Model Checking QCTL Plus on 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, & Shanghai Institute for AI Education, East China Normal University, Shanghai 200062, China

Abstract

Verifying temporal properties of quantum systems, including quantum Markov chains (QMCs), has attracted an increasing interest in the last decade. Typically, the properties are specified by quantum computation tree logic (QCTL), in which reachability analysis plays a central role. However, safety as the dual problem is known little. Motivated by this, we propose a more expressive logic — QCTL$^+$ (QCTL plus), which extends QCTL by allowing the conjunction in path formulas and the negation in the top level of path formulas. The former can be adopted to express conditional events, and the latter can express safety. To deal with conjunction, we present a product construction of classical states in the QMC and the tri-valued truths of atomic path formulas; to deal with negation, we develop an algebraic approach to compute the safety of the bottom strongly connected component subspaces with respect to a super-operator under some necessary and sufficient convergence conditions. Thereby we conditionally decide QCTL$^+$ formulas over QMCs; without the convergence conditions the safety problem still remains open. The complexity of our method is provided in terms of the size of both the input QMC and the QCTL$^+$ formula.

Keywords: Model Checking, Markov Chain, Formal Logic, Quantum Computing

1. Introduction

Quantum computing has attracted more and more interest in the last decades, since it offers the possibility to efficiently solve important problems such as integer factorization [30], unstructured search [17], and solving linear equations [20]. To realize the potential of quantum computing, it is indispensable to develop quantum software that can control quantum devices to execute algorithms and thus solve practical problems [6]. However, it is much more challenging to ensure the correctness of quantum systems, as we can see from various attacks on the quantum key distribution protocol [33, 14]. Therefore, there is an urgent need to develop effective verification techniques to improve the trustworthiness of quantum systems.

Model checking [8, 2] is one of the most successful techniques for the formal verification of classical hardware and software systems. Usually it is based on Markov models. For classical Markov chains (MCs), early work dates back to 1980s. Based on computation tree logic

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)

(CTL) [7], Hansson and Jonsson introduced probabilistic CTL (PCTL) by adding the probability-quantifier, and further gave an algorithm for checking the validity of the PCTL formulas over MCs [18], in which reachability analysis plays a central role. Like CTL, PCTL is a two-level logic consisting of state formulas and path formulas. The syntax of PCTL path formulas allows neither conjunction in path formulas nor negation. The former can be adopted to express conditional events, and the latter can express safety as the dual problem. Whereas, both conjunction and negation are allowed in linear temporal logic (LTL) [29]. A natural extension of PCTL is PCTL*, introduced by Aziz et al. [1], which subsumes PCTL and LTL. The decidability of PCTL* formulas over MCs follows from the fact in [13] that a set of paths satisfying a formula in probabilistic LTL is measurable. Furthermore, Bianco and de Alfaro presented model checking algorithms for PCTL and PCTL* formulas over Markov decision processes (MDP), in which the probabilistic behavior coexists with nondeterminism [4].

Model checking has also been extended to the quantum setting to verify the correctness of quantum programs [37]. Usually, the behaviour of a quantum program can be described by a formal model such as a quantum Markov chain (QMC) [16]. The QMC was shown to be able to describe some hybrid systems [23]. Under it, the authors considered the reachability probability [38], the repeated reachability probability [15], and the model checking of linear time properties [23] and a quantum analogy of CTL (QCTL) [16]. QCTL allows for trace-quantifier formulas, by which the probabilities of specified properties can be taken into consideration. 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 with respect to a given super-operator. After decomposition, all the aforementioned problems were shown to be computable/decidable in polynomial time.

In the current work, we focus on the properties specified by a more expressible logic called QCTL$^+$ (QCTL plus), which extends QCTL [38] by allowing conjunction in path formulas and negation in the top level of path formulas. This logic allows for two kinds of quantifier formulas, instead of probability-quantifier formulas in PCTL: trace-quantifier and fidelity-quantifier formulas. The former employs the notion of *positive operator valued measure* (POVM) to quantify sets of infinite paths in QMCs, and the latter makes use of the notion of *super-operator valued measure* (SOVM). Unlike classical Markov chains, QMCs have transitions weighted by super-operators instead of numerical probabilities, and it is natural to introduce SOVMs as in [16]. A POVM is conceptually more succinct and easier to manipulate, and it has served as the most general formulation of measurements in quantum physics [27], so we also investigate the semantics entailed by this measure [35].

Fidelity is a popular distance measure in quantum computing [31, 12]. It is one of the most widely used quantities to quantify uncertainty of noise in experimental quantum physics and quantum engineering communities; for example, see [26, 5]. When quantifying the degree of satisfaction for a property, we have the freedom to choose a probability or a fidelity, corresponding to POVM and SOVM, respectively. Their difference can be seen from a simple example. Suppose that a quantum system is in the state described by a density operator ρ and some quantum operation $\mathcal{E}$ is applied, changing the quantum system to the state $\mathcal{E}(\rho)$. As an abstraction on the distance between ρ and $\mathcal{E}(\rho)$, the probability measure is mainly determined by the trace of $\mathcal{E}(\rho)$. For instance, the quantum states $\rho = |0\rangle\langle 0|$ and $\mathcal{E}(\rho) = |1\rangle\langle 1|$ (where $\mathcal{E}$ is the bit flip) have the same trace 1, but they are different states. Whereas, the fidelity concerns how well the quantum operation $\mathcal{E}$ has preserved the state ρ of the quantum system, whose arc-cosine value is a precise metric between the aforementioned ρ and $\mathcal{E}(\rho)$. For instance, the fidelity between $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ is 0 as we expected. Hence the probability measure does not suffice to recognize general quantum states, but fidelity does!

To decide the trace-quantifier and fidelity-quantifier formulas, we need to first synthesize the super-operators of path formulas embedded into them. There are three kinds of atomic path formulas — the next formula, the time-bounded until formula, and the time-unbounded until formula. We can directly obtain the super-operators for the former two kinds according to the semantics of QCTL$^+$. Whereas, for the last kind, we have to resort to the matrix representation of the super-operators $\mathcal{F}$ that characterizes state transitions. The BSCC subspaces of $\mathcal{F}$ are subsets of the state space, in which all states are pairwise reachable with probability one under the quantum operation $\mathcal{F}$, and thus yield deadlock. After removing all BSCC subspaces of $\mathcal{F}$, we could get an explicit matrix fraction describing the series of repeatedly applying $\mathcal{F}$.

Proceeding to deal with conjunction and disjunction in atomic path formulas, we present a product construction of classical states in the QMC and the tri-valued truths ("true", "undetermined" and "false") of atomic path formulas. After unrolling with those product states, we reduce the arbitrary conjunction and disjunction in atomic path formulas on the original QMC to a single atomic path formula on the product QMC with SOVM being preserved. Next, we deal with negation in atomic path formulas. The super-operators for the negations of the next formula and the time-bounded until formula can also be obtained according to the semantics of QCTL$^+$. Whereas, for the negation of the time-unbounded until formula, we have to determine the ultimate density operators that stay in the BSCC subspaces with respect to $\mathcal{F}$, which turn out to form a dense set, not a singleton. So we propose the necessary and sufficient convergence conditions that make the semantics unambiguous on the QMC. Under them we synthesize the super-operators. These super-operators are the SOVMs of the properties to be checked. The POVMs follow from them by matrix transformation. However, our approach of synthesizing super-operators would fail without those convergence conditions.

Finally we decide trace-quantifier and fidelity-quantifier formulas using the aforementioned POVMs and SOVMs, respectively. If the input QMC is fed with an initial quantum state, the trace-quantifier and fidelity-quantifier formulas can be decided directly by matrix operations; otherwise we decide the trace-quantifier formula by real root isolation for polynomials and decide the fidelity-quantifier formula by quantifier elimination over real closed fields. The workflow of deciding the QCTL$^+$ formulas on the QMC with an initial quantum state is given in Figure 1.

The main contributions of this paper are summarized as follows.

1. We propose the logic QCTL$^+$ interpreted on QMCs that extends QCTL by allowing conjunction in path formulas and negation in the top level of path formulas.
2. To deal with conjunction, we present a product construction of classical states in the QMC and the tri-valued truths of atomic path formulas.
3. To deal with negation, we develop an algebraic approach for the safety of the BSCC subspaces under the necessary and sufficient convergence conditions.
4. Two running examples — quantum teleportation protocol and quantum Bernoulli factory protocol — are provided to illustrate our method.

Organization. The rest of the paper is structured as follows. In Section 2 we recall some basic concepts and results from quantum computing and number theory. In Section 3 we introduce the model of QMC. In Section 4 we define the syntax and the semantics of QCTL$^+$. We synthesize super-operators for path formulas in Section 5, and decide QCTL$^+$ state formulas and discuss the time complexities in Section 6. Finally, we conclude in Section 7.

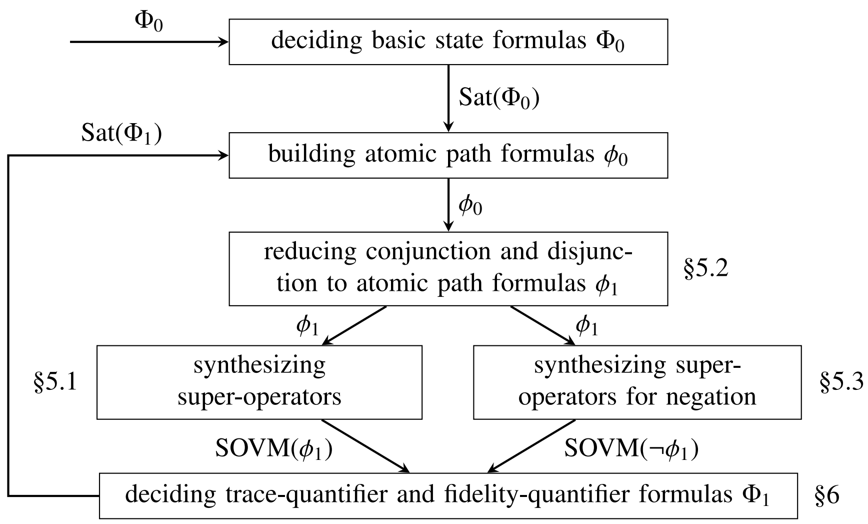

Figure 1: Workflow of deciding the QCTL$^+$ formulas on the QMC with an initial quantum state

2. Preliminaries

2.1. Quantum computing

Here we recall some basic notions and notations in quantum computing. Interested readers can refer to [27, 16] for more details. Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ denote the sets of natural numbers, integers, real numbers, and complex numbers, respectively. In this paper, we adopt the Dirac notations that are standard in quantum computing:

- $|\psi\rangle$ stands for a unit column vector labelled with ψ;
- $\langle\psi| := |\psi\rangle^\dagger$ is the Hermitian adjoint (transpose and complex conjugate entrywise) of $|\psi\rangle$;
- $\langle\psi_1|\psi_2\rangle := \langle\psi_1|\,|\psi_2\rangle$ is the inner product of $|\psi_1\rangle$ and $|\psi_2\rangle$;
- $|\psi_1\rangle\langle\psi_2| := |\psi_1\rangle \otimes \langle\psi_2|$ is the outer product, where $\otimes$ denotes tensor product.

Specifically, $|i\rangle$ with $i \in \mathbb{Z}^+$ denotes the vector whose i-th entry is 1 and the others are 0. Thus $\langle i|i\rangle = 1$ and $\langle i|j\rangle = 0$ hold for all positive integers i, j ($j \neq i$) by orthonormality.

Let $[n]$ ($n \in \mathbb{N}$) denote the finite set $\{1, \ldots, n\}$. Let $\mathcal{H}$ be a Hilbert space with finite dimension $d := \dim(\mathcal{H})$ throughout this paper. Unit elements $|\psi\rangle$ of $\mathcal{H}$ are usually interpreted as *states* of a quantum system. Since $\{|i\rangle : i \in [d]\}$ forms an orthonormal basis of $\mathcal{H}$, any element $|\psi\rangle$ of $\mathcal{H}$ can be expressed as $|\psi\rangle = \sum_{i\in[d]} c_i\,|i\rangle$, where $c_i \in \mathbb{C}$ ($i \in [d]$) satisfy $\sum_{i\in[d]} |c_i|^2 = 1$. That is, the quantum state $|\psi\rangle$ is entirely determined by those coefficients c_i. In a product Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, let $|\psi, \psi'\rangle$ be a shorthand of the product state $|\psi\rangle\,|\psi'\rangle := |\psi\rangle \otimes |\psi'\rangle$ with $|\psi\rangle \in \mathcal{H}$ and $|\psi'\rangle \in \mathcal{H}'$; $|\widehat{\psi\,\psi'}\rangle$ denotes a general joint state in $\mathcal{H} \otimes \mathcal{H}'$ where $\widehat{\psi\,\psi'}$ encoded as a whole symbol is a label. For example, the Bell state $|\text{Bell}\rangle = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$ with label Bell is a general state that cannot be decomposed as a product one. For any $|\psi_1\rangle, |\psi_2\rangle$ in $\mathcal{H}$ and $|\psi_1'\rangle, |\psi_2'\rangle$ in $\mathcal{H}'$, the inner product of two product states $|\psi_1, \psi_1'\rangle$ and $|\psi_2, \psi_2'\rangle$ is defined by $\langle\psi_1, \psi_1' \,|\, \psi_2, \psi_2'\rangle = \langle\psi_1|\psi_2\rangle\,\langle\psi_1' \,|\, \psi_2'\rangle$.

Let $\mathcal{L}_\mathcal{H}$ be the set of linear operators on $\mathcal{H}$, ranged over by letters in bold font, e.g. $\mathbf{E}, \mathbf{F}, \mathbf{I}, \mathbf{P}$. For conciseness, we will omit such a subscript $\mathcal{H}$ afterwards 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 all $|\psi\rangle \in \mathcal{H}$. Given a Hermitian operator γ, we have the spectral decomposition [27, Box 2.2] that

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

where $\lambda_i \in \mathbb{R}$ ($i \in [d]$) are the eigenvalues of γ and $|\psi_i\rangle$ are the corresponding eigenvectors. The *support* of γ is the subspace of $\mathcal{H}$ spanned by all eigenvectors associated with nonzero eigenvalues, i.e., $\mathrm{supp}(\gamma) \coloneqq \mathrm{span}(\{|\psi_i\rangle : i \in [d] \wedge \lambda_i \neq 0\})$. A *projector* $\mathbf{P}$ is a positive operator of the form $\sum_{i\in[m]} |\psi_i\rangle\langle\psi_i|$ with $m \leq d$, where $|\psi_i\rangle$ ($i \in [m]$) are orthonormal. Clearly, there is a bijective map between projectors $\mathbf{P} = \sum_{i\in[m]} |\psi_i\rangle\langle\psi_i|$ and subspaces of $\mathcal{H}$ that are spanned by $\{|\psi_i\rangle : i \in [m]\}$. To summarize, positive operators are Hermitian ones whose eigenvalues are nonnegative; projectors are positive operators whose eigenvalues are 0 or 1.

The *trace* of a linear operator γ is defined as $\mathrm{tr}(\gamma) \coloneqq \sum_{i\in[d]} \langle\psi_i|\gamma|\psi_i\rangle$ for any orthonormal basis $\{|\psi_i\rangle : i \in [d]\}$ of $\mathcal{H}$. A *density operator* (resp. *partial density operator*) ρ on $\mathcal{H}$ is a positive operator with trace 1 (resp. ≤ 1). It gives rise to a generic way to describe quantum states: if a density operator ρ is $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$, it is said to be a *pure* state; otherwise it is a *mixed* one, i.e., $\rho = \sum_{i\in[d]} p_i |\psi_i\rangle\langle\psi_i|$ under the spectral decomposition, where p_i ($i \in [d]$) are positive eigenvalues (interpreted as the *probabilities* of taking the pure states $|\psi_i\rangle$) and their sum is 1. Let $\mathcal{D}^{\leq 1}$ be the set of partial density operators on $\mathcal{H}$, and $\mathcal{D}$ the set of density operators. In a product Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, $\gamma \otimes \gamma'$ with $\gamma \in \mathcal{L}_\mathcal{H}$ and $\gamma' \in \mathcal{L}_{\mathcal{H}'}$ has the partial traces $\mathrm{tr}_{\mathcal{H}'}(\gamma \otimes \gamma') \coloneqq \mathrm{tr}(\gamma')\gamma$ and $\mathrm{tr}_\mathcal{H}(\gamma \otimes \gamma') \coloneqq \mathrm{tr}(\gamma)\gamma'$, which result in linear operators on $\mathcal{H}$ and $\mathcal{H}'$, respectively. The (partial) trace is defined to be linear in its input.

A *super-operator* $\mathcal{E}$ on $\mathcal{H}$ is a linear operator on $\mathcal{L}_\mathcal{H}$, ranged over by letters in calligraphic font, e.g. $\mathcal{E}, \mathcal{F}, \mathcal{I}, \mathcal{P}$. 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 positive operators on $\mathcal{L}_{\mathcal{H}\otimes\mathcal{H}'}$ to positive operators on $\mathcal{L}_{\mathcal{H}\otimes\mathcal{H}'}$, 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 $\mathcal{H}$. By Kraus representation [27, Theorem 8.3], a super-operator $\mathcal{E}$ is completely positive on $\mathcal{H}$ if and only if there are m linear operators $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_m \in \mathcal{L}$ with some $m \leq d^2$ (called *Kraus* operators), such that for any $\gamma \in \mathcal{L}$, we have

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

The description of $\mathcal{E}$ is given by those Kraus operators $\{\mathbf{E}_\ell : \ell \in [m]\}$. Thus, 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 $\{\mathbf{E}_{2,\ell_2}\mathbf{E}_{1,\ell_1} : \ell_1 \in [m_1] \wedge \ell_2 \in [m_2]\}$. In a product Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, for super-operators $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\} \in \mathcal{S}_\mathcal{H}$ and $\mathcal{E}' = \{\mathbf{E}'_\ell : \ell \in [m']\} \in \mathcal{S}_{\mathcal{H}'}$, the product super-operator $\mathcal{E} \otimes \mathcal{E}'$ is given by $\{\mathbf{E}_\ell : \ell \in [m]\} \otimes \{\mathbf{E}'_\ell : \ell \in [m']\} = \{\mathbf{E}_\ell \otimes \mathbf{E}'_{\ell'} : \ell \in [m] \wedge \ell' \in [m']\}$. It is easy to validate that $(\mathcal{E} \otimes \mathcal{E}')(\gamma \otimes \gamma') = \mathcal{E}(\gamma) \otimes \mathcal{E}'(\gamma')$ holds for all $\gamma \in \mathcal{L}_\mathcal{H}$ and $\gamma' \in \mathcal{L}_{\mathcal{H}'}$. The partial trace can be extended to $\mathcal{S}_\mathcal{H} \otimes \mathcal{S}_{\mathcal{H}'}$ as $\mathrm{tr}_\mathcal{H}(\mathcal{E} \otimes \mathcal{E}') \coloneqq \sum_{i\in[d]} \{\langle\psi_i|\mathbf{E}_\ell : \ell \in [m]\} \otimes \mathcal{E}'$ and $\mathrm{tr}_{\mathcal{H}'}(\mathcal{E} \otimes \mathcal{E}') \coloneqq \sum_{i\in[d']} \mathcal{E} \otimes \{\langle\psi'_i|\mathbf{E}'_\ell : \ell \in [m']\}$ for any orthonormal basis $\{|\psi_i\rangle : i \in [d]\}$ of $\mathcal{H}$ and $\{|\psi'_i\rangle : i \in [d']\}$ of $\mathcal{H}'$ and for any $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\} \in \mathcal{S}_\mathcal{H}$ and $\mathcal{E}' = \{\mathbf{E}'_\ell : \ell \in [m']\} \in \mathcal{S}_{\mathcal{H}'}$.

A partial order $\sqsubseteq$ can be defined on $\mathcal{L}$ as: $\rho_1 \sqsubseteq \rho_2$ if $\rho_2 - \rho_1$ is positive. A trace pre-order $\lesssim$ can be defined on $\mathcal{S}$ as: $\mathcal{E}_1 \lesssim \mathcal{E}_2$ if $\mathrm{tr}(\mathcal{E}_1(\rho)) \leq \mathrm{tr}(\mathcal{E}_2(\rho))$ holds for all $\rho \in \mathcal{D}$. The equivalence

$\mathcal{E}_1 \approx \mathcal{E}_2$ means that both $\mathcal{E}_1 \lesssim \mathcal{E}_2$ and $\mathcal{E}_1 \gtrsim \mathcal{E}_2$ hold. For a super-operator $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\}$, the completeness $\mathcal{E} \approx \mathcal{I}$ 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. Let $\mathcal{S}^{\lesssim\mathcal{I}}$ be the set of *trace-nonincreasing* super-operators $\mathcal{E}$, i.e., $\mathcal{S}^{\lesssim\mathcal{I}} = \{\mathcal{E} \in \mathcal{S} : \mathcal{E} \lesssim \mathcal{I}\}$.

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

$$\mathrm{Fid}(\mathcal{E}, \rho) \coloneqq \mathrm{tr}\sqrt{\rho^{1/2}\mathcal{E}(\rho)\rho^{1/2}}; \tag{3a}$$

when ρ is a pure state $|\psi\rangle\langle\psi|$, it is simply

$$\mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|) \coloneqq \sqrt{\langle\psi|\, \mathcal{E}(|\psi\rangle\langle\psi|)\, |\psi\rangle}. \tag{3b}$$

The fidelity reflects how well the quantum operation $\mathcal{E}$ has preserved the quantum state ρ. The better the quantum state is preserved, the larger the fidelity would be. We can see $0 \le \mathrm{Fid}(\mathcal{E}, \rho) \le 1$ where the equality in the first inequality holds if and only if the supports of ρ and $\mathcal{E}(\rho)$ are orthogonal, and the equality in the second inequality holds if and only if $\mathcal{E} = \mathcal{I}$. More technically, the fidelity measures the average angle between the vectors in $\mathrm{supp}(\rho)$ and those in $\mathrm{supp}(\mathcal{E}(\rho))$, which reveals that $\arccos \mathrm{Fid}(\mathcal{E}, \rho)$ would be a standard metric between ρ and $\mathcal{E}(\rho)$. For conservation, we would like to study the (minimum) fidelity of $\mathcal{E}$, which is defined by

$$\underline{\mathrm{Fid}}(\mathcal{E}) \coloneqq \min_{\rho\in\mathcal{D}} \mathrm{Fid}(\mathcal{E}, \rho) = \min_{|\psi\rangle\in\mathcal{H}} \mathrm{Fid}(\mathcal{E}, |\psi\rangle\langle\psi|), \tag{3c}$$

where the last equation comes from the joint concavity [27, Exercise 9.19].

2.2. Number theory

We recall some basic results about dense subsets and algebraic numbers.

Definition 2.1. *For a given set $S \subseteq \mathbb{R}^m$ with $m \in \mathbb{N}$, a subset S' of S is* dense *if any element of S can be approximated up to arbitrarily precision by elements of S'.*

Definition 2.2. *A collection of numbers $\mu_1, \ldots, \mu_m$ are* $\mathbb{Z}$-linearly independent *if no linear relation $\sum_{i\in[m]} z_i\mu_i = 0$ holds for some integer coefficients z_i ($i \in [m]$), not all zero; otherwise they are* $\mathbb{Z}$-linearly dependent.

Theorem 2.3 (Kronecker [19, Theorem 443]). *The set $\{(k\mu_1 \bmod 1, \ldots, k\mu_m \bmod 1) : k \in \mathbb{N}\}$ of m-tuples is dense in $[0, 1)^m$ if $1, \mu_1, \ldots, \mu_m$ are $\mathbb{Z}$-linearly independent.*

Corollary 2.4. *The m-tuple set $\{(k\mu_1 \bmod 2\pi, \ldots, k\mu_m \bmod 2\pi) : k \in \mathbb{N}\}$ is dense in $[0, 2\pi)^m$ if $\pi, \mu_1, \ldots, \mu_m$ are $\mathbb{Z}$-linearly independent.*

Definition 2.5. *A number λ is* algebraic*, denoted by $\lambda \in \mathbb{A}$, if there is a nonzero $\mathbb{Z}$-polynomial $f_\lambda(z)$ of least degree, satisfying $f_\lambda(\lambda) = 0$.*

In the definition, such a polynomial $f_\lambda(z)$ is called the *minimal polynomial* of λ if the coefficients of $f_\lambda(z)$ have no common divisors $\neq \pm 1$. The *degree D* of λ is exactly $\deg_z(f_\lambda)$, and the *height H* is the maximum of the absolute values of the coefficients in $f_\lambda(z)$. So, D and the bit length $\log_2 H$ are reflected in the encoding size $\|\lambda\|$. The standard encoding of λ is the minimal polynomial f_λ plus an isolation disk in the complex plane that distinguishes λ from other roots of f_λ.

Definition 2.6. *Let $\mu_1, \dots, \mu_m$ be a collection of irrational complex numbers. The* field extension *$\mathbb{Q}(\mu_1, \dots, \mu_m) : \mathbb{Q}$ is the smallest set that contains $\mu_1, \dots, \mu_m$ and is closed under arithmetic operations, i.e., addition, subtraction, multiplication and division.*

Here those irrational complex numbers $\mu_1, \dots, \mu_m$ are called the generators of the field extension. A field extension is *simple* if it has only one generator. For instance, the simple field extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is exactly the set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Lemma 2.7 ([24, Algorithm 2]). *Let λ_1 and λ_2 be two algebraic numbers of degree D_1 and D_2, respectively. There is an algebraic number λ_0 of degree at most $D_1 D_2$, such that the field extension $\mathbb{Q}(\lambda_0) : \mathbb{Q}$ is exactly $\mathbb{Q}(\lambda_1, \lambda_2) : \mathbb{Q}$.*

For the collection of algebraic numbers $\lambda_1, \dots, \lambda_m$ appearing in the input instance, by repeatedly applying this lemma, we can obtain a simple field extension $\mathbb{Q}(\lambda_0) : \mathbb{Q}$ that can span all $\lambda_1, \dots, \lambda_m$. Thus we suppose w.l.o.g. that the input instance takes all constants from $\mathbb{Q}(\lambda_0) : \mathbb{Q}$, and $\|\lambda_0\|$ is reflected in the size of the input.

Lemma 2.8 ([9, Corollary 4.1.5]). *Let λ be an algebraic number of degree D, and $f(z)$ a polynomial with degree D_f and coefficients taken from $\mathbb{Q}(\lambda) : \mathbb{Q}$. There is a $\mathbb{Q}$-polynomial $g(z)$ of degree at most DD_f, such that the roots of $f(z)$ are those of $g(z)$.*

The above lemma entails the fact that roots of all $\mathbb{A}$-polynomials are also algebraic.

Theorem 2.9 (Masser [25],[28, Theorem 3.1]). *Let $\lambda_1, \dots, \lambda_m$ be unit algebraic numbers of degree at most D and height at most H. Then the free Abelian (addition) group $\{(z_1, \dots, z_m) \in \mathbb{Z}^m : \lambda_1^{z_1} \cdots \lambda_k^{z_m} = 1\}$ has a basis with entries bounded by $(D \log_2 H)^{O(m^2)}$.*

The above result gives the complexity of finding such a basis, which is in the finite range $(-B, B)^m$ with $B = (D \log_2 H)^{O(m^2)}$ (i.e., **PSPACE** with respect to the number m of algebraic numbers, and **PTIME** with respect to the size $D + \log_2 H$ of algebraic numbers when m is fixed).

3. Quantum Markov Chain

Let AP be a set of atomic propositions throughout this paper. For the consideration of computability, all occurring numbers are supposed to be algebraic, taken from the field extension $\mathbb{Q}(\lambda_0) : \mathbb{Q}$ for an appropriate algebraic number λ_0. This field $\mathbb{Q}(\lambda_0) : \mathbb{Q}$ contains some irrational numbers, say the most common constant $1/\sqrt{2}$ appeared in quantum computing.

Definition 3.1 ([16, Definition 3.1]). *A labelled* quantum Markov chain *(QMC for short) $\mathfrak{C}$ over $\mathcal{H}$ is a tuple (S, Q, L), in which*

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

Usually, a classical state $s_0 \in S$ is appointed as the initial one.

Let $\mathcal{H}_{\mathrm{cq}} \coloneqq C \otimes \mathcal{H}$ be the enlarged Hilbert space with $C = \mathrm{span}(\{|s\rangle : s \in S\})$ corresponding to the whole classical–quantum system. Here $\{|s\rangle : s \in S\}$ is a set of orthonormal states serving as the quantization of classical system S. The dimension of $\mathcal{H}_{\mathrm{cq}}$ is $N \coloneqq nd$ where $n = |S|$ and $d = \dim(\mathcal{H})$. In the QMC $\mathfrak{C}$, a state ρ_{cq} is a density operator on $\mathcal{H}_{\mathrm{cq}}$ with the mixed form $\sum_{s\in S} |s\rangle\langle s| \otimes \rho_s$ where $\rho_s \in \mathcal{D}^{\leq 1}$ $(s \in S)$ satisfy $\sum_{s\in S} \mathrm{tr}(\rho_s) = 1$. Note that only the initial classical state s_0 is specified in the model, while the initial quantum state ρ_{s_0} is not. We will consider the concrete and the parametric models, respectively, afterwards.

The transition super-operator matrix Q is functionally analogous to the transition probability matrix in the ordinary Markov chain (MC). Actually, QMC extends MC by the fact that a QMC would be an MC when $\mathcal{H}$ is one-dimensional. Sometimes, it is convenient to combine all the super-operators in Q together to form a single super-operator, denoted $\mathcal{F} \coloneqq \sum_{s,t\in S} \{|t\rangle\langle s|\} \otimes Q(s,t)$, on the enlarged Hilbert space $\mathcal{H}_{\mathrm{cq}}$.

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

Example 3.2. *Here we consider the quantum teleportation protocol [27]. Its background is described as follows. Suppose there are two partners: Alice and Bob. While together they generated a qubit pair q_2 and q_3, each took one qubit of the pair when they were separated. After that, Alice wants to send a qubit information $|q_1\rangle$ to Bob. She can only use classical information. So she interacts the qubit q_1 with the share of the entangled qubit pair q_2, and measures two qubits in her possession by M_1 and M_2, respectively. Alice then sends the results to Bob. According to the measurement results, Bob performs the certain transformation to his qubit q_3, whose information $|q_3\rangle$ is expected to be Alice's original qubit one $|q_1\rangle$.*

Technically, the protocol can be implemented by the quantum circuit (see Figure 2). The symbols of some basic quantum gates and their meanings are given in Table 1, in which double lines represent classical wires which transmit the classical output after measurement.

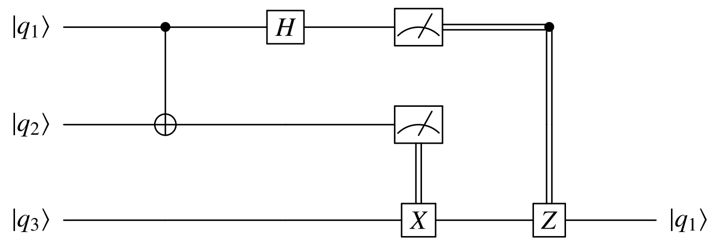

Figure 2: Quantum circuit for the quantum teleportation protocol

We model the quantum teleportation protocol with the QMC $\mathfrak{C}_1 = (S, Q, L)$ shown in Figure 3. The state set S is $\{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\}$, in which s_7 has label ok *and others have no label. Particularly, s_0 is the initial classical state that prepares i) the information $|q_1\rangle$ (on the first qubit) to be sent and ii) the entangled information $|\widehat{q_2\, q_3}\rangle$ (on the second and the third qubits) between Alice and Bob. After a CNOT gate is applied on the first two qubits, we get state s_1; then after a Hadamard gate is applied to the first qubit, we get state s_2. Performing a measurement on the first two qubits gives rise to four outcomes "1,1", "1,2", "2,1" and "2,2", and the system moves to s_3, s_4, s_5 and s_6, respectively. If the states s_3 is obtained, keep the last qubit unchanged, which*

Symbol	Name	Operation
$-\boxed{X}-$	Pauli-X (bit flip)	$\mathbf{X} = \|1\rangle\langle 2\| + \|2\rangle\langle 1\|$
$-\boxed{Z}-$	Pauli-Z (phase flip)	$\mathbf{Z} = \|1\rangle\langle 1\| - \|2\rangle\langle 2\|$
$-\boxed{Y}-$	Pauli-Y (bit-phase flip)	$\mathbf{Y} = -\imath\,\|1\rangle\langle 2\| + \imath\,\|2\rangle\langle 1\|$
$-\boxed{H}-$	Hadamard	$\mathbf{H} = \|+\rangle\langle 1\| + \|-\rangle\langle 2\|$ with $\|\pm\rangle = (\|1\rangle \pm \|2\rangle)/\sqrt{2}$
$\bullet$ $\oplus$	controlled-NOT (CNOT)	$\|1\rangle\langle 1\| \otimes \mathbf{I} + \|2\rangle\langle 2\| \otimes \mathbf{X}$
	measurement	a collection $\{M_i\}$, e.g. $M_i = \|i\rangle\langle i\|$

Table 1: The symbols of some basic quantum gates and their specific operations

leads to the state s_7. If s_4, s_5 and s_6 are obtained, apply the bit, phase, bit–phase flips to the last qubit, respectively, which leads to s_7 too. Finally, s_7 is the goal classical state indicating that the information $|q_1\rangle$ has been delivered to Bob. The transition super-operator matrix Q is given by the following nonzero entries in Kraus representation:

$$
\begin{array}{ll}
Q(s_0, s_1) = \{|1\rangle\langle 1| \otimes \mathbf{I} \otimes \mathbf{I} + |2\rangle\langle 2| \otimes \mathbf{X} \otimes \mathbf{I}\} = CNOT_{1,2}, & \\
Q(s_1, s_2) = \{\mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I}\} = H_1, & Q(s_7, s_7) = \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I}\} = \mathcal{I}, \\
Q(s_2, s_3) = \{|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I}\} = M_{1,2}^{1,1}, & Q(s_2, s_4) = \{|1\rangle\langle 1| \otimes |2\rangle\langle 2| \otimes \mathbf{I}\} = M_{1,2}^{1,2}, \\
Q(s_2, s_5) = \{|2\rangle\langle 2| \otimes |1\rangle\langle 1| \otimes \mathbf{I}\} = M_{1,2}^{2,1}, & Q(s_2, s_6) = \{|2\rangle\langle 2| \otimes |2\rangle\langle 2| \otimes \mathbf{I}\} = M_{1,2}^{2,2}, \\
Q(s_3, s_7) = \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I}\} = I_3 = \mathcal{I}, & Q(s_4, s_7) = \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X}\} = X_3, \\
Q(s_5, s_7) = \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Z}\} = Z_3, & Q(s_6, s_7) = \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Y}\} = Y_3,
\end{array}
$$

where $\mathbf{I} = |1\rangle\langle 1| + |2\rangle\langle 2|$ is the identity operator, and $\mathbf{X}, \mathbf{Z}, \mathbf{Y}, \mathbf{H}$ are referred to the description in Table 1 with subscripts indicating which qubits are operated. Note that the factor $\imath$ in $\imath\mathbf{Y} = \mathbf{ZX}$ yields a global phase of the resulting state, which is ignored in practice since it is not measurable [27, Subsection 2.2.7].

In the QMC, $\omega_1 = s_0, s_1, s_2, s_3, s_7, s_7, \ldots$ is a path in the set Path, while its finite prefix $\bar{\omega}_1 = s_0, s_1, s_2, s_3, s_7$ is in $Path_{\text{fin}}$. Besides, we have to address that the initial quantum state (density operator) on s_0 consists of two independent parts: $|q_1\rangle$ and $|\widehat{q_2\, q_3}\rangle$, which are parameters *in the model. We will algorithmically determine them later.* □

To effectively reason about quantitative properties of QMC, we would restrict the family of basic events in consideration to be a countable set, and study the measures of the closure of that family under union and complement. Formally, we are to establish two measure spaces, named super-operator valued measure (SOVM) space and positive operator valued measure (POVM) space, over paths as follows.

Definition 3.3. *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:*

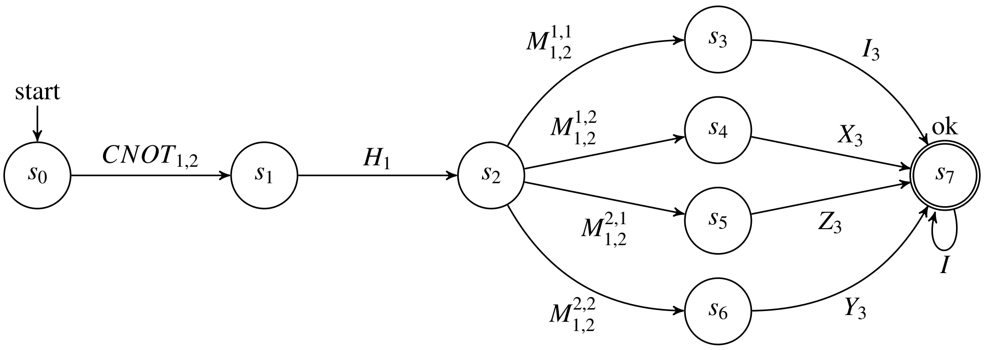

Figure 3: QMC for the quantum teleportation protocol

- $\Omega \in \Sigma$, *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* $A_i \in \Sigma$*;*

a POVM space *is a triple* $(\Omega, \Sigma, \Lambda)$*, where* $\Lambda\colon \Sigma \to \{\mathbf{M} \in \mathcal{L}\colon 0 \sqsubseteq \mathbf{M} \sqsubseteq \mathbf{I}\}$ *is a POVM, satisfying:*

- $\Lambda(\Omega) = \mathbf{I}$, *and*
- $\Lambda(\biguplus_i A_i) = \sum_i \Lambda(A_i)$ *for any pairwise disjoint* $A_i \in \Sigma$.

For a given finite path $\bar{\omega} \in Path_{\mathrm{fin}}$, we define the cylinder set as

$$Cyl(\bar{\omega}) := \{\omega \in Path\colon \omega \text{ has the prefix } \bar{\omega}\}; \tag{4}$$

for $C \subseteq Path_{\mathrm{fin}}$, we extend (4) by $Cyl(C) := \bigcup_{\bar{\omega} \in C} Cyl(\bar{\omega})$. Particularly, we have $Cyl(s_0) = Path$. Let $\Omega = Path$ and $\Pi \subseteq 2^{\Omega}$ be the countable set of all cylinder sets $\{Cyl(\bar{\omega})\colon \bar{\omega} \in Path_{\mathrm{fin}}\}$ 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 $\bar{\omega} = s_0, s_1, \ldots, s_n$, we define the accumulated super-operator along with $\bar{\omega}$ as

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

By [16, 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 $\eqsim$ under the complement A^{c} for some $A \in \Pi$. Hence the triple (Ω, Σ, Δ) forms an SOVM space. Additionally, we would like to address that for two disjoint path sets, we can simply sum up their super-operators to get a total measure; however, the sum is improper when the two path sets are overlapping, which could be resolved by using the measurable space on path sets established as above.

Whereas, we define the accumulated positive operator along with $\bar{\omega}$ as

$$\Lambda(Cyl(\bar{\omega})) := \begin{cases} \mathbf{I} & \text{if } n = 0, \\ Q(s_0, s_1)^\dagger \circ \cdots \circ Q(s_{n-1}, s_n)^\dagger(\mathbf{I}) & \text{otherwise.} \end{cases} \tag{5b}$$

Again, by a simplification of [16, Theorem 3.2], the domain of Λ can be extended to Σ, i.e., $\Lambda\colon \Sigma \to \{\mathbf{M} \in \mathcal{L}\colon 0 \sqsubseteq \mathbf{M} \sqsubseteq \mathbf{I}\}$, which is unique under the countable union $\bigcup_i A_i$ for any $A_i \in \Pi$ and under the complement A^c for some $A \in \Pi$. Hence the triple $(\Omega, \Sigma, \Lambda)$ forms a POVM space.

Example 3.4. *Over the path set Path of $\mathfrak{C}_1$ shown in Example 3.2, we can establish the SOVM and the POVM spaces as follows. For the finite path $\bar{\omega}_1 = s_0, s_1, s_2, s_3, s_7$, we can calculate*

- *the SOVM $\Delta(\bar{\omega}_1)$ as*

$$\begin{aligned} \Delta(\bar{\omega}_1) &= Q(s_3, s_7) \circ Q(s_2, s_3) \circ Q(s_1, s_2) \circ Q(s_0, s_1) \\ &= Q(s_3, s_7) \circ Q(s_2, s_3) \circ \{|+\rangle\langle 1| \otimes \mathbf{I} \otimes \mathbf{I} + |-\rangle\langle 2| \otimes \mathbf{X} \otimes \mathbf{I}\} \\ &= Q(s_3, s_7) \circ \{\tfrac{1}{\sqrt{2}} |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I} + \tfrac{1}{\sqrt{2}} |1\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{I}\} \\ &= \{\tfrac{1}{\sqrt{2}} |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I} + \tfrac{1}{\sqrt{2}} |1\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{I}\}, \end{aligned}$$

- *the POVM $\Lambda(\bar{\omega}_1)$ as*

$$\begin{aligned} \Lambda(\bar{\omega}_1) &= Q(s_0, s_1)^\dagger \circ Q(s_1, s_2)^\dagger \circ Q(s_2, s_3)^\dagger \circ Q(s_3, s_7)^\dagger(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I}) \\ &= Q(s_0, s_1)^\dagger \circ Q(s_1, s_2)^\dagger \circ Q(s_2, s_3)^\dagger(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I}) \\ &= Q(s_0, s_1)^\dagger \circ Q(s_1, s_2)^\dagger(|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I}) \\ &= Q(s_0, s_1)^\dagger((\tfrac{1}{2}\mathbf{I} + \tfrac{1}{2}\mathbf{X}) \otimes |1\rangle\langle 1| \otimes \mathbf{I}) \\ &= \tfrac{1}{2}(|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I} + |1\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{I} + |2\rangle\langle 1| \otimes |2\rangle\langle 1| \otimes \mathbf{I} + |2\rangle\langle 2| \otimes |2\rangle\langle 2| \otimes \mathbf{I}), \end{aligned}$$

  which is exactly $\mathbf{E}^\dagger\mathbf{E}$ with $\mathbf{E} = \frac{1}{\sqrt{2}} |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I} + \frac{1}{\sqrt{2}} |1\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{I}$ being the unique Kraus operator of $\Delta(\bar{\omega}_1)$.

Similarly, we have that the SOVMs of $\bar{\omega}_2 = s_0, s_1, s_2, s_4, s_7$, $\bar{\omega}_3 = s_0, s_1, s_2, s_5, s_7$ and $\bar{\omega}_4 = s_0, s_1, s_2, s_6, s_7$ are

$$\begin{aligned} \Delta(\bar{\omega}_2) &= Q(s_4, s_7) \circ Q(s_2, s_4) \circ Q(s_1, s_2) \circ Q(s_0, s_1) \\ &= \{\tfrac{1}{\sqrt{2}} |1\rangle\langle 1| \otimes |2\rangle\langle 2| \otimes \mathbf{X} + \tfrac{1}{\sqrt{2}} |1\rangle\langle 2| \otimes |2\rangle\langle 1| \otimes \mathbf{X}\}, \\ \Delta(\bar{\omega}_3) &= Q(s_5, s_7) \circ Q(s_2, s_5) \circ Q(s_1, s_2) \circ Q(s_0, s_1) \\ &= \{\tfrac{1}{\sqrt{2}} |2\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{Z} - \tfrac{1}{\sqrt{2}} |2\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{Z}\}, \\ \Delta(\bar{\omega}_4) &= Q(s_6, s_7) \circ Q(s_2, s_6) \circ Q(s_1, s_2) \circ Q(s_0, s_1) \\ &= \{\tfrac{1}{\sqrt{2}} |2\rangle\langle 1| \otimes |2\rangle\langle 2| \otimes \mathbf{Y} - \tfrac{1}{\sqrt{2}} |2\rangle\langle 2| \otimes |2\rangle\langle 1| \otimes \mathbf{Y}\}. \end{aligned}$$ □

From Example 3.4, we have seen the identity $\Lambda(\bar{\omega}) = \Delta(\bar{\omega})^\dagger(\mathbf{I}_{\mathcal{H}})$. Hence, the POVM Λ can be easily obtained, provided that the SOVM Δ is known. The SOVM is indeed generic!

4. Quantum CTL Plus

Now we propose the formal logic considered in this paper — QCTL$^+$ (QCTL plus) — that extends quantum computation tree logic (QCTL) [16] by admitting the conjunction in the path formulas and the negation in the top level of path formulas.

Definition 4.1. *The syntax of QCTL$^+$ is split into the following state formulas Φ and path formulas ϕ:*

$$\Phi := \mathrm{a} \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\phi] \mid \mathfrak{F}^{\mathrm{fid}}_{\leq \tau}[\phi] \mid \mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\neg\phi] \mid \mathfrak{F}^{\mathrm{fid}}_{\leq \tau}[\neg\phi]$$
$$\phi := \mathrm{X}\,\Phi \mid \Phi_1 \mathrm{U}^{\leq k}\Phi_2 \mid \Phi_1 \mathrm{U}\,\Phi_2 \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

where $\mathrm{a} \in AP$ *is an atomic proposition,* $0 \sqsubseteq \mathbf{M} \sqsubseteq \mathbf{I}$ *and* $\tau \in \mathbb{Q}$ *are thresholds, and* $k \geq 0$ *is a time bound.*

In this logic, $\mathrm{X}\,\Phi$ is called the *next formula*, $\Phi_1 \mathrm{U}^{\leq k}\Phi_2$ is the *time-bounded until formula*, $\Phi_1 \mathrm{U}\,\Phi_2$ is the *time-unbounded until formula*, and all of them are atomic path formulas; the former four state formulas are basic ones, $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\cdot]$ is the *trace-quantifier formula* and $\mathfrak{F}^{\mathrm{fid}}_{\leq \tau}[\cdot]$ is the *fidelity-quantifier formula*. The QCTL$^+$ formulas are referred to state formulas. It is generic to consider the comparison operators $\sqsubseteq, \leq$, since other comparison operators $\sqsupset, \sqsupseteq, \sqsubset, >, \geq, <, =$ can be tackled similarly. Next, $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\neg\phi]$ and $\mathfrak{F}^{\mathrm{fid}}_{\leq \tau}[\neg\phi]$ allow us to express the negation acting on the top level of path formulas, not on some arbitrary level of path formulas. The latter should be in the scope of the quantum analogy QCTL* of probabilistic CTL* [1] that is more expressive than our QCTL$^+$. So, under this restriction, we do not directly allow the negation in the syntax of path formulas, but allow the negation in the path formulas embedded into the trace-quantifier and fidelity-quantifier formulas. The reason of imposing this restriction is to effectively synthesize the super-operators in an explicit form, without which there would be nontrivial technical hardness (to be specified at the end of Subsection 5.3).

Definition 4.2. *The semantics of QCTL$^+$ interpreted over a QMC $\mathfrak{C} = (S, Q, L)$ is given by the satisfaction relation $\models$:*

$s \models \mathrm{a}$	if $\mathrm{a} \in L(s)$,
$s \models \neg\Phi$	if $s \not\models \Phi$,
$s \models \Phi_1 \wedge \Phi_2$	if $s \models \Phi_1$ and $s \models \Phi_2$,
$s \models \Phi_1 \vee \Phi_2$	if $s \models \Phi_1$ or $s \models \Phi_2$,
$s \models \mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\phi]$	if $\Lambda(\{\omega \in Path(s) \colon \omega \models \phi\}) \sqsubseteq \mathbf{M}$,
$s \models \mathfrak{F}^{\mathrm{fid}}_{\leq \tau}[\phi]$	if $\underline{\mathrm{Fid}}(\Delta(\{\omega \in Path(s) \colon \omega \models \phi\})) \leq \tau$,
$\omega \models \mathrm{X}\,\Phi$	if $\omega(1) \models \Phi$,
$\omega \models \Phi_1 \mathrm{U}^{\leq k}\Phi_2$	if there is an $i \leq k$ such that $\omega(i) \models \Phi_2$ and $\omega(j) \models \Phi_1$ holds for all $j < i$,
$\omega \models \Phi_1 \mathrm{U}\,\Phi_2$	if there is an i such that $\omega(i) \models \Phi_2$ and $\omega(j) \models \Phi_1$ holds for all $j < i$,
$\omega \models \neg\phi$	if $\omega \not\models \phi$,
$\omega \models \phi_1 \wedge \phi_2$	if $\omega \models \phi_1$ and $\omega \models \phi_2$,
$\omega \models \phi_1 \vee \phi_2$	if $\omega \models \phi_1$ or $\omega \models \phi_2$.

Later on, we will use $\Delta(\bar{\omega})$ and $\Delta(\phi)$ to abbreviate $\Delta(Cyl(\bar{\omega}))$ and $\Delta(\{\omega \in Path\colon \omega \models \phi\})$ respectively, and similar for the POVM Λ.

Example 4.3. *Consider the path $\omega_1 = s_0, s_1, s_2, s_3, s_7, s_7, \ldots$ on the QMC $\mathfrak{C}_1$ shown in Example 3.2. We can see:*

- $s_7 \models \mathrm{ok}$ *and* $s \not\models \mathrm{ok}$ *for each* $s \in S \setminus \{s_7\}$*;*
- $\omega_1 \models \mathrm{X}\,\neg\mathrm{ok}$*, as* $\omega_1(1) = s_1 \not\models \mathrm{ok}$*;*
- $\omega_1 \not\models \mathrm{true}\,\mathrm{U}^{\leq 2}\mathrm{ok}$*, as* $\omega_1(i) \not\models \mathrm{ok}$ *for each* $i \leq 2$*;*
- $\omega_1 \models \mathrm{true}\,\mathrm{U}\,\mathrm{ok}$*, as* $\omega_1(4) = s_7 \models \mathrm{ok}$ *and* $\omega_1(i) \models \mathrm{true}$ *for each* $i < 4$.

The final classical state of the quantum teleportation protocol is s_7 that is uniquely labelled with ok*, and the corresponding map from the initial quantum state to the final one is characterized by the SOVM of all paths ω reaching* ok*, i.e.,* $\Delta(\Diamond\mathrm{ok}) = \Delta(\{\omega \in Path\colon \omega \models \mathrm{true}\,\mathrm{U}\,\mathrm{ok}\})$*. Since there are exactly four disjoint finite paths $\bar{\omega}_1 = s_0, s_1, s_2, s_3, s_7$, $\bar{\omega}_2 = s_0, s_1, s_2, s_4, s_7$, $\bar{\omega}_3 = s_0, s_1, s_2, s_5, s_7$ and $\bar{\omega}_4 = s_0, s_1, s_2, s_6, s_7$ that reach* ok*, we get*

$$\begin{aligned}\Delta(\Diamond\mathrm{ok}) &= \Delta(\bar{\omega}_1) + \Delta(\bar{\omega}_2) + \Delta(\bar{\omega}_3) + \Delta(\bar{\omega}_4)\\ &= \left\{\begin{array}{l} \frac{1}{\sqrt{2}}\,|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{I} + \frac{1}{\sqrt{2}}\,|1\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{I},\\ \frac{1}{\sqrt{2}}\,|1\rangle\langle 1| \otimes |2\rangle\langle 2| \otimes \mathbf{X} + \frac{1}{\sqrt{2}}\,|1\rangle\langle 2| \otimes |2\rangle\langle 1| \otimes \mathbf{X},\\ \frac{1}{\sqrt{2}}\,|2\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathbf{Z} - \frac{1}{\sqrt{2}}\,|2\rangle\langle 2| \otimes |1\rangle\langle 2| \otimes \mathbf{Z},\\ \frac{1}{\sqrt{2}}\,|2\rangle\langle 1| \otimes |2\rangle\langle 2| \otimes \mathbf{Y} - \frac{1}{\sqrt{2}}\,|2\rangle\langle 2| \otimes |2\rangle\langle 1| \otimes \mathbf{Y} \end{array}\right\}.\end{aligned}$$

5. Synthesizing Super-operators of Path Formulas

Let $\mathrm{Sat}(\Phi)$ denote the satisfying set $\{s \in S : s \models \Phi\}$. From a bottom-up fashion (see Figure 1), $\mathrm{Sat}(\Phi)$ for the basic state formulas Φ can be directly calculated by a scan over the labelling function L on S. Whereas, for trace-quantifier and fidelity-quantifier formulas Φ, one has to know the SOVMs of the path formulas ϕ embedded in Φ, which is just the main task of this section. We first review the known method for synthesizing the super-operators of three kinds of atomic path formulas in QCTL$^+$. Then we reduce the conjunction and disjunction in atomic path formulas over the QMC to the time-unbounded until formula over a product QMC. Finally we synthesize the super-operators of the negation in atomic path formulas. Thereby, we synthesize the super-operators of all path formulas required in the syntax of QCTL$^+$. Based on them, we will decide the trace-quantifier and fidelity-quantifier formulas in the coming section.

5.1. Atomic path formulas

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 $\mathcal{P}_\Phi := \{\sum_{s\models\Phi} |s\rangle\langle s|\} \otimes \mathcal{I} = \{\sum_{s\models\Phi} |s\rangle\langle s| \otimes \mathbf{I}\}$. Utilizing the mixed form of the classical–quantum state $\rho = \sum_{s\in S} |s\rangle\langle s| \otimes \rho_s$, we have the decomposition

$$\rho = \sum_{s\models\Phi} |s\rangle\langle s| \otimes \rho_s + \sum_{s\not\models\Phi} |s\rangle\langle s| \otimes \rho_s = \mathcal{P}_\Phi(\rho) + \mathcal{P}_{\neg\Phi}(\rho) \tag{6}$$

for any state formula Φ. After an initial classical state s is fixed, the SOVMs of three kinds of path formulas can be obtained as follows.

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

$$\Delta(\mathrm{X}\,\Phi) = \Delta\left(\biguplus_{t\models\Phi} Cyl(s,t)\right) = \sum_{t\models\Phi}\Delta(s,t) = \sum_{t\models\Phi} Q(s,t). \tag{7a}$$

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

$$\begin{aligned}\Delta(\Phi_1\mathrm{U}^{\le k}\Phi_2) &= \Delta\left(\biguplus_{i=0}^{k}\left\{\omega\in Path\colon \omega(i)\models\Phi_2\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\ &= \sum_{i=0}^{k}\Delta\left(\left\{\omega\in Path\colon \omega(i)\models\Phi_2\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\ &= \sum_{i=0}^{k}\mathrm{tr}_C(\mathcal{P}_{\Phi_2}\circ(\mathcal{F}\circ\mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i\circ\mathcal{P}_s),\end{aligned} \tag{7b}$$

  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

$$\begin{aligned}\Delta(\Phi_1\mathrm{U}\,\Phi_2) &= \Delta\left(\biguplus_{i=0}^{\infty}\left\{\omega\in Path\colon \omega(i)\models\Phi_2\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\ &= \sum_{i=0}^{\infty}\Delta\left(\left\{\omega\in Path\colon \omega(i)\models\Phi_2\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\ &= \sum_{i=0}^{\infty}\mathrm{tr}_C(\mathcal{P}_{\Phi_2}\circ(\mathcal{F}\circ\mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i\circ\mathcal{P}_s).\end{aligned} \tag{7c}$$

For the latter two kinds, all satisfying paths ω can be classified upon the first time-stamp i that $\omega(i)\models\Phi_2$ and $\omega(j)\models\Phi_1$ for each $j<i$ (or equivalently the unique time-stamp i that $\omega(i)\models\Phi_2$ and $\omega(j)\models\Phi_1\wedge\neg\Phi_2$ for each $j<i$). Thereby, we can get the pairwise disjoint resulting sets $A_i=\{\omega\in Path\colon \omega(i)\models\Phi_2\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\}$, whose SOVMs are obtained as $\mathrm{tr}_C(\mathcal{P}_{\Phi_2}\circ(\mathcal{F}\circ\mathcal{P}_{\Phi_1\wedge\neg\Phi_2})^i\circ\mathcal{P}_s)$, respectively.

Example 5.1. *Consider the quantum Bernoulli factory protocol [22]. It goes as follows. Cary and David want to select a leader by coin tossing. Perhaps, the coin is biased. To make the selection fair, they adopt the trick of von Neumann [32] that tosses the coin twice. If the result is "head followed by tail", then Cary wins; if it is "tail followed by head", then David wins; otherwise (either "head followed by head" or "tail followed by tail") repeat the above process. In the quantum setting, we start with a state* $|\widehat{q_1\,q_2}\rangle$ *in the two-qubit Hilbert space; tossing the first (resp. second) coin is modelled by applying the Hadamard gate* H *to the first (resp. second) qubit; the event "head followed by tail" is measured by* $M_1=\{|1,2\rangle\langle 1,2|\}$*, the event "tail followed by head" is measured by* $M_2=\{|2,1\rangle\langle 2,1|\}$*, the complement event is measured by* $M_0=\{|1,1\rangle\langle 1,1|+|2,2\rangle\langle 2,2|\}$*, and together* $\{M_0,M_1,M_2\}$ *form a projective measurement [27, Subsection 2.2.5]. Overall, the protocol is summarized by the quantum program:*

```
|\widehat{q_1 q_2}⟩ :=?;
while M[q_1, q_2] = 0 do
    H[q_1];
    H[q_2];
if M[q_1, q_2] = 1 then return Cary;
if M[q_1, q_2] = 2 then return David;
```

and is expressed by the QMC $\mathfrak{C}_2 = (S, Q, L)$ in Figure 4. The state set S is $\{s_0, s_1, s_2, s_3, s_4\}$, in which s_3 is labelled with win_C (Cary wins), s_4 is labelled with win_D (David wins), and others have no label. The initial classical state s_0 prepares the initial quantum state $|\widehat{q_1 q_2}\rangle$. After measurement it is led to s_2, s_3 or s_4, the latter two are goal classical states. The state s_2 indicates that the coin would be tossed twice, i.e., applying H to q_1 and to q_2, returning to the state s_0 for a restart. The transition super-operator matrix Q is given by the following nonzero entries:

$$\begin{aligned}
Q(s_0, s_2) &= \{|1,1\rangle\langle 1,1| + |2,2\rangle\langle 2,2|\} = M_0, & Q(s_0, s_3) &= \{|1,2\rangle\langle 1,2|\} = M_1,\\
Q(s_0, s_4) &= \{|2,1\rangle\langle 2,1|\} = M_2, & Q(s_2, s_1) &= \{\mathbf{H} \otimes \mathbf{I}\} = H_1,\\
Q(s_1, s_0) &= \{\mathbf{I} \otimes \mathbf{H}\} = H_2, & Q(s_3, s_3) &= Q(s_4, s_4) = \{\mathbf{I} \otimes \mathbf{I}\} = \mathcal{I}.
\end{aligned}$$

We would like to use a single super-operator on $\mathcal{H}_{\mathrm{cq}}$, combining all super-operator entries, as:

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

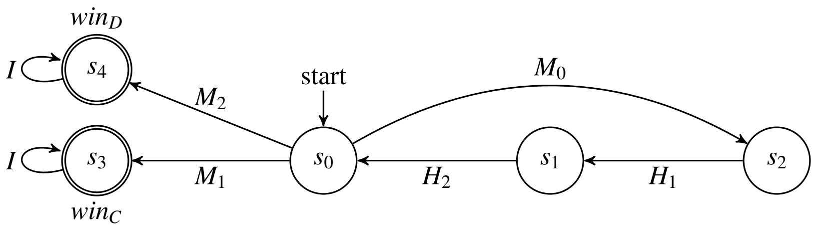

Figure 4: The QMC modelling the quantum Bernoulli factory protocol

After having fixed the initial classical state s_0, the SOVM space over Path can be established to check some interesting properties, say "Cary wins", i.e., $\Diamond\, win_C \equiv \mathrm{true}\, \mathrm{U}\, win_C$. To this end, we first define the projection super-operators $\mathcal{P}_{s_0} = \{|s_0\rangle\langle s_0| \otimes \mathbf{I}\}$, $\mathcal{P}_{win_C} = \{|s_3\rangle\langle s_3| \otimes \mathbf{I}\}$ and $\mathcal{P}_{\neg win_C} = \{(|s_0\rangle\langle s_0| + |s_1\rangle\langle s_1| + |s_2\rangle\langle s_2| + |s_4\rangle\langle s_4|) \otimes \mathbf{I}\}$, and therefore $\mathcal{F} \circ \mathcal{P}_{\neg win_C}$ is given by

$$\begin{aligned}
\{|s_2\rangle\langle s_0|\} \otimes Q(s_0, s_2) + \{|s_3\rangle\langle s_0|\} \otimes Q(s_0, s_3) + \{|s_4\rangle\langle s_0|\} \otimes Q(s_0, s_4) +\\
\{|s_0\rangle\langle s_1|\} \otimes Q(s_1, s_0) + \{|s_1\rangle\langle s_2|\} \otimes Q(s_2, s_1) + \{|s_4\rangle\langle s_4|\} \otimes Q(s_4, s_4).
\end{aligned}$$

The path set satisfying $\Diamond\, win_C$ can be classified as $A_i = \{\omega \in Path\colon \omega(i) \models win_C \wedge \bigwedge_{j=0}^{i-1} \omega(j) \models \neg win_C\}$ ($i \geq 0$), which are pairwise disjoint; their SOVMs are

$$\begin{aligned}
\Delta(A_0) &= \mathrm{tr}_C(\mathcal{P}_{win_C} \circ \mathcal{P}_{s_0}) = \mathrm{tr}_C(0) = 0,\\
\Delta(A_1) &= \mathrm{tr}_C(\mathcal{P}_{win_C} \circ (\mathcal{F} \circ \mathcal{P}_{\neg win_C}) \circ \mathcal{P}_{s_0}) = \mathrm{tr}_C(\{|s_3\rangle\langle s_0|\} \otimes Q(s_0, s_3))\\
&= Q(s_0, s_3) = \{|1,2\rangle\langle 1,2|\},
\end{aligned}$$

$$
\begin{aligned}
\Delta(A_2) &= \mathrm{tr}_C(\mathcal{P}_{win_C} \circ (\mathcal{F} \circ \mathcal{P}_{\neg win_C})^2 \circ \mathcal{P}_{s_0}) = \mathrm{tr}_C(0) = 0,\\
\Delta(A_3) &= \mathrm{tr}_C(\mathcal{P}_{win_C} \circ (\mathcal{F} \circ \mathcal{P}_{\neg win_C})^3 \circ \mathcal{P}_{s_0}) = \mathrm{tr}_C(0) = 0,\\
\Delta(A_4) &= \mathrm{tr}_C(\mathcal{P}_{win_C} \circ (\mathcal{F} \circ \mathcal{P}_{\neg win_C})^4 \circ \mathcal{P}_{s_0})\\
&= \mathrm{tr}_C(\{|s_3\rangle\langle s_0|\} \otimes (Q(s_0, s_3) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)))\\
&= Q(s_0, s_3) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2) = \{\tfrac{1}{2}\, |1, 2\rangle\langle 1, 1| - \tfrac{1}{2}\, |1, 2\rangle\langle 2, 2|\},
\end{aligned}
$$

and so on. Finally, the SOVM $\Delta(\Diamond\, win_C)$ is calculated as the infinite sum $\sum_{i=0}^{\infty} \Delta(A_i)$, which will be used to decide the trace-quantifier and fidelity-quantifier formulas in later, e.g. the nontermination event $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\neg\Diamond(win_C \vee win_D)]$. □

It is worth noticing that the SOVM (7c) is not in a closed form. To overcome it, we would phrase it using matrix series and rephrase it using matrix fraction. By Brouwer's fixed-point theorem [21, Chapter 4], the existence of bottom strongly connected component (BSCC) subspaces (defined below) implies the existence of *fixed-points* that $\mathcal{F} \circ \mathcal{P}_{\Phi_1 \wedge \neg \Phi_2}(\rho_{\mathrm{cq}}) = \rho_{\mathrm{cq}}$, which makes the resulting matrix series divergent. Hence, before using matrix fraction, it is necessary to remove all BSCC subspaces with respect to $\mathcal{F}_{\Phi_1 \wedge \neg \Phi_2} := \mathcal{F} \circ \mathcal{P}_{\Phi_1 \wedge \neg \Phi_2}$. Recall that:

Definition 5.2. *Given 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 a* 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 a* BSCC *if it is a bottom SCC.*

Lemma 5.3 ([34, Lemma 5.4]). *For the super-operator $\mathcal{F}_{\Phi_1 \wedge \neg \Phi_2}$, the direct-sum of all BSCC subspaces can be computed as*

$$\Gamma = \mathrm{span}(\{\mathrm{supp}(\gamma_i) \colon i \in [m]\}), \tag{8}$$

where γ_i ($i \in [m]$) are all linearly independent solutions to the stationary equation $\mathcal{F}_{\Phi_1 \wedge \neg \Phi_2}(\gamma) = \gamma$ ($\gamma = \gamma^\dagger \in \mathcal{L}_{\mathcal{H}}$).

In details, the stationary equation $\mathcal{E}(\gamma) = \gamma$ can be solved in $O(n^3 d^6)$ by Gaussian elimination, whose complexity is cubic in the number nd^2 of real variables in γ. The support $\mathrm{supp}(\gamma_i)$ of an individual solution γ_i can be computed in $O(n^3 d^3)$ by the Gram–Schmidt procedure, whose complexity is cubic in the dimension nd. In total, they are in $O(mn^3 d^3) \subseteq O(n^4 d^5)$ as m is bounded by nd^2, and the complexity of computing the direct-sum of all BSCC subspaces is in $O(N^6)$ where $N = nd$ is the dimension of $\mathcal{H}_{\mathrm{cq}}$. The resulting projectors $\mathbf{P}_\Gamma$ and $\mathbf{P}_{\Gamma^\perp} = \mathbf{I}_{\mathcal{H}_{\mathrm{cq}}} - \mathbf{P}_\Gamma$ are 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 on $\mathcal{H}$.

Example 5.4. *Reconsider the event $\Diamond\, win_C$ over the QMC $\mathfrak{C}_2$ in Example 5.1. The repeated super-operator of the SOVM is $\mathcal{F}_{\neg win_C} := \mathcal{F} \circ \mathcal{P}_{\neg win_C}$ which has been obtained. We solve the stationary equation $\mathcal{F}_{\neg win_C}(\gamma) = \gamma$ where $\gamma = \sum_{s \in S} |s\rangle\langle s| \otimes \gamma_s$ and $\gamma_s = \gamma_s^\dagger \in \mathcal{L}_{\mathcal{H}}$, and obtain the* 5 *linearly independent solutions:*

$$
\begin{aligned}
\gamma_1 = {} & |s_0\rangle\langle s_0| \otimes \tfrac{1}{2}[|1, 1\rangle\langle 1, 1| + |1, 1\rangle\langle 2, 2| + |2, 2\rangle\langle 1, 1| + |2, 2\rangle\langle 2, 2|] +\\
& |s_1\rangle\langle s_1| \otimes \tfrac{1}{2}[|1, +\rangle\langle 1, +| + |1, +\rangle\langle 2, -| + |2, -\rangle\langle 1, +| + |2, -\rangle\langle 2, -|] +\\
& |s_2\rangle\langle s_2| \otimes \tfrac{1}{2}[|1, 1\rangle\langle 1, 1| + |1, 1\rangle\langle 2, 2| + |2, 2\rangle\langle 1, 1| + |2, 2\rangle\langle 2, 2|],\\
\gamma_2 = {} & |s_4\rangle\langle s_4| \otimes |1, 1\rangle\langle 1, 1|,\\
\gamma_3 = {} & |s_4\rangle\langle s_4| \otimes |1, 2\rangle\langle 1, 2|,\\
\gamma_4 = {} & |s_4\rangle\langle s_4| \otimes |2, 1\rangle\langle 2, 1|,\\
\gamma_5 = {} & |s_4\rangle\langle s_4| \otimes |2, 2\rangle\langle 2, 2|.
\end{aligned}
$$

Then the BSCC subspaces Γ *covering all the fixed points of* $\mathcal{F}_{\neg win_C}$ *is* $\mathrm{span}(\mathrm{supp}(\gamma_1) \cup \mathrm{supp}(\gamma_2) \cup \mathrm{supp}(\gamma_3) \cup \mathrm{supp}(\gamma_4) \cup \mathrm{supp}(\gamma_5))$*, in which*

$$\begin{aligned}
\mathrm{supp}(\gamma_1) &= \mathrm{span}(\{|s_0\rangle \otimes [|1,1\rangle + |2,2\rangle], |s_1\rangle \otimes [|1,+\rangle + |2,-\rangle], |s_2\rangle \otimes [|1,1\rangle + |2,2\rangle]\}),\\
\mathrm{supp}(\gamma_2) &= \mathrm{span}(\{|s_4\rangle \otimes |1,1\rangle\}),\\
\mathrm{supp}(\gamma_3) &= \mathrm{span}(\{|s_4\rangle \otimes |1,2\rangle\}),\\
\mathrm{supp}(\gamma_4) &= \mathrm{span}(\{|s_4\rangle \otimes |2,1\rangle\}),\\
\mathrm{supp}(\gamma_5) &= \mathrm{span}(\{|s_4\rangle \otimes |2,2\rangle\}).
\end{aligned}$$

The projection super-operator $\mathcal{P}_\Gamma = \{\mathbf{P}_\Gamma\}$ *onto* Γ *is given by the projector* $\mathbf{P}_\Gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 + \gamma_5$ *as all eigenvectors (with respect to nonzero eigenvalues) of those* γ_i *are orthonormal; the projection super-operator* $\mathcal{P}_{\Gamma^\perp} = \{\mathbf{P}_{\Gamma^\perp}\}$ *onto the orthogonal complement* $\Gamma^\perp$ *of* Γ *is given by* $\mathbf{P}_{\Gamma^\perp} = \mathbf{I}_{\mathcal{H}_{\mathrm{cq}}} - \mathbf{P}_\Gamma$*. Thereby, the composite super-operator* $\mathcal{F}_{\neg win_C} \circ \mathcal{P}_{\Gamma^\perp}$ *is*

$$\{|s_2\rangle\langle s_0| \otimes \mathbf{E}_{0,2}, |s_3\rangle\langle s_0| \otimes \mathbf{E}_{0,3}, |s_4\rangle\langle s_0| \otimes \mathbf{E}_{0,4}, |s_0\rangle\langle s_1| \otimes \mathbf{E}_{1,0}, |s_1\rangle\langle s_2| \otimes \mathbf{E}_{2,1}\},$$

in which

$$\begin{aligned}
\mathbf{E}_{0,2} &= \tfrac{1}{2}[|1,1\rangle\langle 1,1| - |1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|],\\
\mathbf{E}_{0,3} &= |1,2\rangle\langle 1,2|\,,\\
\mathbf{E}_{0,4} &= |2,1\rangle\langle 2,1|\,,\\
\mathbf{E}_{1,0} &= \tfrac{1}{2}[|1,1\rangle\langle 1,+| + |2,2\rangle\langle 2,-| - |1,1\rangle\langle 2,-| - |2,2\rangle\langle 1,+|] + |1,1\rangle\langle 2,-| + |2,1\rangle\langle 2,+|\,,\\
\mathbf{E}_{2,1} &= \tfrac{1}{2}[|+,1\rangle\langle 1,1| - |+,1\rangle\langle 2,2| - |-,2\rangle\langle 1,1| + |-,2\rangle\langle 2,2|] + |+,2\rangle\langle 1,2| + |-,1\rangle\langle 2,1|\,;
\end{aligned}$$

it has no fixed-point. □

The following lemma indicates that the desired SOVM is preserved after all BSCC subspaces are removed.

Lemma 5.5 ([34, 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* $i \geq 0$*, where* Γ *is the direct-sum of all BSCC subspaces with respect to* $\mathcal{F}_{\Phi_1 \wedge \neg\Phi_2}$*.*

We proceed to explicitly represent the SOVMs (7) using POVMs and matrices. Recall from [37, Definition 2.2] that a super-operator $\mathcal{E} = \{\mathbf{E}_\ell : \ell \in [m]\}$ has the matrix representation

$$\mathrm{S2M}(\mathcal{E}) := \sum_{\ell \in [m]} \mathbf{E}_\ell \otimes \mathbf{E}_\ell^*, \tag{9}$$

where $*$ denotes entrywise complex conjugate. Let

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

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

Here, S2M, L2V and V2L are read as "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.

- Supposing $Q(s,t) = \{\mathbf{Q}_{s,t,\ell} \colon \ell \in [L_{s,t}]\}$ in Kraus representation, where $L_{s,t}$ is the number of Kraus operators, the POVM and the matrix representation of the SOVM (7a) are

$$\mathrm{S2M}(\Delta(\mathrm{X}\,\Phi)) = \sum_{t \models \Phi} \sum_{\ell \in [L_{s,t}]} \mathbf{Q}_{s,t,\ell} \otimes \mathbf{Q}^*_{s,t,\ell}, \tag{10a}$$

$$\Lambda(\mathrm{X}\,\Phi) = \sum_{t \models \Phi} \sum_{\ell \in [L_{s,t}]} \mathbf{Q}^\dagger_{s,t,\ell} \mathbf{Q}^{\mathrm{T}}_{s,t,\ell}. \tag{10b}$$

- Supposing $\mathcal{F}_{\Phi_1 \wedge \neg \Phi_2} \circ \mathcal{P}_{\Gamma^\perp} = \bigcup_{u,v \in S} \{|v\rangle\langle u| \otimes \mathbf{F}_{u,v,\ell} \colon \ell \in [L_{u,v}]\}$, the matrix representation of the SOVM (7b) is

$$\begin{aligned}\mathrm{S2M}(\Delta(\Phi_1 \,\mathrm{U}^{\leq k} \Phi_2)) &= \sum_{t \models \Phi_2} \sum_{i=0}^{k} (\langle t| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \mathbb{M}^i (|s\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \\ &= \sum_{t \models \Phi_2} (\langle t| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) [\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}^{k+1}][\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}]^{-1} (|s\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}),\end{aligned} \tag{10c}$$

  where $\mathbb{M} = \sum_{u,v \in S} \sum_{\ell \in [L_{u,v}]} |v\rangle\langle u| \otimes \mathbf{F}_{u,v,\ell} \otimes \mathbf{F}^*_{u,v,\ell}$ is adapted to the vector representation $\sum_{s \in S} |s\rangle \otimes \mathrm{L2V}(\rho_s)$ of the state ρ.

- The matrix representation of the SOVM (7c) is

$$\begin{aligned}\mathrm{S2M}(\Delta(\Phi_1 \,\mathrm{U}\, \Phi_2)) &= \sum_{t \models \Phi_2} \sum_{i=0}^{\infty} (\langle t| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \mathbb{M}^i (|s\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \\ &= \sum_{t \models \Phi_2} (\langle t| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) [\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}]^{-1} (|s\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}).\end{aligned} \tag{10d}$$

Anyway, the POVMs can be analogously obtained as $\Lambda(\phi) = \Delta(\phi)^\dagger(\mathbf{I})$.

Example 5.6. *In Example 5.4, we have obtained the repeated super-operator $\mathcal{F}_{\neg win_C}$ and the corresponding BSCC subspaces Γ for the event "Cary wins" specified by the path formula $\phi = \Diamond\, win_C$. Then the matrix representation of $\mathcal{F}_{\neg win_C} \circ \mathcal{P}_{\Gamma^\perp}$ is*

$$\begin{aligned}\mathbb{M} = {} & |s_2\rangle\langle s_0| \otimes \mathbf{E}_{0,2} \otimes \mathbf{E}^*_{0,2} + |s_3\rangle\langle s_0| \otimes \mathbf{E}_{0,3} \otimes \mathbf{E}^*_{0,3} + |s_4\rangle\langle s_0| \otimes \mathbf{E}_{0,4} \otimes \mathbf{E}^*_{0,4} + \\ & |s_0\rangle\langle s_1| \otimes \mathbf{E}_{1,0} \otimes \mathbf{E}^*_{1,0} + |s_1\rangle\langle s_2| \otimes \mathbf{E}_{2,1} \otimes \mathbf{E}^*_{2,1}.\end{aligned}$$

The eigenvalues of $\mathbb{M}$ are 0 of multiplicity 80. Since $\mathbb{M}$ has no eigenvalue 1, the inverse of $\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}$ is well-defined. Finally, the explicit matrix representation $\mathrm{S2M}(\Delta(\phi))$ of $\Delta(\phi)$ is obtained as

$$\begin{aligned}& (\langle s_3| \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) [\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M}]^{-1} (|s_0\rangle \otimes \mathbf{I}_{\mathcal{H}\otimes\mathcal{H}}) \\ = {} & \tfrac{1}{4} |1,2\rangle\langle 1,1| \otimes |1,2\rangle\langle 1,1| - \tfrac{1}{4} |1,2\rangle\langle 1,1| \otimes |1,2\rangle\langle 2,2| + \tfrac{1}{4} |1,2\rangle\langle 2,2| \otimes |1,2\rangle\langle 2,2| - \\ & \tfrac{1}{4} |1,2\rangle\langle 2,2| \otimes |1,2\rangle\langle 1,1| + |1,2\rangle\langle 1,2| \otimes |1,2\rangle\langle 1,2|.\end{aligned}$$

Moreover, we can get the POVM $\Lambda(\phi)$ as

$$\begin{aligned}\Delta(\phi)^\dagger(\mathbf{I}_{\mathcal{H}}) &= \mathrm{V2L}(\mathrm{S2M}(\Delta^\dagger(\phi))\mathrm{L2V}(\mathbf{I}_{\mathcal{H}})) \\ &= \mathrm{V2L}((\mathrm{S2M}(\Delta(\phi)))^\dagger \mathrm{L2V}(\mathbf{I}_{\mathcal{H}})) \\ &= \tfrac{1}{4} |1,1\rangle\langle 1,1| - \tfrac{1}{4} |1,1\rangle\langle 2,2| - \tfrac{1}{4} |2,2\rangle\langle 1,1| + \tfrac{1}{4} |2,2\rangle\langle 2,2| + |1,2\rangle\langle 1,2|,\end{aligned}$$

where the second equation follows from the identity $\mathrm{S2M}(\Delta^\dagger(\phi)) = (\mathrm{S2M}(\Delta(\phi)))^\dagger$. $\square$

Utilizing the facts that for a matrix $\mathbb{M}$ and a time bound k,

- it is in polynomial time with respect to $\|\mathbb{M}\|$ and linear time with respect to $\lceil \log_2(k+1) \rceil \leq \|\phi\|$ to compute the matrix power $\mathbb{M}^k$, and
- it is in polynomial time with respect to $\|\mathbb{M}\|$ to compute the matrix series $(\mathbf{I}_{\mathcal{H}_{\mathrm{cq}}\otimes\mathcal{H}} - \mathbb{M})^{-1} = \sum_{i=0}^{\infty} \mathbb{M}^i$ if $\mathbb{M}$ has no eigenvalue 1,

we obtain:

Theorem 5.7 ([35, 34]). *The matrix representation of the SOVM $\Delta(\phi)$ and the POVM $\Lambda(\phi)$ for the atomic path formulas ϕ in QCTL$^+$ can be synthesized in time polynomial in the size of $\mathfrak{C}$ and linear in the size of ϕ.*

5.2. Conjunction and disjunction in atomic path formulas

Here we consider how to reduce the conjunction and disjunction in atomic path formulas to a time-unbounded until formula over a product QMC. We first show the reduction on a single conjunction or a single disjunction of two time-unbounded until formulas, then generalize it to the *arbitrary* conjunction and disjunction of finitely many time-unbounded until formulas, and even to the *arbitrary* conjunction and disjunction of finitely many *arbitrary* atomic path formulas.

Classical states s in a QMC $\mathfrak{C}$ are static information that cannot record dynamical behavior along with a path ω of $\mathfrak{C}$. To record dynamical information, we introduce the product state structure, saying $(s, \Phi_{1,3})$ for a conjunction of two time-unbounded until formulas $\phi_1 = \Phi_1 \mathrm{U}\, \Phi_2$ and $\phi_2 = \Phi_3 \mathrm{U}\, \Phi_4$, in which the auxiliary information $\Phi_{1,3}$ is used to record the $(\Phi_1 \wedge \Phi_3)$-states we are in and the Φ_2- and the Φ_4-states are expected to be reached along with ω, i.e., the path formulas ϕ_1 and ϕ_2 whose truth are undetermined at the current state s along with ω. Once one of the two time-unbounded formulas, saying ϕ_1, is satisfied, (s, Φ_3) would be introduced to record the Φ_3-states we are in and the Φ_4-states are expected to be reached. More formally, we construct:

Definition 5.8. *Given a QMC $\mathfrak{C} = (S, Q, L)$ and a conjunction of two time-unbounded until formulas $\phi_1 = \Phi_1 \mathrm{U}\, \Phi_2$ and $\phi_2 = \Phi_3 \mathrm{U}\, \Phi_4$, their* product QMC *$\hat{\mathfrak{C}}$ is the pair $(\hat{S}, \hat{Q})$, where*

- *$\hat{S}$ is the finite state set*

$$\{\bot, \top\} \cup \{(s, \Phi_{1,3}) \colon s \in S\} \cup \{(s, \Phi_3) \colon s \in S\} \cup \{(s, \Phi_1) \colon s \in S\},$$

- *$\hat{Q} \colon \hat{S} \times \hat{S} \to \mathcal{S}^{\lesssim \mathcal{I}}$ is a transition super-operator matrix given by*

$$\text{(i)}\ \frac{}{\hat{Q}(\bot, \bot) = \mathcal{I}} \qquad \text{(ii)}\ \frac{}{\hat{Q}(\top, \top) = \mathcal{I}}$$

$$\text{(iii)}\ \frac{}{\hat{Q}((s, \Phi_{1,3}), \bot) = \sum\{|Q(s,t) \colon t \models (\neg\Phi_1 \wedge \neg\Phi_2 \vee \neg\Phi_3 \wedge \neg\Phi_4)|\}}$$

$$\text{(iv)}\ \frac{t \models (\Phi_1 \wedge \neg\Phi_2 \wedge \Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_{1,3})) = Q(s,t)} \qquad \text{(v)}\ \frac{t \models (\Phi_2 \wedge \Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_3)) = Q(s,t)}$$

$$\text{(vi)}\ \frac{t \models (\Phi_1 \wedge \neg\Phi_2 \wedge \Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_1)) = Q(s,t)} \qquad \text{(vii)}\ \frac{}{\hat{Q}((s, \Phi_{1,3}), \top) = \sum\{|Q(s,t) \colon t \models (\Phi_2 \wedge \Phi_4)|\}}$$

$$\text{(viii)}\ \frac{}{\hat{Q}((s,\Phi_3),\bot) = \sum\{|Q(s,t)\colon t \models (\neg\Phi_3 \wedge \neg\Phi_4)|\}}$$

$$\text{(ix)}\ \frac{t \models (\Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s,\Phi_3),(t,\Phi_3)) = Q(s,t)} \qquad \text{(x)}\ \frac{}{\hat{Q}((s,\Phi_3),\top) = \sum\{|Q(s,t)\colon t \models \Phi_4|\}}$$

$$\text{(xi)}\ \frac{}{\hat{Q}((s,\Phi_1),\bot) = \sum\{|Q(s,t)\colon t \models (\neg\Phi_1 \wedge \neg\Phi_2)|\}}$$

$$\text{(xii)}\ \frac{t \models (\Phi_1 \wedge \neg\Phi_2)}{\hat{Q}((s,\Phi_1),(t,\Phi_1)) = Q(s,t)} \qquad \text{(xiii)}\ \frac{}{\hat{Q}((s,\Phi_1),\top) = \sum\{|Q(s,t)\colon t \models \Phi_2|\}},$$

where $\sum\{|\ \cdot\ |\}$ denotes the summation over the multiset $\{|\ \cdot\ |\}$. (We employ the priority on Boolean connectives that '$\neg$' $\prec$ '$\wedge$' $\prec$ '$\vee$' in this paper.)

In the product construction, the special state $\bot$ indicates the event that either ϕ_1 or ϕ_2 is unsatisfiable; the special state $\top$ represents that both ϕ_1 and ϕ_2 have already been satisfied; the state $(s,\Phi_{1,3})$ represents that ϕ_1 and ϕ_2 are undetermined; (s,Φ_3) represents that ϕ_1 is already satisfied while ϕ_2 is undetermined; (s,Φ_1) represents that ϕ_2 is already satisfied while ϕ_1 is undetermined. There are 13 rules to define the transition super-operator matrix $\hat{Q}$:

- Rules (i)–(ii) characterize that $\bot$ and $\top$ are absorbing states.
- Rules (iii)–(vii) give all possible successors of $(s,\Phi_{1,3})$, depending on the satisfaction relations $t \models \Phi_1$, $t \models \Phi_2$, $t \models \Phi_3$ and $t \models \Phi_4$. Particularly, if the successor $t \models (\neg\Phi_1 \wedge \neg\Phi_2 \vee \neg\Phi_3 \wedge \neg\Phi_4)$, we can infer that the current path refutes ϕ_1 or ϕ_2, leading to the state $\bot$. As there might be more than one dissatisfying successor t, we collect those super-operators as the weight $\hat{Q}((s,\Phi_{1,3}),\bot)$ of the transition by a summation over the multiset, i.e., $\sum\{|Q(s,t)\colon t \models (\neg\Phi_1 \wedge \neg\Phi_2 \vee \neg\Phi_3 \wedge \neg\Phi_4)|\}$.
- Rules (viii)–(x) give all possible successors of (s,Φ_3), depending on the satisfaction relations $t \models \Phi_3$ and $t \models \Phi_4$.
- Rules (xi)–(xiii) give all possible successors of (s,Φ_1), depending on the satisfaction relations $t \models \Phi_1$ and $t \models \Phi_2$.

It is not hard to see $\sum_{\hat{t}\in\hat{S}} \hat{Q}(\hat{s},\hat{t}) \eqsim \mathcal{I}$ for each $\hat{s} \in \hat{S}$. The initial state is supposed to be of the type $(s,\Phi_{1,3})$, i.e., both ϕ_1 and ϕ_2 have undetermined truth at s unless it is trivial.

Example 5.9. *Reconsider the QMC $\mathfrak{C}_2 = (S,Q,L)$ shown in Figure 4. Cary and David play three rounds of the coin-tossing game on the original basis, whose outcomes determine the winner by the principle of majority. It can be modeled by the following QMC $\mathfrak{C}_3 = (S,Q,L)$ in Figure 5, where states s_3, s_8, s_{13} are labelled with win_C, states s_4, s_9, s_{14} are labelled with win_D, which means Cary or David wins the current round, respectively.*

Both Cary and David want to know the measure that they could win the game at least once. The event is specified by the conjunction of two path formulas $\phi_1 = \mathrm{true}\,\mathrm{U}\,win_C$ and $\phi_2 = \mathrm{true}\,\mathrm{U}\,win_D$. To this end, we construct the product QMC $\mathfrak{C} = (\hat{S},\hat{Q})$, in which

- *the state set $\hat{S}$ is $\{\bot,\top\} \cup \{(s_i,\Phi_{1,3})\colon 0 \le i \le 14\} \cup \{(s_i,\Phi_3)\colon 0 \le i \le 14\} \cup \{(s_i,\Phi_1)\colon 0 \le i \le 14\}$ with $(s_0,\Phi_{1,3})$ being the initial one, and*
- *the transition super-operator matrix $\hat{Q}$ is given by the following nonzero entries:*

$$\begin{aligned}\hat{Q}((s_0,\Phi_{1,3}),(s_2,\Phi_{1,3})) &= \hat{Q}((s_5,\Phi_3),(s_7,\Phi_3)) = \hat{Q}((s_5,\Phi_1),(s_7,\Phi_1)) \\ &= \hat{Q}((s_{10},\Phi_3),(s_{12},\Phi_3)) = \hat{Q}((s_{10},\Phi_1),(s_{12},\Phi_1)) = M_0,\end{aligned}$$

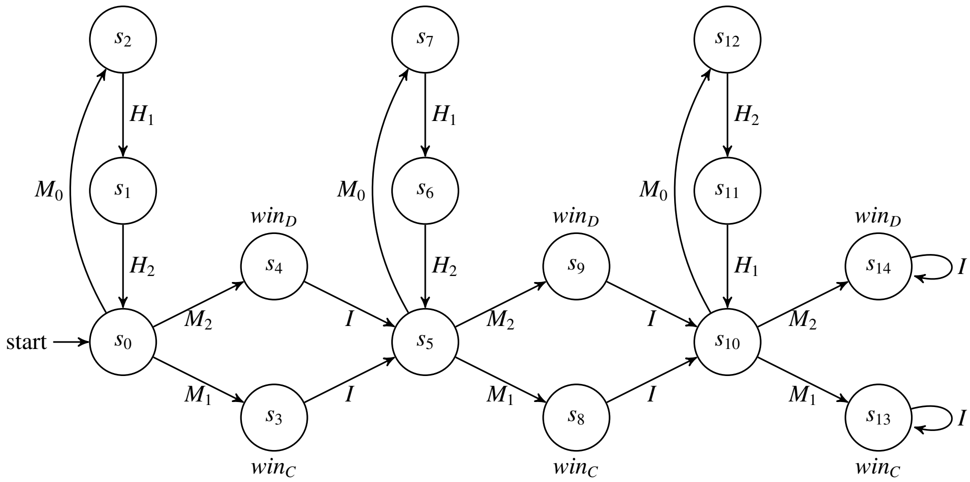

Figure 5: QMC for 3 rounds of the coin-tossing game

$$
\begin{aligned}
\hat{Q}((s_0,\Phi_{1,3}),(s_3,\Phi_3)) &= \hat{Q}((s_5,\Phi_3),(s_8,\Phi_3)) = \hat{Q}((s_5,\Phi_1),\ \top) \\
&= \hat{Q}((s_{10},\Phi_3),(s_{13},\Phi_3)) = \hat{Q}((s_{10},\Phi_1),\ \top) = M_1, \\
\hat{Q}((s_0,\Phi_{1,3}),(s_4,\Phi_1)) &= \hat{Q}((s_5,\Phi_1),(s_9,\Phi_1)) = \hat{Q}((s_5,\Phi_3),\ \top) \\
&= \hat{Q}((s_{10},\Phi_1),(s_{14},\Phi_1)) = \hat{Q}((s_{10},\Phi_3),\ \top) = M_2, \\
\hat{Q}((s_2,\Phi_{1,3}),(s_1,\Phi_{1,3})) &= \hat{Q}((s_7,\Phi_3),(s_6,\Phi_3)) = \hat{Q}((s_7,\Phi_1),(s_6,\Phi_1)) \\
&= \hat{Q}((s_{12},\Phi_3),(s_{11},\Phi_3)) = \hat{Q}((s_{12},\Phi_1),(s_{11},\Phi_1)) = H_1, \\
\hat{Q}((s_1,\Phi_{1,3}),(s_0,\Phi_{1,3})) &= \hat{Q}((s_6,\Phi_3),(s_5,\Phi_3)) = \hat{Q}((s_6,\Phi_1),(s_5,\Phi_1)) \\
&= \hat{Q}((s_{11},\Phi_3),(s_{10},\Phi_3)) = \hat{Q}((s_{11},\Phi_1),(s_{10},\Phi_1)) = H_2, \\
\hat{Q}((s_3,\Phi_3),(s_5,\Phi_3)) &= \hat{Q}((s_4,\Phi_1),(s_5,\Phi_1)) = \hat{Q}((s_8,\Phi_3),(s_{10},\Phi_3)) \\
&= \hat{Q}((s_9,\Phi_1),(s_{10},\Phi_1)) = \hat{Q}((s_{13},\Phi_3),(s_{13},\Phi_3)) \\
&= \hat{Q}((s_{14},\Phi_1),(s_{14},\Phi_1)) = \mathcal{I},
\end{aligned}
$$

where the super-operators M_0, M_1, M_2, H_1 and H_2 are referred to Example 5.1.

The reachable part of $\mathfrak{C}_3$ is shown in Figure 6. Due to space limit, three absorbing states $\top$, (s_{13},Φ_3) and (s_{14},Φ_1) are marked as accepting ones that omit the self-loops labelled with $\mathcal{I}$. □

For a disjunction of two time-unbounded until formulas, the product state structure is similarly introduced. For instance, the auxiliary information $\Phi_{1,3}$ in the product state $(s,\Phi_{1,3})$ is used to record the $(\Phi_1 \wedge \Phi_3)$-states we are in and the Φ_2- or Φ_4-states are expected to be reached along with ω, i.e., the path formulas ϕ_1 and ϕ_2 whose truth are undetermined at the current state s along with ω. Once one of the two time-unbounded until formulas, saying ϕ_1, is dissatisfied, (s,Φ_3) would be introduced to record the Φ_3-states we are in and the Φ_4-states are expected to be reached. More formally, we construct:

Definition 5.10. *Given a QMC $\mathfrak{C} = (S, Q, L)$ and a disjunction of two time-unbounded until formulas $\phi_1 = \Phi_1 \mathrm{U}\, \Phi_2$ and $\phi_2 = \Phi_3 \mathrm{U}\, \Phi_4$, their* product QMC $\hat{\mathfrak{C}}$ *is the pair $(\hat{S}, \hat{Q})$, where*

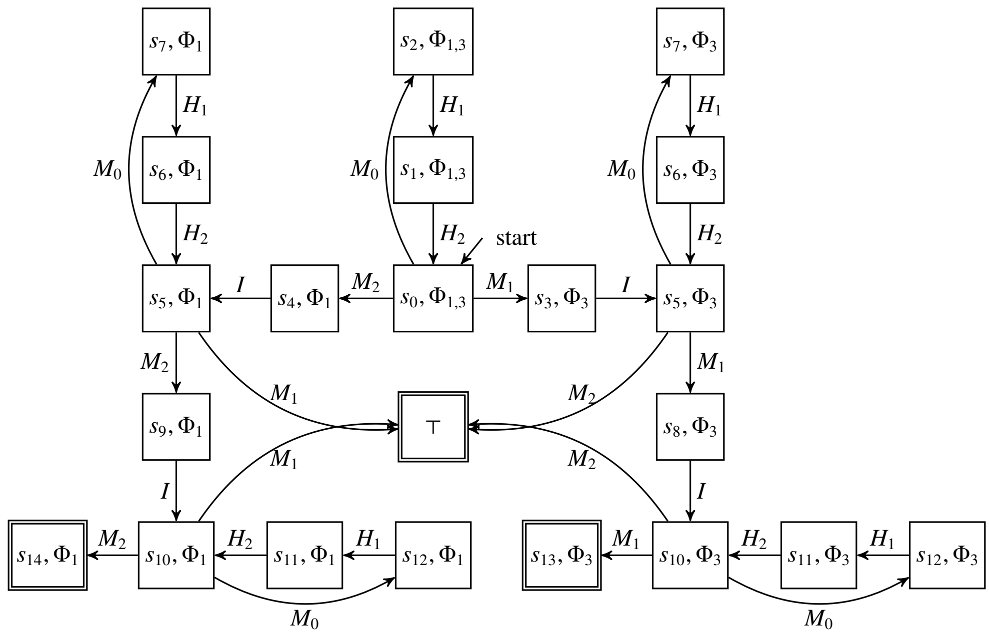

Figure 6: Product QMC for conjunction of two path formulas

- *$\hat{S}$ is the finite state set*

$$\{\bot, \top\} \cup \{(s, \Phi_{1,3}) \colon s \in S\} \cup \{(s, \Phi_3) \colon s \in S\} \cup \{(s, \Phi_1) \colon s \in S\},$$

- *$\hat{Q} \colon \hat{S} \times \hat{S} \to \mathcal{S}^{\lesssim \mathcal{I}}$ is a transition super-operator matrix given by*

$$\text{(i) } \frac{}{\hat{Q}(\bot, \bot) = \mathcal{I}} \qquad \text{(ii) } \frac{}{\hat{Q}(\top, \top) = \mathcal{I}}$$

$$\text{(iii) } \frac{}{\hat{Q}((s, \Phi_{1,3}), \bot) = \sum\{|Q(s,t) \colon t \models (\neg\Phi_1 \wedge \neg\Phi_2 \wedge \neg\Phi_3 \wedge \neg\Phi_4)|\}}$$

$$\text{(iv) } \frac{t \models (\Phi_1 \wedge \neg\Phi_2 \wedge \Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_{1,3})) = Q(s,t)} \qquad \text{(v) } \frac{t \models (\neg\Phi_1 \wedge \neg\Phi_2 \wedge \Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_3)) = Q(s,t)}$$

$$\text{(vi) } \frac{t \models (\Phi_1 \wedge \neg\Phi_2 \wedge \neg\Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_{1,3}), (t, \Phi_1)) = Q(s,t)} \qquad \text{(vii) } \frac{}{\hat{Q}((s, \Phi_{1,3}), \top) = \sum\{|Q(s,t) \colon t \models (\Phi_2 \vee \Phi_4)|\}}$$

$$\text{(viii) } \frac{}{\hat{Q}((s, \Phi_3), \bot) = \sum\{|Q(s,t) \colon t \models (\neg\Phi_3 \wedge \neg\Phi_4)|\}}$$

$$\text{(ix) } \frac{t \models (\Phi_3 \wedge \neg\Phi_4)}{\hat{Q}((s, \Phi_3), (t, \Phi_3)) = Q(s,t)} \qquad \text{(x) } \frac{}{\hat{Q}((s, \Phi_3), \top) = \sum\{|Q(s,t) \colon t \models \Phi_4|\}}$$

$$\text{(xi) } \frac{}{\hat{Q}((s, \Phi_1), \bot) = \sum\{|Q(s,t) \colon t \models (\neg\Phi_1 \wedge \neg\Phi_2)|\}}$$

$$\text{(xii) } \frac{t \models (\Phi_1 \wedge \neg\Phi_2)}{\hat{Q}((s, \Phi_1), (t, \Phi_1)) = Q(s,t)} \qquad \text{(xiii) } \frac{}{\hat{Q}((s, \Phi_1), \top) = \sum\{|Q(s,t) \colon t \models \Phi_2|\}}.$$

Let $[\![\phi]\!]$ denote the truth of a path formula ϕ. For a time-unbounded until formula ℓ, the truth $[\![\ell]\!]$ is determined along with some concrete path ω. During this process, there are three possible values “true” T, “undertermined” U and “false” F of $[\![\ell]\!]$. Initially, w.l.o.g., the value of $[\![\ell]\!]$ is U, which would be changed upon the encountered state $\omega(k)$. Specifically, it would be changed to be T if the finite path $\omega(0), \dots, \omega(k)$ satisfies ℓ, to be F if $\omega(0), \dots, \omega(k)$ refutes ℓ, and keep U otherwise. The truth $[\![\phi]\!]$ is correspondingly obtained as the conjunction and disjunction of $[\![\ell_j]\!]$ for all distinct time-unbounded until formulas ℓ_j in ϕ. Formally, we construct:

Definition 5.11. *Given a QMC $\mathfrak{C} = (S, Q, L)$ and a path formula $\phi(\ell_1, \dots, \ell_m)$ where ℓ_j ($j \in [m]$) denote all distinct time-unbounded until formulas $\Phi_{j,1} \mathrm{U}\, \Phi_{j,2}$ in ϕ, their* product QMC $\hat{\mathfrak{C}}$ *is the pair $(\hat{S}, \hat{Q})$, in which*

- *$\hat{S}$ is the finite state set*

$$\{\bot, \top\} \cup \{(s, [\![\ell_1]\!], \dots, [\![\ell_m]\!]) \colon s \in S \wedge \forall j \in [m] \colon [\![\ell_j]\!] \in \{\mathrm{T}, \mathrm{F}, \mathrm{U}\}\},$$

- *$\hat{Q} \colon \hat{S} \times \hat{S} \to \mathcal{S}^{\lesssim \mathcal{I}}$ is a transition super-operator matrix given by:*

$$\text{(i)}\ \frac{}{\hat{Q}(\bot, \bot) = \mathcal{I}} \qquad \text{(ii)}\ \frac{}{\hat{Q}(\top, \top) = \mathcal{I}}$$

$$\text{(iii)}\ \frac{\phi([\![\ell_1]\!], \dots, [\![\ell_m]\!]) = \mathrm{F}}{\hat{Q}((s, [\![\ell_1]\!], \dots, [\![\ell_m]\!]), \bot) = \mathcal{I}} \qquad \text{(iv)}\ \frac{\phi([\![\ell_1]\!], \dots, [\![\ell_m]\!]) = \mathrm{T}}{\hat{Q}((s, [\![\ell_1]\!], \dots, [\![\ell_m]\!]), \top) = \mathcal{I}}$$

$$\text{(v)}\ \frac{\phi([\![\ell_1]\!], \dots, [\![\ell_m]\!]) = \mathrm{U}}{\hat{Q}((s, [\![\ell_1]\!], \dots, [\![\ell_m]\!]), (t, \delta_1([\![\ell_1]\!], t), \dots, \delta_m([\![\ell_m]\!], t))) = Q(s, t)},$$

where for $j \in [m]$,

$$\delta_j([\![\ell_j]\!], t) = \begin{cases} \mathrm{F} & \text{if } [\![\ell_j]\!] = \mathrm{F} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models (\neg\Phi_{j,1} \wedge \neg\Phi_{j,2}), \\ \mathrm{U} & \text{if } [\![\ell_j]\!] = \mathrm{U} \wedge t \models (\Phi_{j,1} \wedge \neg\Phi_{j,2}), \\ \mathrm{T} & \text{if } [\![\ell_j]\!] = \mathrm{T} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models \Phi_{j,2}. \end{cases}$$

Lemma 5.12. *The SOVM $\Delta(\phi)$ in the QMC $\mathfrak{C} = (S, Q, L)$ is the SOVM $\Delta(\Diamond\top)$ in the product QMC $\hat{\mathfrak{C}} = (\hat{S}, \hat{Q})$ as in Definition 5.11, which can be constructed in time polynomial in the size of $\mathfrak{C}$ and exponential in the size of ϕ.*

Proof. We will show that the reduction preserves the SOVM in both directions. Let $\bar{\omega} = s_0, s_1, \dots, s_n$ be a minimal finite path of $\mathfrak{C}$ that satisfies ϕ. The term ‘minimal’ means there is no proper prefix of $\bar{\omega}$ that satisfies ϕ. Then we have that the truth $\phi([\![\ell_1]\!], \dots, [\![\ell_m]\!])$ of $\phi(\ell_1, \dots, \ell_m)$ is U for all proper prefixes of $\bar{\omega}$ and it is T for $\bar{\omega}$. So the states s in $\bar{\omega}$ equipped with the truth $[\![\ell_1]\!], \dots, [\![\ell_m]\!]$ upon prefixes of $\bar{\omega}$ are the product states $(s, [\![\ell_1]\!], \dots, [\![\ell_m]\!])$ in $\hat{\mathfrak{C}}$, all of which make up a minimal finite path of $\hat{\mathfrak{C}}$ that reaches $\top$ and has the same SOVM according the rules defining the transition super-operator matrix $\hat{Q}$. Conversely, for a minimal finite path of $\hat{\mathfrak{C}}$ that reaches $\top$, after removing the truth $[\![\ell_1]\!], \dots, [\![\ell_m]\!]$ in the product states $(s, [\![\ell_1]\!], \dots, [\![\ell_m]\!])$, we would get a minimal finite path of $\mathfrak{C}$ that satisfies ϕ and has the same SOVM. Hence the SOVM $\Delta(\phi)$ in $\mathfrak{C}$ is exactly the SOVM $\Delta(\Diamond\top)$ in $\hat{\mathfrak{C}}$.

Since the number of states in $\hat{\mathfrak{C}}$ is at most $3^m n + 2$ where $n = |S|$ and m is the number of disjunct time-unbounded until formulas, and the number of transitions is bounded polynomially in $3^m n$, each transition costs at most $O(\|Q\|)$ operations, the construction is in time polynomial in $\|\mathfrak{C}\|$ and exponential in $m \leq \|\phi\|$. □

Here, counting all paths that satisfy ϕ is not easier than counting all satisfying assignments to an arbitrary instance of the SAT problem, which is in **#P**, i.e., no polynomial-time algorithm is known yet. So the exponential hierarchy with respect to $\|\phi\|$ is tight.

Now we further tackle time-unbounded until formulas together with next formulas and time-bounded until formulas. Let TB denote the time bound of an atomic path formula ℓ, i.e.,

$$\mathrm{TB}(\ell) = \begin{cases} \infty & \textbf{if } \ell = \Phi_1 \mathrm{U}\, \Phi_2, \\ k & \textbf{if } \ell = \Phi_1 \mathrm{U}^{\leq k} \Phi_2, \\ 1 & \textbf{if } \ell = \mathrm{X}\, \Phi, \end{cases}$$

and K be the maximum of finite time bounds of atomic path formulas ℓ in ϕ. The product QMC of a general path formula is obtained from the one in Definition 5.11 by extending the transformation function $\tilde{\delta}$ that depends on the additional time variable k ranging over $\{0, \ldots, K, \infty\}$.

Example 5.13. *Consider three different atomic path formulas $\ell_1 = \mathrm{X}\, win_D$, $\ell_2 = \mathrm{true}\, \mathrm{U}^{\leq 5}\, win_D$, $\ell_3 = \mathrm{true}\, \mathrm{U}\, win_D$ and a concrete path $\omega = s_0, s_1, s_2, s_0, s_1, s_2, s_0, s_4, s_4, \ldots$ of the QMC $\mathfrak{C}_2 = (S, Q, L)$ shown in Figure 4. We describe all states equipped with the auxiliary information $[\![\ell_j]\!]$ ($j \in [3]$) as follows:*

- *Initially, ℓ_j ($j \in [3]$) have the truth* U*, as none of them has been satisfied or refuted by s_0, i.e., $[\![\ell_j]\!] = \mathrm{U}$;*
- *for time $k = 1$, upon the state $\omega(1) = s_1 \not\models win_D$ which refutes ℓ_1, the truth $[\![\ell_1]\!]$ of ℓ_1 changes to* F *and keeps* F *for all $k > 1$;*
- *the truth $[\![\ell_2]\!]$ of ℓ_2 keeps* U *until time $k = 5$, then upon the state $\omega(5) = s_2 \not\models win_D$ which refutes ℓ_2, the truth $[\![\ell_2]\!]$ changes to* F *and keeps* F *for all $k > 5$;*
- *the truth $[\![\ell_3]\!]$ of ℓ_3 keeps* U *until time $k = 7$, then upon the state $\omega(7) = s_4 \models win_D$ which satisfies ℓ_3, the truth $[\![\ell_3]\!]$ changes to* T *and keeps* T *for all $k > 7$.*

Thus, we can determine all involved product states $(s, k, [\![\ell_1]\!], [\![\ell_2]\!], [\![\ell_3]\!])$ using the above rules. For instance, when time k varies from 4 to 5, the product state $(s_1, 4, \mathrm{F}, \mathrm{U}, \mathrm{U})$ would be changed to $(s_2, 5, \mathrm{F}, \mathrm{F}, \mathrm{U})$. $\square$

More formally and completely, we construct:

Definition 5.14. *Given a QMC $\mathfrak{C} = (S, Q, L)$ and a path formula $\phi(\ell_1, \ldots, \ell_m)$ where ℓ_j ($j \in [m]$) denote all distinct atomic path formulas, their* product QMC *$\tilde{\mathfrak{C}}$ is the pair $(\tilde{S}, \tilde{Q})$, in which*

- *$\tilde{S}$ is the finite state set*

$$\{\bot, \top\} \cup \{(s, k, [\![\ell_1]\!], \ldots, [\![\ell_m]\!]) \colon s \in S \wedge k \in \{0, \ldots, K, \infty\} \wedge \bigwedge_{j=1}^{m} [\![\ell_j]\!] \in \{\mathrm{T}, \mathrm{F}, \mathrm{U}\}\},$$

- *$\tilde{Q} \colon \tilde{S} \times \tilde{S} \to \mathcal{S}^{\lesssim \mathcal{I}}$ is a transition super-operator matrix given by:*

$$\text{(i)}\ \frac{}{\hat{Q}(\bot, \bot) = \mathcal{I}} \qquad \text{(ii)}\ \frac{}{\hat{Q}(\top, \top) = \mathcal{I}}$$

$$\text{(iii)}\ \frac{\phi([\![\ell_1]\!],\ldots,[\![\ell_m]\!]) = \mathrm{F}}{\hat{Q}((s,k,[\![\ell_1]\!],\ldots,[\![\ell_m]\!]),\bot) = \mathcal{I}} \qquad \text{(iv)}\ \frac{\phi([\![\ell_1]\!],\ldots,[\![\ell_m]\!]) = \mathrm{T}}{\hat{Q}((s,k,[\![\ell_1]\!],\ldots,[\![\ell_m]\!]),\top) = \mathcal{I}}$$

$$\text{(v)}\ \frac{k < K, \phi([\![\ell_1]\!],\ldots,[\![\ell_m]\!]) = \mathrm{U}}{\hat{Q}((s,k,[\![\ell_1]\!],\ldots,[\![\ell_m]\!]),(t,k+1,\tilde{\delta}_1(k,[\![\ell_1]\!],t),\ldots,\tilde{\delta}_m(k,[\![\ell_m]\!],t))) = Q(s,t)}$$

$$\text{(vi)}\ \frac{k \geq K, \phi([\![\ell_1]\!],\ldots,[\![\ell_m]\!]) = \mathrm{U}}{\hat{Q}((s,k,[\![\ell_1]\!],\ldots,[\![\ell_m]\!]),(t,\infty,\tilde{\delta}_1(k,[\![\ell_1]\!],t),\ldots,\tilde{\delta}_m(k,[\![\ell_m]\!],t))) = Q(s,t)},$$

where for $j \in [m]$,

– *if ℓ_j is a next formula,*

$$\tilde{\delta}_j(k,[\![\ell_j]\!],t) = \begin{cases} \mathrm{F} & \text{if } [\![\ell_j]\!] = \mathrm{F} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models \neg\Phi, \\ \mathrm{T} & \text{if } [\![\ell_j]\!] = \mathrm{T} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models \Phi; \end{cases}$$

– *if ℓ_j is a time-bounded until formula,*

$$\tilde{\delta}_j(k,[\![\ell_j]\!],t) = \begin{cases} \mathrm{F} & \text{if } [\![\ell_j]\!] = \mathrm{F} \vee [\![\ell_j]\!] = \mathrm{U} \wedge \left[\begin{array}{l} k = \mathrm{TB}(\ell_j) \wedge t \models \neg\Phi_{j,2} \vee \\ k < \mathrm{TB}(\ell_j) \wedge t \models (\neg\Phi_{j,1} \wedge \neg\Phi_{j,2}) \end{array} \right], \\ \mathrm{U} & \text{if } [\![\ell_j]\!] = \mathrm{U} \wedge k < \mathrm{TB}(\ell_j) \wedge t \models (\Phi_{j,1} \wedge \neg\Phi_{j,2}), \\ \mathrm{T} & \text{if } [\![\ell_j]\!] = \mathrm{T} \vee [\![\ell_j]\!] = \mathrm{U} \wedge k \leq \mathrm{TB}(\ell_j) \wedge t \models \Phi_{j,2}; \end{cases}$$

– *if ℓ_j is a time-unbounded until formula,*

$$\tilde{\delta}_j(k,[\![\ell_j]\!],t) = \begin{cases} \mathrm{F} & \text{if } [\![\ell_j]\!] = \mathrm{F} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models (\neg\Phi_{j,1} \wedge \neg\Phi_{j,2}), \\ \mathrm{U} & \text{if } [\![\ell_j]\!] = \mathrm{U} \wedge t \models (\Phi_{j,1} \wedge \neg\Phi_{j,2}), \\ \mathrm{T} & \text{if } [\![\ell_j]\!] = \mathrm{T} \vee [\![\ell_j]\!] = \mathrm{U} \wedge t \models \Phi_{j,2}. \end{cases}$$

By noticing that the construction is at most $K + 2$ times of the product QMC $\hat{\mathfrak{C}} = (\hat{S}, \hat{Q})$, it follows from Lemma 5.12 that:

Corollary 5.15. *The SOVM $\Delta(\phi)$ in the QMC $\mathfrak{C} = (S, Q, L)$ is the SOVM $\Delta(\Diamond\top)$ in the product QMC $\tilde{\mathfrak{C}} = (\tilde{S}, \tilde{Q})$ as in Definition 5.14, which can be constructed in time polynomial in the size of $\mathfrak{C}$ and exponential in the size of ϕ.*

Combining Theorem 5.7 with Corollary 5.15, we obtain:

Theorem 5.16. *The matrix representation of the SOVM $\Delta(\phi)$ and the POVM $\Lambda(\phi)$ for the conjunction and disjunction ϕ of atomic path formulas in QCTL$^+$ can be synthesized in time polynomial in the size of $\mathfrak{C}$ and exponential in the size of ϕ.*

We have to address that the synthesis is in polynomial time when the size of ϕ is fixed, like the single conjunction and the single disjunction in the most common cases.

5.3. Negation in path formulas

In the previous subsection, we have reduced an arbitrary conjunction and disjunction in atomic path formulas over the QMC to an atomic path formula over a product QMC. Here we will synthesize the super-operators of the negation in atomic path formulas. That completes the super-operator synthesis of the path formulas required in the syntax of QCTL$^+$. For the negation of time-unbounded path formulas, it is necessary to consider the ultimate density operators that are the density operators at sufficiently large time. These ultimate density operators turn out to form a dense set, not a singleton. The super-operators of the negation of atomic path formulas are therefore synthesized conditionally.

After an initial classical state s is fixed, the SOVMs of the negation of three kinds of atomic path formulas can be obtained as follows.

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

$$\Delta(\neg(\mathrm{X}\,\Phi)) = \Delta\left(\biguplus_{t\not\models\Phi} Cyl(s,t)\right) = \sum_{t\not\models\Phi}\Delta(s,t) = \sum_{t\not\models\Phi} Q(s,t). \tag{11a}$$

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

$$\begin{aligned}
&\Delta(\neg(\Phi_1 \mathrm{U}^{\leq k}\Phi_2))\\
&= \Delta\left(\biguplus_{i=0}^{k-1}\left\{\omega\in Path\colon\, \omega(i)\models(\neg\Phi_1\wedge\neg\Phi_2)\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right.\\
&\qquad \left.\uplus\left\{\omega\in Path\colon\, \omega(k)\models\neg\Phi_2\wedge\bigwedge_{j=0}^{k-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\
&= \sum_{i=0}^{k-1}\Delta\left(\left\{\omega\in Path\colon\, \omega(i)\models(\neg\Phi_1\wedge\neg\Phi_2)\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\
&\qquad +\Delta\left(\left\{\omega\in Path\colon\, \omega(k)\models\neg\Phi_2\wedge\bigwedge_{j=0}^{k-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\
&= \sum_{i=0}^{k-1}\mathrm{tr}_C(\mathcal{P}_{\neg\Phi_1\wedge\neg\Phi_2}\circ\mathcal{F}^i_{\Phi_1\wedge\neg\Phi_2}\circ\mathcal{P}_s)+\mathrm{tr}_C(\mathcal{P}_{\neg\Phi_2}\circ\mathcal{F}^k_{\Phi_1\wedge\neg\Phi_2}\circ\mathcal{P}_s)\\
&= \Delta((\Phi_1\wedge\neg\Phi_2)\mathrm{U}^{\leq k-1}(\neg\Phi_1\wedge\neg\Phi_2))+\mathrm{tr}_C(\mathcal{P}_{\neg\Phi_2}\circ\mathcal{F}^k_{\Phi_1\wedge\neg\Phi_2}\circ\mathcal{P}_s).
\end{aligned}\tag{11b}$$

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

$$\begin{aligned}
&\Delta(\neg(\Phi_1 \mathrm{U}\,\Phi_2))\\
&= \Delta\left(\biguplus_{i=0}^{\infty}\left\{\omega\in Path\colon\, \omega(i)\models(\neg\Phi_1\wedge\neg\Phi_2)\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right.\\
&\qquad \left.\uplus\left\{\omega\in Path\colon\, \bigwedge_{j=0}^{\infty}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\
&= \sum_{i=0}^{\infty}\Delta\left(\left\{\omega\in Path\colon\, \omega(i)\models(\neg\Phi_1\wedge\neg\Phi_2)\wedge\bigwedge_{j=0}^{i-1}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)\\
&\qquad +\Delta\left(\left\{\omega\in Path\colon\, \bigwedge_{j=0}^{\infty}\omega(j)\models(\Phi_1\wedge\neg\Phi_2)\right\}\right)
\end{aligned}$$

$$= \sum_{i=0}^{\infty} \mathrm{tr}_C(\mathcal{P}_{\neg\Phi_1\wedge\neg\Phi_2} \circ \mathcal{F}^i_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_s) + \mathrm{tr}_C(\mathcal{F}^\infty_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_s)$$

$$= \Delta((\Phi_1 \wedge \neg\Phi_2)\mathrm{U}\,(\neg\Phi_1 \wedge \neg\Phi_2)) + \mathrm{tr}_C(\mathcal{F}^\infty_{\Phi_1\wedge\neg\Phi_2} \circ \mathcal{P}_s). \tag{11c}$$

Example 5.17. *Again, continued to consider Example 5.1, we now calculate the SOVMs for the path formulas $\phi_1 = \neg(\mathrm{true}\,\mathrm{U}^{\leq 4} win_C)$ and $\phi_2 = \neg(\mathrm{true}\,\mathrm{U}\, win_C)$. For the former, we have*

$$\begin{aligned}\Delta(\phi_1) &= \Delta((\mathrm{true} \wedge \neg win_C)\mathrm{U}^{\leq 3}(\mathrm{false} \wedge \neg win_C)) + \mathrm{tr}_C(\mathcal{P}_{\neg win_C} \circ \mathcal{F}^4_{\mathrm{true}\wedge\neg win_C} \circ \mathcal{P}_{s_0})\\ &= \Delta(\neg win_C\,\mathrm{U}^{\leq 3}\mathrm{false}) + \mathrm{tr}_C(\mathcal{P}_{\neg win_C} \circ \mathcal{F}^4_{\neg win_C} \circ \mathcal{P}_{s_0})\\ &= \mathrm{tr}_C(\mathcal{P}_{\neg win_C} \circ \mathcal{F}^4_{\neg win_C} \circ \mathcal{P}_{s_0}).\end{aligned}$$

By calculating $\Delta(A_4)$ in Example 5.1, we have seen

$$\begin{aligned}\mathcal{F}^4_{\neg win_C} \circ \mathcal{P}_{s_0} = {} & \{|s_2\rangle\langle s_0|\} \otimes (Q(s_0, s_2) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)) +\\ & \{|s_3\rangle\langle s_0|\} \otimes (Q(s_0, s_3) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)) +\\ & \{|s_4\rangle\langle s_0|\} \otimes (Q(s_0, s_4) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)) +\\ & \{|s_4\rangle\langle s_0|\} \otimes (Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_0, s_4)).\end{aligned}$$

So, we get

$$\begin{aligned}\Delta(\phi_1) &= \mathrm{tr}_C(\{|s_2\rangle\langle s_0|\} \otimes (Q(s_0, s_2) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)) +\\ &\qquad \{|s_4\rangle\langle s_0|\} \otimes (Q(s_0, s_4) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2)) +\\ &\qquad \{|s_4\rangle\langle s_0|\} \otimes (Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_0, s_4)))\\ &= Q(s_0, s_2) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2) +\\ &\qquad Q(s_0, s_4) \circ Q(s_1, s_0) \circ Q(s_2, s_1) \circ Q(s_0, s_2) +\\ &\qquad Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_4, s_4) \circ Q(s_0, s_4)\\ &= \{\tfrac{1}{2}\,|1,1\rangle\langle 1,1| + \tfrac{1}{2}\,|2,2\rangle\langle 1,1| + \tfrac{1}{2}\,|1,1\rangle\langle 2,2| + \tfrac{1}{2}\,|2,2\rangle\langle 2,2|\,, |2,1\rangle\langle 2,1|\}.\end{aligned}$$

Whereas, for ϕ_2, we obtain

$$\Delta(\phi_2) = \Delta(\neg win_C\,\mathrm{U}\,\mathrm{false}) + \mathrm{tr}_C(\mathcal{F}^\infty_{\mathrm{true}\wedge\neg win_C} \circ \mathcal{P}_{s_0}) = \mathrm{tr}_C(\mathcal{F}^\infty_{\mathrm{true}\wedge\neg win_C} \circ \mathcal{P}_{s_0}),$$

which we will reconsider later in Example 5.19. □

It is worth noticing that all super-operators occurring in (11), apart from $\mathcal{F}^\infty_{\Phi_1\wedge\neg\Phi_2}$, have been already covered in Subsection 5.1. The super-operator $\mathrm{tr}_C(\mathcal{F}^\infty_{\mathrm{true}\wedge\neg win_C} \circ \mathcal{P}_{s_0})$ concerns a safety property, which is under the restriction that the negation only occurs on the top level of path formulas. The QCTL$^+$ proposed in this paper can express both the reachability property and the safety property to the sense.

To deal with $\mathcal{F}^\infty_{\Phi_1\wedge\neg\Phi_2}$, it is necessary to know the ultimate density operators ρ_∞ that stay into the BSCC subspaces with respect to $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$ for a given initial density operator ρ_0, i.e., $\mathrm{ULT} := \{\mathcal{F}^k_{\Phi_1\wedge\neg\Phi_2}(\rho_0)\colon k \text{ is sufficiently large}\}$. The following lemma indicates that such ultimate density operators are not convergent in general.

Lemma 5.18. *For an initial density operator $\rho_0 \in \mathcal{D}_{\mathcal{H}_{\mathrm{cq}}}$, the ultimate density operators $\rho = \lim_{k\to\infty} \mathcal{F}^k_{\Phi_1\wedge\neg\Phi_2}(\rho_0)$ are dense in a computable algebraic subset Ξ of $\mathcal{D}_{\mathcal{H}_{\mathrm{cq}}}$.*

Proof. We will analyze the algebraic structure of ρ_∞ using the discrete-time dynamical system $\mathbb{V}(k) = \mathbb{M}^k\mathbb{V}(0)$, where $\mathbb{M} = \mathrm{S2M}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})$, $\mathbb{V}(0) = \mathrm{L2V}(\rho_0)$ and $\rho_k = \mathrm{V2L}(\mathbb{V}(k))$. Thus ULT is exactly the set of elements $\lim_{k\to\infty}\rho_k = \lim_{k\to\infty}\mathrm{V2L}(\mathbb{V}(k))$. It is known that every entry of $\mathbb{V}(k)$ is in the form

$$\sum_{i,j} c_{i,j}k^j\lambda_i^k, \tag{12}$$

where $c_{i,j} \in \mathbb{A}$ are coefficients and $\lambda_j \in \mathbb{A}$ are eigenvalues of $\mathbb{M}$ with multiplicities by Lemma 2.8, since all entries of $\mathbb{M}$ are algebraic. Suppose that $\mathbb{V}(k)$ is determined under an appropriate orthonormal basis of $\mathcal{H}$, such that ρ_k is diagonal. We can infer there is no term $c_{i,j}k^j\lambda_i^k$ in (12) with $|\lambda_i| > 1$ or $|\lambda_i| = 1 \wedge j > 0$, since otherwise the entry would have absolute value greater than 1 as k goes to infinity, which destroys the trace-nonincreasing property of $\mathcal{F}_{\Phi_1\wedge\neg\Phi_2}$. On the other hand, all terms $c_{i,j}k^j\lambda_i^k$ with $|\lambda_i| < 1$ would vanish as k goes to infinity. Hence the ultimate density operators ρ_∞ consist of only entries in the form

$$\sum_i c_i \lim_{k\to\infty}\exp(\imath k\theta_i), \tag{13}$$

where θ_i are the magnitudes of the unit eigenvalues of $\mathbb{M}$. That is, ULT is the set of elements $\rho_\infty = \sum_i \mathbf{C}_i \lim_{k\to\infty}\exp(\imath k\theta_i)$ with $\mathbb{A}$-matrix coefficients $\mathbf{C}_i$.

Let $\theta_1, \ldots, \theta_l$ be all distinct magnitudes in (13). By Theorem 2.9, we can obtain a $\mathbb{Z}$-linearly independent basis $\{\pi/\kappa, \mu_1, \ldots, \mu_m\}$, such that

$$\begin{bmatrix}\theta_1\\ \theta_2\\ \vdots\\ \theta_l\end{bmatrix} = \begin{bmatrix} z_{1,0} & z_{1,1} & \cdots & z_{1,m}\\ z_{2,0} & z_{2,1} & \cdots & z_{2,m}\\ \vdots & \vdots & \ddots & \vdots\\ z_{l,0} & z_{l,1} & \cdots & z_{l,m}\end{bmatrix}\begin{bmatrix}\pi/\kappa\\ \mu_1\\ \vdots\\ \mu_m\end{bmatrix},$$

where $\kappa, z_{i,j} \in \mathbb{Z}$ satisfy $\gcd(\{z_{i,j} \colon i \in [l]\}) = 1$ for each $j \in [m]$. By Corollary 2.4, we can see

- $\{(k\mu_1 \bmod 2\pi, \ldots, k\mu_m \bmod 2\pi) \colon k \in \mathbb{N}\}$ is dense in $[0, 2\pi)^m$,
- $\{(\exp(\imath k\mu_1), \ldots, \exp(\imath k\mu_m)) \colon k \in \mathbb{N}\}$ is dense in $\{w \in \mathbb{C} \colon |w| = 1\}^m$, and
- $\{(\cos(k\mu_1), \sin(k\mu_1), \ldots, \cos(k\mu_m), \sin(k\mu_m)) \colon k \in \mathbb{N}\}$ is dense in $\{(x, y) \in \mathbb{R}^2 \colon x^2+y^2 = 1\}^m$.

For each $j \in [l]$, we have

$$\begin{aligned}\exp(\imath k\theta_j) &= \exp(z_{j,0}\pi/\kappa)\prod_{i=1}^m \exp(\imath z_{j,i}k\mu_i)\\ &= \exp(z_{j,0}\pi/\kappa)\prod_{i=1}^m (\cos(z_{j,i}k\mu_i) + \imath\sin(z_{j,i}k\mu_i)),\end{aligned}$$

which results in an $\mathbb{A}$-polynomial p_j in $\cos(k\mu_j)$ and $\sin(k\mu_j)$ by trigonometric identities. After introducing real variables $x_j = \cos(k\mu_j)$ and $y_j = \sin(k\mu_j)$ for $i \in [m]$, we can characterize $\{\exp(\imath k\theta_j) \colon k \in \mathbb{N}\}$ by the range of $p_j(\mathbf{x}, \mathbf{y})$ on $\{(x, y) \in \mathbb{R}^2 \colon x^2 + y^2 = 1\}^m$, in which the former set is dense in the latter set. The same holds for the set ULT of elements $\rho_\infty = \sum_i \mathbf{C}_i \lim_{t\to\infty} c_i \exp(\imath k\theta_i)$, whose range is a computable algebraic set Ξ by quantifier elimination [3, Algorithm 14.5]. $\square$

Example 5.19. *In Example 5.4, we have obtained the repeated super-operator $\mathcal{F}_{\neg win_C}$. Suppose that all classical states in S are ordered as $s_0 \prec \cdots \prec s_4$. Then states $|s_0\rangle$ through $|s_4\rangle$ are indexed by $|1\rangle$ through $|5\rangle$, respectively. The matrix representation* $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$ *is*

$$|3\rangle\langle 1| \otimes \mathbf{Q}_{0,2} \otimes \mathbf{Q}^*_{0,2} + |4\rangle\langle 1| \otimes \mathbf{Q}_{0,3} \otimes \mathbf{Q}^*_{0,3} + |5\rangle\langle 1| \otimes \mathbf{Q}_{0,4} \otimes \mathbf{Q}^*_{0,4} +$$
$$|1\rangle\langle 2| \otimes \mathbf{Q}_{1,0} \otimes \mathbf{Q}^*_{1,0} + |2\rangle\langle 3| \otimes \mathbf{Q}_{2,1} \otimes \mathbf{Q}^*_{2,1} + |5\rangle\langle 5| \otimes \mathbf{Q}_{4,4} \otimes \mathbf{Q}^*_{4,4},$$

where $\mathbf{Q}_{i,j}$ are the unique Kraus operators of those super-operators $Q(s_i, s_j)$ in $\mathfrak{C}_2$. By Jordan decomposition, we have $\mathrm{S2M}(\mathcal{F}_{\neg win_C}) = \mathbf{S}^{-1}\mathbf{J}\mathbf{S}$*, in which:*

- $\mathbf{J}$ *is the Jordan canonical form of* $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$ *that is*

$$\mathrm{diag}(\underbrace{\mathbf{J}_{0;1}, \dots, \mathbf{J}_{0;1}}_{15 \text{ copies}},\ \underbrace{\mathbf{J}_{0;3}, \dots, \mathbf{J}_{0;3}}_{11 \text{ copies}},\ \mathbf{J}_{0;6},\ \mathbf{J}_{0;7},\ \underbrace{\mathbf{J}_{1;1}, \dots, \mathbf{J}_{1;1}}_{17 \text{ copies}},\ \mathbf{J}_{\exp(2\imath\pi/3);1},\ \mathbf{J}_{\exp(-2\imath\pi/3);1}),$$

  where $\mathbf{J}_{\lambda;m}$ denotes the Jordan block of eigenvalue λ and order m, i.e.,

$$\begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}_{m\times m};$$

- $\mathbf{S}$ *is the corresponding transformation matrix (omitted here for conciseness, but available at the bottom of Bernoulli Factory.nb at https://github.com/meijingyi/CheckQCTLPlus).*

Since the entries of $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$ *are algebraic, it follows that the diagonal entries of* $\mathbf{J}$ *that are eigenvalues of* $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$*, as well as the entries of* $\mathbf{S}$ *whose columns are (generalized) eigenvectors, are algebraic too.*

When k is sufficiently large, say $k > 7$, we can see that $\mathrm{S2M}(\mathcal{F}_{\neg win_C})^k$ *is* $\mathbf{S}^{-1}\mathbf{J}^k\mathbf{S}$ *with*

$$\mathbf{J}^k = \mathrm{diag}(\underbrace{0, \dots, 0}_{61 \text{ copies}},\ \underbrace{1, \dots, 1}_{17 \text{ copies}},\ \exp(-2\imath k\pi/3),\ \exp(2\imath k\pi/3)),$$

since

$$\mathbf{J}^k_{\lambda;m} = \begin{bmatrix} \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \binom{k}{m-2}\lambda^{k-m+2} & \binom{k}{m-1}\lambda^{k-m+1} \\ 0 & \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \binom{k}{m-3}\lambda^{k-m+3} & \binom{k}{m-2}\lambda^{k-m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} \\ 0 & 0 & 0 & \cdots & 0 & \binom{k}{0}\lambda^k \end{bmatrix}_{m\times m};$$

$\mathbf{J}^k_{0;3}$, $\mathbf{J}^k_{0;6}$ *and* $\mathbf{J}^k_{0;7}$ *vanish then. It implies that given an initial density operator $\rho_0 \in \mathcal{D}_{\mathcal{H}_{\mathrm{cq}}}$, every entry of the final density operators $\rho_k = \mathcal{F}^k_{\neg win_C}(\rho_0)$ can be expressed as*

$$c_0 + c_1 \exp(2\imath k\pi/3) + c_2 \exp(-2\imath k\pi/3)$$

for some algebraic coefficients c_0, c_1, c_2 *(or equivalently* $c_0 + d_1 \cos(2k\pi/3) + d_2 \sin(2k\pi/3)$ *for some algebraic coefficients* c_0, d_1, d_2*). For example, we have that:*

$$\begin{aligned} \rho_7 &= \mathbf{C}_0 + \mathbf{C}_1 \exp(2\imath\pi/3) + \mathbf{C}_2 \exp(-2\imath\pi/3), \\ \rho_8 &= \mathbf{C}_0 + \mathbf{C}_1 \exp(-2\imath\pi/3) + \mathbf{C}_2 \exp(2\imath\pi/3), \\ \rho_9 &= \mathbf{C}_0 + \mathbf{C}_1 + \mathbf{C}_2, \end{aligned} \tag{14}$$

hold for some $\mathbb{A}$*-matrices* $\mathbf{C}_0$*,* $\mathbf{C}_1$*,* $\mathbf{C}_2$*;* $\rho_k = \rho_{k-3}$ *holds for any* $k \geq 10$*. Thus all the density operators* ρ_k *(*$k \geq 7$*) plainly form a finite set* $\Xi = \{\rho_7, \rho_8, \rho_9\}$*, thus being not convergent.* □

In the above example, if we first remove the BSCC subspaces as a pretreatment, those terms corresponding to unit eigenvalues ($\neq 1$) would also be removed, thus simplifying the result (14). However, in the general case, there are newly-produced quantum states that would enter in the BSCC subspaces when the quantum system evolves, and the pretreatment of removing BSCC subspaces does not suffice then. Additionally, since the composite super-operator along with the loop $s_0 \to s_2 \to s_1 \to s_0$ is $H_2 \circ H_1 \circ M_0 = \{|+,+\rangle\langle 1,1| + |-,-\rangle\langle 2,2|\}$ and $(H_2 \circ H_1 \circ M_0)^k = \{\frac{1}{2}(|1,1\rangle\langle 1,1| + |2,2\rangle\langle 1,1| + |1,1\rangle\langle 2,2| + |2,2\rangle\langle 2,2|)\}$ for any $k > 1$, it ensures that all nonzero eigenvalues in the result (14) are unit.

From Lemma 5.18, we have seen that $\mathcal{F}^{\infty}_{\Phi_1 \wedge \neg\Phi_2}$ is not a function (super-operator) in general, since the singleton initial density operator ρ_0 is associated with a set ULT of ultimate density operators ρ_∞. To effectively synthesize the super-operator of the negation, we have to propose the following convergence conditions.

Definition 5.20. *A super-operator* $\mathcal{E}$ *is* convergent *on an initial density operator* ρ_0 *if the possible unit eigenvalue of* $\mathrm{S2M}(\mathcal{E})$ *whose eigenvector is not orthogonal to* $\mathrm{L2V}(\rho_0)$ *is* 1*. A super-operator* $\mathcal{E}$ *is* uniformly convergent *if the possible unit eigenvalue of* $\mathrm{S2M}(\mathcal{E})$ *is* 1*.*

Note that, by Theorem 2.9, these convergence conditions are checkable in **PSPACE** with respect to the dimension d, and in **PTIME** with respect to the size of $\mathfrak{C}$ when d is fixed. If the conditions fail, the super-operator of the negation cannot be synthesized. Afterwards we would only consider those convergent instances, thus establish the decidability conditionally.

Example 5.21. *Continue to consider Example 5.19. The unit eigenvalues of* $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$ *are* 1 *and* $\exp(\pm 2\imath k\pi/3)$*. It turns out to have periodic final density operators as shown in Example 5.19, thus* $\mathcal{F}_{\neg win_C}$ *does not meet the uniformly convergence condition. However, consider the initial density operator* $\rho_0 = \rho' + \rho''$ *with*

$$\begin{aligned} \rho' = {} & |s_0\rangle\langle s_0| \otimes \tfrac{1}{8}[|1,1\rangle\langle 1,1| + |1,1\rangle\langle 2,2| + |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|] + \\ & |s_1\rangle\langle s_1| \otimes \tfrac{1}{8}[|1,+\rangle\langle 1,+| + |1,+\rangle\langle 2,-| + |2,-\rangle\langle 1,+| + |2,-\rangle\langle 2,-|] + \\ & |s_2\rangle\langle s_2| \otimes \tfrac{1}{8}[|1,1\rangle\langle 1,1| + |1,1\rangle\langle 2,2| + |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|] \\ \rho'' = {} & |s_2\rangle\langle s_2| \otimes \tfrac{1}{8}[|+,-\rangle\langle +,-| + |-,+\rangle\langle -,+|]. \end{aligned}$$

After performing $\mathcal{F}^k_{\neg win_C}$ *(*$k \geq 4$*) on* ρ_0*, the final density operators* ρ_k *would be the same as* $\rho_4 = \rho' + \rho'''$ *with*

$$\rho''' = |s_4\rangle\langle s_4| \otimes \tfrac{1}{8}\, |1,2\rangle\langle 1,2|\,,$$

which is independent from k, since both $\mathrm{L2V}(\rho')$ *and* $\mathrm{L2V}(\rho''')$ *are eigenvectors (corresponding to eigenvalue* 1*) of* $\mathrm{S2M}(\mathcal{F}_{\neg win_C})$*. Hence* $\mathcal{F}_{\neg win_C}$ *meets the convergence condition on this* ρ_0*.* □

Theorem 5.22. *Under the convergence conditions described in Definition 5.20, the matrix representation of the SOVM $\mathcal{F}^{\infty}_{\Phi_1 \wedge \neg\Phi_2}$ can be synthesized in time polynomial in the size of $\mathfrak{C}$.*

Proof. It suffices to determine the algebraic structure of $\rho_\infty = \sum_i \mathbf{C}_i \lim_{k\to\infty} \exp(\imath k\theta_i)$, where θ_i are the magnitudes of the unit eigenvalues of $\mathrm{S2M}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})$ and $\mathbf{C}_i$ are $\mathbb{A}$-matrices. By Lemma 2.8 and the known algorithms that:

- it is in $O(D^4)$ to determine the characteristic polynomial of a matrix of dimension D [3, Algorithm 8.17], and
- it is in $O(D^6)$ to determine roots of a $\mathbb{Q}$-polynomial of degree D [3, Algorithm 10.4],

we obtain that:

- the characteristic polynomial $f(z)$ of $\mathrm{S2M}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})$ is an $\mathbb{A}$-polynomial of degree d^2 where $d = \dim(\mathcal{H})$, and coefficients taken from $\mathbb{Q}(\lambda_0) : \mathbb{Q}$, where the degree of λ_0 is bounded by $\|\lambda_0\| \leq \|\mathfrak{C}\|$,
- the roots of $f(z)$ are those of a $\mathbb{Q}$-polynomial $g(z)$ of degree not greater than $d^2\|\lambda_0\|$, and
- the roots of $g(z)$ can be determined in $O(d^{12}\|\lambda_0\|^6)$, as well as the eigenvalues of the matrix $\mathrm{S2M}(\mathcal{F}_{\Phi_1\wedge\neg\Phi_2})$. □

Finally, we have to address the hardness of synthesizing the SOVMs for the *arbitrary* negation in path formulas. In the previous two subsections, we employ the strategy (see Figure 1) of i) reducing the conjunction and disjunction in path formulas to a time-unbounded until formula over a product QMC; and ii) synthesizing the SOVM of the latter path formula. However, it does not imply that one could employ the strategy of i) synthesizing the SOVMs of individual atomic path formulas; and ii) combining these SOVMs according to the corresponding conjunction and disjunction in path formulas, since the SOVMs are defined on path formulas and once the SOVMs are obtained, the path formulas could not be recovered. After dealing with negation on a path formula ϕ in this subsection, we would get the SOVM of $\neg\phi$, not an atomic path formula, which makes it fail to be incorporated with the previous subsections. To avoid such technical hardness, we focus on the sublogic QCTL$^+$ of the quantum analogy QCTL* of PCTL* [1] in this paper.

6. Deciding the QCTL Plus State Formulas

In this section, we aim to decide basic state formulas, trace-quantifier formulas (resp. fidelity-quantifier) formulas in turn, using the POVMs (resp. SOVMs) obtained in the previous section, over the QMC fed with and without an initial quantum state. The complexity of checking QCTL$^+$ formulas will be summarized. Here we suppose that the generator λ_0 of all numbers appearing in the input QMC is defined in the standard way: the minimal polynomial $f_{\lambda_0}(z) \in \mathbb{Q}[z]$ with degree D plus the disk with center c and radius r that distinguishes λ_0 from other roots of f_{λ_0}, i.e., λ_0 is the unique solution to the constraint $f_{\lambda_0}(z) = 0 \wedge |z - c| < r$.

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

- $\mathrm{Sat}(\mathrm{a}) = \{s \in S : \mathrm{a} \in L(s)\}$;
- $\mathrm{Sat}(\neg\Phi) = S \setminus \mathrm{Sat}(\Phi)$, provided that $\mathrm{Sat}(\Phi)$ is known;

- $\mathrm{Sat}(\Phi_1 \wedge \Phi_2) = \mathrm{Sat}(\Phi_1) \cap \mathrm{Sat}(\Phi_2)$, provided that $\mathrm{Sat}(\Phi_1)$ and $\mathrm{Sat}(\Phi_2)$ are known;
- $\mathrm{Sat}(\Phi_1 \vee \Phi_2) = \mathrm{Sat}(\Phi_1) \cup \mathrm{Sat}(\Phi_2)$, provided that $\mathrm{Sat}(\Phi_1)$ and $\mathrm{Sat}(\Phi_2)$ 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 $O(n)$. Hence, deciding basic state formulas is linear time with respect to the size of $\mathfrak{C}$.

For the trace-quantifier formula $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\phi]$, we have:

- If the QMC $\mathfrak{C}$ is fed with an initial quantum state ρ_s, $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\phi]$ holds if and only if $\mathrm{tr}((\mathbf{M} - \Lambda(\phi))\rho_s)$ is nonnegative. It is checkable in time $O(d^3)$, as it is dominated by multiplication over d-dimensional matrices.
- If the QMC $\mathfrak{C}$ is not fed with any initial quantum state, $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\phi]$ holds if and only if the eigenvalues of $\mathbf{M} - \Lambda(\phi)$ are nonnegative. For the latter, it suffices to determine roots of the characteristic polynomial of $\mathbf{M} - \Lambda(\phi)$, which has degree not greater than d and takes coefficients from $\mathbb{Q}(\lambda_0) : \mathbb{Q}$. Hence, the latter can be checked in time $O(d^6 D^6)$, since roots of that characteristic polynomial are roots of a $\mathbb{Q}$-polynomial with degree dD by Lemma 2.8 and [3, Algorithm 10.4].

Particularly, the trace-quantifier formula $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\neg\phi]$ reduces to $\Lambda(\neg\phi) = \mathbf{I} - \Lambda(\phi)$.

Example 6.1. *Now, we consider the nontermination of the quantum Bernoulli factory protocol in Example 5.1. To this end, we are to decide the trace-quantifier formula with form* $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\neg\Diamond(win_C \vee win_D)]$, *where* $\mathbf{M} = \frac{1}{2}(|1,1\rangle\langle 1,1| - |1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|)$ *is a threshold. From Example 5.6, we have*

$$\Lambda(\Diamond\, win_C) = \tfrac{1}{4}(|1,1\rangle\langle 1,1| - |1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|) + |1,2\rangle\langle 1,2|,$$

and we could get $\Lambda(\Diamond\, win_D)$ *in the same way as follows:*

$$\Lambda(\Diamond\, win_D) = \tfrac{1}{4}(|1,1\rangle\langle 1,1| - |1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|) + |2,1\rangle\langle 2,1|.$$

Since both the unique win_C*-state* s_3 *and the unique* win_D*-state* s_4 *are absorbing (i.e., having self-loops weighted by* $\mathcal{I}$*), the POVM of nontermination can be computed as*

$$\begin{aligned}\Lambda(\neg\Diamond(win_C \vee win_D)) &= \mathbf{I} - \Lambda(\Diamond\, win_C) - \Lambda(\Diamond\, win_D)\\ &= \tfrac{1}{2}(|1,1\rangle\langle 1,1| + |1,1\rangle\langle 2,2| + |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|).\end{aligned}$$

Thus the matrix $\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)) = -|1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1|$ *has eigenvector*

$$\rho' = \tfrac{1}{2}(|1,1\rangle\langle 1,1| - |1,1\rangle\langle 2,2| - |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|)$$

corresponding to eigenvalue 1 *and eigenvector*

$$\rho'' = \tfrac{1}{2}(|1,1\rangle\langle 1,1| + |1,1\rangle\langle 2,2| + |2,2\rangle\langle 1,1| + |2,2\rangle\langle 2,2|)$$

corresponding to eigenvalue -1. *These eigenvectors* ρ' *and* ρ'' *can be obtained by spectral decomposition in polynomial time* $O(\|\mathfrak{C}_2\|^6)$. *Then we decide the truth of the trace-quantifier formula* $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq\mathbf{M}}[\neg\Diamond(win_C \vee win_D)]$ *respectively in the following two cases:*

- *When we feed $\mathfrak{C}_2$ with the initial quantum state $\frac{2}{3}\rho' + \frac{1}{3}\rho''$, we could calculate*

$$
\begin{aligned}
&\mathrm{tr}((\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)))(\tfrac{2}{3}\rho' + \tfrac{1}{3}\rho''))\\
&= \tfrac{2}{3}\cdot \mathrm{tr}((\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)))\rho') + \tfrac{1}{3}\cdot \mathrm{tr}((\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)))\rho'')\\
&= \tfrac{2}{3}\cdot(1)\cdot \mathrm{tr}(\rho') + \tfrac{1}{3}\cdot(-1)\cdot \mathrm{tr}(\rho'') = \tfrac{2}{3}\cdot(1) + \tfrac{1}{3}\cdot(-1) = \tfrac{1}{3}.
\end{aligned}
$$

  Hence $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\neg\Diamond(win_C \vee win_D)]$ is decided to be true over this $\mathfrak{C}_2$ with initial quantum state $\frac{2}{3}\rho' + \frac{1}{3}\rho''$.

- *When we feed $\mathfrak{C}_2$ with the initial quantum state $\frac{1}{3}\rho' + \frac{2}{3}\rho''$, we could calculate* $\mathrm{tr}((\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)))(\frac{1}{3}\rho' + \frac{2}{3}\rho'')) = -\frac{1}{3}$, *i.e.,* $\min_\rho \mathrm{tr}((\mathbf{M} - \Lambda(\neg\Diamond(win_C \vee win_D)))\rho) < 0$. *Hence $\mathfrak{F}^{\mathrm{tr}}_{\sqsubseteq \mathbf{M}}[\neg\Diamond(win_C \vee win_D)]$ is decided to be false over this $\mathfrak{C}_2$ with some initial quantum state.*

Overall, it is in polynomial time to decide the trace-quantifier formula. □

For the fidelity-quantifier formula $\mathfrak{F}^{\mathrm{fid}}_{\leq\tau}[\phi]$, we have:

- If the QMC $\mathfrak{C}$ is fed with an initial quantum state ρ_s, $\mathfrak{F}^{\mathrm{fid}}_{\leq\tau}[\phi]$ holds if and only if

$$\mathrm{tr}\sqrt{\rho_s^{1/2}\mathrm{V2L}(\mathrm{S2M}(\Delta(\phi))\mathrm{L2V}(\rho_s))\rho_s^{1/2}} \leq \tau.$$

  For the latter, it is dominated by the spectral decomposition of ρ_s [27, Box 2.2] to get $\rho_s^{1/2}$. So we have to determine the eigenvalues of ρ_s, which is checkable in time $O(d^6D^6)$ by real root isolation [3, Algorithm 10.4].

- If the QMC $\mathfrak{C}$ is not fed with any initial quantum state, $\mathfrak{F}^{\mathrm{fid}}_{\leq\tau}[\phi]$ holds if and only if for any pure state $|\psi\rangle$, $\langle\psi|\,\mathrm{V2L}(\mathrm{S2M}(\Delta(\phi))\mathrm{L2V}(|\psi\rangle\langle\psi|))\,|\psi\rangle$ is not greater than τ^2. Here we confine the initial quantum state to be pure, i.e., $\rho_s = |\psi\rangle\langle\psi|$, which does not lose the generality by the joint concavity [27, Exercise 9.19]. After introducing d complex variables $\mathbf{x}$ to denote the quantum state $|\psi\rangle$, subject to the purity $\|\mathbf{x}\|^2 = 1$, the latter is reformulated as

$$
\begin{aligned}
\zeta &\equiv \forall\ |\psi\rangle \in \mathcal{H}\colon \mathrm{Fid}(\Delta(\phi), |\psi\rangle\langle\psi|) \leq \tau^2\\
&\equiv \forall\ |\psi\rangle \in \mathcal{H}\colon\ \langle\psi|\,\mathrm{V2L}(\mathrm{S2M}(\Delta(\phi))\mathrm{L2V}(|\psi\rangle\langle\psi|))\,|\psi\rangle \leq \tau^2\\
&\equiv \forall\, \mathbf{x} \in \mathbb{C}^d\colon \|\mathbf{x}\|^2 = 1 \to \left(\sum_{i,j\in[d]} x_i^* x_j \langle i,j|\right)\mathrm{S2M}(\Delta(\phi))\left(\sum_{i,j\in[d]} x_i x_j^* |i,j\rangle\right) \leq \tau^2.
\end{aligned}
$$

  Additionally, as $\mathrm{S2M}(\Delta(\phi))$ admits the algebraic number λ_0, we further reformulate the latter as the $\mathbb{Q}$-polynomial formula

$$
\begin{aligned}
\zeta(\lambda_0) \equiv \forall\, z \in \mathbb{C}\,\forall\, \mathbf{x} \in \mathbb{C}^d\colon\ & [f_{\lambda_0}(z) = 0 \wedge |z - c| < r \wedge \|\mathbf{x}\|^2 = 1]\ \to\\
&\underbrace{\left(\sum_{i,j\in[d]} x_i^* x_j \langle i,j|\right)}_{\deg=2}\underbrace{\mathrm{S2M}(\Delta(\phi))}_{\deg=1}\underbrace{\left(\sum_{i,j\in[d]} x_i x_j^* |i,j\rangle\right)}_{\deg=2} \leq \tau^2,
\end{aligned}
\tag{15}
$$

  which has the following size parameters:

- a block of $2d+2$ universally quantified real variables taken from real and imaginary parts of $\mathbf{x}$ and z, and
- 4 distinct polynomials of degree at most the maximum of 5 and D.

Hence, the latter can be checked in time exponential in d, i.e., $\max(5, D)^{O(d)}$, by quantifier elimination over real closed fields (see Appendix Appendix A for more details).

The fidelity-quantifier formula $\mathfrak{F}^{\mathrm{fid}}_{\leq\tau}[\neg\phi]$ can be similarly dealt with, since the matrix representation of $\Delta(\neg\phi)$ has been synthesized in Subsection 5.3. Note that if ϕ is a time-unbounded until formula, it is required to meet the convergence conditions described in Definition 5.20.

Example 6.2. *Continue to consider the QMC $\mathfrak{C}_1$ shown in Example 3.2. To validate the correctness of the quantum teleportation protocol, it needs to decide whether $\underline{\mathrm{Fid}}(\Diamond s_7) = 1$ holds for some initial state $|\widehat{q_2\, q_3}\rangle$, or more generally compute the set of the initial states $|\widehat{q_2\, q_3}\rangle$ on which $\underline{\mathrm{Fid}}(\Diamond s_7) = 1$ holds. The latter is characterized by the following quantified formula*

$$\begin{aligned} & \forall\ |q_1\rangle : \mathrm{Fid}(|q_1\rangle\langle q_1|, \mathrm{tr}_{\mathcal{H}_{1,2}}(\Delta(\Diamond\,\mathrm{ok})(|q_1, \widehat{q_2\, q_3}\rangle\langle q_1, \widehat{q_2\, q_3}|))) = 1 \\ \equiv\ & \forall\ |q_1\rangle :\ |q_1\rangle\langle q_1| = \mathrm{tr}_{\mathcal{H}_{1,2}}(\Delta(\Diamond\,\mathrm{ok})(|q_1, \widehat{q_2\, q_3}\rangle\langle q_1, \widehat{q_2\, q_3}|)), \end{aligned} \tag{16}$$

where $\mathrm{tr}_{\mathcal{H}_{1,2}} = \{\langle i, j| \otimes \mathbf{I} : i \in [2], j \in [2]\}$ traces out the Hilbert spaces on $|q_1\rangle$ and $|q_2\rangle$. So, the formula (16) means that the information $|q_1\rangle$ in the initial density operator is preserved as the information $|q_3\rangle$ in the final density operator, since $\underline{\mathrm{Fid}}(\Diamond s_7) = 1$ holds if and only if the initial qubit $|q_1\rangle$ is the same as the final qubit $|q_3\rangle$, regardless of a global phase.

To rewrite the formula (16) as a polynomial one, we first introduce complex variables $\mathbf{x} = (x_i)_{i\in[4]}$ to encode the state $|\widehat{q_2\, q_3}\rangle$ as $x_1\,|1,1\rangle + x_2\,|1,2\rangle + x_3\,|2,1\rangle + x_4\,|2,2\rangle$ and $\mathbf{y} = (y_i)_{i\in[2]}$ to encode the state $|q_1\rangle$ as $y_1\,|1\rangle + y_2\,|2\rangle$. Then the encoded initial density operator is the pure state $|q_1, \widehat{q_2\, q_3}\rangle\langle q_1, \widehat{q_2\, q_3}|$ with $|q_1, \widehat{q_2\, q_3}\rangle$ being $(y_1\,|1\rangle + y_2\,|2\rangle)(x_1\,|1,1\rangle + x_2\,|1,2\rangle + x_3\,|2,1\rangle + x_4\,|2,2\rangle)$. After applying the SOVM $\Delta(\Diamond\,\mathrm{ok}) = \Delta(\mathrm{true}\,\mathrm{U}\,\mathrm{ok})$ (obtained in Example 4.3) on the initial state, the final density operator $\Delta(\Diamond\,\mathrm{ok})(|q_1, \widehat{q_2\, q_3}\rangle\langle q_1, \widehat{q_2\, q_3}|)$ turns out to be the mixed state which can be expressed as

$$\tfrac{1}{2}(|1,1\rangle\langle 1,1| \otimes |\psi_1\rangle\langle\psi_1| + |1,2\rangle\langle 1,2| \otimes |\psi_2\rangle\langle\psi_2| + |2,1\rangle\langle 2,1| \otimes |\psi_3\rangle\langle\psi_3| + |2,2\rangle\langle 2,2| \otimes |\psi_4\rangle\langle\psi_4|),$$

where

$$\begin{aligned} |\psi_1\rangle &= \tfrac{1}{\sqrt{2}}[(y_1x_1 + y_2x_3)\,|1\rangle + (y_1x_2 + y_2x_4)\,|2\rangle], \\ |\psi_2\rangle &= \tfrac{1}{\sqrt{2}}[(y_1x_4 + y_2x_2)\,|1\rangle + (y_1x_3 + y_2x_1)\,|2\rangle], \\ |\psi_3\rangle &= \tfrac{1}{\sqrt{2}}[(y_1x_1 - y_2x_3)\,|1\rangle - (y_1x_2 - y_2x_4)\,|2\rangle], \\ |\psi_4\rangle &= \tfrac{1}{\sqrt{2}}[(y_1x_4 - y_2x_2)\,|1\rangle - (y_1x_3 - y_2x_1)\,|2\rangle]. \end{aligned}$$

Thus we have $\mathrm{tr}_{\mathcal{H}_{1,2}}(\Delta(\Diamond\,\mathrm{ok})(|q_1, \widehat{q_2\, q_3}\rangle\langle q_1, \widehat{q_2\, q_3}|) = \sum_{i=1}^{4} |\psi_i\rangle\langle\psi_i|$. Utilizing the trace-preserving property of the SOVM $\Delta(\Diamond\,\mathrm{ok})$, these four final state vectors $|\psi_i\rangle$ are required to be proportional to the initial state vector $|q_1\rangle$. For instance, $|\psi_1\rangle$ should satisfy $(y_1x_1 + y_2x_3)y_2 = (y_1x_2 + y_2x_4)y_1$. In the same way, we can get

$$\begin{aligned} (y_1x_4 + y_2x_2)y_2 &= (y_1x_3 + y_2x_1)y_1, \\ (y_1x_1 - y_2x_3)y_2 &= -(y_1x_2 - y_2x_4)y_1, \\ (y_1x_4 - y_2x_2)y_2 &= -(y_1x_3 - y_2x_1)y_1. \end{aligned}$$

After further introducing the real variables $\boldsymbol{\mu} = \Re(\mathbf{x})$, $\boldsymbol{\nu} = \Im(\mathbf{x})$, $\boldsymbol{\mu}' = \Re(\mathbf{y})$ *and* $\boldsymbol{\nu}' = \Im(\mathbf{y})$, *the formula* (16) *could be encoded into the polynomial one*

$$
\begin{aligned}
&\forall\{\mathrm{y}_1,\mathrm{y}_2\}\colon |\mathrm{y}_1|^2+|\mathrm{y}_2|^2=1 \to \begin{bmatrix} |x_1|^2+|x_2|^2+|x_3|^2+|x_4|^2=1\ \wedge \\ (y_1x_1+y_2x_3)y_2=(y_1x_2+y_2x_4)y_1\ \wedge \\ (y_1x_4+y_2x_2)y_2=(y_1x_3+y_2x_1)y_1\ \wedge \\ (y_1x_1-y_2x_3)y_2=-(y_1x_2-y_2x_4)y_1\ \wedge \\ (y_1x_4-y_2x_2)y_2=-(y_1x_3-y_2x_1)y_1 \end{bmatrix} \\
\equiv\ &\forall\{\mu_1',\nu_1',\mu_2',\nu_2'\}\colon \mu_1'^2+\nu_1'^2+\mu_2'^2+\nu_2'^2=1\ \to \\
&\begin{bmatrix}
\mu_1^2+\nu_1^2+\mu_2^2+\nu_2^2+\mu_3^2+\nu_3^2+\mu_4^2+\nu_4^2=1\ \wedge \\
\mu_1\mu_1'\mu_2'+\mu_3\mu_2'^2-\mu_2'\nu_1\nu_1'-\mu_1'\nu_1\nu_2'-2\mu_2'\nu_3\nu_2'-\mu_1\nu_1'\nu_2'-\mu_3\nu_2'^2= \\
\mu_2\mu_1'^2+\mu_4\mu_1'\mu_2'-2\mu_1'\nu_2\nu_1'-\mu_2'\nu_4\nu_1'-\mu_2\nu_1'^2-\mu_1'\nu_4\nu_2'-\mu_4\nu_1'\nu_2'\ \wedge \\
\mu_1'\mu_2'\nu_1+\mu_2'^2\nu_3+\mu_1\mu_2'\nu_1'+\mu_1\mu_1'\nu_2'+2\mu_3\mu_2'\nu_2'-\nu_1\nu_1'\nu_2'-\nu_3\nu_2'^2= \\
\mu_1'^2\nu_2+\mu_1'\mu_2'\nu_4+2\mu_2\mu_1'\nu_1'+\mu_4\mu_2'\nu_1'-\nu_2\nu_1'^2+\mu_4\mu_1'\nu_2'-\nu_4\nu_1'\nu_2'\ \wedge \\
\mu_4\mu_1'\mu_2'+\mu_2\mu_2'^2-\mu_2'\nu_4\nu_1'-2\mu_2'\nu_2\nu_2'-\mu_1'\nu_4\nu_2'-\mu_4\nu_1'\nu_2'-\mu_2\nu_2'^2= \\
\mu_3\mu_1'^2+\mu_1\mu_1'\mu_2'-\mu_2'\nu_1\nu_1'-2\mu_1'\nu_3\nu_1'-\mu_3\nu_1'^2-\mu_1'\nu_1\nu_2'-\mu_1\nu_1'\nu_2'\ \wedge \\
\mu_2'^2\nu_2+\mu_1'\mu_2'\nu_4+\mu_4\mu_2'\nu_1'+\mu_4\mu_1'\nu_2'+2\mu_2\mu_2'\nu_2'-\nu_4\nu_1'\nu_2'-\nu_2\nu_2'^2= \\
\mu_1'\mu_2'\nu_1+\mu_1'^2\nu_3+2\mu_3\mu_1'\nu_1'+\mu_1\mu_2'\nu_1'-\nu_3\nu_1'^2+\mu_1\mu_1'\nu_2'-\nu_1\nu_1'\nu_2'\ \wedge \\
\mu_1\mu_1'\mu_2'-\mu_3\mu_2'^2-\mu_2'\nu_1\nu_1'-\mu_1'\nu_1\nu_2'+2\mu_2'\nu_3\nu_2'-\mu_1\nu_1'\nu_2'+\mu_3\nu_2'^2= \\
-\mu_2\mu_1'^2+\mu_4\mu_1'\mu_2'+2\mu_1'\nu_2\nu_1'-\mu_2'\nu_4\nu_1'+\mu_2\nu_1'^2-\mu_1'\nu_4\nu_2'-\mu_4\nu_1'\nu_2'\ \wedge \\
\mu_1'\mu_2'\nu_1-\mu_2'^2\nu_3+\mu_1\mu_2'\nu_1'+\mu_1\mu_1'\nu_2'-2\mu_3\mu_2'\nu_2'-\nu_1\nu_1'\nu_2'+\nu_3\nu_2'^2= \\
-\mu_1'^2\nu_2+\mu_1'\mu_2'\nu_4-2\mu_2\mu_1'\nu_1'+\mu_4\mu_2'\nu_1'+\nu_2\nu_1'^2+\mu_4\mu_1'\nu_2'-\nu_4\nu_1'\nu_2'\ \wedge \\
\mu_4\mu_1'\mu_2'-\mu_2\mu_2'^2-\mu_2'\nu_4\nu_1'+2\mu_2'\nu_2\nu_2'-\mu_1'\nu_4\nu_2'-\mu_4\nu_1'\nu_2'+\mu_2\nu_2'^2= \\
-\mu_3\mu_1'^2+\mu_1\mu_1'\mu_2'-\mu_2'\nu_1\nu_1'+2\mu_1'\nu_3\nu_1'+\mu_3\nu_1'^2-\mu_1'\nu_1\nu_2'-\mu_1\nu_1'\nu_2'\ \wedge \\
-\mu_2'^2\nu_2+\mu_1'\mu_2'\nu_4+\mu_4\mu_2'\nu_1'+\mu_4\mu_1'\nu_2'-2\mu_2\mu_2'\nu_2'-\nu_4\nu_1'\nu_2'+\nu_2\nu_2'^2= \\
\mu_1'\mu_2'\nu_1-\mu_1'^2\nu_3-2\mu_3\mu_1'\nu_1'+\mu_1\mu_2'\nu_1'+\nu_3\nu_1'^2+\mu_1\mu_1'\nu_2'-\nu_1\nu_1'\nu_2'
\end{bmatrix},
\end{aligned}
\tag{17}
$$

which can be solved in exponential time $2^{O(\|\mathfrak{C}_1\|^2)}$ *by Algorithm 1.*

Using the tool Reduce *(a.k.a.* Redlog *[11]), we obtain that* $\mu_1 = \mu_4$, $\nu_1 = \nu_4$ *and the other free variables are 0. Thus the satisfying initial states are exactly* $c(|1,1\rangle + |2,2\rangle)/\sqrt{2}$ *for an arbitrarily unit complex number c interpreted as global phase. As a corollary, the quantum teleportation protocol is proven to be correct on the Bell state* $(|1,1\rangle + |2,2\rangle)/\sqrt{2}$. ☐

Combining the above analysis with Theorems 5.7,5.16,5.22, we obtain the main result:

Theorem 6.3. *Under the convergence conditions described in Definition 5.20, the QCTL*$^+$ *formulas are decidable over QMCs. Furthermore, the complexity (specified in terms of the size of the input QMC* $\|\mathfrak{C}\|$ *and the QCTL*$^+$ *formula as default) is summarized in Table 2, where 'matrix' is short for the matrix representation of SOVM.*

As a by-product, we immediately get:

Corollary 6.4. *The safety property* $\Lambda[\Box\Phi] \sqsubseteq \mathbf{M}$ *with* $\Box\Phi \equiv \neg\Diamond(\neg\Phi)$ *over QMCs can be checked in polynomial time.*

Implementation. The prototypes of the algorithms listed in Table 2 have been well implemented in the Wolfram language on Mathematica 11.3 with Intel Core i7-10700 CPU at 2.90GHz, available at `https://github.com/meijingyi/CheckQCTLPlus`. We have implemented all the

Table 2: Summary on Deciding QCTL$^+$ Formulas

formula type	QMC w/ an initial state	QMC w/o an initial state
atomic path formulas	matrix & POVM, **PTIME** [35, 34]	
$\{\wedge, \vee\}$ of atomic path formulas	matrix & POVM, **PTIME** w.r.t. $\|\mathfrak{C}\|$, **EXPTIME** w.r.t. $\|\phi\|$	
$\{\neg\}$ of path formulas	matrix (if convergent) & POVM, **PTIME**	
basic state formulas	**PTIME** [16]	**PTIME** [16]
trace-quantifier formulas	POVM, **PTIME** [35]	POVM, **PTIME** [35]
fidelity-quantifier formulas	matrix, **PTIME** [34]	matrix, **EXPTIME** [34]

function prototypes required for checking QCTL$^+$ properties, and delivered them as user-friendly interface modules in the online file Functions.nb. The main functions are introduced as follows.

- `QMCinitialize` constructs and initializes QMC model with given information;
- `ComputeBSCC` computes the direct-sum of all BSCC subspaces with respect to a specified super-operator;
- `UBuntilSOVM` (resp. `UBuntilPOVM`), `BuntilSOVM` (resp. `BuntilPOVM`), `NextSOVM` (resp. `NextPOVM`) synthesize the super-operators of three kinds of atomic path formulas by establishing SOVM spaces (resp. POVM spaces);
- `isConvgtwithInit` (resp. `isConvgt`) checks whether a specified super-operator satisfies the convergence condition on an initial density operator (resp. uniform convergence condition);
- `NegUBuntilSOVM` (resp. `NegUBuntilPOVM`), `NegBuntilSOVM` (resp. `NegBuntilPOVM`), `NegNextSOVM` (resp. `NegNextPOVM`) synthesize the super-operators of the negation of three kinds of atomic path formulas by establishing SOVM spaces (resp. POVM spaces);
- `TracewithInit` (resp. `Trace`), `FidelitywithInit` (resp. `Fidelity`) decide the truth of trace-quantifier and fidelity-quantifier formulas over a QMC fed with an initial quantum state (resp. without any initial one).

After inputing the dimension of the Hilbert space, a QMC model $\mathfrak{C}$, a QCTL$^+$ state formula Φ or path formula ϕ, and an initial quantum state ρ_0, one can invoke the algorithms by calling the above functions respectively. In addition, we validate the correctness of the quantum teleportation protocol in file QTEL-Reduce.nb. We carry on the running example of quantum Bernoulli factory protocol in the file Bernoulli Factory.nb. It takes an overall consumption of 6.78 seconds in time and 123.66 MB in memory, since the efficiency is guaranteed by the fact that all functions involved have the complexity **PTIME**. Whereas, it is not guaranteed only for the function `Fidelity` due to the complexity **EXPTIME**.

7. Conclusion

We have proposed a more expressive logic — QCTL$^+$ to specify temporal properties over quantum Markov chains. This logic extends QCTL by allowing the conjunction in path formulas and the negation in the top level of path formulas. To deal with conjunction, we have presented a product construction of classical states in the QMC and the tri-valued truths of atomic path formulas; to deal with negation, we have developed an algebraic approach to computing the safety of the bottom strongly connected component subspace with respect to a super-operator under the necessary and sufficient convergence conditions. We partially solve the model checking problem of QCTL$^+$ on QMC. If the convergence conditions are not met, it is still unclear to us whether the safety problem is decidable. Finally, the complexity of our method was provided in terms of the size of both the input QMC and the QCTL$^+$ formula.

For future work, we would like to:

- consider how to conditionally drop the restriction that the negation is allowed to act on the top level of path formulas;
- study how to check such a logic for a more complex model, such as quantum Markov decision process [39] and quantum continuous-time Markov chain [36];
- incorporate the method into an automated verification tool and apply it to more scenarios.

Acknowledgements

The authors are grateful to the anonymous reviewers 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, the Research Funds of Happiness Flower ECNU (No. 2020ECNU-XFZH005), and the Inria-CAS joint project Quasar.

References

[1] Aziz, A., Singhal, V., Balarin, F., Brayton, R. K., Sangiovanni-Vincentelli, A. L., 1995. It usually works: The temporal logic of stochastic systems. In: Wolper, P. (Ed.), Computer Aided Verification: 7th International Conference, CAV'95. Vol. 939 of LNCS. Springer, pp. 155–165.

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

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

[4] Bianco, A., de Alfaro, L., 1995. Model checking of probabilistic and nondeterministic systems. In: Thiagarajan, P. S. (Ed.), Foundations of Software Technology and Theoretical Computer Science. Vol. 1026 of LNCS. Springer, pp. 499–513.

[5] Burrell, A. H., Szwer, D. J., Webster, S. C., Lucas, D. M., 2010. Scalable simultaneous multiqubit readout with 99.99% single-shot fidelity. Physical Review A 81, article no. 040302.

[6] Chong, F., Franklin, D., Martonosi, M., 2017. Programming languages and compiler design for realistic quantum hardware. Nature 549, 180–187.

[7] Clarke, E. M., Emerson, E. A., Sistla, A. P., 1986. Automatic verification of finite-state concurrent systems using temporal logic specifications. ACM Transactions on Programming Languages and Systems 8 (2), 244–263.

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

[9] Cohen, H., 1996. A Course in Computational Algebraic Number Theory. Springer.

[10] 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.

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

[12] Duan, Z., Niu, L., 2018. Some properties of quantum fidelity in infinite-dimensional quantum systems. International Journal of Quantum Information 16 (03), article no. 1850028.

[13] Emerson, E. A., 1990. Temporal and modal logic. In: van Leeuwen, J. (Ed.), Handbook of Theoretical Computer Science. Volume B, Formal Models and Sematics. Elsevier, pp. 995–1072.

[14] Fei, Y.-Y., Meng, X.-D., Gao, M., Wang, H., Ma, Z., 2018. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. Scientific Reports 8, 4283.

[15] 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 fuer Informatik, pp. 35:1–35:16.

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

[17] 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.

[18] 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.

[19] Hardy, G. H., Wright, E. M., 1979. An Introduction to the Theory of Numbers, 5th Edition. Oxford University Press.

[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] Keane, M. S., O'Brien, G. L., 1994. A Bernoulli factory. ACM Transactions on Modeling and Computer Simulation 4 (2), 213–219.

[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] Loos, R., 1983. Computing in algebraic extensions. In: Buchberger, B., Collins, G. E., Loos, R. (Eds.), Computer Algebra: Symbolic and Algebraic Computation, 2nd Edition. Springer, pp. 173–187.

[25] Masser, D. W., 1988. Linear relations on algebraic groups. In: Baker, A. (Ed.), New Advances in Transcendence Theory. Cambridge University Press, pp. 248–262.

[26] Myerson, A. H., Szwer, D. J., Webster, S. C., Allcock, D. T. C., Curtis, M. J., Imreh, G., Sherman, J. A., Stacey, D. N., Steane, A. M., Lucas, D. M., 2008. High-fidelity readout of trapped-ion qubits. Physical Review Letters 100, article no. 200502.

[27] Nielsen, M. A., Chuang, I. L., 2000. Quantum Computation and Quantum Information, 10th Anniversary Edition Edition. Cambridge University Press.

[28] Ouaknine, J., Worrell, J., 2014. Ultimate positivity is decidable for simple linear recurrence sequences. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (Eds.), Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Part II. Vol. 8573 of LNCS. Springer, pp. 330–341.

[29] Pnueli, A., 1977. The temporal logic of programs. In: Proc. 18th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, pp. 46–57.

[30] 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.

[31] Uhlmann, A., 2000. On "partial" fidelities. Reports on Mathematical Physics 45 (3), 407–418.

[32] von Neumann, J., 1951. Various techniques used in connection with random digits. In: Householder, A. S., Forsythe, G. E., Germond, H. H. (Eds.), Monte Carlo Method. US Government Printing Office, Washington, DC, pp. 36–38.

[33] Xu, F., Qi, B., Lo, H.-K., 2010. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New Journal of Physics 12, article no. 113026.

[34] Xu, M., Fu, J., Mei, J., Deng, Y., 2021. An algebraic method to fidelity-oriented model checking over quantum Markov chains. CoRR abs/2101.04971, available at https://arxiv.org/abs/2101.04971.

[35] Xu, M., Huang, C.-C., Feng, Y., 2021. Measuring the constrained reachability in quantum Markov chains. Acta Informatica 58 (6), 653–674.

[36] Xu, M., Mei, J., Guan, J., Yu, N., 2021. Model checking quantum continuous-time Markov chains. In: Haddad, S., Varacca, D. (Eds.), 32th International Conference on Concurrency Theory, CONCUR 2021. Vol. 203 of LIPIcs. Schloss Dagstuhl, pp. 13:1–13:17.

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

[38] 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.

[39] Ying, S., Ying, M., 2018. Reachability analysis of quantum Markov decision processes. Information and Computation 263, 31–51.

Appendix A. Quantifier Elimination over Real Closed Fields

Algorithm 1 Quantifier Elimination over Real Closed Fields [3, Algorithm 14.5]

$$G(\mathbf{y}) \leftarrow \mathrm{QE}(\mathrm{Q}_1\,\mathbf{x}_1 \cdots \mathrm{Q}_\ell\,\mathbf{x}_\ell\colon F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y}))$$

Input: $\mathrm{Q}_1\,\mathbf{x}_1 \cdots \mathrm{Q}_\ell\,\mathbf{x}_\ell\colon F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$ is a quantified polynomial formula, in which

- $\mathbf{x}_i$ ($i \in \{1, \ldots, \ell\}$) are blocks of k_i variables quantified by $\mathrm{Q}_i \in \{\forall, \exists\}$,
- $\mathbf{y}$ is a block of l free variables,
- 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 $\mathbb{P}$,
- s is the cardinality of $\mathbb{P}$, and
- d is the maximum degree of the polynomials in $\mathbb{P}$.

Output: $G(\mathbf{y})$ is a quantifier-free polynomial formula, which is equivalent to $\mathrm{Q}_1\,\mathbf{x}_1 \cdots \mathrm{Q}_\ell\,\mathbf{x}_\ell\colon F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$. For each realizable sign condition of $\mathbb{P}$ with respect to the variable partition $\{\{\mathbf{x}_1\}, \ldots, \{\mathbf{x}_\ell\}, \{\mathbf{y}\}\}$, the sample is also provided by a subroutine [3, Algorithm 13.2].

Complexity: $s^{(k_1+1)\cdots(k_\ell+1)(l+1)} d^{O(k_1)\cdots O(k_\ell) O(l)}$.

To make Algorithm 1 more intuitive, we briefly describe its process in the setting as follows. For the input $(\sum_{i=1}^{\ell} k_i + l)$-variate polynomial formula $F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$, we extract all polynomials in F as the polynomial collection $\mathbb{P}$. From the polynomials p in $\mathbb{P}$, the algorithm firstly applies variable elimination to get some critical polynomials of fewer and fewer variables, with which the zeros of p could be cylindrically indexed as a tree structure. Then it computes all realizable sign conditions of $\mathbb{P}$ and those critical polynomials, each sign condition gives the signs of all polynomials in $\mathbb{P}$ and those critical polynomials, which is realized by some sample in $\mathbb{R}^{\sum_{i=1}^{\ell} k_i + l}$. Furthermore, since these samples are cylindrically indexed, the universal quantifier could be replaced with a finite conjunction over samples and the existential quantifier could be replaced with a finite disjunction. Thereby, the original formula $\mathrm{Q}_1\,\mathbf{x}_1 \cdots \mathrm{Q}_\ell\,\mathbf{x}_\ell\colon F(\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{y})$ is equivalent to the disjunction (quantifier-free) of all solution sign conditions with respect to free variables, each of which is realized by some sample.

There are many tools that have implemented Algorithm 1, such as Reduce (a.k.a. RedLog [11]) and Z3 [10].