ on the QMC $\mathfrak{C}_1$ shown in Example 3.2 where only state s_5 has the label* ok*, we can see*

- $\omega_1 \models \mathtt{true}\,\mathrm{U}\,\mathtt{ok}$*, as $\omega_1(4) \models \mathtt{ok}$ and $\omega_1(j) \models \mathtt{true}$ for each $j < 4$.*

The SOVM $\Delta(\hat{\omega}_1)$ has been obtained as $\Delta(\mathit{Cyl}(\hat{\omega}_1)) = \{\frac{576\sqrt{2}}{3125}\,|1,2\rangle\langle 1,2|\}$ in Example 3.7. Since $\omega_1 \in \Omega = \mathit{Path}(s_3)$ and $\omega_1 \models \mathtt{true}\,\mathrm{U}\,\mathtt{ok}$, the SOVM $\Delta(\mathtt{true}\,\mathrm{U}\,\mathtt{ok})$ has the lower bound $\{\frac{576\sqrt{2}}{3125}\,|1,2\rangle\langle 1,2|\}$.

Finally, we point out the difference between the PCTL in [19], the QCTL in [11] and our QCTL. The PCTL extends CTL by introducing a probability-quantifier $\mathfrak{P}_{\leq\tau}(\phi)$ that compares the probability of the measurable event specified by ϕ with the threshold τ, and decides it over an MC with a specific initial ID (probability distribution over classical states). The QCTL in [11] introduces an SOVM-quantifier $\mathfrak{Q}_{\lesssim\mathcal{E}}(\phi)$ that compares the SOVM of ϕ with the super-operator threshold $\mathcal{E}$ under the trace pre-order $\lesssim$, and decides it over a QMC with a specific initial ID (density operator on $\mathcal{H}_{\mathrm{cq}}$). Whereas, ours introduces a fidelity-quantifier $\mathfrak{F}_{\leq\tau}(\phi)$ that compares the fidelity of the SOVM of ϕ with the threshold τ, and aims to decide it over a QMC with a parametric initial quantum state. The parametric model is more expressive, and thus our method would be potentially applicable. How to consider the SOVM-quantifier on a parametric QMC would be one of our future work.

5. Model Checking Algorithm

In this section, we present the main model checking algorithm for a given QMC $\mathfrak{C} = (S, Q, L)$ and a QCTL state formula Φ. The algorithm would decide $s \models \Phi$ for a given state $s \in S$, or equivalently compute the set of all states satisfying Φ, i. e., $\mathit{Sat}(\Phi) := \{s \in S : s \models \Phi\}$. Since the definition of QCTL is mutually inductive, this goal will be reached in three steps:

1. deciding basic state formulas (except for the fidelity-quantifier one),
2. synthesizing the super-operators of path formulas, and
3. deciding the fidelity-quantifier formula.

5.1. Deciding basic state formulas

For basic state formulas, the satisfying sets are directly calculated by their definitions:

- $Sat(\mathrm{a}) = \{s \in S : \mathrm{a} \in L(s)\}$;
- $Sat(\neg\Phi) = S \setminus Sat(\Phi)$, provided that $Sat(\Phi)$ is known, and
- $Sat(\Phi_1 \wedge \Phi_2) = Sat(\Phi_1) \cap Sat(\Phi_2)$, provided that $Sat(\Phi_1)$ and $Sat(\Phi_2)$ are known.

Obviously, the top-level logic connective of those formulas requires merely a scan over the labelling function L on S, which is in $O(n)$ with $n = |S|$. Hence, deciding basic state formulas is in linear time w. r. t. the size of $\mathfrak{C}$.

Example 5.1. *From the QMC $\mathfrak{C}_1$ shown in Example 3.2, it is easy to calculate*

- $Sat(\mathtt{ok}) = \{s_5\}$*,* $Sat(\mathtt{error}) = \{s_4\}$*;*
- $Sat(\neg\mathtt{ok}) = S \setminus Sat(\mathtt{ok}) = \{s_0, s_1, s_2, s_3, s_4\}$*;*
- $Sat(\neg\mathtt{error}) = S \setminus Sat(\mathtt{error}) = \{s_0, s_1, s_2, s_3, s_5\}$*, and*
- $Sat(\neg(\mathtt{ok} \vee \mathtt{error})) = Sat(\neg\mathtt{ok} \wedge \neg\mathtt{error}) = Sat(\neg\mathtt{ok}) \cap Sat(\neg\mathtt{error}) = \{s_0, s_1, s_2, s_3\}$*.*

5.2. Synthesizing the super-operators of path formulas

According to the semantics of path formulas ϕ in QCTL and the SOVM Δ defined on ϕ, we will show that $\Delta(\phi)$ is a countable (*possibly infinite*) sum of the SOVMs of disjoint cylinder sets. Then we reformulate $\Delta(\phi)$ using matrix representation to get an explicit (*surely finite*) form.

5.2.1. SOVM form

To characterize the disjointness of cylinder sets, we employ the tool of orthogonal projection on density operators. Let $\mathcal{P}_s$ denote the projection super-operator $\{|s\rangle\langle s|\} \otimes \mathcal{I} = \{|s\rangle\langle s| \otimes \mathbf{I}\}$ on the enlarged Hilbert space $\mathcal{H}_{\mathrm{cq}}$, and $\mathcal{P}_\Phi := \{\sum_{s\models\Phi} |s\rangle\langle s|\} \otimes \mathcal{I} = \{\sum_{s\models\Phi} |s\rangle\langle s| \otimes \mathbf{I}\}$. The split $\varrho = \mathcal{P}_\Phi(\varrho) + \mathcal{P}_{\neg\Phi}(\varrho)$ does not hold for a general density operator ϱ on $\mathcal{H}_{\mathrm{cq}}$, e. g. for $C = \mathrm{span}(\{|s\rangle, |t\rangle\})$,

$$\begin{aligned}\varrho &= |s\rangle\langle s| \otimes \rho_{s,s} + |s\rangle\langle t| \otimes \rho_{s,t} + |t\rangle\langle s| \otimes \rho_{t,s} + |t\rangle\langle t| \otimes \rho_{t,t} \\ &\neq |s\rangle\langle s| \otimes \rho_{s,s} + |t\rangle\langle t| \otimes \rho_{t,t} \\ &= \mathcal{P}_s(\varrho) + \mathcal{P}_t(\varrho),\end{aligned}$$

in which the quantum information $|s\rangle\langle t| \otimes \rho_{s,t} + |t\rangle\langle s| \otimes \rho_{t,s}$ is lost by projection. However, thanks to the mixed structure of the classical–quantum state $\varrho = \sum_{s\in S} |s\rangle\langle s| \otimes \rho_s$ posed on the QMC, we have the nice property

$$\varrho = \sum_{s\models\Phi} |s\rangle\langle s| \otimes \rho_s + \sum_{s\models\neg\Phi} |s\rangle\langle s| \otimes \rho_s = \mathcal{P}_\Phi(\varrho) + \mathcal{P}_{\neg\Phi}(\varrho). \tag{8}$$

Note that the super-operator $\mathcal{F} = \sum_{s,t\in S} \{|t\rangle\langle s|\} \otimes Q(s,t)$ defined in Section 3 keeps the mixed structure of the classical–quantum state, i. e., $\mathcal{F}(\varrho)$ is also of the mixed structure. Thus, the split using projection on classical system does not lose any quantum information, which is an important ingredient to build up disjoint cylinder sets over paths.

Fixing an initial classical state s, we have established the SOVM space over *Path*(s) in Section 3. The SOVMs of three kinds of path formulas — the next, the bounded-until and the unbounded-until formulas — are obtained as follows.

- Supposing that *Sat*(Φ) is known, we have

$$\Delta(\mathrm{X}\,\Phi) = \Delta\left(\biguplus_{t\models\Phi} \mathit{Cyl}(s\,t)\right) = \sum_{t\models\Phi} \Delta(s\,t) = \sum_{t\models\Phi} Q(s,t), \tag{9a}$$

  where $\uplus$ denotes disjoint union.

- Supposing that *Sat*(Φ_1) and *Sat*(Φ_2) are known, we have

$$\begin{aligned}\Delta(\Phi_1\mathrm{U}^{\le k}\Phi_2) &= \Delta\left(\biguplus_{i=0}^{k}\left\{\omega\in \mathit{Path}(s) : \omega(i)\models\Phi_2 \wedge \bigwedge_{j=0}^{i-1}\omega(j)\models\Phi_1\wedge\neg\Phi_2\right\}\right)\\ &= \sum_{i=0}^{k}\Delta\left(\left\{\omega\in \mathit{Path}(s) : \omega(i)\models\Phi_2 \wedge \bigwedge_{j=0}^{i-1}\omega(j)\models\Phi_1\wedge\neg\Phi_2\right\}\right)\\ &= \sum_{i=0}^{k}\mathrm{tr}_C(\mathcal{P}_{\Phi_2}\circ(\mathcal{F}\circ\mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i\circ\mathcal{P}_s),\end{aligned} \tag{9b}$$

  where tr_C is the partial trace that traces out the classical system C.

- Supposing that *Sat*(Φ_1) and *Sat*(Φ_2) are known, we have

$$\begin{aligned}\Delta(\Phi_1\mathrm{U}\,\Phi_2) &= \Delta\left(\biguplus_{i=0}^{\infty}\left\{\omega\in \mathit{Path}(s) : \omega(i)\models\Phi_2 \wedge \bigwedge_{j=0}^{i-1}\omega(j)\models\Phi_1\wedge\neg\Phi_2\right\}\right)\\ &= \sum_{i=0}^{\infty}\Delta\left(\left\{\omega\in \mathit{Path}(s) : \omega(i)\models\Phi_2 \wedge \bigwedge_{j=0}^{i-1}\omega(j)\models\Phi_1\wedge\neg\Phi_2\right\}\right)\\ &= \sum_{i=0}^{\infty}\mathrm{tr}_C(\mathcal{P}_{\Phi_2}\circ(\mathcal{F}\circ\mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i\circ\mathcal{P}_s).\end{aligned} \tag{9c}$$

For the latter two cases, we classify all satisfying paths ω upon the first timestamp i that satisfies $\omega(i) \models \Phi_2$ and $\omega(j) \models \Phi_1$ for each $j < i$ (or equivalently the unique timestamp i that satisfies $\omega(i) \models \Phi_2$ and $\omega(j) \models \Phi_1 \wedge \neg\Phi_2$ for each $j < i$). Thereby, the resulting sets $A_i = \{\omega \in \mathit{Path}(s) : \omega(i) \models \Phi_2 \wedge \bigwedge_{j=0}^{i-1} \omega(j) \models \Phi_1 \wedge \neg\Phi_2\}$ are pairwise disjoint, while their SOVMs are obtained as $\mathrm{tr}_C(\mathcal{P}_{\Phi_2} \circ (\mathcal{F} \circ \mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i \circ \mathcal{P}_s)$.

Example 5.2. *Under the SOVM space* (Ω, Σ, Δ) *with* $\Omega = \mathit{Path}(s_3)$ *established in Example 3.7, we consider the path formula* $\phi_1 = \mathtt{true}\,\mathrm{U}\,\mathtt{ok}$. *The satisfying path sets are pairwise disjoint* $A_i = \{\omega \in \Omega : \omega(i) \models \mathtt{ok} \wedge \bigwedge_{j=0}^{i-1} \omega(j) \models \neg\mathtt{ok}\}$ *(*$i \geq 0$*), and their SOVMs are:*

$$\begin{aligned}
\Delta(A_0) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ \mathcal{P}_{s_3}) = 0,\\
\Delta(A_1) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ (\mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}}) \circ \mathcal{P}_{s_3}) = 0,\\
\Delta(A_2) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ (\mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}})^2 \circ \mathcal{P}_{s_3}) = \{\tfrac{36\sqrt{2}}{125}\,|1,2\rangle\langle 1,2|\,, \tfrac{12}{25}\,|2\rangle\langle 2| \otimes \mathbf{Z}, \tfrac{12}{25}\,|2\rangle\langle 2| \otimes \mathbf{I}\},\\
\Delta(A_3) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ (\mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}})^3 \circ \mathcal{P}_{s_3}) = 0,\\
\Delta(A_4) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ (\mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}})^4 \circ \mathcal{P}_{s_3}) = \{\tfrac{576\sqrt{2}}{3125}\,|1,2\rangle\langle 1,2|\},\\
\Delta(A_5) &= \mathrm{tr}_C(\mathcal{P}_{\mathtt{ok}} \circ (\mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}})^5 \circ \mathcal{P}_{s_3}) = \{\tfrac{1728\sqrt{2}}{15625}\,|2,2\rangle\langle 1,2|\,, \tfrac{1296\sqrt{2}}{15625}\,|2,1\rangle\langle 1,2|\},
\end{aligned}$$

and so on.

5.2.2. Preparation for the matrix form

We have obtained the SOVMs (9) of the three kinds of path formulas. But the super-operators are not expressed in an explicit form, i. e., there are too many Kraus operators to make up the super-operators $\Delta(\phi)$. In particular, $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$ in (9c) is even not expressed in a closed form. We notice that super-operators are linear functions in its input, e. g. $\mathcal{E}(a\gamma_1 + b\gamma_2) = a\mathcal{E}(\gamma_1) + b\mathcal{E}(\gamma_2)$ for any $a, b \in \mathbb{C}$. It implies that super-operators could be represented in matrix form. In the next subsubsection, we will construct explicit matrix representations for these super-operators, particularly for $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$. Our approach has two steps:

1. using the non-explicit matrix representation of $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$, which is analogous to a geometric series with common ratio — the matrix representation of $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2} := \mathcal{F} \circ \mathcal{P}_{\Phi_1 \wedge \neg\Phi_2}$, since $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$ is calculated as an infinite sum in (9c);
2. reformulating it as an explicit matrix fraction.

However, $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$ may have some fixed-point γ (or equivalently the matrix representation of $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$ has eigenvalue 1), which makes the directly obtained matrix fraction divergent. To overcome the trouble, inspired by [10], we are to remove the bottom strongly connected component (BSCC) subspaces Γ that cover all fixed-points γ of $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$, i. e., $\mathrm{supp}(\gamma) \subseteq \Gamma$. Recall that:

Definition 5.3. *For a super-operator* $\mathcal{E} \in \mathcal{S}$*, a subspace* Γ *of* $\mathcal{H}$ *is* bottom *if for any pure state* $|\psi\rangle \in \Gamma$*, the support of* $\mathcal{E}(|\psi\rangle\langle\psi|)$ *is contained in* Γ*; it is* SCC *if for any pure states* $|\psi_1\rangle\,, |\psi_2\rangle \in \Gamma$*,* $|\psi_2\rangle$ *is in* $\mathrm{span}(\bigcup_{i=0}^{\infty} \mathrm{supp}(\mathcal{E}^i(|\psi_1\rangle\langle\psi_1|)))$*; it is* BSCC *if it is bottom and SCC.*

The bottom subspace means that any state $|\psi\rangle$ in Γ cannot leave Γ under the mapping of $\mathcal{E}$; the SCC means that any two states $|\psi_1\rangle\,, |\psi_2\rangle$ in Γ can reach each other with some positive probability; the BSCC means that any two states $|\psi_1\rangle\,, |\psi_2\rangle$ in Γ can reach each other almost surely.

We characterize the fixed-point of $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$ by the stationary equation

$$\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}(\gamma) = \gamma \qquad (\gamma = \gamma^\dagger \in \mathcal{L}_{\mathcal{H}_{\mathrm{cq}}}), \tag{10}$$

where γ are unknown variables and $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$ gives rise to coefficients. It is a system of homogeneous linear equations. Let γ_i ($i \in [m]$) be all linearly independent solutions of (10). Thanks to the property $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2} = \sum_{s \in S} \mathcal{P}_s \circ \mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$, the number of real variables in the Hermitian operator $\gamma = \sum_{s \in S} |s\rangle\langle s| \otimes \gamma_s$ on $\mathcal{H}_{\mathrm{cq}}$ are bounded by nd^2, as each Hermitian operator γ_s on $\mathcal{H}$ can be determined by d^2 real variables. So the number m of these linearly independent solutions is also bounded by the number nd^2 of real variables in γ. We proceed to find out the BSCC subspaces by the following lemma.

Lemma 5.4. *The direct-sum of all BSCC subspaces w. r. t.* $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ *is* $\mathrm{span}(\bigcup_{i\in[m]}\mathrm{supp}(\gamma_i))$.

Proof. We first prove $\Gamma := \mathrm{span}(\bigcup_{i\in[m]}\mathrm{supp}(\gamma_i))$ is the direct-sum of *some* BSCC subspaces that covers all fixed-point of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$, and then show it is the direct-sum of *all* BSCC subspaces.

Let $\gamma_i = \sum_{j\in[N]}\lambda_{i,j}|\Psi_{i,j}\rangle\langle\Psi_{i,j}|$ be the spectral decomposition of γ_i, where $\lambda_{i,j}\in\mathbb{R}$ ($j\in[N]$) are all eigenvalues of γ_i and $|\Psi_{i,j}\rangle$ are the corresponding eigenvectors. Define

$$\begin{aligned}\gamma_i^+ &:= \sum\{|\,\lambda_{i,j}|\Psi_{i,j}\rangle\langle\Psi_{i,j}| : j\in[N]\wedge\lambda_{i,j}>0\,|\}\\ \gamma_i^- &:= \sum\{|\,\lambda_{i,j}|\Psi_{i,j}\rangle\langle\Psi_{i,j}| : j\in[N]\wedge\lambda_{i,j}<0\,|\},\end{aligned}$$

where $\{|\cdot|\}$ denotes a multiset, as the positive and the negative parts of γ_i, respectively. Utilizing the fact that $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ is completely positive, the positive part of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i)$ is exactly $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i^+)$ while the negative part of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i)$ is $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i^-)$. Since $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i)=\gamma_i$, we have $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i^+)=\gamma_i^+$ and $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma_i^-)=\gamma_i^-$. So we can see that γ_i^+ and $-\gamma_i^-$ ($i\in[m]$) are positive solutions of (10) that together can linearly express any solution of (10).

For a fixed positive solution $\gamma=\sum_j\lambda_j|\Psi_j\rangle\langle\Psi_j|$ in the solution set $\{\gamma_i^+ : i\in[m]\}\cup\{-\gamma_i^- : i\in[m]\}\setminus\{0\}$, we have

$$\begin{aligned}\gamma-\lambda_j\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi_j\rangle\langle\Psi_j|) &= \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma)-\lambda_j\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi_j\rangle\langle\Psi_j|)\\ &= \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\gamma-\lambda_j|\Psi_j\rangle\langle\Psi_j|)\end{aligned}$$

is positive for each $|\Psi_j\rangle$ ($j\in[m]$), which implies $\mathrm{supp}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi_j\rangle\langle\Psi_j|))$ is contained in $\mathrm{supp}(\gamma)$ $=\mathrm{span}(\cup_j\{|\Psi_j\rangle\})$. In other words, for any Kraus operator $\mathbf{F}_\ell$ of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$, $\mathbf{F}_\ell|\Psi_j\rangle$ is in $\mathrm{supp}(\gamma)$, i. e., $(\sum_l|\Psi_l\rangle\langle\Psi_l|)\mathbf{F}_\ell|\Psi_j\rangle=\mathbf{F}_\ell|\Psi_j\rangle$. Furthermore, for any $|\Psi\rangle\in\mathrm{supp}(\gamma)$, after expressing it as $\sum_j c_j|\Psi_j\rangle$ with $\sum_{i\in[d]}|c_i|^2=1$, we have

$$\begin{aligned}\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi\rangle\langle\Psi|) &= \sum_\ell\mathbf{F}_\ell\left(\sum_j\sum_l c_jc_l^*|\Psi_j\rangle\langle\Psi_l|\right)\mathbf{F}_\ell^\dagger\\ &= \left(\sum_j|\Psi_j\rangle\langle\Psi_j|\right)\left[\sum_\ell\mathbf{F}_\ell\left(\sum_j\sum_l c_jc_l^*|\Psi_j\rangle\langle\Psi_l|\right)\mathbf{F}_\ell^\dagger\right]\left(\sum_j|\Psi_j\rangle\langle\Psi_j|\right)\\ &= \left(\sum_j|\Psi_j\rangle\langle\Psi_j|\right)\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi\rangle\langle\Psi|)\left(\sum_j|\Psi_j\rangle\langle\Psi_j|\right),\end{aligned}$$

which implies $\mathrm{supp}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(|\Psi\rangle\langle\Psi|))$ is contained in $\mathrm{supp}(\gamma)$. Thus $\mathrm{supp}(\gamma)$ is bottom w. r. t. $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$. Additionally, $\mathrm{span}(\bigcup_{k=0}^\infty\mathrm{supp}(\mathcal{F}^k(|\Psi_j\rangle\langle\Psi_j|)))$ forms a BSCC subspace w. r. t. $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$. Hence, $\mathrm{supp}(\gamma_i)$ is the direct-sum of some BSCC subspaces of $\mathcal{H}_{\mathrm{cq}}$, as well as Γ. The latter covers all fixed-points of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$, since any fixed-point of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ can be linearly expressed by $\{\gamma_i^+ : i\in[m]\}\cup\{-\gamma_i^- : i\in[m]\}$, whose supports are contained in Γ.

We proceed to prove that Γ is the direct-sum of all BSCC subspaces. By the decomposition [29, Theorem 5] and [17, Theorem 1], we have

$$\mathcal{H}_{\mathrm{cq}}=\mathcal{T}\oplus\bigoplus_i\Gamma_i,$$

where $\mathcal{T}$ is the maximal transient subspace w. r. t. $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ and each Γ_i is a BSCC subspace; although the decomposition is not unique, the maximal transient subspace $\mathcal{T}$ is unique as well as the direct-sum of all BSCC subspaces Γ_i. We assume by contradiction that Γ does not contain all BSCC subspaces. Then there is a BSCC subspace Γ_0 orthogonal to Γ. It is easy to see that

- the set $\mathcal{D}^1_{\Gamma_0}$ of density operators ϱ on Γ_0 with unit trace is a convex and compact set in the viewpoint of *probabilistic ensemble* form $\{(p_i, |\psi_i\rangle) : p_i > 0 \wedge i \in [d]\}$ that is obtained from the spectral decomposition $\varrho = \sum_{i\in[d]} p_i |\psi_i\rangle\langle\psi_i|$;
- $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ is a continuous function mapping $\mathcal{D}^1_{\Gamma_0}$ to itself.

By Brouwer's fixed-point theorem [21, Chapter 4] that for a continuous function f mapping a convex and compact set $\mathcal{X}$ to itself, there is a point $x \in \mathcal{X}$ such that $f(x) = x$, we know there is a fixed-point ϱ_0 of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ in $\mathcal{D}^1_{\Gamma_0}$. From the construction of Γ, however, we have $\mathrm{supp}(\varrho_0) \subseteq \Gamma$, which implies Γ_0 is not orthogonal to Γ and thus contradicts the assumption. Hence we obtain that Γ is exactly the direct-sum of all BSCC subspaces w. r. t. $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$. □

We describe the procedure of computing the direct-sum Γ of all BSCC subspaces w. r. t. $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ in Algorithm 1. By invoking it on the super-operator $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ and the Hilbert space $\mathcal{H}_{\mathrm{cq}}$, we would obtain the direct-sum Γ in $O(N^6)$ *arithmetic operations*, which is more efficient than the existing method [10, Procedure GetBSCC] in $O(N^7)$ *field* operations.[2]

Algorithm 1 Computing the direct-sum of all BSCC subspaces.

$$\Gamma \leftarrow \mathsf{BSCC}(\mathcal{E}, \mathcal{H})$$

Input: $\mathcal{E} \in \mathcal{S}$ is a super-operator on the Hilbert space $\mathcal{H}$ of dimension d.
Output: Γ is the direct-sum of all BSCC subspaces w. r. t. $\mathcal{E}$.

```
Γ ← {0};                                              ▷ initializing Γ as the null space
compute all linearly independent solutions $\gamma_i$ ($i \in [m]$) of $\mathcal{E}(\gamma) = \gamma$ ($\gamma = \gamma^\dagger \in \mathcal{L}_{\mathcal{H}}$);
for each $i \in [m]$ do
    $\Gamma \leftarrow \mathrm{span}(\Gamma \cup \mathrm{supp}(\gamma_i))$;
return $\Gamma$.
```

Complexity: $O(d^6)$.

Complexity of Algorithm 1. The stationary equation $\gamma = \mathcal{E}(\gamma)$ can be solved in $O(d^6)$ by Gaussian elimination, whose complexity is cubic in the number d^2 of real variables in γ. The support $\mathrm{supp}(\gamma_i)$ of an individual solution γ_i and the extended space $\mathrm{span}(\Gamma \cup \mathrm{supp}(\gamma_i))$ can be computed in $O(d^3)$ by the Gram–Schmidt procedure, whose complexity is cubic in the dimension d. Totally they are in $O(md^3) \subseteq O(d^5)$, as the number m of linearly independent solutions is bounded by d^2.

[2] In [10], the authors need to determine all individual BSCC subspaces, collect those individual BSCC subspaces of the desired parity, and thus check the ω-regular properties. To this end, [10, Procedure GetBSCC] first computes the direct-sum of BSCC subspaces corresponding to positive eigenvalues and the direct-sum of BSCC subspaces corresponding to negative eigenvalues. If those direct-sums consist of more than one BSCC subspace, the procedure would be respectively applied to the two direct-sums in a recursive manner. The overall complexity is $O(N^7)$. In our setting, it suffices to compute the direct-sum of all BSCC subspaces, which saves the recursion to complexity $O(N^6)$. Additionally, determining positive/negative eigenvalues is a typical kind of field operations beyond arithmetic ones (addition, subtraction, multiplication, and division). Obviously, the latters are of lower computational cost.

In the following, we will remove the direct-sum Γ of all BSCC subspaces using projection. Let $\mathcal{P}_\Gamma = \{\mathbf{P}_\Gamma\}$ where $\mathbf{P}_\Gamma$ is the projector onto Γ, i. e., $\mathbf{P}_\Gamma(\mathcal{H}_{\mathrm{cq}}) = \Gamma$; $\mathcal{P}_{\Gamma^\perp} = \{\mathbf{P}_{\Gamma^\perp}\}$ where $\Gamma^\perp$ is the orthogonal complement of Γ, i. e., $\Gamma \oplus \Gamma^\perp = \mathcal{H}_{\mathrm{cq}}$. Again, thanks to the fact that the IDs of the QMC are with the mixed structure $\varrho = \sum_{s\in S} |s\rangle\langle s| \otimes \rho_s$, we have that $\mathbf{P}_\Gamma$ is of the form $\sum_{s\in S} |s\rangle\langle s| \otimes \mathbf{P}_s$ where $\mathbf{P}_s$ $(s \in S)$ are positive operators, as well as $\mathbf{P}_{\Gamma^\perp} = \mathbf{I}_{\mathcal{H}_{\mathrm{cq}}} - \mathbf{P}_\Gamma$.

Example 5.5. *Consider the path formula $\phi_4 = \mathtt{true}\,\mathrm{U}^{\leq 15}(\mathtt{ok} \vee \mathtt{error})$ on the QMC $\mathfrak{C}_1$ in Example 3.2. The repeated super-operator in the SOVM $\Delta(\phi_4)$ is*

$$\begin{aligned}
&\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}} := \mathcal{F} \circ \mathcal{P}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}} = \mathcal{F} \circ \mathcal{P}_{\mathtt{true}\wedge\neg(\mathtt{ok}\vee\mathtt{error})} \\
&= \left\{ \begin{array}{l}
|s_1\rangle\langle s_0| \otimes |1,+\rangle\langle 1,1|\,,\ \tfrac{4}{5}\,|s_1\rangle\langle s_0| \otimes |1,-\rangle\langle 1,2|\,,\ \tfrac{3}{5}\,|s_5\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2|\,, \\
|s_5\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I},\ |s_0\rangle\langle s_1| \otimes |1,1\rangle\langle 1,+|\,,\ \tfrac{4}{5}\,|s_0\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|\,, \\
\tfrac{3}{5}\,|s_2\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|\,,\ |s_2\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I},\ \tfrac{12}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{I}, \\
\tfrac{9}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{X},\ \tfrac{16}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{I},\ \tfrac{12}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{X}, \\
\tfrac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{Z},\ \tfrac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{I},\ \tfrac{16}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{I},\ \tfrac{9}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{Z}
\end{array} \right\}.
\end{aligned}$$

By solving the stationary equation $\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}}(\gamma) = \gamma$ with $\gamma = \sum_{s\in S} |s\rangle\langle s| \otimes \gamma_s$ and $\gamma_s = \gamma_s^\dagger$, we obtain the unique solution $|s_0\rangle\langle s_0| \otimes |1,1\rangle\langle 1,1| + |s_1\rangle\langle s_1| \otimes |1,+\rangle\langle 1,+|$.

The BSCC subspaces Γ covering all the fixed-points of $\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}}$ is actually $\mathrm{span}(\{|s_0\rangle \otimes |1,1\rangle\,, |s_1\rangle \otimes |1,+\rangle\})$. *The projection super-operator $\mathcal{P}_\Gamma = \{\mathbf{P}_\Gamma\}$ onto Γ is given by the projector $\mathbf{P}_\Gamma = |s_0\rangle\langle s_0| \otimes |1,1\rangle\langle 1,1| + |s_1\rangle\langle s_1| \otimes |1,+\rangle\langle 1,+|$; the projection super-operator $\mathcal{P}_{\Gamma^\perp} = \{\mathbf{P}_{\Gamma^\perp}\}$ onto $\Gamma^\perp$ is given by $\mathbf{P}_{\Gamma^\perp} = \mathbf{I}_{\mathcal{H}_{\mathrm{cq}}} - \mathbf{P}_\Gamma$. Thereby, the composite super-operator $\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}} \circ \mathcal{P}_{\Gamma^\perp}$ would have no fixed-point. More computational details could be found in Appendix A.*

By the following lemma, we could see that the effect of $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$ is unchanged before and after removing all BSCC subspaces.

Lemma 5.6. *The identity $\mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^i = \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp})^i$ holds for each $i \geq 0$.*

Proof. We will prove it by induction on i. When $i = 0$, the identity follows trivially. Assume the identity holds for $i < k$. We proceed to show that it holds for $i = k$. Let $\mathcal{P}_\Gamma = \{\mathbf{P}_\Gamma\}$ and $\mathcal{P}_{\Gamma^\perp} = \{\mathbf{P}_{\Gamma^\perp}\}$. For any $|\Psi\rangle \in \mathcal{H}_{\mathrm{cq}}$, we have

$$\begin{aligned}
&\mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^k(|\Psi\rangle\langle\Psi|) \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^k[(\mathbf{P}_\Gamma + \mathbf{P}_{\Gamma^\perp})\,|\Psi\rangle\langle\Psi|\,(\mathbf{P}_\Gamma + \mathbf{P}_{\Gamma^\perp})] \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^k[\mathcal{P}_\Gamma(|\Psi\rangle\langle\Psi|) + \mathbf{P}_\Gamma\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_{\Gamma^\perp} + \mathbf{P}_{\Gamma^\perp}\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_\Gamma + \mathcal{P}_{\Gamma^\perp}(|\Psi\rangle\langle\Psi|)] \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^{k-1}[\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_\Gamma(|\Psi\rangle\langle\Psi|) + \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_\Gamma\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_{\Gamma^\perp}) + \\
&\qquad \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_{\Gamma^\perp}\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_\Gamma) + \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(|\Psi\rangle\langle\Psi|)] \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})^{k-1}[\mathcal{P}_\Gamma \circ \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_\Gamma(|\Psi\rangle\langle\Psi|) + \mathbf{P}_\Gamma\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_\Gamma\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_{\Gamma^\perp}) + \\
&\qquad \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_{\Gamma^\perp}\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_\Gamma)\mathbf{P}_\Gamma + \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(|\Psi\rangle\langle\Psi|)] \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp})^{k-1}(\mathcal{P}_\Gamma \circ \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_\Gamma(|\Psi\rangle\langle\Psi|) + \mathbf{P}_\Gamma\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_\Gamma\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_{\Gamma^\perp}) + \\
&\qquad \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(\mathbf{P}_{\Gamma^\perp}\,|\Psi\rangle\langle\Psi|\,\mathbf{P}_\Gamma)\mathbf{P}_\Gamma + \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(|\Psi\rangle\langle\Psi|)) \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp})^{k-1} \circ \mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(|\Psi\rangle\langle\Psi|) \\
&= \mathcal{P}_{\Phi_2} \circ (\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp})^k(|\Psi\rangle\langle\Psi|),
\end{aligned}$$

where the fourth equation follows from the facts:

- $\mathbf{P}_\Gamma \left|\Psi\right\rangle$ is in Γ, and
- letting $\mathbf{F}$ be a Kraus operator of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$, then $\mathbf{F}\mathbf{P}_\Gamma \left|\Psi\right\rangle$ is still in Γ;

the sixth equation follows from the facts:

- for $k > 1$, Γ is orthogonal to $\Gamma^\perp$, and
- for $k = 1$, letting $\mathcal{P}_{\Phi_1\wedge\neg\Phi_2} = \{\mathbf{P}_{\Phi_1\wedge\neg\Phi_2}\}$ and $\mathcal{P}_{\neg\Phi_2} = \{\mathbf{P}_{\neg\Phi_2}\}$, then $\Gamma \subseteq \mathbf{P}_{\Phi_1\wedge\neg\Phi_2}(\mathcal{H}_{\mathrm{cq}}) \subseteq \mathbf{P}_{\neg\Phi_2}(\mathcal{H}_{\mathrm{cq}})$ is orthogonal to $\mathbf{P}_{\Phi_2}(\mathcal{H}_{\mathrm{cq}})$.

5.2.3. Matrix form

Now we are going to represent $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$ using explicit matrices, which is based on the matrix representation of the super-operators on $\mathcal{H}$. Recall from [28, Definition 2.2] that, given a super-operator $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\}$ on $\mathcal{H}$, it has the matrix representation

$$\mathrm{S2M}(\mathcal{E}) := \sum_{\ell\in[m]} \mathbf{E}_\ell \otimes \mathbf{E}_\ell^*, \tag{11}$$

where $*$ denotes complex conjugate. Let

- $\mathrm{L2V}(\gamma) := \sum_{i,j\in[n]} \left\langle i\right| \gamma \left|j\right\rangle \left|i,j\right\rangle$ be the function that rearranges entries of the linear operator γ as a column vector;
- $\mathrm{V2L}(\mathbf{v}) := \sum_{i,j\in[n]} \left\langle i,j\right| \mathbf{v} \left|i\right\rangle\!\left\langle j\right|$ be the function that rearranges entries of the column vector $\mathbf{v}$ as a linear operator.

Here, S2M, L2V and V2L are pronounced “super-operator to matrix”, “linear operator to vector” and “vector to linear operator”, respectively. Then, we have the identities $\mathrm{V2L}(\mathrm{L2V}(\gamma)) = \gamma$, $\mathrm{L2V}(\mathcal{E}(\gamma)) = \mathrm{S2M}(\mathcal{E})\mathrm{L2V}(\gamma)$, and $\mathrm{S2M}(\mathcal{E}_2 \circ \mathcal{E}_1) = \mathrm{S2M}(\mathcal{E}_2)\mathrm{S2M}(\mathcal{E}_1)$. Therefore, all involved super-operator manipulations can be converted to matrix manipulations.

Next, we are to represent the super-operators on $\mathcal{H}_{\mathrm{cq}}$. Suppose that all classical states in S are ordered as $s_1 \prec \cdots \prec s_n$ where s_1 is the initial one, i. e., $\Omega = \mathit{Path}(s_1)$. We notice that for any classical-quantum state $\varrho = \sum_{i\in[n]} \left|s_i\right\rangle\!\left\langle s_i\right| \otimes \rho_i$ in $\mathcal{D}_{\mathcal{H}_{\mathrm{cq}}}$, $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(\varrho)$ and $\mathcal{P}_{\Phi_2}(\varrho)$ keep the mixed form $\sum_{i\in[n]} \left|s_i\right\rangle\!\left\langle s_i\right| \otimes \rho_i'$ for some $\rho_i' \in \mathcal{D}$. So, we can compressively define the matrix representation of the density operator ϱ on $\mathcal{H}_{\mathrm{cq}}$ as a column vector, consisting of n blocks as entries, in which the ith entry is the column vector $\mathrm{L2V}(\rho_i)$ for ρ_i, i. e., $\mathbb{M}_1 = \sum_{i\in[n]} \left|s_i\right\rangle \otimes \mathrm{L2V}(\rho_i)$.

After representing the density operator ϱ as a column vector of dimension nd^2, we proceed to represent the super-operator $\mathcal{F}$ as a square matrix adapted to that vector. Let $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} = \sum_{i,j\in[n]}\{\left|s_j\right\rangle\!\left\langle s_i\right|\}\otimes\mathcal{Q}(s_i, s_j) = \bigcup_{i,j\in[n]} \bigcup_\ell \{\left|s_j\right\rangle\!\left\langle s_i\right| \otimes \mathbf{Q}_{i,j,\ell}\}$ where $\mathbf{Q}_{i,j,\ell}$ are Kraus operators of $\mathcal{Q}(s_i, s_j)$ and $\mathcal{P}_{\Gamma^\perp} = \{\sum_{k\in[n]} \left|s_k\right\rangle\!\left\langle s_k\right| \otimes \mathbf{P}_k\}$. Then, $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}$ is

$$\bigcup_{i,j\in[n]} \bigcup_\ell \left\{ \sum_{k\in[n]} \left|s_j\right\rangle\!\left\langle s_i\right| \left|s_k\right\rangle\!\left\langle s_k\right| \otimes \mathbf{Q}_{i,j,\ell}\mathbf{P}_k \right\} = \bigcup_{i,j\in[n]} \bigcup_\ell \left\{ \left|s_j\right\rangle\!\left\langle s_i\right| \otimes \mathbf{Q}_{i,j,\ell}\mathbf{P}_i \right\}. \tag{12}$$

Using it, we further define:

- the matrix representation of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}$ as a square matrix, consisting of n^2 blocks as entries, in which the (j, i)-th entry is $\sum_\ell \mathbf{Q}_{i,j,\ell}\mathbf{P}_i \otimes \mathbf{Q}_{i,j,\ell}^*\mathbf{P}_i^*$, i. e.,

$$\mathbb{M}_2 = \sum_{i,j\in[n]} \sum_\ell \left|j\right\rangle\!\left\langle i\right| \otimes \mathbf{Q}_{i,j,\ell}\mathbf{P}_i \otimes \mathbf{Q}_{i,j,\ell}^*\mathbf{P}_i^*; \tag{13a}$$

- the matrix representation of the projection super-operator $\mathcal{P}_{\Phi_2}$ as a diagonal matrix, consisting of n blocks as diagonal entries, in which the ith entry is $\mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}$ if $s_i \models \Phi_2$ holds and 0 otherwise, i. e.,
$$\mathbb{M}_3 = \sum \{\mid |i\rangle\langle i| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}} : i \in [n] \wedge s_i \models \Phi_2 \mid\}, \tag{13b}$$
where $\{\mid \cdot \mid\}$ denotes a multiset.

All these matrix representations have been obtained by extending (11) on $\mathcal{H}$ to the enlarged $\mathcal{H}_{\mathrm{cq}}$.

Lemma 5.7. *The matrix* $\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2$ *is invertible.*

Proof. It suffices to show $\mathbb{M}_2$ has no eigenvalue 1. We assume by contradiction that there is an eigenvector $\mathbf{v}$ of $\mathbb{M}_2$ associated with eigenvalue 1. That is, $\mathbb{M}_2\mathbf{v} = \mathbf{v} \neq 0$. Then,
$$\gamma = \sum_{i\in[n]} |s_i\rangle\langle s_i| \otimes \mathrm{V2L}((\langle i| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbf{v})$$
is a linear operator on $\mathcal{H}_{\mathrm{cq}}$, satisfying $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(\gamma) = \gamma \neq 0$, while $\gamma_0 = \gamma + \gamma^\dagger$ also a linear operator on $\mathcal{H}_{\mathrm{cq}}$, satisfying $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(\gamma_0) = \gamma_0 \neq 0$. By the definition of Γ, we have $\mathrm{supp}(\gamma_0) \subseteq \Gamma$, and thus $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_{\Gamma^\perp}(\gamma_0) = \mathcal{F}_{\Phi_1\wedge\neg\Phi_2}(0) = 0 \neq \gamma_0$, which contradicts the assumption. □

Theorem 5.8 (Matrix representation). *Let* $\mathbb{M}_2$ *and* $\mathbb{M}_3$ *be the matrices as defined in* (13). *Then it is in polynomial time to obtain:*

1. *the explicit matrix representation of the super-operator* $\Delta(\mathrm{X}\,\Phi)$ *as* $\sum_{s\models\Phi} \mathrm{S2M}(Q(s_1, s))$,
2. *the explicit matrix representation of* $\Delta(\Phi_1 \mathrm{U}^{\leq k} \Phi_2)$ *as*
$$\sum_{i\in[n]} (\langle i| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2^{k+1})(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}(|s_1\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}),$$
3. *the explicit matrix representation of* $\Delta(\Phi_1 \mathrm{U}\, \Phi_2)$ *as*
$$\sum_{i\in[n]} (\langle i| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}(|s_1\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}).$$

Proof. The matrix representations directly follow from the semantics of the next formula $\mathrm{X}\,\Phi$, the bounded-until formula $\Phi_1 \mathrm{U}^{\leq k} \Phi_2$, and the unbounded-until formula $\Phi_1 \mathrm{U}\, \Phi_2$. For complexity, we will analyze them in turn.

1. It is a sum of at most nd^2 matrix tensor products, each costs $O(d^4)$. In total, it is in $O(nd^6) \subseteq O(N^6)$.
2. The matrix $\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2$ is of dimension nd^2. Computing its inverse costs $O(n^3d^6)$. The matrix power $\mathbb{M}_2^{k+1}$ amounts to
$$\mathbb{M}_2^{b_0\cdot 2^0}\mathbb{M}_2^{b_1\cdot 2^1}\cdots\mathbb{M}_2^{b_l\cdot 2^l},$$
where $(b_l, \dots, b_1, b_0)$ is the binary code of the positive integer $k+1$ with $l = \lceil \log_2(k+2) \rceil - 1$, i. e., $k + 1 = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \cdots + b_l \cdot 2^l$ with $b_j \in \{0, 1\}$. Computing $\mathbb{M}_2^{k+1}$ requires sequentially computing all the factors $\mathbb{M}_2^{2^j}$ ($j \in [l]$), each of which costs $O(n^3d^6)$; then computing the product of those factors corresponding to $b_j = 1$ costs $O(n^3d^6 \log_2(k))$. Other operations are merely a few matrix-vector multiplications over an nd^2-dimensional vector space, which costs $O(n^2d^4)$. Totally, it is in $O(n^3d^6 \log_2(k)) \subseteq O(N^6 \log_2(k))$.

3. It is clearly in $O(N^6)$ by the previous analysis.

As a result, the complexity is polynomial time w. r. t. $N = nd$ (reflected in the size of $\mathfrak{C}$) and linear time w. r. t. $\log_2(k)$ (reflected in the size of ϕ). □

Example 5.9. *Consider the two path formulas*

$$\phi_3 = \texttt{true}\,\mathrm{U}\,(\texttt{ok} \vee \texttt{error}) \qquad \text{and} \qquad \phi_4 = \texttt{true}\,\mathrm{U}^{\leq 15}(\texttt{ok} \vee \texttt{error})$$

on the QMC $\mathfrak{C}_1$ shown in Example 3.2. For ϕ_4, the repeated super-operator $\mathcal{F}_{\neg\texttt{ok}\wedge\neg\texttt{error}}$ and the projector $\mathbf{P}_\Gamma$ whose support covers all its fixed-points have been computed in Example 5.5. Then the matrix representations are calculated as

$$\begin{aligned}
\mathbb{M}_1 = {} & |s_3\rangle\langle s_3| \otimes \mathrm{L2V}(\rho_3), \\
\mathbb{M}_2 = {} & \tfrac{16}{25}\, |s_1\rangle\langle s_0| \otimes |1,-\rangle\langle 1,2| \otimes |1,-\rangle\langle 1,2| + \tfrac{9}{25}\, |s_5\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2| \otimes |1,2\rangle\langle 1,2| + \\
& |s_5\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I} \otimes |2\rangle\langle 2| \otimes \mathbf{I} + \tfrac{16}{25}\, |s_0\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-| \otimes |1,2\rangle\langle 1,-| + \\
& \tfrac{9}{25}\, |s_2\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-| \otimes |1,2\rangle\langle 1,-| + |s_2\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I} \otimes |2\rangle\langle 2| \otimes \mathbf{I} + \\
& \tfrac{144}{625}\, |s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} + \tfrac{81}{625}\, |s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X} + \tfrac{256}{625}\, |s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} + \\
& \tfrac{144}{625}\, |s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} + \tfrac{144}{625}\, |s_0\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} + \tfrac{144}{625}\, |s_0\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I} + \\
& \tfrac{256}{625}\, |s_4\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} + \tfrac{81}{625}\, |s_4\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z}, \\
\mathbb{M}_3 = {} & |s_4\rangle\langle s_4| \otimes \mathbf{I} \otimes \mathbf{I} + |s_5\rangle\langle s_5| \otimes \mathbf{I} \otimes \mathbf{I},
\end{aligned}$$

in which all eigenvalues of $\mathbb{M}_2$ are $\pm\frac{8}{125}\sqrt{50 + 2\sqrt{1273}}$, $\pm\frac{8\mathrm{i}}{125}\sqrt{50 + 2\sqrt{1273}}$ and 0 of multiplicity 92. Since $\mathbb{M}_2$ has no eigenvalue 1, the matrix inverse $(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}$ is well-defined as expected. Finally the explicit matrix representation of $\Delta(\phi_3)$ and $\Delta(\phi_4)$ are obtained as

$$\begin{aligned}
\mathrm{S2M}(\Delta(\phi_3)) &= \sum_{s\in S} (\langle s| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}(|s_3\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}), \\
\mathrm{S2M}(\Delta(\phi_4)) &= \sum_{s\in S} (\langle s| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2^{16})(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}(|s_3\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}).
\end{aligned}$$

More computational details could be found in Appendix A.

5.3. Deciding the fidelity-quantifier formula

In the previous subsection, we have constructed an explicit matrix representation $\mathbb{M} := \mathrm{S2M}(\mathcal{E})$ for $\mathcal{E} = \Delta(\phi)$ where ϕ is the path formula in the fidelity-quantifier formula $\mathfrak{F}_{\sim\tau}(\phi)$. Now we present an algebraic approach to compare the minimum fidelity $\underline{\mathrm{Fid}}(\mathcal{E})$ with the threshold τ, so that $s \models \mathfrak{F}_{\sim\tau}(\phi)$ can be decided.

To facilitate our analysis, we first do the simplification:

- $s \models \mathfrak{F}_{\leq\tau}(\phi)$ amounts to the quantified constraint

$$\begin{aligned}
\zeta_1 &\equiv \exists\, |\psi\rangle \in \mathcal{H} : [\mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \leq \tau \wedge \forall\, |\varphi\rangle \in \mathcal{H} : \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \leq \mathrm{Fid}(\mathcal{E}, |\varphi\rangle\langle\varphi|)] \\
&\equiv \exists\, |\psi\rangle \in \mathcal{H} : \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \leq \tau; \qquad (14a)
\end{aligned}$$

- $s \models \mathfrak{F}_{\geq\tau}(\phi)$ amounts to the quantified constraint

$$\begin{aligned}\zeta_2 \equiv{}& \exists\, |\psi\rangle \in \mathcal{H} : [\mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \geq \tau \wedge \forall\, |\varphi\rangle \in \mathcal{H} : \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \leq \mathrm{Fid}(\mathcal{E}, |\varphi\rangle\langle\varphi|)] \\ \equiv{}& \forall\, |\psi\rangle \in \mathcal{H} : \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \geq \tau; \qquad (14b)\end{aligned}$$

- other comparison operators $=, <, >$ and $\neq$ can be easily derived by logic connectives as
  - $s \models \mathfrak{F}_{=\tau}(\phi)$ amounts to $\zeta_1 \wedge \zeta_2$;
  - $s \models \mathfrak{F}_{<\tau}(\phi)$ amounts to $\neg\zeta_2$;
  - $s \models \mathfrak{F}_{>\tau}(\phi)$ amounts to $\neg\zeta_1$;
  - $s \models \mathfrak{F}_{\neq\tau}(\phi)$ amounts to $\neg\zeta_1 \vee \neg\zeta_2$.

Suppose all entries in the Kraus operators $\mathbf{E}$ of $\mathcal{E}$ are algebraic numbers for the consideration of computability. Recall that:

Definition 5.10. *A number λ is* algebraic*, denoted by $\lambda \in \mathbb{A}$, if there is a nonzero $\mathbb{Q}$-polynomial $f(z)$ of least degree, satisfying $f(\lambda) = 0$. Such a polynomial $f(z)$ is called the* minimal polynomial *f_λ of λ.*

Clearly, algebraic numbers widely occur in quantum information, such as the irrational number $1/\sqrt{2}$ appearing in the definition of the most common quantum state $|\pm\rangle = (|1\rangle \pm |2\rangle)/\sqrt{2}$. We will formulate the constraints (14) as $\mathbb{Q}$-polynomial (polynomial with rational coefficients) formulas in the decidable theory — real closed fields [26]:

Definition 5.11. *The theory of* real closed fields *is a first-order theory $Th(\mathbb{R}; +, \cdot; =, >; 0, 1)$, in which*

- *the domain is $\mathbb{R}$,*
- *the functions are addition '$+$' and multiplication '$\cdot$',*
- *the predicates are equality '$=$' and order '$>$', and*
- *the constants are 0 and 1.*

Roughly speaking, the elements in $Th(\mathbb{R}; +, \cdot; =, >; 0, 1)$ are $\mathbb{Q}$-polynomial formulas that are composed from polynomial equations and inequalities (as atomic formulas), using logic connectives '$\neg$', '$\wedge$', '$\vee$', '$\rightarrow$', '$\leftrightarrow$' and quantifiers '$\forall$', '$\exists$'.

The constraints (14) are the *sentences* — the formulas whose variables $|\psi\rangle$ are all (existentially or universally) quantified, i. e., no free variable. We will encode them as $\mathbb{A}$-polynomial formulas, and further encode them as $\mathbb{Q}$-polynomial formulas.

Since $|\psi\rangle\langle\psi|$ is pure, we predefine $|\psi\rangle = \sum_{i\in[d]} x_i\, |i\rangle$ where x_i ($i \in [d]$) are complex parameters, subject to $\sum_{i\in[d]} x_i x_i^* = 1$. Under the purity, we have

$$\begin{aligned}\mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \leq \tau \;\equiv\;& \langle\psi|\, \mathcal{E}(|\psi\rangle\langle\psi|)\, |\psi\rangle \leq \tau^2 \\ \equiv\;& \left(\sum_{i\in[d]} x_i^*\, \langle i|\right) \mathcal{E}\left(\sum_{i,j\in[d]} x_i x_j^*\, |i\rangle\langle j|\right) \left(\sum_{j\in[d]} x_j\, |j\rangle\right) \leq \tau^2 \\ \equiv\;& \left(\sum_{i,j\in[d]} x_i^* x_j\, \langle i, j|\right) \mathbb{M} \left(\sum_{i,j\in[d]} x_i x_j^*\, |i, j\rangle\right) \leq \tau^2, \qquad (15)\end{aligned}$$

which results in an $\mathbb{A}$-polynomial formula. Denote all parameters introduced here by $\mathbf{x} = (x_i)_{i\in[d]}$. Further, we encode the constraint (14a) as

$$\zeta_1 \equiv \exists\,\mathbf{x} : \left[\sum_{i\in[d]} x_i x_i^* = 1 \wedge \left(\sum_{i,j\in[d]} x_i^* x_j \langle i,j|\right) \mathbb{M} \left(\sum_{i,j\in[d]} x_i x_j^* |i,j\rangle\right) \leq \tau^2\right], \tag{16a}$$

which is the desired $\mathbb{A}$-polynomial formula, involving at most

- $2d$ real variables (converted from d complex variables $\mathbf{x}$) for expressing $|\psi\rangle$,
- one quadratic equation for the purity, and
- one quartic inequality for the comparison.

Similarly, the $\mathbb{A}$-polynomial formula for encoding the constraint (14b) is

$$\zeta_2 \equiv \forall\,\mathbf{x} : \left[\sum_{i\in[d]} x_i x_i^* = 1 \rightarrow \left(\sum_{i,j\in[d]} x_i^* x_j \langle i,j|\right) \mathbb{M} \left(\sum_{i,j\in[d]} x_i x_j^* |i,j\rangle\right) \geq \tau^2\right]. \tag{16b}$$

Suppose the input $\mathcal{E}$ involves real algebraic numbers $\Lambda = \{\lambda_j : j \in [e]\}$. Then the $\mathbb{A}$-polynomial formulas (16) are named by $\zeta_1(\Lambda)$ and $\zeta_2(\Lambda)$, respectively. To effectively deal with them, we resort to the standard encoding of real algebraic number λ that uses minimal polynomial f_λ plus isolation interval I_λ, which is given by linear inequalities, like $z \in I_\lambda \equiv L < z < U$ for some rational endpoints L and U of I_λ, to distinguish λ from other real roots of f_λ. In such a way, to encode each real algebraic number λ, we introduce at most

- one real variable z,
- one equation $f_\lambda = 0$ of degree $\deg(f_\lambda)$, and
- two linear inequalities $z > L$ and $z < U$ from the isolation interval I_λ of λ.

For instance, the aforementioned algebraic number $1/\sqrt{2}$ occurring in $|\pm\rangle$ can be encoded as the unique solution to $z^2 = \frac{1}{2} \wedge 0 < z < 1$.

The $\mathbb{A}$-polynomial formulas $\zeta_1(\Lambda)$ and $\zeta_2(\Lambda)$ can be rewritten as the $\mathbb{Q}$-polynomial ones:

$$\zeta_1(\Lambda) \equiv \exists\,\mathbf{z} : \left[\bigwedge_{j\in[e]} (f_{\lambda_j}(z_j) = 0 \wedge z_j \in I_{\lambda_j}) \wedge \zeta_1(\mathbf{z})\right] \tag{17a}$$

$$\zeta_2(\Lambda) \equiv \forall\,\mathbf{z} : \left[\bigwedge_{j\in[e]} (f_{\lambda_j}(z_j) = 0 \wedge z_j \in I_{\lambda_j}) \rightarrow \zeta_2(\mathbf{z})\right], \tag{17b}$$

where $\mathbf{z} = (z_j)_{j\in[e]}$ are real variables introduced to symbolize Λ. Note that the existential quantifier $\exists\,\mathbf{z}$ and the universal quantifier $\forall\,\mathbf{z}$ can be mutually converted here, since for each $j \in [e]$, the solution (i. e., λ_j) to the subformula $f_{\lambda_j}(z_j) = 0 \wedge z_j \in I_{\lambda_j}$ uniquely exists by the standard encoding of λ_j.

Finally, applying the existential theory of the reals [4, Theorem 13.13], we obtain:

Theorem 5.12 (Decidability). *It is in exponential time to decide the fidelity-quantifier formula $\mathfrak{F}_{\sim\tau}(\phi)$.*

Proof. It suffices to show that the formulating subprocedure is in polynomial time, and that the deciding subprocedure is in exponential time.

The encoding on the purity is plainly in $O(d)$. Encoding the left hand side of the comparison (e. g. the formula (15)) involves a few matrix-vector multiplications over a d^2-dimensional vector space, which costs $O(d^4)$. Thus encoding the polynomial formulas (17) is in $O(d^4)$, which means that the formulating subprocedure is in polynomial time.

Then we analyze the deciding subprocedure, which invokes the following Algorithm 2 on the formulas (17). Technically, the formulas (17) have

- a block of $2d+e$ real variables $\mathbf{x}$ and $\mathbf{z}$ quantified all by '$\exists$' for (17a) or all by '$\forall$' for (17b),
- at most $C = 2 + 3e$ distinct polynomials of degree at most $D = \max(4, \max_{j\in[e]} \deg(f_{\lambda_j}))$.

Thereby, the complexity is in $C^{2d+e+1}D^{O(2d+e)}$, an exponential hierarchy. □

Algorithm 2 Existential Theory of the Reals [4, Theorem 13.13].

$$\texttt{true/false} \leftarrow \mathsf{QE}(\mathrm{Q}\,\mathbf{x} : F(\mathbf{x}))$$

Input: $\mathrm{Q}\,\mathbf{x} : F(\mathbf{x})$ is a quantified polynomial formula, in which

- $\mathbf{x}$ is a block of k real variables, which is quantified by $\mathrm{Q} \in \{\forall, \exists\}$,
- each atomic formula in F is in the form $p \sim 0$ where $\sim \in \{<, \leq, =, \geq, >, \neq\}$,
- all distinct polynomials p, regardless of a constant factor, extracted from those atomic formulas $p \sim 0$ form a polynomial collection $\mathbb{P}$,
- C is the cardinality of $\mathbb{P}$, and
- D is the maximum degree of the polynomials in $\mathbb{P}$.

Output: `true/false` is the truth of $\mathrm{Q}\,\mathbf{x} : F(\mathbf{x})$.
Complexity: $C^{k+1}D^{O(k)}$.

There are many packages that have implemented Algorithm 2, such as Reduce (a.k.a. Redlog [9]) and Z3 [7].

Example 5.13. *We reconsider the path formulas ϕ_3 and ϕ_4 in Example 5.9. For the bounded-until formula $\phi_4 = \texttt{true}\,\mathrm{U}^{\leq 15}(\texttt{ok} \vee \texttt{error})$, the explicit matrix representation $\mathbb{M}$ of $\Delta(\phi_4)$ has been obtained. Now we are to decide the fidelity-quantifier formula $\mathfrak{F}_{\leq\tau}(\phi_4)$.*

After introducing the real variables $\boldsymbol{\mu} = \mathfrak{R}(\mathbf{x})$ and $\boldsymbol{\nu} = \mathfrak{I}(\mathbf{x})$ where $\mathbf{x} = (x_i)_{i\in[4]}$ encodes the pure state $|\psi\rangle\langle\psi|$, we have the desired polynomial formula

$$\exists\{\boldsymbol{\mu}, \boldsymbol{\nu}\} : [||\boldsymbol{\mu}|| + ||\boldsymbol{\nu}|| = 1 \wedge h(\boldsymbol{\mu}, \boldsymbol{\nu}) \leq \tau^2],$$

where $||\boldsymbol{\mu}|| + ||\boldsymbol{\nu}|| = 1$ encodes the purity and $h(\boldsymbol{\mu}, \boldsymbol{\nu}) \leq \tau^2$ encodes the comparison. The detailed expressions could be found in Appendix A.

Using Reduce [9], the fidelity-quantifier formula $\mathfrak{F}_{\leq 3351/5000}(\phi_4)$ is decided to be true while $\mathfrak{F}_{\leq 67/100}(\phi_4)$ is false. In other words, $\underline{\mathrm{Fid}}(\Delta(\phi_4))$ is in $(\frac{67}{100}, \frac{3351}{5000}]$, which entails that nearly 67% of the original quantum information at s_3 would be delivered at the terminal s_4 or s_5 within 15 steps through the noisy channel $\mathfrak{C}_1$.

path formula	fidelity-quantifier formula	decision	minimum fidelity
$\phi_3 = \texttt{true}\,\mathrm{U}\,(\texttt{ok} \vee \texttt{error})$	$\mathfrak{F}_{\leq 3351/5000}(\phi_3)$ $\mathfrak{F}_{\leq 6703/10000}(\phi_3)$	false true	$(\frac{3351}{5000}, \frac{6703}{10000}]$
$\phi_4 = \texttt{true}\,\mathrm{U}^{\leq 15}(\texttt{ok} \vee \texttt{error})$	$\mathfrak{F}_{\leq 67/100}(\phi_4)$ $\mathfrak{F}_{\leq 3351/5000}(\phi_4)$	false true	$(\frac{67}{100}, \frac{3351}{5000}]$

Table 1: Results on deciding the fidelity-quantifier formulas

Similarly, for the unbounded-until formula $\phi_3 = \texttt{true}\,\mathrm{U}\,(\texttt{ok} \vee \texttt{error})$*, we have that both* $\mathfrak{F}_{>3351/5000}(\phi_3)$ *and* $\mathfrak{F}_{\leq 6703/10000}(\phi_3)$ *hold, as the above bounded-until formula approaches the unbounded-until one. All the experimental results are summarized in Table 1.*

Remark 5.14. *When the initial density operator* ρ *is given and all the entries in the Kraus operators of* $Q(s,t)$ *with* $s, t \in S$ *are rational, it would be in polynomial time to decide* $(s,\rho) \models \mathfrak{F}_{\sim\tau}(\phi)$*, since the time-consuming quantifier elimination is saved then. It is consistent with the existing work [28].*

Implementation. We have implemented the presented method in Wolfram language on the platform Mathematica, incorporated with the built-in tool Reduce [9]. We provide all the function prototypes of the proposed methods for deciding the fidelity-quantifier formulas, and package them into user-friendly interfaces for users to call in the Wolfram file Functions.nb. The core functions are delivered as follows:

- `QMCinitialize` constructs and initializes QMC model with given information;
- `ComputeBSCC` computes the direct-sum of all BSCC subspaces w. r. t. a specified super-operator;
- `NextSOVM`, `BuntilSOVM` and `UBuntilSOVM` synthesize the super-operator of three kinds of path formulas respectively and return the corresponding matrix representation;
- `DecideFidQuantifierFormu` decides the truth of fidelity-quantifier formulas over a QMC with parametric initial quantum state for a given threshold.

Thus we can for instance ensure good interactivity after inputting the data for QMC model that compiles with the specification. Under a PC with Intel Core i7-6700 CPU and 8 GB RAM, the overall performance of our running examples is acceptable and the detailed performance when deciding the fidelity-quantifier formulas corresponding to four instances in Example 5.13 is shown in Table 2. Finally, we have to address that the fidelity computation for the QMC with a *concrete* initial quantum state is always much efficient (usually within 1 second); while the fidelity computation for the QMC with a *parametric* initial quantum state may be inefficient, since in the worst case the quantifier elimination is exponential-time. We carry on the running examples in the paper in file Example-BasicInfo.nb. The source code of the implementation and more guidance for users are available at: `https://github.com/melonysuga/PaperFidelityExamples-.git`.

path formula	fidelity-quantifier formula	memory (MB)	time (s)
$\phi_3 = \mathtt{true}\,\mathrm{U}\,(\mathtt{ok} \vee \mathtt{error})$	$\mathfrak{F}_{\leq 3351/5000}(\phi_3)$	76.60	1.66
	$\mathfrak{F}_{\leq 6703/10000}(\phi_3)$	76.61	1.59
$\phi_4 = \mathtt{true}\,\mathrm{U}^{\leq 15}(\mathtt{ok} \vee \mathtt{error})$	$\mathfrak{F}_{\leq 67/100}(\phi_4)$	127.68	2.78
	$\mathfrak{F}_{\leq 3351/5000}(\phi_4)$	120.428	2.25

Table 2: Performance on deciding the fidelity-quantifier formulas

6. Conclusion

In this paper, we introduced a quantum extension of computation tree logic (QCTL), which consisted of state formulas and path formulas. A model checking algorithm was presented over the quantum Markov chains (QMCs). We gave a simple polynomial time procedure that could remove all fixed-points w. r. t. a super-operator. Then we synthesized the super-operators of path formulas using explicit matrix representation, and decided the fidelity-quantifier formulas by a reduction to quantifier elimination in the existential theory of the reals. Finally, model checking QCTL formulas against QMCs were shown to be decidable in exponential time.

We believe that the proposed method could be extended to:

- synthesize the SOVM for the multiphase until formula $\Phi_1 \mathrm{U}^{\mathbb{I}_1} \Phi_2 \mathrm{U}^{\mathbb{I}_2} \cdots \Phi_{k-1} \mathrm{U}^{\mathbb{I}_{k-1}} \Phi_k$ with proper time intervals $\mathbb{I}_i$ that cannot be expressed by any nested binary until formula, like $\Phi_1 \mathrm{U}^{\mathbb{I}_1} (\Phi_2 \mathrm{U}^{\mathbb{I}_2} \cdots (\Phi_{k-1} \mathrm{U}^{\mathbb{I}_{k-1}} \Phi_k) \cdots)$, since all the time intervals $\mathbb{I}_i$ in a multiphase until formula are measured from the start of the path while all time intervals $\mathbb{I}_i$ in a nested binary until formula are measured from the immediately prior transition points (please refer to [27] for more details);

- synthesize the SOVM for the conjunction $\phi_1 \wedge \phi_2$, so that the conditional fidelity, similar to conditional probability [1, 13], could be established;

- synthesize the SOVM for the negation $\neg\phi$, so that the safety property $\Box\,\Phi = \neg(\mathtt{true}\,\mathrm{U}\,\neg\Phi)$ could be analyzed;

- decide the analogy of SOVM-quantifier formula over parametric QMCs. The positive-operator valued measure (POVM) would be a key tool to attack it.

Acknowledgements

The authors are grateful to the anonymous reviewer whose careful and insightful comments significantly improve the presentation and resolve inconsistencies. This work is supported by the National Natural Science Foundation of China (Nos. 11871221, 61832015, and 62072176), the National Key R&D Program of China (No. 2018YFA0306704), the Fundamental Research Funds for the Central Universities (No. 2021JQRH014), the Research Funds of Happiness Flower ECNU (No. 2020ECNU-XFZH005), and the Inria-CAS joint project Quasar.

Appendix A. Some Computational Details

In Example 5.5, we have computed the projection $\mathbf{P}_\Gamma$ of the subspace Γ covering all fixed-points of $\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}}$, and thus we get

$$\begin{aligned}
\mathbf{P}_{\Gamma^\perp} &= \mathbf{I}_{\mathcal{H}_{\mathrm{cq}}} - \mathbf{P}_\Gamma \\
&= (|s_0\rangle\langle s_0| + |s_1\rangle\langle s_1| + |s_2\rangle\langle s_2| + |s_3\rangle\langle s_3| + |s_4\rangle\langle s_4| + |s_5\rangle\langle s_5|) \otimes \mathbf{I} \otimes \mathbf{I} - \\
&\quad (|s_0\rangle\langle s_0| \otimes |1,1\rangle\langle 1,1| + |s_1\rangle\langle s_1| \otimes |1,+\rangle\langle 1,+|) \\
&= |s_0\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2| + |s_0\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I} + |s_1\rangle\langle s_1| \otimes |1,-\rangle\langle 1,-| + |s_1\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I} + \\
&\quad (|s_2\rangle\langle s_2| + |s_3\rangle\langle s_3| + |s_4\rangle\langle s_4| + |s_5\rangle\langle s_5|) \otimes \mathbf{I} \otimes \mathbf{I}.
\end{aligned}$$

Applying the rule that the composition $\mathcal{E}_2 \circ \mathcal{E}_1$ is given by $\{\mathbf{E}_{2,\ell_2}\mathbf{E}_{1,\ell_1} : \ell_1 \in [m_1] \wedge \ell_2 \in [m_2]\}$, we calculate the Kraus representation of the super-operator $\mathcal{F}_{\neg\mathtt{ok}\wedge\neg\mathtt{error}} \circ \mathcal{P}_{\Gamma^\perp}$ as

$$\begin{aligned}
&\left\{\begin{array}{l}
|s_1\rangle\langle s_0| \otimes |1,+\rangle\langle 1,1|,\ \frac{4}{5}\,|s_1\rangle\langle s_0| \otimes |1,-\rangle\langle 1,2|,\ \frac{3}{5}\,|s_5\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2|, \\
|s_5\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I},\ |s_0\rangle\langle s_1| \otimes |1,1\rangle\langle 1,+|,\ \frac{4}{5}\,|s_0\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|, \\
\frac{3}{5}\,|s_2\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|,\ |s_2\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I},\ \frac{12}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{I}, \\
\frac{9}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{X},\ \frac{16}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{I},\ \frac{12}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{X}, \\
\frac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{Z},\ \frac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{I},\ \frac{16}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{I},\ \frac{9}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{Z}
\end{array}\right\} \circ \\
&\left\{\begin{array}{l}
|s_0\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2| + |s_0\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I} + |s_1\rangle\langle s_1| \otimes |1,-\rangle\langle 1,-| + |s_1\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I} \\
+ |s_2\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{I} + |s_3\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{I} + |s_4\rangle\langle s_4| \otimes \mathbf{I} \otimes \mathbf{I} + |s_5\rangle\langle s_5| \otimes \mathbf{I} \otimes \mathbf{I}
\end{array}\right\} \\
= &\left\{\begin{array}{l}
\frac{4}{5}\,|s_1\rangle\langle s_0| \otimes |1,-\rangle\langle 1,2|,\ \frac{3}{5}\,|s_5\rangle\langle s_0| \otimes |1,2\rangle\langle 1,2|,\ |s_5\rangle\langle s_0| \otimes |2\rangle\langle 2| \otimes \mathbf{I}, \\
\frac{4}{5}\,|s_0\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|,\ \frac{3}{5}\,|s_2\rangle\langle s_1| \otimes |1,2\rangle\langle 1,-|,\ |s_2\rangle\langle s_1| \otimes |2\rangle\langle 2| \otimes \mathbf{I}, \\
\frac{12}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{I},\ \frac{9}{25}\,|s_0\rangle\langle s_2| \otimes \mathbf{X} \otimes \mathbf{X},\ \frac{16}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{I}, \\
\frac{12}{25}\,|s_3\rangle\langle s_2| \otimes \mathbf{I} \otimes \mathbf{X},\ \frac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{Z},\ \frac{12}{25}\,|s_0\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{I}, \\
\frac{16}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{I} \otimes \mathbf{I},\ \frac{9}{25}\,|s_4\rangle\langle s_3| \otimes \mathbf{Z} \otimes \mathbf{Z}
\end{array}\right\}.
\end{aligned}$$

Each Kraus operator after tracing out the classical information is actually the corresponding element $\mathbf{Q}_{i,j,\ell}\mathbf{P}_k$ in the matrix representation (13a). Then the explicit matrix form of $\mathbb{M}_2$ can be computed as presented in Example 5.9. The same is applied to the computation of the matrix representation $\mathbb{M}_3$.

The matrix representation $\mathrm{S2M}(\Delta(\phi_4))$ of $\Delta(\phi_4)$ in Example 5.9 is

$$\begin{aligned}
&\sum_{i\in[6]} (\langle i| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2^{16})(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}_2)^{-1}(|4\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \\
= &\tfrac{7}{25}\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} + \tfrac{13517224848031700360533738291 2}{56843418860808014869689941406 25}\,|1,1\rangle\langle 1,2| \otimes |1,1\rangle\langle 1,2| + \\
&\tfrac{19525058428669063739008861826 88}{56843418860808014869689941406 25}\,|1,2\rangle\langle 1,2| \otimes |1,2\rangle\langle 1,2| + \\
&\tfrac{162}{625}(|1,2\rangle\langle 1,2| + |2,1\rangle\langle 2,1|) \otimes (|1,2\rangle\langle 1,2| + |2,1\rangle\langle 2,1|) + \\
&\tfrac{162}{625}(|1,1\rangle\langle 1,1| + |2,2\rangle\langle 2,2|) \otimes (|1,1\rangle\langle 1,1| + |2,2\rangle\langle 2,2|) + \tfrac{288}{625}\,|2,1\rangle\langle 2,1| \otimes |2,1\rangle\langle 2,1| + \\
&\tfrac{288}{625}\,|2,2\rangle\langle 2,2| \otimes |2,2\rangle\langle 2,2| + \tfrac{2256213346296092419228554 24}{9094947017729282379150390625}\,|2,1\rangle\langle 1,2| \otimes |2,1\rangle\langle 1,2| + \\
&\tfrac{401104594897083096751742976}{9094947017729282379150390625}\,|2,2\rangle\langle 1,2| \otimes |2,2\rangle\langle 1,2|,
\end{aligned}$$

and the matrix representation $\mathrm{S2M}(\Delta(\phi_3))$ is

$$\begin{aligned}
&\sum_{i\in[6]}(\langle i|\otimes\mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\mathbb{M}_3(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}}-\mathbb{M}_2)^{-1}(|4\rangle\otimes\mathbf{I}_{\mathcal{H}\otimes\mathcal{H}})\\
=\ &\tfrac{7}{25}\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{I}+\tfrac{223617024}{9272485625}\,|1,1\rangle\langle 1,2|\otimes|1,1\rangle\langle 1,2|+\tfrac{3210041376}{9272485625}\,|1,2\rangle\langle 1,2|\otimes|1,2\rangle\langle 1,2|\ +\\
&\tfrac{162}{625}(|1,2\rangle\langle 1,2|+|2,1\rangle\langle 2,1|)\otimes(|1,2\rangle\langle 1,2|+|2,1\rangle\langle 2,1|)+\\
&\tfrac{162}{625}(|1,1\rangle\langle 1,1|+|2,2\rangle\langle 2,2|)\otimes(|1,1\rangle\langle 1,1|+|2,2\rangle\langle 2,2|)+\\
&\tfrac{288}{625}\,|2,1\rangle\langle 2,1|\otimes|2,1\rangle\langle 2,1|+\tfrac{288}{625}\,|2,2\rangle\langle 2,2|\otimes|2,2\rangle\langle 2,2|\ +\\
&\tfrac{373248}{14835977}\,|2,1\rangle\langle 1,2|\otimes|2,1\rangle\langle 1,2|+\tfrac{663552}{14835977}\,|2,2\rangle\langle 1,2|\otimes|2,2\rangle\langle 1,2|\,.
\end{aligned}$$

The expression $||\boldsymbol{\mu}||+||\boldsymbol{\nu}||$ in Example 5.13 is $\mu_1^2+\nu_1^2+\mu_2^2+\nu_2^2+\mu_3^2+\nu_3^2+\mu_4^2+\nu_4^2$. Based on the explicit matrix form $\mathbb{M}=\mathrm{S2M}(\Delta(\phi_4))$ obtained in Example 5.9, we can expand the expression $h(\boldsymbol{\mu},\boldsymbol{\nu})$ in the constraint (16a) as

$$\begin{aligned}
&\tfrac{337}{625}\nu_1^4+\tfrac{3318403704685565836307974101662}{5684341886080801486968994140625}\nu_1^2\nu_2^2+\tfrac{5017502987841674535674567823313}{5684341886080801486968994140625}\nu_2^4+\tfrac{14}{25}\nu_1^2\nu_3^2+\\
&\tfrac{1003361219854886735959863667 4}{909494701772928237915039062 5}\nu_2^2\nu_3^2+\nu_3^4+\tfrac{674}{625}\nu_1^2\nu_4^2+\tfrac{549427492482548122907596172 6}{909494701772928237915039062 5}\nu_2^2\nu_4^2+\\
&\tfrac{14}{25}\nu_3^2\nu_4^2+\nu_4^4+\tfrac{674}{625}\nu_1^2\mu_1^2+\tfrac{3318403704685565836307974101662}{5684341886080801486968994140625}\nu_2^2\mu_1^2+\tfrac{14}{25}\nu_3^2\mu_1^2+\tfrac{674}{625}\nu_4^2\mu_1^2+\\
&\tfrac{337}{625}\mu_1^4+\tfrac{3318403704685565836307974101662}{5684341886080801486968994140625}\nu_1^2\mu_2^2+\tfrac{1003500597568334907134913564662 6}{5684341886080801486968994140625}\nu_2^2\mu_2^2+\\
&\tfrac{1003361219854886735959863667 4}{909494701772928237915039062 5}\nu_3^2\mu_2^2+\tfrac{549427492482548122907596172 6}{909494701772928237915039062 5}\nu_4^2\mu_2^2+\\
&\tfrac{3318403704685565836307974101662}{5684341886080801486968994140625}\mu_1^2\mu_2^2+\tfrac{5017502987841674535674567823313}{5684341886080801486968994140625}\mu_2^4+\tfrac{14}{25}\nu_1^2\mu_3^2+\\
&\tfrac{1003361219854886735959863667 4}{909494701772928237915039062 5}\nu_2^2\mu_3^2+2\nu_3^2\mu_3^2+\tfrac{14}{25}\nu_4^2\mu_3^2+\tfrac{14}{25}\mu_1^2\mu_3^2+\tfrac{1003361219854886735959863667 4}{909494701772928237915039062 5}\mu_2^2\mu_3^2+\\
&\mu_3^4+\tfrac{674}{625}\nu_1^2\mu_4^2+\tfrac{549427492482548122907596172 6}{909494701772928237915039062 5}\nu_2^2\mu_4^2+\tfrac{14}{25}\nu_3^2\mu_4^2+2\nu_4^2\mu_4^2+\tfrac{674}{625}\mu_1^2\mu_4^2+\\
&\tfrac{549427492482548122907596172 6}{909494701772928237915039062 5}\mu_2^2\mu_4^2+\tfrac{14}{25}\mu_3^2\mu_4^2+\mu_4^4.
\end{aligned}$$

References

[1] Andrés, M. E., van Rossum, P., 2008. Conditional probabilities over probabilistic and nondeterministic systems. In: Ramakrishnan, C. R., Rehof, J. (Eds.), Tools and Algorithms for the Construction and Analysis of Systems: 14th International Conference, TACAS 2008. Vol. 4963 of LNCS. Springer, pp. 157–172.

[2] Baier, C., Katoen, J.-P., 2008. Principles of Model Checking. MIT Press.

[3] Ball, P., 2021. First quantum computer to pack 100 qubits enters crowded race. URL `https://www.nature.com/articles/d41586-021-03476-5`

[4] Basu, S., Pollack, R., Roy, M.-F., 2006. Algorithms in Real Algebraic Geometry, 2nd Edition. Springer.

[5] Bennett, C. H., Brassard, G., 1984. Quantum cryptography: Public key distribution and coin tossing. In: Proc. of IEEE International Conference on Computers, Systems and Signal Processing, 1984. IEEE Computer Society, pp. 175–179.

[6] Clarke, E. M., Grumberg, O., Peled, D. A., 1999. Model Checking. MIT Press.

[7] de Moura, L., Bjørner, N., 2008. Z3: An efficient SMT solver. In: Ramakrishnan, C. R., Rehof, J. (Eds.), Tools and Algorithms for the Construction and Analysis of Systems: 14th International Conference, TACAS 2008. Vol. 4963 of LNCS. Springer, pp. 337–340.

[8] Dehnert, C., Junges, S., Katoen, J.-P., Volk, M., 2017. A Storm is coming: A modern probabilistic model checker. In: Majumdar, R., Kuncak, V. (Eds.), Computer Aided Verification: 29th International Conference, CAV 2017, Part II. Vol. 10427 of LNCS. Springer, pp. 592–600.

[9] Dolzmann, A., Sturm, T., 1997. Redlog: Computer algebra meets computer logic. ACM SIGSAM Bulletin 31 (2), 2–9.

[10] Feng, Y., Hahn, E. M., Turrini, A., Ying, S., 2017. Model checking ω-regular properties for quantum Markov chains. In: Meyer, R., Nestmann, U. (Eds.), 28th International Conference on Concurrency Theory, CONCUR 2017. Vol. 85 of LIPIcs. Schloss Dagstuhl — Leibniz-Zentrum für Informatik, pp. 35:1–35:16.

[11] Feng, Y., Yu, N., Ying, M., 2013. Model checking quantum Markov chains. Journal of Computer and System Sciences 79 (7), 1181–1198.

[12] Fu, C., Hahn, E. M., Li, Y., Schewe, S., Sun, M., Turrini, A., Zhang, L., 2022. EPMC gets knowledge in multi-agent systems. In: Finkbeiner, B., Wies, T. (Eds.), Verification, Model Checking, and Abstract Interpretation - 23rd International Conference, VMCAI 2022. Vol. 13182 of LNCS. Springer, pp. 93–107.

[13] Gao, Y., Xu, M., Zhan, N., Zhang, L., 2013. Model checking conditional CSL for continuous-time Markov chains. Information Processing Letters 113 (1-2), 44–50.

[14] Gay, S. J., Nagarajan, R., Papanikolaou, N., 2006. Probabilistic model-checking of quantum protocols. In: Proc. 2nd International Workshop on Developments in Computational Models. pp. 15+2.

[15] Gay, S. J., Nagarajan, R., Papanikolaou, N., 2008. QMC: A model checker for quantum systems. In: Gupta, A., Malik, S. (Eds.), Computer Aided Verification, 20th International Conference, CAV 2008. Vol. 5123 of LNCS. Springer, pp. 543–547.

[16] Grover, L. K., 1996. A fast quantum mechanical algorithm for database search. In: Proc. 28th Annual ACM Symposium on the Theory of Computing. ACM, pp. 212–219.

[17] Guan, J., Feng, Y., Ying, M., 2018. Decomposition of quantum Markov chains and its applications. Journal of Computer and System Sciences 95, 55–68.

[18] Han, T., Katoen, J.-P., Damman, B., 2009. Counterexample generation in probabilistic model checking. IEEE Transactions on Software Engineering 35 (2), 241–257.

[19] Hansson, H., Jonsson, B., 1989. A framework for reasoning about time and reliability. In: Proc. IEEE Real-Time Systems Symposium, 1989. IEEE Computer Society, pp. 102–111.

[20] Harrow, A. W., Hassidim, A., Lloyd, S., 2009. Quantum algorithm for solving linear systems of equations. Physical Review Letters 103 (15), article no. 150502.

[21] Istrăţescu, V. I., 2001. Fixed Point Theory: An Introduction. Springer.

[22] Kwiatkowska, M., Norman, G., Parker, D., 2011. PRISM 4.0: Verification of probabilistic real-time systems. In: Gopalakrishnan, G., Qadeer, S. (Eds.), Computer Aided Verification: 23rd International Conference, CAV 2011. Vol. 6806 of LNCS. Springer, pp. 585–591.

[23] Li, L., Feng, Y., 2015. Quantum Markov chains: Description of hybrid systems, decidability of equivalence, and model checking linear-time properties. Information and Computation 244, 229–244.

[24] Nielsen, M. A., Chuang, I. L., 2000. Quantum Computation and Quantum Information. Cambridge University Press.

[25] Shor, P. W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proc. 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, pp. 124–134.

[26] Tarski, A., 1951. A Decision Method for Elementary Algebra and Geometry, 2nd Edition. University of California Press.

[27] Xu, M., Zhang, L., Jansen, D. N., Zhu, H., Yang, Z., 2016. Multiphase until formulas over Markov reward models: An algebraic approach. Theoretical Computer Science 611, 116–135.

[28] Ying, M., Yu, N., Feng, Y., Duan, R., 2013. Verification of quantum programs. Science of Computer Programming 78 (9), 1679–1700.

[29] Ying, S., Feng, Y., Yu, N., Ying, M., 2013. Reachability probabilities of quantum Markov chains. In: D'Argenio, P. R., Melgratti, H. C. (Eds.), CONCUR 2013: Concurrency Theory—24th International Conference. Vol. 8052 of LNCS. Springer, pp. 334–348.

[30] Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Qin, J., Wu, D., Ding, X., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., You, L., Wang, Z., Li, L., Liu, N.-L., Lu, C.-Y., Pan, J.-W., 2020. Quantum computational advantage using photons. Science 370 (6523), 1460–1463.