

(Un)decidable Problems about Reachability of Quantum Systems

Yangjia Li and Mingsheng Ying
TNLIST, Dept. of CS, Tsinghua University, China
QCIS, FEIT, University of Technology, Sydney, Australia
liyangjia@gmail.com

Abstract

We study the reachability problem of a quantum system modelled by a quantum automaton. The reachable sets are chosen to be boolean combinations of (closed) subspaces of the state space of the quantum system. Four different reachability properties are considered: eventually reachable, globally reachable, ultimately forever reachable, and infinitely often reachable. The main result of this paper is that all of the four reachability properties are undecidable in general; however, the last three become decidable if the reachable sets are boolean combinations without negation.

1 Introduction

Recently, verification of quantum systems has simultaneously emerged as an important problem from several very different fields. First, it was identified by leading physicists as one of the key steps in the simulation of many-body quantum systems [9]. Secondly, verification techniques for quantum protocols [11, 3] become indispensable as quantum cryptography is being commercialised. Thirdly, verification of quantum programs [26, 27] will certainly attract more and more attention, in particular after the announcement of several scalable quantum programming languages like Quipper [12].

Reachability is a fundamental issue in the verification and model-checking of both classical and probabilistic systems because a large class of verification problems can be reduced to reachability analysis [4]. Reachability of quantum systems also started to receive attention in recent years. For example, Eisert, Müller and Gogolin's notion of quantum measurement occurrence in physics [10] is essentially the reachability of null state; a certain reachability problem [25] lies at the heart of quantum control theory since the controllability of a quantum mechanical system requires that all states are reachable by choosing the Hamiltonian of the system [1]. Reachability of quantum systems modelled by quantum automata, or more generally by quantum Markov chains, was stud-

ied by the authors [28] with an application in termination analysis of quantum programs [16, 29].

This paper is a continuation of our previous work [28, 16, 29], where only reachability to a single (closed) subspace of the state Hilbert space of a quantum system was considered. In this paper, we consider a class of much more general reachability properties; that is, we use subspaces of the state space as the basic properties (atomic propositions) about the quantum system, and then reachability properties can be defined as certain temporal logical formulas over general properties, which are formalized as boolean combinations of the subspaces. The reason for using boolean combinations rather than orthomodular lattice-theoretic combinations in the Birkhoff-von Neumann quantum logic [6] is that in applications these reachability properties will be used as a high-level specification language where boolean connectives are suitable; for example, when a physicist says that a particle will eventually enter region A or region B , the word “or” here is usually meant to be the boolean “or” but not the orthomodular “or” (see Example 2.1). The reachability properties that we are concerned with are:

- eventually reachability denoted by the temporal logic formula $\mathbf{F}f$;
- globally reachability denoted by $\mathbf{G}f$;
- ultimately forever reachability denoted by $\mathbf{U}f$;
- infinitely often reachability denoted by $\mathbf{I}f$,

where f is a boolean combination of the subspaces of the state Hilbert space.

We use quantum automata [14] as a formal model for quantum systems. Then the reachability problem can be described as: decide whether or not all the execution paths of a quantum automaton satisfy $\mathbf{F}f$, $\mathbf{G}f$, $\mathbf{U}f$, or $\mathbf{I}f$. There are two reasons for adopting this model. First, it contains unitary operations so that a lot of closed physical systems can be modelled, e.g., quantum circuits. Second, without probabilistic choices (which occur in other operations such as quantum measurements and super-operators) it can be seen more clear that the reachability problem for quantum systems is essentially more difficult than that for classical systems. In fact, we note that reachability analysis is challenging in the quantum scenario, since the state space is a continuum where some techniques that have been successfully used in the classical case will become ineffective.

1.1 Contributions of the paper

- We prove undecidability of the above reachability problem, even with f in a very simple form containing the boolean negation. Undecidability of $\mathbf{G}f$ (globally reachable), $\mathbf{U}f$ (ultimately forever reachable) and $\mathbf{I}f$ (infinitely often reachable) comes from a straightforward reduction from the emptiness problem for quantum automata [7]. However, undecidability of $\mathbf{F}f$ (eventually reachable) requires a careful reduction from the halting

problem for 2-counter Minsky machines [18]. In particular, a novel strategy is introduced in this reduction to simulate a (possibly irreversible) classical computation using a quantum automaton which is definitely reversible. These undecidability results present an impressive difference between quantum systems and classical systems because the reachability properties considered in this paper are decidable for classical systems.

- We prove decidability of the reachability problem for $\mathbf{G}f$, $\mathbf{U}f$, and $\mathbf{I}f$ with f being positive; that is, containing no negation. A key strategy in proving this decidability is to characterize how a set of states can be reached infinitely often in execution paths of a quantum automaton. For the special case where the quantum automaton has only a single unitary operator and f is an atomic proposition, it is shown based on the Skolem-Mahler-Lech Theorem [24, 17, 15] that states are reached periodically, and thus the execution can be represented by a cycle graph. In general, we show that this execution graph becomes a general directed graph representing a reversible DFA (deterministic finite automaton), which can be inductively constructed.

1.2 Organization of the paper

The main results are stated in Sec. 2 after introducing several basic definitions. In Sec. 3 we first give a brief discussion about the Skolem’s problem and relate it to a special case of the quantum reachability problem. Then we prove undecidability of $\mathbf{G}f$, $\mathbf{U}f$ and $\mathbf{I}f$. The undecidability of $\mathbf{F}f$ is separately proved in Sec. 4 by using 2-counter Minsky machines. The proofs of decidable results about $\mathbf{G}f$, $\mathbf{U}f$ and $\mathbf{I}f$ for positive f and related algorithms are presented in Sec. 5. A brief conclusion is drawn in Sec. 6. Some technical lemmas are collected in Appendix.

2 Basic Definitions and Main Results

2.1 A Propositional Logic for Quantum Systems

We first introduce a propositional logical language to describe boolean combinations of the subspaces of a Hilbert space. Let \mathcal{H} be the state Hilbert space of a quantum system. A basic property of the system can be described by a (closed) subspace V of \mathcal{H} . In quantum mechanics, to check whether or not this property is satisfied, a binary (yes-no) measurement $\{P_V, P_{V^\perp}\}$ would be performed on the system’s current state $|\psi\rangle$, where P_V and P_{V^\perp} are the projection on V and its ortho-complement V^\perp , respectively. The measurement outcome is generally nondeterministic: X is considered as being satisfied in $|\psi\rangle$ with probability $\langle\psi|P_V|\psi\rangle$, and it is not satisfied with probability $\langle\psi|P_{V^\perp}|\psi\rangle = 1 - \langle\psi|P_V|\psi\rangle$. A quantitative satisfaction relation can be defined by setting a threshold $\lambda \in [0, 1]$ to the probability of satisfaction:

$$V \text{ is } (\lambda, \triangleright) - \text{satisfied in } |\psi\rangle \text{ if } \langle\psi|P_V|\psi\rangle \triangleright \lambda$$

where $\triangleright \in \{<, \leq, >, \geq\}$. In this paper, we only consider the *qualitative* satisfaction, namely, the $(\lambda, \triangleright)$ -satisfaction with the threshold λ being 0 or 1. Obviously, we have:

- $V = \{|\psi\rangle \in \mathcal{H}|V \text{ is } (1, \geq) \text{ - satisfied in } |\psi\rangle\}$;
- $V^\perp = \{|\psi\rangle \in \mathcal{H}|V \text{ is } (0, \leq) \text{ - satisfied in } |\psi\rangle\}$.

Thus, it is reasonable to choose the set of atomic propositions to be $AP = \{V|V \text{ is a (closed) subspace of } \mathcal{H}\}$. Furthermore, we define a (classical) propositional logic over AP so that we can talk about, for example, that “the current state of the quantum system is in subspace U , or in V but not in W ”. The logical formulas are generated from AP by using boolean connectives \neg , \wedge and \vee , and their semantics are inductively defined as follows: for any state $|\psi\rangle \in \mathcal{H}$,

- If $f \in AP$, then $|\psi\rangle \models f$ if $|\psi\rangle \in f$;
- $|\psi\rangle \models \neg f$ if $|\psi\rangle \models f$ does not hold;
- $|\psi\rangle \models f_1 \wedge f_2$ if $|\psi\rangle \models f_1$ and $|\psi\rangle \models f_2$;
- $|\psi\rangle \models f_1 \vee f_2$ if $|\psi\rangle \models f_1$ or $|\psi\rangle \models f_2$.

For a logical formula f , we write $\|f\|$ for the set of states that satisfy f . In general, $\|f\|$ might not be a subspace of \mathcal{H} . For example, for a subspace V of \mathcal{H} , we have:

- $\|\neg V\| = \{|\psi\rangle \in \mathcal{H}|V \text{ is } (1, <) \text{ - satisfied in } |\psi\rangle\}$;
- $\|\neg(V^\perp)\| = \{|\psi\rangle \in \mathcal{H}|V \text{ is } (0, >) \text{ - satisfied in } |\psi\rangle\}$.

It is clear that these classical connectives are different from their quantum counterparts interpreted as the operations in the orthomodular lattice of (closed) subspaces of \mathcal{H} [6].

2.2 Reachability of Quantum Automata

Definition 2.1 *A quantum automaton is a 4-tuple $\mathcal{A} = (\mathcal{H}, Act, \{U_\alpha | \alpha \in Act\}, \mathcal{H}_{ini})$, where*

1. \mathcal{H} is the state Hilbert space;
2. Act is a finite set of action names;
3. for each name $\alpha \in Act$, U_α is a unitary operator in \mathcal{H} ;
4. $\mathcal{H}_{ini} \subseteq \mathcal{H}$ is the subspace of initial states.

We say that automaton \mathcal{A} is finite-dimensional if its state space \mathcal{H} is finite-dimensional. Throughout this paper, we only consider finite-dimensional quantum automata.

A path of \mathcal{A} is generated by successively performing actions, starting in an initial state:

$$p = |\psi_0\rangle \xrightarrow{U_{\alpha_0}} |\psi_1\rangle \xrightarrow{U_{\alpha_1}} |\psi_2\rangle \xrightarrow{U_{\alpha_2}} \dots,$$

where $|\psi_0\rangle \in \mathcal{H}_{ini}$, $\alpha_n \in Act$, and $|\psi_{n+1}\rangle = U_{\alpha_n}|\psi_n\rangle$ for all $n \geq 0$. For a given initial state $|\psi_0\rangle$ and a sequence of actions $w = \alpha_0\alpha_1\alpha_2 \dots \in Act^\omega$, we write the corresponding path as $p = p(|\psi_0\rangle, w)$. We further write $\sigma(p) = |\psi_0\rangle|\psi_1\rangle|\psi_2\rangle \dots$ for the sequence of states in p . Sometimes, we simply call $\sigma(p)$ a path of \mathcal{A} .

Now let f be a logical formula defined in the above subsection representing a boolean combination of the subspaces of the state Hilbert space, and let $\sigma = |\psi_0\rangle|\psi_1\rangle|\psi_2\rangle \dots$ be an infinite sequence of states in \mathcal{H} . Formally, we define:

- (Eventually reachable): $\sigma \models \mathbf{F}f$ if $\exists i \geq 0. |\psi_i\rangle \models f$;
- (Globally reachable): $\sigma \models \mathbf{G}f$ if $\forall i \geq 0. |\psi_i\rangle \models f$;
- (Ultimately forever reachable): $\sigma \models \mathbf{U}f$ if $\overset{\infty}{\forall} i \geq 0. |\psi_i\rangle \models f$;
- (Infinitely often reachable): $\sigma \models \mathbf{I}f$ if $\overset{\infty}{\exists} i \geq 0. |\psi_i\rangle \models f$.

Here, $\overset{\infty}{\forall} i \geq 0$ means “ $\exists j \geq 0, \forall i \geq j$ ”, and $\overset{\infty}{\exists} i \geq 0$ means “ $\forall j \geq 0, \exists i \geq j$ ”. These reachability properties can be directly applied to quantum automata.

Definition 2.2 Let \mathcal{A} be a quantum automaton. Then for $\Delta \in \{\mathbf{F}, \mathbf{G}, \mathbf{U}, \mathbf{I}\}$, we define:

$$\mathcal{A} \models \Delta f \text{ if } \sigma(p) \models \Delta f \text{ for all paths } p \text{ in } \mathcal{A}.$$

The reachability of a quantum automaton \mathcal{A} can be stated in a different way. For any action string $s = \alpha_0\alpha_1 \dots \alpha_n \in Act^*$, we write $U_s = U_{\alpha_n} \dots U_{\alpha_1} U_{\alpha_0}$. If $U_s|\psi_0\rangle \models f$ for some initial state $|\psi_0\rangle \in \mathcal{H}_{ini}$, then we say that s is accepted by \mathcal{A} with f . The set of all accepted action strings is called the language accepted by \mathcal{A} with f , and denoted by $\mathcal{L}(\mathcal{A}, f)$. We say that a set $S \subseteq Act^*$ satisfies the *liveness* property, if

$$\forall w = \alpha_0\alpha_1\alpha_2 \dots \in Act^\omega, \overset{\infty}{\exists} n \geq 0, \alpha_0\alpha_1 \dots \alpha_n \in S. \quad (1)$$

Lemma 2.1 Let \mathcal{A} be a quantum automaton with $\dim \mathcal{H}_{ini} = 1$. Then:

1. $\mathcal{A} \models \mathbf{F}f$ iff $Act^\omega = \mathcal{L}(\mathcal{A}, f) \cdot Act^\omega$;
2. $\mathcal{A} \models \mathbf{I}f$ iff $\mathcal{L}(\mathcal{A}, f)$ satisfies the liveness condition;
3. $\mathcal{A} \models \mathbf{G}f$ iff $\mathcal{L}(\mathcal{A}, f) = Act^*$ (i.e. $\mathcal{L}(\mathcal{A}, \neg f) = \emptyset$);
4. $\mathcal{A} \models \mathbf{U}f$ iff $Act^* - \mathcal{L}(\mathcal{A}, f)$ (i.e. $\mathcal{L}(\mathcal{A}, \neg f)$) is finite.

Here, $X \cdot Y$ in clause 1) is the concatenation of X and Y .

Proof: Clauses 1), 2) and 3) can be derived by definition. We only prove clause 4). Let $|\psi_0\rangle \in \mathcal{H}_{ini}$. If $Act^* - \mathcal{L}(\mathcal{A}, f)$ is finite, then there exists some $N \geq 0$ such that $s \in \mathcal{L}(\mathcal{A}, f)$ and thus $U_s|\psi_0\rangle \in \|f\|$ for all action strings $s = \alpha_0\alpha_1 \cdots \alpha_n \in Act^*$ with $n \geq N$. Furthermore for any path p of \mathcal{A} , and $\sigma(p) = |\psi_0\rangle|\psi_1\rangle \cdots$, we have $|\psi_n\rangle \in \|f\|$ for all $n \geq N + 1$, and it follows that $\sigma(p) \models \mathbf{U}f$. Therefore, $\mathcal{A} \models \mathbf{U}f$. On the other hand, if $Act^* - \mathcal{L}(\mathcal{A}, f)$ is infinite, then according to the König's infinity lemma, there exists an infinite sequence $w = \alpha_0\alpha_1 \cdots \in Act^\omega$ such that $\exists n \geq 0, \alpha_0\alpha_1 \cdots \alpha_n \in Act^* - \mathcal{L}(\mathcal{A}, f)$. For the corresponding path $p = p(|\psi_0\rangle, w)$, we have $\sigma(p) \not\models \mathbf{U}f$. So $\mathcal{A} \not\models \mathbf{U}f$. \square

2.3 An Illustrative Example

Example 2.1 Consider a quantum walk on a quadrilateral with the state Hilbert space $\mathcal{H}_4 = \text{span}\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. Its behaviour is described as follows:

1. Initialize the system in state $|0\rangle$.
2. Perform a measurement $\{P_{\text{yes}}, P_{\text{no}}\}$, where $P_{\text{yes}} = |2\rangle\langle 2|$, $P_{\text{no}} = I_4 - |2\rangle\langle 2|$. Here, I_4 is the 4×4 unit matrix. If the outcome is “yes”, then the walk terminates; otherwise execute step 3).
3. Nondeterministically choose one of the two unitary operators:

$$W_{\pm} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 0 & \mp 1 \\ \pm 1 & \mp 1 & \pm 1 & 0 \\ 0 & 1 & 1 & \pm 1 \\ 1 & 0 & -1 & \pm 1 \end{pmatrix}$$

and apply it. Then go to step 2).

It was proved in [16] that this walk terminates with a probability less than 1 if and only if a diverging state (i.e. a state with terminating probability 0) can be reached, and the set of diverging states is $PD_1 \cup PD_2$, where

$$PD_1 = \text{span}\{|0\rangle, (|1\rangle - |3\rangle)/\sqrt{2}\},$$

$$PD_2 = \text{span}\{|0\rangle, (|1\rangle + |3\rangle)/\sqrt{2}\}.$$

So, termination of the walk can be expressed as a reachability property $\mathcal{A} \models \mathbf{G}\neg(PD_1 \vee PD_2)$. Here, “ \vee ” is obviously boolean disjunction rather than the disjunction in Birkhoff-von Neumann quantum logic.

2.4 Main Theorems

Now we are ready to present the main problem considered in this paper. For $\Delta \in \{\mathbf{F}, \mathbf{G}, \mathbf{U}, \mathbf{I}\}$, the decision problem for the Δ -reachability is defined as follows:

Problem 2.1 *Given a finite-dimensional quantum automaton \mathcal{A} and a logical formula f representing a boolean combination of the subspaces of the state Hilbert space of \mathcal{A} , decide whether or not $\mathcal{A} \models \Delta f$.*

For the algorithmic purpose, it is reasonable to make the convention: we identify a subspace of \mathcal{H} with the projection operator on it, and assume that all the projection operators and unitary operators in automaton \mathcal{A} and formula f are represented by complex matrices in a fixed orthonormal basis. Furthermore, we assume that all complex numbers are rational.

The main results of this paper can be stated as the following two theorems:

Theorem 2.1 (*Undecidability*) *For $\Delta \in \{\mathbf{F}, \mathbf{G}, \mathbf{U}, \mathbf{I}\}$, the problem whether or not $\mathcal{A} \models \Delta f$ is undecidable.*

Theorem 2.2 (*Decidability*) *For $\Delta \in \{\mathbf{G}, \mathbf{U}, \mathbf{I}\}$, if f contains no negation, then the problem whether or not $\mathcal{A} \models \Delta f$ is decidable.*

3 Relating Quantum Reachability to The Skolem's Problem

3.1 The Skolem's Problem for Linear Recurrence Sequences

For convenience of the reader, we first recall several results about the Skolem's problem. A linear recurrence sequence is a sequence $\{a_n\}_{n=0}^{\infty}$ satisfying a linear recurrence relation given as follows:

$$a_{n+d} = c_{d-1}a_{n+d-1} + c_{d-2}a_{n+d-2} + \cdots + c_0a_n, \quad (2)$$

for all $n \geq 0$, where c_0, c_1, \dots, c_{d-1} are constants with $c_0 \neq 0$, and d is called the order of this relation. Let

$$Z = \{n \in \mathbb{N} | a_n = 0\} \quad (3)$$

be the set of indices of null elements of the sequence $\{a_n\}_{n=0}^{\infty}$. The problem of characterising Z was first studied by Skolem [24] in 1934, and his result was generalised by Mahler [17] and Lech [15].

Theorem 3.1 (Skolem-Mahler-Lech) *In a field of characteristic 0, for any linear recurrence sequence $\{a_n\}_{n=0}^{\infty}$, the set Z of indices of its null elements is semi-linear; that is, it is the union of a finite set and finitely many arithmetic progressions.*

The above Skolem's problem was further considered in terms of decidability. The problem of deciding whether or not Z is infinite was solved by Berstel and Mignotte [5] who found an algorithm for generating all arithmetic progressions used in Theorem 3.1. The problem of deciding the finiteness of the complement of Z was studied by Salomaa and Soittola [23]. Their results are summarised as the following:

Theorem 3.2 (Berstel-Mignotte-Salomaa-Soittola) *For linear recurrence sequences $\{a_n\}_{n=0}^\infty$, it is decidable whether or not*

1. Z is infinite;
2. $Z = \mathbb{N}$;
3. Z contains all except finitely many natural numbers.

The following emptiness problem dual to item 2) in Theorem 3.2 was also considered in the literature, but it is still open; for details, we refer to [13, 22].

Problem 3.1 *Given a linear recurrence sequence $\{a_n\}_{n=0}^\infty$, decide whether or not Z is empty.*

3.2 Skolem's Problem in Matrix Form

In this subsection, we show a useful connection between the quantum reachability problem and the Skolem's problem. The linear recurrence relation Eq. (2) can be written in a matrix form:

$$a_n = u^T M^n v, \quad (4)$$

where M is the $d \times d$ matrix

$$\begin{bmatrix} c_{d-1} & c_{d-2} & \cdots & c_1 & c_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

$u = [1, 0, \dots, 0]^T$ and $v = [a_{d-1}, a_{d-2}, \dots, a_0]^T$ are d -dimensional column vectors, and T stands for transpose. On the other hand, if $\{a_n\}_{n=0}^\infty$ is of form Eq. (4) for general u, v and M with dimension d , then the minimal polynomial $g(x)$ of M is of order at most d , $g(M) = 0$, and a linear recurrence relation of order no greater than d is satisfied by $\{a_n\}_{n=0}^\infty$. Therefore, the Skolem's problem can be equivalently considered in the matrix form Eq. (4).

Let us consider Problem 2.1 in a special case: (1) $|Act| = 1$, i.e., there is only one unitary operator U_α of A , (2) $f = V$ is a subspace of \mathcal{H} , and (3) $\dim \mathcal{H}_{ini} = \dim V^\perp = 1$. Let $|\psi_0\rangle \in \mathcal{H}_{ini}$ and $|\varphi\rangle \in V^\perp$. Then we have $\mathcal{L}(A, f) = \{n \in \mathbb{N} | \langle \varphi | U_\alpha^n |\psi_0\rangle = 0\}$. It is actually the set Z in Eq. (3) if we think of U_α , $|\varphi\rangle$ and $|\psi_0\rangle$ as M , u , and v in Eq. (4). From Lemma 2.1, the emptiness of Z (Problem 3.1), and the properties 1), 2) and 3) of Z in Theorem 3.2 are equivalent to $\mathcal{A} \models \mathbf{F}V$, $\mathcal{A} \models \mathbf{I}V$, $\mathcal{A} \models \mathbf{G}V$, and $\mathcal{A} \models \mathbf{U}V$, respectively. From this point of view, our decidability for a general f (Theorem 2.2) is somewhat a generalization of the decidable results (Theorem 3.2) of Skolem's problem where f is taken to be a subspace.

3.3 Undecidability of $\mathcal{A} \models \mathbf{G}f$, $\mathcal{A} \models \mathbf{U}f$ and $\mathcal{A} \models \mathbf{I}f$

Now we consider an undecidable result relevant to the Skolem's problem. Instead of $\{M^n | n \in \mathbb{N}\}$ in Eq. (4), there is a semi-group generated by a finite number of matrices M_1, M_2, \dots, M_k , written as $\langle M_1, M_2, \dots, M_k \rangle$. Then the emptiness problem can be generalised as follows:

Problem 3.2 *Provided $d \times d$ matrices M_1, M_2, \dots, M_k and d -dimensional vectors u and v , decide whether or not $\exists M \in \langle M_1, M_2, \dots, M_k \rangle$ s.t. $u^T M v = 0$.*

The above problem was proved to be undecidable in [20] and [8], through a reduction from the Post's Correspondence Problem (PCP) [21]. Similar to the discussion in last subsection, we can choose M_i as unitary operators and u, v as quantum states, and then the emptiness of $\mathcal{L}(\mathcal{A}, f)$ for $f = V$ and $\dim \mathcal{H}_{ini} = \dim V^\perp = 1$ but with $|Act| > 1$ being allowed can be regarded as a special case of Problem 3.2. In fact, this problem was also proved to be undecidable by Blondel et. al. [7].

Theorem 3.3 (Blondel-Jeandel-Koiran-Portier) *It is undecidable whether or not $\mathcal{L}(\mathcal{A}, V)$ is empty, given a quantum automaton \mathcal{A} and a subspace V with $\dim \mathcal{H}_{ini} = \dim V^\perp = 1$.*

We can use this undecidable result to prove the Theorem 2.1 for $\Delta \in \{\mathbf{G}, \mathbf{U}, \mathbf{I}\}$. We first prove undecidability of $\mathcal{A} \models \mathbf{G}f$. Let automaton \mathcal{A} be the same as in Theorem 3.3, but put $f = \neg V$ (not V). Then according to clause 3) of Lemma 2.1, $\mathcal{A} \models \mathbf{G}f$ is equivalent to the emptiness of $\mathcal{L}(\mathcal{A}, \neg(\neg V)) = \mathcal{L}(\mathcal{A}, V)$. The undecidability follows immediately from Theorem 3.3.

To prove undecidability of $\mathcal{A} \models \mathbf{U}f$ and $\mathcal{A} \models \mathbf{I}f$, we slightly modify each quantum automaton $\mathcal{A} = (\mathcal{H}, Act, \{U_\alpha | \alpha \in Act\}, \mathcal{H}_{ini})$ by adding a silent action τ . Assume that $\tau \notin Act$ and $U_\tau = I$ (the identity operator in \mathcal{H}). Put $\mathcal{A}' = (\mathcal{H}, Act \cup \{\tau\}, \{U_\alpha | \alpha \in Act \cup \{\tau\}\}, \mathcal{H}_{ini})$. Then we claim:

$$\mathcal{A} \models \mathbf{G}f \text{ iff } \mathcal{A}' \models \mathbf{U}f \text{ iff } \mathcal{A}' \models \mathbf{I}f. \quad (5)$$

In fact, it is obvious that $\mathcal{A} \models \mathbf{G}f \Rightarrow \mathcal{A}' \models \mathbf{U}f \Rightarrow \mathcal{A}' \models \mathbf{I}f$ because U_τ is silent. Conversely, if $\mathcal{A} \not\models \mathbf{G}f$, then there exists $s = \alpha_0 \alpha_1 \dots \alpha_n \in Act^*$ such that $U_s |\psi_0\rangle \not\models f$. We consider the infinite sequence of actions $w = s\tau^\omega \in (Act \cup \{\tau\})^\omega$. It is clear that $\sigma(p(|\psi_0\rangle, w)) \not\models \mathbf{U}f$ and $\sigma(p(|\psi_0\rangle, w)) \not\models \mathbf{I}f$, and so $\mathcal{A}' \not\models \mathbf{U}f$ and $\mathcal{A}' \not\models \mathbf{I}f$. Finally, undecidability of $\mathcal{A} \models \mathbf{U}f$ and $\mathcal{A} \models \mathbf{I}f$ follows immediately from Eq. (5) and undecidability of $\mathcal{A} \models \mathbf{G}f$. Remarkably, the simple form of $f = \neg V$ is sufficient for undecidability.

4 Reduction from The halting problem for 2-counter Minsky machines

The aim of this section is to prove undecidability of $\mathcal{A} \models \mathbf{F}f$. Our strategy is a reduction from the halting problem for 2-counter Minsky machines to reachability of quantum automata.

4.1 2-counter Minsky Machine

A 2-counter Minsky machine [18] is a program \mathcal{M} consisting of two variables (counters) a and b of natural numbers \mathbb{N} , and a finite set of instructions, labeled by l_0, l_1, \dots, l_m . This program starts at l_0 and halts at l_m . Each of instructions l_0, l_1, \dots, l_{m-1} is one of the following two types:

$$\begin{array}{ll} \mathbf{increment} & l_i : c \leftarrow c + 1; \text{ goto } l_j; \\ \mathbf{test-and-decrement} & l_i : \text{ if } c = 0 \text{ then goto } l_{j_1}; \\ & \text{ else } c \leftarrow c - 1; \text{ goto } l_{j_2}; \end{array}$$

where $c \in \{a, b\}$ is one of the counters. The halting problem is as follows: given a 2-counter Minsky machine \mathcal{M} together with the initial values of a and b , decide whether the computation of \mathcal{M} will terminate or not. This problem is known to be undecidable.

For convenience of relating \mathcal{M} to a quantum automaton, we slightly modify the definition of \mathcal{M} without changing its termination:

1. Without loss of generality, we assume the initial values of a and b to be both 0. This can be done because any value can be achieved from zero by adding some instructions of increment at the beginning.
2. For each instruction l_i of test-and-decrement of c , we rewrite it as

$$\begin{aligned} l_i &: \text{ if } c = 0 \text{ then goto } l'_i; \text{ else goto } l''_i; \\ l'_i &: \text{ goto } l_{j_1}; \\ l''_i &: c \leftarrow c - 1; \text{ goto } l_{j_2}; \end{aligned} \tag{6}$$

where l'_i and l''_i are new instructions. For $c \in \{a, b\}$, we write L_{1c} for the set of all instructions of increment of c ; and we write L_{2c} , L'_{2c} and L''_{2c} for the set of instructions l_i , the set of instructions l'_i and the set of instructions l''_i given in Eq. (6), respectively. Now the set of all instructions of \mathcal{M} becomes

$$L = L_{1a} \cup L_{1b} \cup L_{2a} \cup L_{2b} \cup L'_{2a} \cup L'_{2b} \cup L''_{2a} \cup L''_{2b} \cup \{l_m\}.$$

3. We rewrite l_m as

$$l_m : \text{ goto } l_m;$$

and we define that \mathcal{M} terminates if l_m is reachable during the computation.

Obviously, the halting problem is also undecidable for 2-counter Minsky machines defined in this way.

We will encode 2-counter Minsky machines into quantum automata so that undecidability of $\mathcal{A} \models \mathbf{F}f$ is derived from the undecidability of halting problem. More precisely, for any given 2-counter Minsky machine \mathcal{M} , we will construct a quantum automaton \mathcal{A} and find two subspaces V and W of \mathcal{H} such that

$$\mathcal{M} \text{ terminates} \Leftrightarrow \mathcal{A} \models \mathbf{F}(V \wedge \neg W). \tag{7}$$

The basic ideas of this construction are outlined as follows:

1. A state of \mathcal{M} is of form (a, b, x) , where $a, b \in \mathbb{N}$ are the values of the two counters, and $x \in L$ is the instruction to be executed immediately. We will use quantum states $|\phi_n\rangle$ and $|l\rangle$ to encode nature numbers n and instructions l , respectively. Then the corresponding quantum state in \mathcal{A} is chosen as the product state $|\psi\rangle = |\phi_a\rangle|\phi_b\rangle|l\rangle$.
2. The computation of \mathcal{M} is represented by the sequence of its states:

$$\sigma_{\mathcal{M}} = (a_0, b_0, x_0)(a_1, b_1, x_1)(a_2, b_2, x_2) \cdots, \quad (8)$$

where $(a_0, b_0, x_0) = (0, 0, l_0)$ is the initial state and $(a_{i+1}, b_{i+1}, x_{i+1})$ is the successor of (a_i, b_i, x_i) for all $i \geq 0$. We will construct unitary operators of \mathcal{A} to encode the transitions from a state to its successor. Then by successively taking the corresponding unitary operators, the quantum computation

$$\sigma_0 = |\psi_0\rangle|\psi_1\rangle \cdots, \quad \forall i \geq 0 \quad |\psi_i\rangle = |\phi_{a_i}\rangle|\phi_{b_i}\rangle|x_i\rangle \quad (9)$$

is achieved in \mathcal{A} to encode $\sigma_{\mathcal{M}}$.

3. From the correspondence between $\sigma_{\mathcal{M}}$ and σ_0 , termination of \mathcal{M} will be encoded as certain reachability property of σ_0 (Lemma 4.1).
4. Besides σ_0 , infinitely many computation paths are achievable in \mathcal{A} . So there is still a gap between reachability of σ_0 and that of \mathcal{A} . Our solution is to construct two subspaces V and W such that $\sigma \models \mathbf{F}(V \wedge \neg W)$ for all paths σ of \mathcal{A} except σ_0 (Lemma 4.2). Then

$$\mathcal{A} \models \mathbf{F}(V \wedge \neg W) \Leftrightarrow \sigma_0 \models \mathbf{F}(V \wedge \neg W),$$

and Eq. (7) will be proved from this equivalence.

4.2 Encoding Classical States into Quantum States

This subsection is the first step of constructing quantum automaton \mathcal{A} . We show how to encode the states of \mathcal{M} into quantum states in a finite dimensional Hilbert space. First, we use qubit states in the 2-dimensional Hilbert space $\mathcal{H}_2 = \text{span}\{|0\rangle, |1\rangle\}$ to encode natural numbers. Consider the following unitary operator acting on \mathcal{H}_2 :

$$G = |+\rangle\langle +| + e^{i\theta}|-\rangle\langle -|,$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $e^{i\theta} = (3 + 4i)/5$. It is easy to see that for any integer n , $G^n|0\rangle = |0\rangle \Leftrightarrow n = 0$. So for each integer n , we can use $G^n|0\rangle$ to encode n . Moreover, operator G can be thought of as the successor function $g(n) = n + 1$. Now, let $\mathcal{H}_a = \mathcal{H}_b = \mathcal{H}_2$ and we use states in \mathcal{H}_a and \mathcal{H}_b to encode the counters a and b , respectively. Specifically, for each value n of $c \in \{a, b\}$, the corresponding state is $|\phi_n\rangle = G_c^n|0\rangle \in \mathcal{H}_c$.

We simply encode the instruction labels l as orthonormal quantum states $|l\rangle$ and construct the Hilbert space $\mathcal{H}_L = \text{span}\{|l\rangle | l \in L\}$. Then a state (a, b, x) of \mathcal{M} can be encoded as the quantum state $|\phi_a\rangle|\phi_b\rangle|x\rangle \in \mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_L$. Moreover, the computation $\sigma_{\mathcal{M}}$ of \mathcal{M} is encoded as the sequence σ_0 of quantum states. We note that \mathcal{M} terminates if and only if $x_i = l_m$ for some state (a_i, b_i, x_i) in $\sigma_{\mathcal{M}}$. This condition is equivalent to $|\psi_i\rangle \in V_0$, where

$$V_0 = \mathcal{H}_a \otimes \mathcal{H}_b \otimes \text{span}\{|l_m\rangle\}. \quad (10)$$

So the termination of \mathcal{M} is reduced to reachability of σ_0 as follows:

Lemma 4.1 \mathcal{M} terminates iff $\sigma_0 \models \mathbf{F}V_0$.

4.3 Construction of Unitary Operators of \mathcal{A}

In this subsection, we construct unitary operators of \mathcal{A} to encode the state transitions of \mathcal{M} . For any state (a, b, x) of \mathcal{M} , we consider the transition from this state to its successor. There are two cases:

1. $x \in L_{1a} \cup L_{1b} \cup L'_{2a} \cup L'_{2b} \cup L''_{2a} \cup L''_{2b} \cup \{l_m\}$. Then from the definition of L , x is of form

$$x : c \leftarrow c + e; \text{ goto } y;$$

where $c \in \{a, b\}$, $y \in L$ and $e = 1, 0, -1$ for $l \in L_{1c}, L'_{2c} \cup \{l_m\}, L''_{2c}$, respectively. So the successor of (a, b, x) is as $(\tilde{a}, \tilde{b}, y)$, where $\tilde{a} = a + e$, $\tilde{b} = b$ for $c = a$, and $\tilde{a} = a$, $\tilde{b} = b + e$ for $c = b$. We construct a unitary operator corresponding to x :

$$U_x = O_c^e \otimes O_{xy},$$

where $O_a = G_a \otimes I_b$ and $O_b = I_a \otimes G_b$ are unitary operators on $\mathcal{H}_a \otimes \mathcal{H}_b$, and O_{xy} is a unitary operator on \mathcal{H}_L satisfying $O_{xy}|x\rangle = |y\rangle$. Obviously, we have $|\phi_{\tilde{a}}\rangle|\phi_{\tilde{b}}\rangle|y\rangle = U_x|\phi_a\rangle|\phi_b\rangle|x\rangle$ for any a, b . So U_x is what we want.

2. $x \in L_{2a} \cup L_{2b}$. Then x is of form

$$x : \text{ if } c = 0 \text{ then goto } y; \text{ else goto } z;$$

where $c \in \{a, b\}$, $y \in L'_{2c}$ and $z \in L''_{2c}$. The successor of (a, b, x) is (a, b, y) for $c = 0$, and is (a, b, z) for $c \neq 0$. We construct two unitary operators corresponding to x :

$$U_{x0} = I_a \otimes I_b \otimes O_{xy} \text{ and } U_{x1} = I_a \otimes I_b \otimes O_{xz},$$

where $O_{xy}|x\rangle = |y\rangle$ and $O_{xz}|x\rangle = |z\rangle$. Thus, U_{x0} is used when $c = 0$, and U_{x1} is used when $c \neq 0$.

Now, we only need to specifically construct the unitary operator O_{xy} for given $x, y \in L$. To this end, we construct for each $l \in L$ a new quantum state $|\hat{l}\rangle$

to be the result of $O_{xy}|l\rangle$ (for $x \neq l$). Formally, we construct a new state space $\hat{\mathcal{H}}_L = \text{span}\{|\hat{l}\rangle : x \in L\}$ and extend \mathcal{H}_L to

$$\mathcal{H}_{2L} = \mathcal{H}_L \oplus \hat{\mathcal{H}}_L = \text{span}\{|l\rangle, |\hat{l}\rangle | l \in L\}.$$

Then O_{xy} is defined in \mathcal{H}_{2L} as

$$\begin{aligned} O_{xy}|x\rangle &= |y\rangle, \quad O_{xy}|l\rangle = |\hat{l}\rangle \quad (\forall l \in L, l \neq x), \\ O_{xy}|\hat{y}\rangle &= |\hat{x}\rangle, \quad O_{xy}|\hat{l}\rangle = |l\rangle \quad (\forall l \in L, l \neq y). \end{aligned} \quad (11)$$

Notably, O_{xy} satisfies the following property:

$$O_{xy}|z\rangle \in \hat{\mathcal{H}}_L, \forall z \in L \text{ and } z \neq x. \quad (12)$$

Finally, quantum automaton \mathcal{A} is constructed as follows: the state space is $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_{2L}$, the unitary operators are $\{U_\alpha | \alpha \in Act\}$, where

$$Act = \{x0, x1 | x \in L_{2a} \cup L_{2b}\} \cup L \setminus (L_{2a} \cup L_{2b}),$$

and the initial state is $|\psi_0\rangle = |0\rangle|0\rangle|l_0\rangle$. From the construction of the unitary operators, we see that the sequence σ_0 of quantum states defined by Eq. (9) is achievable in \mathcal{A} .

4.4 Construction of V and W

This subsection is the last step to achieve Eq. (7): construction of subspaces V and W . First, we find a way to distinguish σ_0 from other paths of \mathcal{A} . Specifically, we consider a state $|\psi_n\rangle = |\phi_{a_n}\rangle|\phi_{b_n}\rangle|x_n\rangle$ in σ_0 to be transformed by a ‘‘mismatched’’ unitary operator in $\{U_\alpha | \alpha \in Act\}$; namely, this unitary operator transforms $|\psi_n\rangle$ into a state $|\psi'\rangle$ other than $|\psi_{n+1}\rangle$. Each unitary operator in \mathcal{A} is of form U_y, U_{y0} , or U_{y1} , where y is the corresponding instruction. If $y \neq x_n$, then it is definitely mismatched. It follows from the Eq. (12) that $|\psi'\rangle \in \hat{V}$, where $\hat{V} = \mathcal{H}_a \otimes \mathcal{H}_b \otimes \hat{\mathcal{H}}_L$.

Now we only need to consider the case of $y = x_n$. We have $x_n \in L_{2a} \cup L_{2b}$, because there are two unitary operators corresponding to x_n : the one mismatched and the one not. For $x \in L_{2a}$, there are two cases:

1. $a_n = 0$ and the mismatched unitary operator is U_{x_n1} . From the definition of U_{x_n1} , we have

$$|\psi'\rangle = U_{x_n1}|0\rangle|\phi_{b_n}\rangle|x_n\rangle = |0\rangle|\phi_{b_n}\rangle|z\rangle,$$

where $z \in L''_{2a}$. We write

$$V_{2a} = \text{span}\{|0\rangle\} \otimes \mathcal{H}_b \otimes \text{span}\{|l\rangle : l \in L''_{2a}\}.$$

Then $|\psi'\rangle \in V_{2a}$.

2. $a_n > 0$ and the mismatched one is $U_{x_n 0}$. From the definition of $U_{x_n 0}$, we have

$$|\psi'\rangle = U_{x_n 0}|\phi_{a_n}\rangle|\phi_{b_n}\rangle|x_n\rangle = |\phi_{a_n}\rangle|\phi_{b_n}\rangle|y\rangle,$$

where $y \in L'_{2a}$. We write

$$\begin{aligned} V_{1a} &= \mathcal{H}_a \otimes \mathcal{H}_b \otimes \text{span}\{|l\rangle : l \in L'_{2a}\}, \\ W_a &= \text{span}\{|0\rangle\} \otimes \mathcal{H}_b \otimes \text{span}\{|l\rangle : l \in L'_{2a}\}. \end{aligned}$$

Then $|\psi'\rangle \in V_{1a} \setminus W_a$.

Similarly, for $x_n \in L_{2b}$ we can prove that $|\psi'\rangle \in V_{2b}$ for $b_n = 0$ and $|\psi'\rangle \in V_{1b} \setminus W_b$ for $b_n > 0$, where

$$\begin{aligned} V_{1b} &= \mathcal{H}_a \otimes \mathcal{H}_b \otimes \text{span}\{|l\rangle : l \in L'_{2b}\}, \\ V_{2b} &= \mathcal{H}_a \otimes \text{span}\{|0\rangle\} \otimes \text{span}\{|l\rangle : l \in L''_{2b}\}, \\ W_b &= \mathcal{H}_a \otimes \text{span}\{|0\rangle\} \otimes \text{span}\{|l\rangle : l \in L'_{2b}\}. \end{aligned}$$

We have actually proved that a state

$$|\psi'\rangle \in \hat{V} \cup (V_{1a} \setminus W_a) \cup (V_{1b} \setminus W_b) \cup V_{2a} \cup V_{2b} \quad (13)$$

is always reachable in computation paths of \mathcal{A} other than σ_0 . On the other hand, it is also easy to verify that such a state cannot be in σ_0 . So σ_0 can be distinguished by this reachability property.

Now we put

$$\begin{aligned} V &= V_0 + \hat{V} + V_{1a} + V_{1b} + V_{2a} + V_{2b}, \\ W &= W_a + W_b, \end{aligned}$$

where V_0 is defined by Eq. (10). Then we have:

Lemma 4.2 *For all paths p in \mathcal{A} with state sequences $\sigma(p) \neq \sigma_0$, we have $\sigma(p) \models \mathbf{F}(V \wedge \neg W)$.*

Proof: We only need to note that the union of five sets in Eq. (13) is included in $\{0\} \cup (V \setminus W)$, and then this result is straightforward from our discussion above. \square

Moreover, we have the following result:

Lemma 4.3 $\sigma_0 \models \mathbf{F}(V \wedge \neg W)$ iff $\sigma_0 \models \mathbf{F}V_0$.

Proof: It suffices to prove that for any state $|\psi_n\rangle$ in σ_0 ,

$$|\psi_n\rangle \in V \setminus W \text{ iff } |\psi_n\rangle \in V_0.$$

The ‘‘if’’ part is obvious since $V_0 \subseteq V$ and $V_0 \cap W = \{0\}$. We now prove the ‘‘only if’’ part. As $|\psi_n\rangle = |\phi_{a_n}\rangle|\phi_{b_n}\rangle|x_n\rangle$ is a state in σ_0 , (a_n, b_n, x_n) is a state

in $\sigma_{\mathcal{M}}$ and thus $x_n \in L$. From the definition of L and Eq. (6), $|\psi_n\rangle$ is checked in the following cases of x_n :

$$\begin{aligned} x_n \in L_{1a} \cup L_{1b} \cup L_{2a} \cup L_{2b}, & \text{ thus } |\psi_n\rangle \notin V; \\ x_n \in L'_{1a} \Rightarrow a_n = 0, & \text{ thus } |\psi_n\rangle \in W_a; \\ x_n \in L'_{1b} \Rightarrow b_n = 0, & \text{ thus } |\psi_n\rangle \in W_b; \\ x_n \in L''_{2a} \Rightarrow a_n \neq 0, & \text{ thus } |\psi_n\rangle \notin V; \\ x_n \in L''_{2b} \Rightarrow b_n \neq 0, & \text{ thus } |\psi_n\rangle \notin V. \end{aligned}$$

None of them satisfies $|\psi_n\rangle \in V \setminus W$. So the only possibility is $x_n = l_m$, and then $|\psi_n\rangle \in V_0$. \square

Finally, we obtain Eq. (7) by simply combining Lemmas 4.1, 4.2 and 4.3. Undecidability of $\mathcal{A} \models \mathbf{F}f$ is so proved, even for the simple form of $f = V \wedge \neg W$.

5 Decidable Results

We prove Theorem 2.2 in this section. We write f in the disjunctive normal form. As it contains no negation, for each conjunctive clause f_i of f , $\|f_i\|$ is a subspace of \mathcal{H} . We write $V_i = \|f_i\| \in AP$, then f can be equivalently written as $f = \bigvee_{i=1}^m V_i$ and $\|f\| = \bigcup_{i=1}^m V_i$ is a union of finitely many subspaces of the state Hilbert space \mathcal{H} of quantum automaton \mathcal{A} .

To decide whether or not $\mathcal{A} \models \Delta f$, we need to compute the set of all predecessor states with respect to a reachability property. Formally, for any given quantum automaton $\mathcal{A} = (\mathcal{H}, Act, \{U_\alpha | \alpha \in Act\}, \mathcal{H}_{ini})$ and any $|\psi\rangle \in \mathcal{H}$, we consider the automaton $\mathcal{A}(\psi) = (\mathcal{H}, Act, \{U_\alpha | \alpha \in Act\}, \text{span}\{|\psi\rangle\})$ for the paths starting in $|\psi\rangle$. Then for any $\Delta \in \{\mathbf{G}, \mathbf{U}, \mathbf{I}\}$, $|\psi\rangle$ is called a (Δ, f) -predecessor state if $\mathcal{A}(\psi) \models \Delta f$, and we write the set of all predecessor states as

$$Y(\mathcal{A}, \Delta, f) = \{|\psi\rangle \in \mathcal{H} | \mathcal{A}(\psi) \models \Delta f\}.$$

Then $\mathcal{A} \models \Delta f$ can be decided by checking whether or not $\mathcal{H}_{ini} \subseteq Y(\mathcal{A}, \Delta, f)$.

5.1 Decidability of $\mathcal{A} \models \mathbf{I}f$ for Single Unitary Operator

We will prove the decidability of $\mathcal{A} \models \mathbf{I}f$ by constructing the set $Y(\mathcal{A}, \mathbf{I}, f)$. In this subsection, we do this for a special case in which $|Act| = 1$ and $m = 1$, i.e., \mathcal{A} contains only a single unitary operator, and $f = V$ is a subspace. It should be pointed out that the result for this special case was proved in [5] as the decidability of finiteness Skolem's problem in the single matrix form. Here, we present our new proof as it would be useful for us to obtain a general result for finitely many unitary operators in next subsection. For convenience, we simply write Y for $Y(\mathcal{A}, \mathbf{I}, f)$ in these two subsections.

Let $Act = \{\alpha\}$, and the string α^n is simply represented by n . By an algorithm, we show that Y is a union of finitely many subspaces Y_0, Y_1, \dots, Y_{p-1} which forms a cycle graph under the unitary transformation, namely $Y_{r+1} =$

$U_\alpha Y_r$ for all $0 \leq r \leq p-2$ and $Y_0 = U_\alpha Y_{p-1}$. Then Y can be written as $Y = \bigcup_{r=0}^{p-1} U_\alpha^r Y_0$ and $Y_0 = U_\alpha^p Y_0$. The following lemma is required for proving correctness of our algorithm.

Lemma 5.1 *For any unitary operator U on \mathcal{H} , there exists a positive integer p such that for any subspace K of \mathcal{H} , $U^p K = K$ provided $U^n K = K$ for some integer n . We call this integer p the period of U .*

We put the technical proof of the above lemma into Appendix A. Now Y can be computed by Algorithm 1. Step 1) can be done as described in the proof of

Algorithm 1:

1. Compute the period p of U_α ;
 2. Compute the maximal subspace K of V such that $U_\alpha^p K = K$;
 3. $Y = \bigcup_{r=0}^{p-1} U_\alpha^r K$.
-

Lemma 5.1. Step 2) can be done as follows: initially put $K_0 = V$, repeatedly compute $K_{n+1} = K_n \cap U_\alpha^p K_n$ until $K_{n+1} = K_n$, and then $K = K_n$. Sometimes, we write K as $K(U_\alpha, V)$ to show dependence of K on U_α and V . Correctness of this algorithm is proved in Appendix B.

5.2 Decidability of $\mathcal{A} \models \mathbf{I}f$ for General Case

Now, we construct $Y = Y(\mathcal{A}, \mathbf{I}, f)$ for a general input: \mathcal{A} and $f = \bigvee_{i=1}^m V_i$. Like the case of single unitary operator, we can prove that Y is a union of finitely many subspaces. The result can be specifically described as follows:

Lemma 5.2 *Let $X = \{Y_1, Y_2, \dots, Y_q\}$ be a set of subspaces of \mathcal{H} satisfying the following three conditions:*

1. *For any Y_i and $\alpha \in \text{Act}$, there exists Y_j such that $U_\alpha Y_i = Y_j$. In other words, under the unitary transformations, these subspaces form a more general directed graph than a simple cycle graph in the case of single unitary operator.*
2. *For any simple loop (namely $Y_{r_i} \neq Y_{r_j}$ for different i and j in the loop)*

$$Y_{r_0} \xrightarrow{U_{\alpha_0}} Y_{r_1} \xrightarrow{U_{\alpha_1}} \dots \xrightarrow{U_{\alpha_{k-2}}} Y_{r_{k-1}} \xrightarrow{U_{\alpha_{k-1}}} Y_{r_0},$$

there exists some $i \in \{0, 1, \dots, k-1\}$ and $j \in \{1, 2, \dots, m\}$ such that $Y_{r_i} \subseteq V_j$.

3. $Y \subseteq Y_1 \cup Y_2 \cup \dots \cup Y_q$.

Then $Y = Y_1 \cup Y_2 \cup \dots \cup Y_q$.

Proof: From condition 3), it suffices to prove that if X satisfies the first two conditions, then $\cup X \subseteq Y$. We only need to prove that for any $|\psi_0\rangle \in \cup X$, we have $|\psi_0\rangle \in Y$, namely, $\mathcal{A}(\psi_0) \models \mathbf{I}f$. From the definition, it suffices to prove that

$$\forall w = \alpha_0 \alpha_1 \cdots \in Act^\omega \exists n \geq 0 \text{ s.t. } |\psi_n\rangle \in \|f\|,$$

where $|\psi_{n+1}\rangle = U_{\alpha_n} |\psi_n\rangle$ for $n = 0, 1, \dots$.

Now we choose $Y_{r_0} \in X$ such that $|\psi_0\rangle \in Y_{r_0}$. According to the first condition, let $Y_{r_{n+1}} = U_{\alpha_n} Y_{r_n}$, $n = 0, 1, \dots$. Then $|\psi_n\rangle \in Y_{r_n}$. Consider any pairs of r_i and r_j such that $i < j$, $r_i = r_j$, and $r_i, r_{i+1}, \dots, r_{j-1}$ are pairwise different. Applying the second condition in the simple loop

$$Y_{r_i} \xrightarrow{U_{\alpha_i}} Y_{r_{i+1}} \xrightarrow{U_{\alpha_{i+1}}} \cdots \xrightarrow{U_{\alpha_{j-2}}} Y_{r_{j-1}} \xrightarrow{U_{\alpha_{j-1}}} Y_{r_i},$$

there exists some n such that $i \leq n < j$ and $Y_{r_n} \subseteq \|f\|$. Then $|\psi_n\rangle \in \|f\|$. As we can choose infinitely many pairs (r_i, r_j) in the sequence w , we can find infinitely many n 's. Thus $|\psi_0\rangle \in Y$. \square

Therefore, to construct Y we only need to find an algorithm for constructing a set of subspaces $X = \{Y_1, Y_2, \dots, Y_q\}$ satisfying the three conditions of Lemma 5.2. To this end, we invoke a lemma which is proved in [16]:

Lemma 5.3 *Suppose that X_k is the union of a finite number of subspaces of \mathcal{H} for all $k \geq 0$. If $X_0 \supseteq X_1 \supseteq \cdots \supseteq X_k \supseteq \cdots$, then there exists $n \geq 0$ such that $X_k = X_n$ for all $k \geq n$.*

Now the set X can be computed by Algorithm 2. Step 2) is the key step

Algorithm 2:

1. Initially put $X \leftarrow \{\mathcal{H}\}$ then jump to step 2);
 2. If X satisfies condition 1) and condition 2) of Lemma 5.2, then return X ; otherwise construct a new set X' of subspaces of \mathcal{H} satisfying $Y \subseteq \cup X' \subset \cup X$, and put $X \leftarrow X'$, then repeat step 2). Here notation “ \subset ” is for “proper subset”.
-

in the algorithm, in which X can be replaced by a “smaller” one X' if it is not available. Due to Lemma 5.3, this step can only be executed a finite number of times and thus an output X satisfying condition 1) and condition 2) of Lemma 5.2 should be returned by the algorithm. We also note that condition 3) of Lemma 5.2 is always satisfied by X during the execution. So this output is just what we need.

Now we give a detailed description of step 2). It can be properly formalized as a lemma:

Lemma 5.4 *Given a set $X = \{Y_1, Y_2, \dots, Y_q\}$ of subspaces in which any two subspaces Y_i and Y_j do not include each other, if X satisfies condition 3) but*

does not satisfy condition 1) or condition 2) of Lemma 5.2, then we can algorithmically find some $Y_i \in X$ and its proper subspaces W_1, W_2, \dots, W_l , such that

$$Y \cap Y_i \subseteq W_1 \cup W_2 \cup \dots \cup W_l. \quad (14)$$

The proof of the above lemma is postponed to Appendix C. From this lemma, we can construct X' for any given X as follows. First, we eliminate all such Y_i from X that $Y_i \subset Y_j$ for some $Y_j \in X$. Then from Lemma 5.4 we can find some $Y_i \in X$ and its subspaces W_1, W_2, \dots, W_l satisfying Eq. (14). We put $X' = X \cup \{W_k | 1 \leq k \leq l\} \setminus \{Y_i\}$, and then $\cup X' \subset \cup X$. As $Y \subseteq \cup X$, we also have $Y \subseteq \cup X'$ from Eq. (14).

5.3 Decidability of $\mathcal{A} \models \mathbf{G}f$ and $\mathcal{A} \models \mathbf{U}f$

We now prove Theorem 2.2 for $\Delta \in \{\mathbf{G}, \mathbf{U}\}$. We first prove the decidability of $\mathcal{A} \models \mathbf{G}f$ by computing $Y = Y(\mathcal{A}, \mathbf{G}, f)$. According to clause 3) in Lemma 2.1, we have

$$\begin{aligned} Y &= \{|\psi\rangle \in \mathcal{H} | \mathcal{L}(\mathcal{A}(\psi), f) = Act^*\} \\ &= \{|\psi\rangle \in \mathcal{H} | U_s|\psi\rangle \in \|f\|, \forall s \in Act^*\}. \end{aligned} \quad (15)$$

Then we obtain $\forall \alpha \in Act$, $U_\alpha Y \subseteq Y \subseteq \|f\|$. In fact, Y can be computed by Algorithm 3, and thus Y is the maximal one of sets satisfying $\forall \alpha \in Act$, $U_\alpha Y = Y \subseteq \|f\|$.

Algorithm 3:

1. $Y \leftarrow V_1 \cup V_2 \cup \dots \cup V_m$;
 2. If $U_\alpha Y \neq Y$, for some $\alpha \in Act$, then $Y \leftarrow U_\alpha^{-1} Y \cap Y$; otherwise return Y .
-

Correctness of Algorithm 3: We write Y_0, Y_1, \dots for the instances of Y during the execution of the algorithm. Then $Y_0 = V_1 \cup V_2 \cup \dots \cup V_m$ and $Y_{n+1} = U_\alpha^{-1} Y_n \cap Y_n$ for some $\alpha \in Act$. It can be proved by induction on n that each Y_n is a union of finitely many subspaces of \mathcal{H} . Note that $Y_0 \supset Y_1 \supset Y_2 \supset \dots$ is a descending chain. According to Lemma 5.3, this chain would terminate at some n , and the algorithm output is Y_n . We have $U_\alpha Y_n = Y_n$ for all $\alpha \in Act$. Now we prove $Y_n = Y$. First, since $Y \subseteq \|f\| = Y_0$ and $Y \subseteq U_\alpha^{-1} Y$ for all $\alpha \in Act$, it can be proved by induction on k that $Y \subseteq Y_k$ for all k , and particularly, $Y \subseteq Y_n$. On the other hand, As $U_s Y_n = Y_n \subseteq \|f\|$ for all $s \in Act^*$, we have $Y_n \subseteq Y$ from the definition of Y . So $Y_n = Y$. \square

Next we prove the decidability of $\mathcal{A} \models \mathbf{U}f$. Indeed, we can prove the following lemma from which it follows that $Y(\mathcal{A}, \mathbf{U}, f) = Y(\mathcal{A}, \mathbf{G}, f)$.

Lemma 5.5 $\mathcal{A} \models \mathbf{U}f$ iff $\mathcal{H}_{ini} \subseteq Y(\mathcal{A}, \mathbf{G}, f)$.

Proof: The “if” part can be verified by observation of

$$\mathcal{A} \models \mathbf{G}f \Rightarrow \mathcal{A} \models \mathbf{U}f.$$

So we only need to prove the “only if” part. We assume $\mathcal{A} \models \mathbf{U}f$. Then for any $|\psi_0\rangle \in \mathcal{H}_{ini}$, we have $\mathcal{A}(\psi_0) \models \mathbf{U}f$. According to clause 4) of Lemma 2.1, we know that $Act^* - \mathcal{L}(\mathcal{A}(\psi_0), f)$ is finite. Then there exists some integer $N \geq 0$ such that $s \in \mathcal{L}(\mathcal{A}(\psi_0), f)$ whenever $|s| \geq N$. We choose $s = \alpha^N$. Then $U_\alpha^N |\psi_0\rangle \in Y$ for any $\alpha \in Act$. Note that $U_\alpha Y = Y$, we have $|\psi_0\rangle \in U_\alpha^{-N} Y = Y$. \square

6 Conclusion

We have investigated the decision problem of quantum reachability: decide whether or not a set of quantum states is reachable by a quantum system modelled by a quantum automaton. The reachable sets considered in this paper are defined as boolean combinations of (or described by classical propositional logical formula over) the set of (closed) subspaces of the state Hilbert space of the system. Four types of reachability properties have been studied: eventually reachable, globally reachable, ultimately forever reachable, and infinitely often reachable. Our major contribution is the (un)decidable results:

- All of these four reachability properties are undecidable even for a certain class of the reachable sets which are formalized by logical formulas of a simple form;
- Whenever the reachable set is a union of finitely many subspaces, the problem is decidable for globally reachable, ultimately forever reachable and infinitely often reachable. In particular, it is decidable when the reachable set contains only finitely many quantum states.

One of our main proof techniques is to demonstrate that quantum reachability problem is a generalization of the Skolem’s problem for unitary matrices. The undecidable results for global reachability, ultimately forever reachability and infinitely often reachability have been derived directly by employing the undecidability of a relevant emptiness problem. Nevertheless, the celebrated Skolem-Mahler-Lech theorem has been applied to the development of algorithms showing the decidable results. Another technique we have employed is to encode a 2-counter Minsky machine using a quantum automaton. It was used to prove undecidability of the eventually reachable property. This approach is interesting, since it provides a new way to demonstrate quantum undecidability other than reduction from the PCP that has been the main technique for the same purpose in previous works.

The problem whether or not $\mathcal{A} \models \mathbf{F}f$ is decidable for $\|f\|$ being a finite union of subspaces has been left unsolved. In fact, this problem is difficult even for a very special case where $|Act| = 1$ and $\|f\|$ is a single subspace. We have shown that such a reachability problem is equivalent to the emptiness Skolem’s

problem 3.1 for $\{a_n\}_{n=0}^\infty$ defined by Eq. (4) with M being a unitary operator. Unfortunately, the emptiness Skolem's problem is still open even for $n = 5$ [22].

The model of quantum systems used in this paper is quantum automata. Another problem for further studies is (un)decidability of the reachability properties considered in this paper for a more general model, namely quantum Markov chains [28] where actions can be not only unitary transformations but also super-operators.

References

- [1] C. Altafini, and F. Ticozzi, Modeling and control of quantum systems: An introduction, *IEEE Transactions on Automatic Control*, 57(2012)1898.
- [2] M. Amano, and K. Iwama. Undecidability on quantum finite automata, in: *Proceedings of the thirty-first annual ACM symposium on Theory of computing (STOC)*, 1999 pp. 368-375.
- [3] E. Ardeshir-Larijani, S. J. Gay and R. Nagarajan, Equivalence checking of quantum protocols, in: *Proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, Springer LNCS 7795, 2013, pp. 478-492.
- [4] C. Baier and J. -P. Katoen, *Principles of Model Checking*, MIT Press, Cambridge, Massachusetts, 2008.
- [5] J. Berstel and M. Mignotte, Deux propriétés décidables des suites récurrentes linéaires, *Bull. Soc. Math. France*, 104(1976)175-184.
- [6] G. Birkhoff and J. von Neumann, The Logic of Quantum Mechanics, *Annals of Mathematics*, 37(1936)823-843.
- [7] V. D. Blondel, E. Jeandel, P. Koiran and N. Portier, Decidable and undecidable problems about quantum automata, *SIAM Journal on Computing*, 34(2005)1464-1473.
- [8] J. Cassaigne and J. Karhumäki: Examples of undecidable problems for 2-generator matrix semigroups, *Theoretical Computer Science* 204(1998)29-34.
- [9] J. I. Cirac and P. Zoller, Goals and opportunities in quantum simulation, *Nature Physics*, 8(2012)264-266.
- [10] J. Eisert, M. P. Müller and C. Gogolin, Quantum measurement occurrence is undecidable, *Physical Review Letters*, 108(2012)260501.
- [11] S. J. Gay, R. Nagarajan, and N. Papanikolaou, Specification and verification of quantum protocols, in: *Semantic Techniques in Quantum Computation* (S. J. Gay and I. Mackie, eds.), Cambridge University Press, 2010, pp. 414-472.

- [12] A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger and B. Valiron, Quipper: A scalable quantum programming language, in: *Proceedings of the 34th ACM Conference on Programming Language Design and Implementation (PLDI)*, 2013, pp. 333-342.
- [13] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki, *Skolem's Problem: On the Border between Decidability and Undecidability*, Technical Report 683, Turku Centre for Computer Science, 2005.
- [14] A. Kondacs and J. Watrous, On the power of quantum finite state automata, in: *Proc. 38th Symposium on Foundation of Computer Science (FOCS)*, 1997, pp. 66-75.
- [15] C. Lech, A note on recurring series, *Ark. Mat.* 2(1953)417-421.
- [16] Y. J. Li, N. K. Yu and M. S. Ying, Termination of nondeterministic quantum programs, *Acta Informatica* (published online October 2013; also short presentation of LICS'2012).
- [17] K. Mahler, Eine arithmetische eigenschaft der Taylor koeffizienten rationaler funktionen, in: *Proc. Akad. Wet. Amsterdam*, 38, 1935.
- [18] M. L. Minsky, *Computation: finite and infinite machines*, Prentice-Hall, 1967.
- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [20] A. Paz, *Introduction to probabilistic automata*, Academic Press, New York, 1971.
- [21] E. L. Post, A variant of a recursively unsolvable problem, *Bulletin of the American Mathematical Society*, 52(1946)264-268.
- [22] J. Ouaknine and J. Worrell, Decision Problems for Linear Recurrence Sequences, in: *Reachability Problems*, Springer LNCS 7550, 2012, pp. 21-28.
- [23] A. Salomaa and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*, Springer-Verlag, 1978.
- [24] T. Skolem, Ein verfahren zur behandlung gewisser exponentialer gleichungen, in: *Proceedings of the 8th Congress of Scandinavian Mathematicians*, Stockholm, 1934, pp. 163-188.
- [25] S. G. Schirmer, A. I. Solomon and J. V. Leahy, Criteria for reachability of quantum states, *Journal of Physics A: Mathematical and General*, 35(2002)8551-8562.
- [26] M. S. Ying, Floyd-Hoare logic for quantum programs, *ACM Transactions on Programming Languages and Systems*, (2011) art. no. 19.

- [27] M. S. Ying, N. K. Yu, Y. Feng, and R. Y. Duan, Verification of quantum programs, *Science of Computer Programming*, 78(2013)1679-1700.
- [28] S. G. Ying, Y. Feng, N. K. Yu and M. S. Ying, Reachability probabilities of quantum Markov chains, in: *Proceedings of the 24th International Conference on Concurrency Theory (CONCUR)*, Springer LNCS 8052, 2013, pp. 334-348.
- [29] N. K. Yu and M. S. Ying, Reachability and termination analysis of concurrent quantum programs, in: *Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR)*, Springer LNCS 7454, 2012, pp. 69-83.

Appendix

A. Proof of Lemma 5.1

We algorithmically construct a positive integer p satisfying the following condition: for any two eigenvalues λ and μ of U_α , if $(\lambda/\mu)^n = 1$ for some integer n , then $(\lambda/\mu)^p = 1$. Note that all roots of the characteristic polynomial $f(x)$ of $U \otimes U^\dagger$ are exactly all quotients λ/μ of two eigenvalues of U . If for some quotient and integer n , $(\lambda/\mu)^n = 1$, we let n be the minimal positive integer number satisfying this condition. Then λ/μ should also be a root of the n th cyclotomic polynomial $\Phi_n(x)$. Thus $\Phi_n(x)$ should be a divisor of $f(x)$ since $\Phi_n(x)$ is irreducible. Therefore, all of such n 's can be obtained by checking whether or not $\Phi_n(x)|f(x)$. Finally, we put p to be the least common multiple of them. It is easy to verify that $(\lambda/\mu)^p = 1$ for all such quotients.

Now we prove that p is really what we want. Suppose $U^n K = K$, then there exists a basis of K such that all states of this basis are eigenstates of U^n . It suffices to prove that any eigenstate of U^n is also an eigenstate of U^p . Now we prove it by showing that any eigenspace W of U^n is also an eigenspace of U^p . Since all eigenstates of U are eigenstates of U^n , we can choose a set of eigenstates of U to form a basis of W . Consider any two of these states, written as $|\psi\rangle$ and $|\phi\rangle$, and written as λ and μ , respectively, for the corresponding eigenvalues of U . Then we have $(\lambda/\mu)^n = 1$, and according to our choice of p , $(\lambda/\mu)^p = 1$. So $|\psi\rangle$ and $|\phi\rangle$ are in the same eigenspace of U^p . As these two states are arbitrarily chosen, it implies that all of states in this basis of W are in the same eigenspace of U^p . Thus W is an eigenspace of U^p . \square

B. Correctness of Algorithm 1

For any $q \in \mathbb{N}$, we write K_q as the maximal subspace of V such that $U_\alpha^q K_q = K_q$. Then $K_p = K = K(U_\alpha, V)$. We prove that K_q can be characterized as the following set of sates:

$$\{|\psi\rangle \in V | \forall n \in \mathbb{N}, U_\alpha^{qn} |\psi\rangle \in V\}.$$

In fact, it is easy to verify that any state in K_q is also in this set. On the other hand, for any state $|\psi\rangle$ in this set, $\text{span}\{U_\alpha^{qn}|\psi\rangle|n=0,1,\dots\}$ is both a subspace of V and an invariant subspace of U_α^q , so it is a subspace of K_q according to the maximality of K_q . Then $|\psi\rangle \in K_q$. Therefore K_q is equal to the set.

Now for each $|\psi\rangle \in \mathcal{H}$, according to clause 2) in Lemma 2.1, $\mathcal{A}(\psi) \models \mathbf{IV}$ iff $\mathcal{L}(\mathcal{A}(\psi), V) = \{n \geq 0 | U_\alpha^n |\psi\rangle \in V\}$ satisfies liveness condition Eq. (1), namely it is infinite in this case. Note that $U_\alpha^n |\psi\rangle \in V$ iff $\text{tr}(P_{V^\perp} \mathcal{U}^n(\psi)) = 0$, where ψ is the density operator of $|\psi\rangle$, P_{V^\perp} is the projection operator of V^\perp and \mathcal{U} is the super-operator of U_α . Since $\{\text{tr}(P_{V^\perp} \mathcal{U}^n(\psi))\}_{n=0}^\infty$ is a linear recurrence sequence, according to Theorem 3.1, $\mathcal{L}(\mathcal{A}(\psi), V)$ is semi-linear, and thus it is infinite if and only if it contains an arithmetic progression $\{qn+r\}_{n=0}^\infty$. Then

$$\begin{aligned}
Y &= \{|\psi\rangle | \mathcal{L}(\mathcal{A}(\psi), V) \text{ is infinite}\} \\
&= \{|\psi\rangle | \exists q, r \in \mathbb{N}. \forall n \in \mathbb{N}. U_\alpha^{qn+r} |\psi\rangle \in V\} \\
&= \{|\psi\rangle | \exists q, r \in \mathbb{N}. U_\alpha^r |\psi\rangle \in K_q\} \\
&= \{|\psi\rangle | \exists q, r \in \mathbb{N}. |\psi\rangle \in U_\alpha^{q-r} K_q\} \\
&= \bigcup_{q,r \geq 0} U_\alpha^r K_q = \bigcup_{r=0}^\infty U_\alpha^r K_p = \bigcup_{r=0}^{p-1} U_\alpha^r K.
\end{aligned} \tag{16}$$

The last two equalities in Eq. (16) come from the following observation. For each integer q , since $U_\alpha^q K_q = K_q$, by Lemma 5.1 we have $U_\alpha^p K_q = K_q$. Thus $K_q \subseteq K_p = K$ follows from maximality of K . \square

C. Proof of Lemma 5.4

We need to consider the two following cases:

- Case 1. Condition 1) in Lemma 5.2 is not satisfied by X .
- Case 2. Condition 1) in Lemma 5.2 is satisfied by X but condition 2) is not.

Proof for case 1: Since condition 1) is not satisfied, we can find all Y_i and $\alpha \in \text{Act}$ such that $U_\alpha Y_i$ is not any Y_j . We choose Y_i with the maximal dimension and claim that for any $\alpha \in \text{Act}$, $U_\alpha Y_i$ can not be included in any Y_j . Otherwise, $U_\alpha Y_i$ is a proper subspace of some Y_j , and $\dim Y_j > \dim Y_i$. It is easy to prove by induction on n that all the subspaces $U_\alpha^n Y_j$ ($n = 0, 1, \dots$) are in $\{Y_1, Y_2, \dots, Y_m\}$. So, there exists some n_1 and n_2 such that $n_2 > n_1$ and $U_\alpha^{n_1} Y_j = U_\alpha^{n_2} Y_j$. Then Y_i is a proper subset of $U_\alpha^{-1} Y_j = U_\alpha^{n_2 - n_1 - 1} Y_j$, which is in $\{Y_1, Y_2, \dots, Y_m\}$. This contradicts to the assumption that any two subspaces in $\{Y_1, Y_2, \dots, Y_m\}$ do not include each other.

Now we choose $W_j = Y_i \cap U_\alpha^{-1} Y_j$ ($j = 1, 2, \dots, m$) for Y_i . All of these are proper subspaces of Y_i . On the other hand, from the definition of Y , one can easily verify that $U_\alpha |\psi\rangle \in Y$ for all $|\psi\rangle \in Y$ and for all $\alpha \in \text{Act}$. Then for any state $|\psi\rangle \in Y \cap Y_i$, we know that $U_\alpha |\psi\rangle \in Y \subseteq \cup X$. So $|\psi\rangle$ is in some $U_\alpha^{-1} Y_j$, and thus $|\psi\rangle \in Y_i \cap U_\alpha^{-1} Y_j = W_j$. Then Eq. (14) holds. \square

To prove Lemma 5.4 for case 2, we need the following:

Lemma 6.1 *For any $|\psi_0\rangle \in Y$ and $\alpha_1, \alpha_2, \dots, \alpha_k \in \text{Act}$, there exists some $r \in \{0, \dots, k-1\}$, some $t \in \{1, 2, \dots, m\}$, and some $n \in \mathbb{N}$, such that*

$$|\psi_0\rangle \in U_{\alpha_1}^{-1} U_{\alpha_2}^{-1} \dots U_{\alpha_r}^{-1} T^n K(T, V_t), \quad (17)$$

where $T = U_{\alpha_{r+1}} \dots U_{\alpha_k} U_{\alpha_1} \dots U_{\alpha_r}$, and $K(T, V_t)$ is defined as in Algorithm 1.

Proof: We consider the path p of repeatedly performing $U_{\alpha_1}, U_{\alpha_2}, \dots, U_{\alpha_k}$ from the initial state $|\psi_0\rangle$:

$$\begin{aligned} p = & |\psi_0\rangle \xrightarrow{U_{\alpha_1}} |\psi_1\rangle \xrightarrow{U_{\alpha_2}} \dots \xrightarrow{U_{\alpha_{k-1}}} |\psi_{k-1}\rangle \xrightarrow{U_{\alpha_k}} \\ & |\psi_k\rangle \xrightarrow{U_{\alpha_1}} |\psi_{k+1}\rangle \xrightarrow{U_{\alpha_2}} \dots \xrightarrow{U_{\alpha_{k-1}}} |\psi_{2k-1}\rangle \xrightarrow{U_{\alpha_k}} \\ & \dots \end{aligned} \quad (18)$$

Then $|\psi_{kn+r+1}\rangle = U_{\alpha_{r+1}} |\psi_{kn+r}\rangle$, for all $n \in \mathbb{N}$ and $r \in \{0, \dots, k-1\}$. Since $\sigma(p) \models \mathbf{I}f$, we have $|\psi_n\rangle \in \|f\|$ for infinitely many n . This further implies that there exists some $r \in \{0, 1, \dots, k-1\}$ and some $t \in \{1, 2, \dots, m\}$ such that $|\psi_{kn+r}\rangle \in V_t$ for infinitely many n . We put $T = U_{\alpha_{r+1}} \dots U_{\alpha_k} U_{\alpha_1} \dots U_{\alpha_r}$. Then the set $\{n | T^n |\psi_r\rangle \in V_t\}$ is infinite. According to the result of single unitary case, we have $|\psi_r\rangle \in T^n K(T, V_t)$. This is exactly Eq. (17). \square

Now we are able to prove Lemma 5.4 for case 2.

Proof for case 2: Since the condition 1) is satisfied but condition 2) is not, we can find a simple loop

$$Y_{r_0} \xrightarrow{U_{\alpha_1}} Y_{r_1} \xrightarrow{U_{\alpha_2}} \dots \xrightarrow{U_{\alpha_{k-1}}} Y_{r_{k-1}} \xrightarrow{U_{\alpha_k}} Y_{r_0},$$

such that $Y_{r_i} \not\subseteq V_t$ for all $i \in \{0, 1, \dots, k-1\}$ and all $t \in \{1, 2, \dots, m\}$. We choose Y_{r_0} and construct W_1, W_2, \dots, W_l to be proper subspaces of it. In fact, for each i , we write $T_i = U_{\alpha_{i+1}} \dots U_{\alpha_k} U_{\alpha_1} \dots U_{\alpha_i}$. It holds that $T_i^n Y_{r_i} = Y_{r_i} \not\subseteq V_t$, and $Y_{r_i} \not\subseteq T_i^n K(T_i, V_t)$ for all integer n . Put

$$R_{i,t,n} = U_{\alpha_1}^{-1} U_{\alpha_2}^{-1} \dots U_{\alpha_i}^{-1} T_i^n K(T_i, V_t),$$

then it actually means $Y_{r_0} \not\subseteq R_{i,t,n}$. Note that $T_i^{p_i} K(T_i, V_t) = K(T_i, V_t)$ for the period p_i of T_i . So the set $\{R_{i,t,n} | n = 0, \pm 1, \pm 2, \dots\}$ is a finite set for any $i = 0, 1, \dots, k-1$ and any $t = 1, 2, \dots, m$. Therefore, we can choose W_1, W_2, \dots, W_l to be all of the $Y_{r_0} \cap R_{i,t,n}$'s. The condition of Eq. (14) can be easily verified, since for any state $|\psi\rangle \in Y \cap Y_{r_0}$, we have $|\psi\rangle$ is in some $R_{i,t,n}$ according to Lemma 6.1. \square