CHAPTER

Analysis of quantum programs

5

Chapter 4 developed logical tools for reasoning about correctness of quantum programs. This chapter turns to algorithmic analysis of the behavior of quantum programs, with a focus on termination analysis. The theoretical results and algorithms presented in this chapter will be useful for the design of compilers for quantum programming languages and optimization of quantum programs.
The chapter is organized as follows:

- In Section 5.1, we examine the behavior of quantum extension of the **while**-loop defined in Section 3.1, including termination and average running time. This section is divided into three subsections: Subsection 5.1.1 considers a class of simple quantum loops with a unitary operator as their body, Subsection 5.1.2 further deals with quantum loops with a general quantum operation as their body, and Subsection 5.1.3 presents an example that computes the average running time of a quantum walk on an n-circle.
- Motivated by quantum **while**-loops, we identify quantum Markov chains as the semantic model of quantum programs. Furthermore, we argue that termination analysis of quantum programs can be reduced to the reachability problem of quantum Markov chains. Reachability analysis techniques for classical Markov chains heavily depend on algorithms for graph-reachability problems. Likewise, a kind of graphical structure in Hilbert spaces, called quantum graphs, play a crucial role in the reachability analysis of quantum Markov chains. So, Section 5.2 gives an introduction to quantum graph theory, which provides a mathematical basis of Section 5.3.
- In Section 5.3, we study the reachability problems for quantum Markov chains. In particular, we present several (classical) algorithms for computing the reachability, repeated reachability and persistence probabilities of quantum Markov chains.
- For readability, the proofs of several technical lemmas in Sections 5.1 to 5.3 are postponed to the last section of this chapter, Section 5.4.

Since our main aim is to develop algorithms for analyzing quantum programs, the state Hilbert spaces considered in this chapter are always assumed to be finite-dimensional. Although a few results in this chapter may also be used in an

Foundations of Quantum Programming.http://dx.doi.org/10.1016/B978-0-12-802306-8.00005-7

infinite-dimensional state Hilbert space, the majority cannot be. Analysis of quantum programs in infinite-dimensional state spaces is a challenging problem and requires radically new ideas, and it should be a very important topic for future research.

5.1 TERMINATION ANALYSIS OF QUANTUM WHILE-LOOPS

As in classical programming, difficulty in the analysis of quantum programs essentially comes from loops and recursions. This section focuses on the quantum extension of the **while**-loop introduced in Section 3.1. We mainly consider termination of a quantum loop, but its average running time is also briefly discussed.

5.1.1 QUANTUM WHILE-LOOPS WITH UNITARY BODIES

To ease understanding, let us start from a special form of quantum **while**-loop:

$$S \equiv \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ \overline{q} := U[\overline{q}]\ \textbf{od} \tag{5.1}$$

where:

- $\overline{q}$ denotes quantum register $q_1, \ldots, q_n$, and its state Hilbert space is $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_{q_i}$;
- the loop body is the unitary transformation $\overline{q} := U[\overline{q}]$ with U being a unitary operator in $\mathcal{H}$;
- the yes-no measurement $M = \{M_0, M_1\}$ in the loop guard is projective; that is, $M_0 = P_{X^\perp}$ and $M_1 = P_X$ with X being a subspace of $\mathcal{H}$ and $X^\perp$ being the orthocomplement of X (see Definition 2.1.7(ii)).

The execution of the quantum loop S in equation (5.1) is clearly described by its operational and denotational semantics presented in Sections 3.2 and 3.3. To help the reader further understand the behavior of loop S, here we examine its computational process in a slightly different manner. For any input state $\rho \in \mathcal{D}(\mathcal{H})$, the behavior of the loop S can be described in the following unwound way:

(i) *Initial step*: The loop performs the projective measurement

$$M = \{M_0 = P_{X^\perp}, M_1 = P_X\}$$

on the input state ρ. If the outcome is 1, then the program performs the unitary operation U on the post-measurement state. Otherwise, the program terminates. More precisely, we have:

- The loop terminates with probability

$$p_T^{(1)}(\rho) = tr(P_{X^\perp}\rho).$$

In this case, the output at this step is

$$\rho_{out}^{(1)} = \frac{P_{X^\perp}\rho P_{X^\perp}}{p_T^{(1)}(\rho)}.$$

- The loop continues with probability

$$p_{NT}^{(1)}(\rho) = 1 - p_T^{(1)}(\rho) = tr(P_X\rho).$$

In this case, the program state after the measurement is

$$\rho_{mid}^{(1)} = \frac{P_X\rho P_X}{p_{NT}^{(1)}(\rho)}.$$

Furthermore, $\rho_{mid}^{(1)}$ is fed to the unitary operation U and then the state

$$\rho_{in}^{(2)} = U\rho_{mid}^{(1)}U^\dagger$$

is returned. Note that $\rho_{in}^{(2)}$ will be used as the input state in the next step.

(ii) *Induction step*: Suppose that the loop has run n steps, and it did not terminate at the nth step; that is, $p_{NT}^{(n)} > 0$. If $\rho_{in}^{(n+1)}$ is the program state at the end of the nth step, then in the $(n+1)$th step, $\rho_{in}^{(n+1)}$ is the input, and we have:

- The termination probability is

$$p_T^{(n+1)}(\rho) = tr(P_{X^\perp}\rho_{in}^{(n+1)})$$

and the output at this step is

$$\rho_{out}^{(n+1)} = \frac{P_{X^\perp}\rho_{in}^{(n+1)}P_{X^\perp}}{p_T^{(n+1)}(\rho)}.$$

- The loop continues to perform the unitary operation U on the post-measurement state

$$\rho_{mid}^{(n+1)} = \frac{P_X\rho_{in}^{(n+1)}P_X}{p_{NT}^{(n+1)}(\rho)}$$

with probability

$$p_{NT}^{(n+1)}(\rho) = 1 - p_T^{(n+1)}(\rho) = tr(P_X\rho_{in}^{(n+1)}),$$

and the state

$$\rho_{in}^{(n+2)} = U\rho_{mid}^{(n+1)}U^\dagger$$

will be returned. Then state $\rho_{in}^{(n+2)}$ will be the input of the $(n+2)$th step.

The reader may like to compare this description of the execution of quantum loop S with its semantics given in Section 3.2. Based on this description, we can introduce the notion of termination.

Definition 5.1.1

(i) *If probability* $p_{NT}^{(n)}(\rho) = 0$ *for some positive integer* n*, then we say that the loop* (5.1) *terminates from input* ρ.

(ii) *The nontermination probability of the loop* (5.1) *from input* ρ *is*

$$p_{NT}(\rho) = \lim_{n\to\infty} p_{NT}^{(\leq n)}(\rho)$$

where

$$p_{NT}^{(\leq n)}(\rho) = \prod_{i=1}^{n} p_{NT}^{(i)}(\rho)$$

denotes the probability that the loop does not terminate after n *steps.*

(iii) *We say that the loop* (5.1) *almost surely terminates from input* ρ *whenever nontermination probability* $p_{NT}(\rho) = 0$.

Intuitively, a quantum loop almost surely terminates if for any $\epsilon > 0$, there exists a large enough positive integer $n(\epsilon)$ such that the probability that the loop terminates within $n(\epsilon)$ steps is greater than $1 - \epsilon$.

In this definition, termination was considered for a single input. We can also define termination for all possible inputs.

Definition 5.1.2. *A quantum loop is terminating (respectively, almost surely terminating) if it terminates (respectively, almost surely terminates) from all input* $\rho \in \mathcal{D}(\mathcal{H})$.

In the computational process of a quantum loop, a density operator is taken as input, and a density operator is given as output with a certain probability at each step. Thus, we can obtain the overall output by synthesizing these density operators returned at all steps into a single one according to the respective probabilities. Note that sometimes the loop does not terminate with a nonzero probability. So, the synthesized output may not be a density operator but only a partial density operator, and thus a quantum loop defines a function from density operators to partial density operators in $\mathcal{H}$.

Definition 5.1.3. *The function* $\mathcal{F} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ *computed by the quantum loop* (5.1) *is defined by*

$$\mathcal{F}(\rho) = \sum_{n=1}^{\infty} p_{NT}^{(\leq n-1)}(\rho) \cdot p_T^{(n)}(\rho) \cdot \rho_{out}^{(n)}$$

for each $\rho \in \mathcal{D}(\mathcal{H})$.

It should be noted that in the defining equation of $\mathcal{F}(\rho)$ the quantity

$$p_{NT}^{(\leq n-1)}(\rho)\cdot p_T^{(n)}(\rho)$$

is the probability that the loop does not terminate at steps from 1 to $n-1$ but it terminates at the nth step.

For any operator A in the Hilbert space $\mathcal{H}$ and any subspace X of $\mathcal{H}$, we write:

$$A_X = P_X A P_X$$

where P_X is the projection onto X; that is, A_X is the restriction of A in X. Then the computational process of quantum loop (5.1) can be summarized as:

Lemma 5.1.1. *Let ρ be an input state to the loop (5.1). Then we have:*

(i)

$$p_{NT}^{(\leq n)}(\rho) = tr(U_X^{n-1}\rho_X U_X^{\dagger n-1})$$

for any positive integer n;

(ii)

$$\mathcal{F}(\rho) = P_{X^\perp}\rho P_{X^\perp} + P_{X^\perp}U\left(\sum_{n=0}^{\infty} U_X^n \rho_X U_X^{\dagger n}\right)U^\dagger P_{X^\perp},$$

where X is the subspace defining the projective measurement in the loop guard, and U is the unitary transformation in the loop body.

Exercise 5.1.1. *Prove Lemma 5.1.1.*

The following exercise further shows that the function computed by quantum loop S in equation (5.1) coincides with the denotational semantics of S according to Definition 3.3.1.

Exercise 5.1.2. *Prove that $\mathcal{F}(\rho) = [\![S]\!](\rho)$ for any $\rho \in \mathcal{D}(\mathcal{H})$.*

As shown in the following exercise, almost sure termination of a quantum loop can also be characterized in terms of the function computed by it.

Exercise 5.1.3. *Show that for each $\rho \in \mathcal{D}(\mathcal{H})$, we have:*

(i) *$\langle\varphi|\mathcal{F}(\rho)|\psi\rangle = 0$ if $|\varphi\rangle$ or $|\psi\rangle \in X$;*

(ii) *$tr(\mathcal{F}(\rho)) = tr(\rho) - p_{NT}(\rho)$. Thus, $tr(\mathcal{F}(\rho)) = tr(\rho)$ if and only if the loop (5.1) almost surely terminates from input state ρ.*

Termination:

Obviously, it is hard to decide directly by Definition 5.1.1 when the quantum loop (5.1) terminates. Now we try to find a necessary and sufficient condition for its termination. This can be done through several reduction steps.

First of all, the next lemma allows us to decompose an input density matrix into a sequence of simpler input density matrices when examining termination of a quantum loop.

Lemma 5.1.2. *Let $\rho = \sum_i p_i \rho_i$ with $p_i > 0$ for all i. Then the loop (5.1) terminates from input ρ if and only if it terminates from input ρ_i for all i.*

Exercise 5.1.4. *Prove Lemma 5.1.2.*

If $\{(p_i, |\psi_i\rangle)\}$ is an ensemble with $p_i > 0$ for all i, and density operator

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|,$$

then the previous lemma asserts that the loop (5.1) terminates from input mixed state ρ if and only if it terminates from input pure state $|\psi_i\rangle$ for all i. In particular, we have:

Corollary 5.1.1. *A quantum loop is terminating if and only if it terminates from all pure input states.*

Secondly, the termination problem of a quantum loop may be reduced to a corresponding problem of a classical loop in the field of complex numbers. We decompose the subspace X and its ortho-complement $X^\perp$ defining the projective measurement in the guard of quantum loop (5.1). Let $\{|m_1\rangle, \ldots, |m_l\rangle\}$ be an orthonormal basis of $\mathcal{H}$ such that

$$\sum_{i=1}^{k} |m_i\rangle\langle m_i| = P_X \quad \text{and} \quad \sum_{i=k+1}^{l} |m_i\rangle\langle m_i| = P_{X^\perp},$$

where $1 \leq k \leq l$. In other words, the basis $\{|m_1\rangle, \ldots, |m_l\rangle\}$ of $\mathcal{H}$ is divided into two parts $\{|m_1\rangle, \ldots, |m_k\rangle\}$ and $\{|m_{k+1}\rangle, \ldots, |m_l\rangle\}$ with the former being a basis of X and the latter a basis of $X^\perp$. Without any loss of generality, we assume in the sequel that the matrix representations of operators U (the unitary transformation in the loop body), U_X (the restriction of U in X), ρ_X (the restriction of input ρ in X), denoted also by U, U_X, ρ_X respectively for simplicity, are taken according to this basis. Also, for each pure state $|\psi\rangle$ we write $|\psi\rangle_X$ for the vector representation of projection $P_X|\psi\rangle$ in this basis.

Lemma 5.1.3. *The following two statements are equivalent:*

(i) *The quantum loop (5.1) terminates from input $\rho \in \mathcal{D}(\mathcal{H})$;*

(ii) *$U_X^n \rho_X U_X^{\dagger n} = \mathbf{0}_{k\times k}$ for some nonnegative integer n, where $\mathbf{0}_{k\times k}$ is the $(k \times k)$-zero matrix.*

In particular, it terminates from pure input state $|\psi\rangle$ if and only if $U_X^n|\psi\rangle_X = \mathbf{0}$ for some nonnegative integer n, where $\mathbf{0}$ is the k-dimensional zero vector.

Proof. This result follows from Lemma 5.1.1 (i) and the fact that $tr(A) = 0$ if and only if $A = \mathbf{0}$ when A is positive. □

It should be noticed that the condition $U_X^n|\psi\rangle_X = \mathbf{0}$ in Lemma 5.1.3 is actually a termination condition for the following loop:

$$\textbf{while } \mathbf{v} \neq \mathbf{0} \textbf{ do } \mathbf{v} := U_X\mathbf{v} \textbf{ od} \tag{5.2}$$

This loop must be understood as a classical computation in the field of complex numbers.

Thirdly, we can show certain invariance of termination of a classical loop under a nonsingular transformation.

Lemma 5.1.4. *Let S be a nonsingular $(k \times k)$-complex matrix. Then the following two statements are equivalent:*

(i) *The classical loop (5.2) (with $\mathbf{v} \in \mathbf{C}^k$) terminates from input $\mathbf{v}_0 \in \mathbf{C}^k$.*
(ii) *The classical loop:*

$$\textbf{while } \mathbf{v} \neq \mathbf{0} \textbf{ do } \mathbf{v} := (SU_X S^{-1})\mathbf{v} \textbf{ od}$$

(with $\mathbf{v} \in \mathbf{C}^k$) terminates from input $S\mathbf{v}_0$.

Proof. Note that $S\mathbf{v} \neq \mathbf{0}$ if and only if $\mathbf{v} \neq \mathbf{0}$ because S is nonsingular. Then the conclusion follows from a simple calculation. □

Furthermore, we shall need the Jordan normal form theorem in the proof of the main results in this section. The proof of this normal form theorem can be found in any standard textbook on matrix theory; e.g., [40].

Lemma 5.1.5. *[Jordan normal form theorem] For any $(k \times k)$-complex matrix A, there is a nonsingular $(k \times k)$-complex matrix S such that*

$$A = SJ(A)S^{-1}$$

where

$$\begin{aligned} J(A) &= \bigoplus_{i=1}^{l} J_{k_i}(\lambda_i) \\ &= diag(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \ldots, J_{k_l}(\lambda_l)) \\ &= \begin{pmatrix} J_{k_1}(\lambda_1) & & & & \\ & J_{k_2}(\lambda_2) & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & J_{k_l}(\lambda_l) \end{pmatrix} \end{aligned}$$

is the Jordan normal form of A, $\sum_{i=1}^{l} k_i = k$, and

$$J_{k_i}(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_i \end{pmatrix}. \tag{5.3}$$

is a $(k_i \times k_i)$-Jordan block for each $1 \leq i \leq l$. Furthermore, if the Jordan blocks corresponding to each distinct eigenvalue are presented in decreasing order of the

block size, then the Jordan normal form is uniquely determined once the ordering of the eigenvalues is given.

The following technical lemma about the powers of Jordan blocks is also needed in the discussions following.

Lemma 5.1.6. *Let $J_r(\lambda)$ be a $(r \times r)$-Jordan block and $\mathbf{v}$ an r-dimensional complex vector. Then*

$$J_r(\lambda)^n \mathbf{v} = \mathbf{0}$$

for some nonnegative integer n if and only if $\lambda = 0$ or $\mathbf{v} = \mathbf{0}$, where $\mathbf{0}$ is the r-dimensional zero vector.

Proof. The "if" part is clear. We now prove the "only if" part. By a routine calculation we obtain:

$$J_r(\lambda)^n = \begin{pmatrix} \lambda^n & \binom{n}{1}\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{r-2}\lambda^{n-r+2} & \binom{n}{r-1}\lambda^{n-r+1} \\ 0 & \lambda^n & \binom{n}{1}\lambda^{n-1} & \cdots & \binom{n}{r-3}\lambda^{n-r+3} & \binom{n}{r-2}\lambda^{n-r+2} \\ 0 & 0 & \lambda^n & \cdots & \binom{n}{r-4}\lambda^{n-r+4} & \binom{n}{r-3}\lambda^{n-r+3} \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & \lambda^n & \binom{n}{1}\lambda^{n-1} \\ 0 & 0 & 0 & \cdots & 0 & \lambda^n \end{pmatrix}.$$

Notice that $J_r(\lambda)^n$ is an upper triangular matrix with the diagonal entries being λ^n. So if $\lambda \neq 0$ then $J_r(\lambda)^n$ is nonsingular, and $J_r(\lambda)^n \mathbf{v} = \mathbf{0}$ implies $\mathbf{v} = \mathbf{0}$. □

Now we are able to present one of the main results of this section, which gives a necessary and sufficient condition for termination of a quantum loop from a pure input state.

Theorem 5.1.1. *Suppose the Jordan decomposition of U_X is*

$$U_X = SJ(U_X)S^{-1}$$

where

$$J(U_X) = \bigoplus_{i=1}^{l} J_{k_i}(\lambda_i) = diag(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \ldots, J_{k_l}(\lambda_l)).$$

Let $S^{-1}|\psi\rangle_X$ be divided into l sub-vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l$ such that the length of $\mathbf{v}_i$ is k_i. Then the quantum loop (5.1) terminates from input $|\psi\rangle$ if and only if for each $1 \leq i \leq l$, $\lambda_i = 0$ or $\mathbf{v}_i = \mathbf{0}$, where $\mathbf{0}$ is the k_i-dimensional zero vector.

Proof. Using Lemmas 5.1.3 and 5.1.4 we know that the quantum loop (5.1) terminates from input $|\psi\rangle$ if and only if

$$J(U_X)^n S^{-1}|\psi\rangle_X = \mathbf{0} \tag{5.4}$$

for some nonnegative integer n. A simple calculation yields

$$J(U_X)^n S^{-1}|\psi\rangle_X = ((J_{k_1}(\lambda_1)^n \mathbf{v}_1)^T, (J_{k_2}(\lambda_2)^n \mathbf{v}_2)^T, \ldots, (J_{k_l}(\lambda_l)^n \mathbf{v}_l)^T)^T$$

where $\mathbf{v}^T$ stands for the transpose of vector $\mathbf{v}$; that is, if $\mathbf{v}$ is a column vector then $\mathbf{v}^T$ is a row vector, and vice versa. Therefore, equation (5.4) holds for some nonnegative integer n if and only if for each $1 \leq i \leq l$, there exists a nonnegative integer n_i such that

$$J_{k_i}(\lambda_i)^{n_i} \mathbf{v}_i = \mathbf{0}.$$

Then we complete the proof by using Lemma 5.1.6. □

Obviously, we can decide whether the quantum loop (5.1) terminates from any given mixed state by combining Lemma 5.1.2 and Theorem 5.1.1.

Corollary 5.1.2. *The quantum loop* (5.1) *is terminating if and only if U_X has only zero eigenvalues.*

Almost sure termination:

We now turn to consider almost sure termination. A necessary and sufficient condition for almost sure termination of the quantum loop (5.1) can also be derived by several steps of reduction. We first give a lemma similar to Lemma 5.1.2 so that a mixed input state can be reduced to a family of pure input states.

Lemma 5.1.7. *Let $\rho = \sum_i p_i \rho_i$ with $p_i > 0$ for all i. Then the quantum loop* (5.1) *almost surely terminates from input ρ if and only if it almost surely terminates from input ρ_i for all i.*

Exercise 5.1.5. *Prove Lemma 5.1.7.*

Corollary 5.1.3. *A quantum loop is almost surely terminating if and only if it almost surely terminates from all pure input states.*

We then present a technical lemma, which forms a key step in the proof of Theorem 5.1.2 following.

Lemma 5.1.8. *The quantum loop* (5.1) *almost surely terminates from pure input state $|\psi\rangle$ if and only if*

$$\lim_{n\to\infty} ||U_X^n|\psi\rangle|| = 0.$$

Proof. From Lemma 5.1.1, we have:

$$p_{NT}^{(\leq n)}(|\psi\rangle) = \|U_X^{n-1}|\psi\rangle\|^2.$$

Note that in the left-hand side of the preceding equation $|\psi\rangle$ actually stands for its corresponding density operator $|\psi\rangle\langle\psi|$. So $p_{NT}(|\psi\rangle) = 0$ if and only if $\lim_{n\to\infty} ||U_X^n|\psi\rangle|| = 0$. □

The following theorem gives a necessary and sufficient condition for almost sure termination of a quantum loop from a pure input state.

Theorem 5.1.2. *Suppose that U_X, S, $J(U_X)$, $J_{k_i}(\lambda_i)$ and $\mathbf{v}_i$ $(1 \leq i \leq l)$ are given as in Theorem 5.1.1. Then the quantum loop* (5.1) *almost surely terminates from input*

$|\psi\rangle$ if and only if for each $1 \leq i \leq l$, $|\lambda_i| < 1$ or $\mathbf{v}_i = \mathbf{0}$, where $\mathbf{0}$ is the k_i-dimensional zero vector.

Proof. First, for any nonnegative integer n, we have:

$$U_X^n|\psi\rangle = SJ(U_X)^n S^{-1}|\psi\rangle.$$

Then $\lim_{n\to\infty} ||U_X^n|\psi\rangle|| = 0$ if and only if

$$\lim_{n\to\infty} ||J(U_X)^n S^{-1}|\psi\rangle|| = 0 \tag{5.5}$$

since S is nonsingular. Using Lemma 5.1.8 we know that the loop (5.1) almost surely terminates from input $|\psi\rangle$ if and only if equation (5.5) holds. Note that

$$J(U_X)^n S^{-1}|\psi\rangle = ((J_{k_1}(\lambda_1)^n \mathbf{v}_1)^T, (J_{k_2}(\lambda_2)^n \mathbf{v}_2)^T, \ldots, (J_{k_l}(\lambda_l)^n \mathbf{v}_l)^T)^T$$

where $\mathbf{v}^T$ stands for the transpose of vector $\mathbf{v}$. Then equation (5.5) holds if and only if

$$\lim_{n\to\infty} ||J_{k_i}(\lambda_i)^n \mathbf{v}_i|| = 0 \tag{5.6}$$

for all $1 \leq i \leq l$. Furthermore, we have:

$$J_r(\lambda)^n \mathbf{v} = \left(\sum_{i=0}^{r-1} \binom{n}{i} \lambda^{n-i} v_{i+1}, \sum_{i=0}^{r-2} \binom{n}{i} \lambda^{n-i} v_{i+2}, \cdots, \lambda^n v_{r-1} + \binom{n}{1} \lambda^{n-1} v_r, \lambda^n v_r \right)^T.$$

So, equation (5.6) holds if and only if the following system of k_i equations are valid:

$$\begin{cases} \lim_{n\to\infty} \sum_{j=0}^{k_i-1} \binom{n}{j} \lambda_i^{n-j} v_{i(j+1)} = 0, \\ \lim_{n\to\infty} \sum_{j=0}^{k_i-2} \binom{n}{j} \lambda_i^{n-j} v_{i(j+2)} = 0, \\ \cdots\cdots\cdots\cdots\cdots \\ \lim_{n\to\infty} [\lambda_i^n v_{i(k_i-1)} + \binom{n}{1} \lambda_i^{n-1} v_{ik_i}] = 0, \\ \lim_{n\to\infty} \lambda_i^n v_{ik_i} = 0, \end{cases} \tag{5.7}$$

where it is assumed that $\mathbf{v}_i = (v_{i1}, v_{i2}, \ldots, v_{ik_i})$.

We now consider two cases. If $|\lambda_i| < 1$, then

$$\lim_{n\to\infty} \binom{n}{j} \lambda_i^{n-j} = 0$$

for any $0 \leq j \leq k_i - 1$, and all of the equations in (5.7) follow. On the other hand, if $|\lambda_i| \geq 1$, then from the last equation in (5.7) we know that $v_{ik} = 0$. Putting $v_{ik} = 0$ into the second equation from the bottom in (5.7) we obtain $v_{i(k-1)} = 0$. We can

further move from bottom to top in the system (5.7) of equations in this way, and finally we get:

$$v_{i1} = v_{i2} = \cdots = v_{i(k_i-1)} = v_{ik_i} = 0.$$

This completes the proof. □

Corollary 5.1.4. *Quantum loop* (5.1) *is almost surely terminating if and only if all the eigenvalues of* U_X *have norms less than 1.*

This subsection only considered a special class of quantum loops with a unitary transformation as their body. It can be seen as a warming up for the next subsection. But the termination conditions presented in this subsection are of independent significance because they are much easier to check than the corresponding conditions in the next subsection given for more general quantum loops.

5.1.2 GENERAL QUANTUM WHILE-LOOPS

Termination of a special class of quantum **while**-loops with unitary bodies was carefully studied in the last subsection. However, the expressive power of this kind of quantum loop is very limited; for example, they cannot model the case where a measurement occurs in the loop body or a quantum loop is nested in another. Now we consider a general quantum **while**-loop as defined in Section 3.1:

$$\textbf{while } M[\overline{q}] = 1 \textbf{ do } S \textbf{ od} \tag{5.8}$$

where $M = \{M_0, M_1\}$ is a yes-no measurement, $\overline{q}$ is a quantum register, and the loop body S is a general quantum program. As we saw in Section 3.3, the denotational semantics of S is a quantum operation $[\![S]\!] = \mathcal{E}$ in the state Hilbert space of $\overline{q}$ (if the quantum variables $qvar(S) \subseteq \overline{p}$). So, the loop (5.8) can be equivalently rewritten as:

$$\textbf{while } M[\overline{q}] = 1 \textbf{ do } \overline{q} := \mathcal{E}[\overline{q}] \textbf{ od}. \tag{5.9}$$

This subsection focuses on quantum loop (5.9). Let us see how the loop (5.9) is executed. Roughly speaking, the loop consists of two parts. The loop body "$\overline{q} := \mathcal{E}[\overline{q}]$" transforms a density operator σ to density operator $\mathcal{E}(\sigma)$. The loop guard "$M[\overline{q}] = 1$" is checked at each execution step. For $i = 0, 1$, we define quantum operation $\mathcal{E}_i$ from the measurement $M = \{M_0, M_1\}$ in the loop guard as follows:

$$\mathcal{E}_i(\sigma) = M_i \sigma M_i^\dagger \tag{5.10}$$

for any density operator σ. Moreover, for any two quantum operations $\mathcal{F}_1, \mathcal{F}_2$, we write $\mathcal{F}_2 \circ \mathcal{F}_1$ for their composition; that is,

$$(\mathcal{F}_2 \circ \mathcal{F}_1)(\rho) = \mathcal{F}_2(\mathcal{F}_1(\rho))$$

for all $\rho \in \mathcal{D}(\mathcal{H})$. For a quantum operation $\mathcal{F}$, $\mathcal{F}^n$ denotes the nth power of $\mathcal{F}$, i.e., the composition of n copies of $\mathcal{F}$. Then the execution of the loop with input state ρ can be more precisely described as follows:

(i) *Initial step*: We first perform the termination measurement $\{M_0, M_1\}$ on the input state ρ.

- The probability that the program terminates, that is, the measurement outcome is 0, is

$$p_T^{(1)}(\rho) = tr[\mathcal{E}_0(\rho)],$$

and the program state after termination is

$$\rho_{out}^{(1)} = \mathcal{E}_0(\rho)/p_T^{(1)}(\rho).$$

We encode probability $p_T^{(1)}(\rho)$ and density operator $\rho_{out}^{(1)}$ into a partial density operator

$$p_T^{(1)}(\rho)\rho_{out}^{(1)} = \mathcal{E}_0(\rho).$$

So, $\mathcal{E}_0(\rho)$ is the partial output state at the first step.

- The probability that the program does not terminate, that is, the measurement outcome is 1, is

$$p_{NT}^{(1)}(\rho) = tr[\mathcal{E}_1(\rho)], \tag{5.11}$$

and the program state after the outcome 1 is obtained is

$$\rho_{mid}^{(1)} = \mathcal{E}_1(\rho)/p_{NT}^{(1)}(\rho).$$

Then it is transformed by the loop body $\mathcal{E}$ to

$$\rho_{in}^{(2)} = (\mathcal{E} \circ \mathcal{E}_1)(\rho)/p_{NT}^{(1)}(\rho),$$

upon which the second step will be executed. We can combine $p_{NT}^{(1)}$ and $\rho_{in}^{(2)}$ into a partial density operator

$$p_{NT}^{(1)}(\rho)\rho_{in}^{(2)} = (\mathcal{E} \circ \mathcal{E}_1)(\rho).$$

(ii) *Induction step*: We write

$$p_{NT}^{(\leq n)} = \prod_{i=1}^{n} p_{NT}^{(i)}$$

for the probability that the program does not terminate within n steps, where $p_{NT}^{(i)}$ is the probability that the program does not terminate at the ith step for every $1 \leq i \leq n$. The program state after the nth measurement with outcome 1 is

$$\rho_{mid}^{(n)} = \frac{\left[\mathcal{E}_1 \circ (\mathcal{E} \circ \mathcal{E}_1)^{n-1}\right](\rho)}{p_{NT}^{(\leq n)}},$$

which is then transformed by the loop body $\mathcal{E}$ into

$$\rho_{in}^{(n+1)} = \frac{(\mathcal{E} \circ \mathcal{E}_1)^n(\rho)}{p_{NT}^{(\leq n)}}.$$

We combine $p_{NT}^{(\leq n)}$ and $\rho_{in}^{(n+1)}$ into a partial density operator

$$p_{NT}^{(\leq n)}(\rho)\rho_{in}^{(n+1)} = (\mathcal{E} \circ \mathcal{E}_1)^n(\rho).$$

Now the $(n+1)$st step is executed upon $\rho_{in}^{(n+1)}$.

- The probability that the program terminates at the $(n+1)$st step is then

$$p_T^{(n+1)}(\rho) = tr\left[\mathcal{E}_0\left(\rho_{in}^{(n+1)}\right)\right],$$

  and the probability that the program does not terminate within n steps but it terminates at the $(n+1)$st step is

$$q_T^{(n+1)}(\rho) = tr\left(\left[\mathcal{E}_0 \circ (\mathcal{E} \circ \mathcal{E}_1)^n\right](\rho)\right).$$

  The program state after the termination is

$$\rho_{out}^{(n+1)} = [\mathcal{E}_0 \circ (\mathcal{E} \circ \mathcal{E}_1)^n](\rho)/q_T^{(n+1)}(\rho).$$

  Combining $q_T^{(n+1)}(\rho)$ and $\rho_{out}^{(n+1)}$ yields the partial output state of the program at the $(n+1)$st step:

$$q_T^{(n+1)}(\rho)\rho_{out}^{(n+1)} = [\mathcal{E}_0 \circ (\mathcal{E} \circ \mathcal{E}_1)^n](\rho).$$

- The probability that the program does not terminate within $(n+1)$ steps is then

$$p_{NT}^{(\leq n+1)}(\rho) = tr([\mathcal{E}_1 \circ (\mathcal{E} \circ \mathcal{E}_1)^n](\rho)). \tag{5.12}$$

As pointed out in Section 3.1, the major difference between a classical loop and a quantum loop comes from the checking of the loop guard. During checking the guard of a classical loop, the program state is not changed. However, the quantum measurement in the guard of a quantum loop disturbs the state of the system. Thus, the quantum program state after checking the loop guard may be different from that before checking. The change of program state caused by measurement M is depicted by quantum operations $\mathcal{E}_0$ and $\mathcal{E}_1$.

The preceding description of the computational process of quantum loop (5.9) is a generalization of the execution of loop (5.1) described in Subsection 5.1.1. Now Definitions 5.1.1, 5.1.2 and 5.1.3 for the special quantum loop (5.1) can be easily extended to the general quantum loop (5.9).

Definition 5.1.4

(i) *We say that quantum loop* (5.9) *terminates from input state* ρ *if probability* $p_{NT}^{(n)}(\rho) = 0$ *for some positive integer n.*

(ii) *We say that loop* (5.9) *almost surely terminates from input state* ρ *if the nontermination probability*

$$p_{NT}(\rho) = \lim_{n\to\infty} p_{NT}^{(\leq n)}(\rho) = 0$$

where $p_{NT}^{(\leq n)}$ *is the probability that the program does not terminate within n steps.*

Definition 5.1.5. *The quantum loop* (5.9) *is terminating (respectively, almost surely terminating) if it terminates (respectively, almost surely terminates) from any input* ρ.

The (total) output state of a quantum loop is obtained by summing up its partial computing results obtained at all steps. Formally, we have:

Definition 5.1.6. *The function* $\mathcal{F} : \mathcal{D}(H) \to \mathcal{D}(H)$ *computed by the quantum loop* (5.9) *is defined by*

$$\mathcal{F}(\rho) = \sum_{n=1}^{\infty} q_T^{(n)}(\rho)\rho_{out}^{(n)} = \sum_{n=0}^{\infty} \left[\mathcal{E}_0 \circ (\mathcal{E} \circ \mathcal{E}_1)^n\right](\rho)$$

for each $\rho \in \mathcal{D}(\mathcal{H})$, *where*

$$q_T^{(n)} = p_{NT}^{(\leq n-1)} p_T^{(n)}$$

is the probability that the program does not terminate within $n-1$ *steps but it terminates at the nth step.*

Obviously, the previous three definitions degenerate to the corresponding definitions in the last subsection whence the loop body is a unitary operator.

The following proposition gives a recursive characterization of the function $\mathcal{F}$ computed by quantum loop (5.9). It is essentially a restatement of Corollary 3.3.1, and can be easily proved by definition.

Proposition 5.1.1. *The quantum operation* $\mathcal{F}$ *computed by loop* (5.9) *satisfies the following recursive equation:*

$$\mathcal{F}(\rho) = \mathcal{E}_0(\rho) + \mathcal{F}[(\mathcal{E} \circ \mathcal{E}_1)(\rho)]$$

for all density operators ρ.

Matrix Representation of Quantum Operations:

The remaindering part of this subsection is devoted to termination and running time analysis of quantum loop (5.9). Since iterations of quantum operations $\mathcal{E}, \mathcal{E}_0, \mathcal{E}_1$ are involved in the definitions of termination and the computed function $\mathcal{F}$ of loop (5.9), dealing with these iterations in its analysis is unavoidable. However, it is usually very difficult to compute the iterations of quantum operations. To overcome this difficulty, we introduce a useful mathematical tool, namely the matrix representation of a quantum operation, which is usually easier to manipulate than the quantum operation itself.

Definition 5.1.7. *Suppose quantum operation $\mathcal{E}$ in a d-dimensional Hilbert space $\mathcal{H}$ has the Kraus operator-sum representation:*

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

for all density operators ρ. Then the matrix representation of $\mathcal{E}$ is the $d^2 \times d^2$ matrix:

$$M = \sum_i E_i \otimes E_i^*,$$

where A^* stands for the conjugate of matrix A, i.e., $A^* = (a_{ij}^*)$ with a_{ij}^* being the conjugate of complex number a_{ij}, whenever $A = (a_{ij})$.

The effect of matrix representation of quantum operations in analysis of quantum programs is mainly based on the next lemma, which establishes a connection between the image of a matrix A under a quantum operation $\mathcal{E}$ and the multiplication of the matrix representation of $\mathcal{E}$ and the cylindrical extension of A. Actually, this lemma will play a key role in the proofs of all the main results in this subsection.

Lemma 5.1.9. *Suppose that* $\dim \mathcal{H} = d$. *We write*

$$|\Phi\rangle = \sum_j |jj\rangle$$

for the (unnormalized) maximally entangled state in $\mathcal{H} \otimes \mathcal{H}$, where $\{|j\rangle\}$ is an orthonormal basis of $\mathcal{H}$. Let M be the matrix representation of quantum operation $\mathcal{E}$. Then for any $d \times d$ matrix A, we have:

$$(\mathcal{E}(A) \otimes I)|\Phi\rangle = M(A \otimes I)|\Phi\rangle \tag{5.13}$$

where I stands for the $d \times d$-unit matrix.

Proof. We first observe the matrix equality: for any matrices A, B and C,

$$(A \otimes B)(C \otimes I)|\Phi\rangle = (ACB^T \otimes I)|\Phi\rangle,$$

where B^T stands for the transpose of matrix B. This equality can be easily proved by a routine matrix calculation. Now it follows that

$$\begin{aligned} M(A\otimes I)|\Phi\rangle &= \sum_i \left(E_i \otimes E_i^*\right)(A\otimes I)\,|\Phi\rangle \\ &= \sum_i \left(E_i A E_i^\dagger \otimes I\right)|\Phi\rangle \\ &= (\mathcal{E}(A)\otimes I)|\Phi\rangle. \end{aligned}$$

□

It is interesting to observe that the maximally entangled state $|\Phi\rangle$ enables us to represent a $d\times d$-matrix $A=\left(a_{ij}\right)$ to a d^2-dimensional vector in the following way:

$$(A\otimes I)|\Phi\rangle = (a_{11},\ldots,a_{1d},a_{21},\ldots,a_{2d},\ldots,a_{d1},\ldots,a_{dd})^T.$$

Furthermore, it helps to translate a quantum operation $\mathcal{E}$ in a d-dimensional Hilbert space to a $d^2\times d^2$-matrix M through equation (35).

The preceding lemma has an immediate application showing that the matrix representation of a quantum operation is well-defined: if

$$\mathcal{E}(\rho)=\sum_i E_i\rho E_i^\dagger = \sum_j F_j\rho F_j^\dagger$$

for all density operators ρ, then

$$\sum_i E_i\otimes E_i^* = \sum_j F_j\otimes F_j^*.$$

This conclusion can be easily seen from the arbitrariness of matrix A in equation (5.13).

After preparing the mathematical tool of the matrix representation of a quantum operation, we now come back to consider the quantum loop (5.9). Assume that the quantum operation $\mathcal{E}$ in the loop body has the operator-sum representation:

$$\mathcal{E}(\rho)=\sum_i E_i\rho E_i^\dagger$$

for all density operators ρ. Let $\mathcal{E}_i$ $(i=0,1)$ be the quantum operations defined by the measurement operations M_0, M_1 in the loop guard according to equation (5.10). We write $\mathcal{G}$ for the composition of $\mathcal{E}$ and $\mathcal{E}_1$:

$$\mathcal{G}=\mathcal{E}\circ\mathcal{E}_1.$$

Then $\mathcal{G}$ has the operator-sum representation:

$$\mathcal{G}(\rho)=\sum_i (E_iM_1)\rho(M_1^\dagger E_i^\dagger)$$

for all density operators ρ. Furthermore, the matrix representations of $\mathcal{E}_0$ and $\mathcal{G}$ are

$$\begin{aligned} N_0 &= M_0 \otimes M_0^*, \\ R &= \sum_i (E_i M_1) \otimes (E_i M_1)^*, \end{aligned} \tag{5.14}$$

respectively. Suppose that the Jordan decomposition of R is

$$R = SJ(R)S^{-1}$$

where S is a nonsingular matrix, and $J(R)$ is the Jordan normal form of R:

$$J(R) = \bigoplus_{i=1}^{l} J_{k_i}(\lambda_i) = diag(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \cdots, J_{k_l}(\lambda_l))$$

with $J_{k_s}(\lambda_s)$ being a $k_s \times k_s$-Jordan block of eigenvalue λ_s $(1 \leq s \leq l)$ (see Lemma 5.1.5).

The following is a key technical lemma that describes the structure of the matrix representation R of quantum operation $\mathcal{G}$.

Lemma 5.1.10

(i) $|\lambda_s| \leq 1$ *for all* $1 \leq s \leq l$.
(ii) *If* $|\lambda_s| = 1$ *then the sth Jordan block is* 1*-dimensional; that is,* $k_s = 1$.

For readability, we postpone the lengthy proof of this lemma to Section 5.4.

Termination and Almost Sure Termination:

Now we are ready to study termination of the quantum loop (5.9). First of all, the following lemma gives a simple termination condition in terms of the matrix representation of quantum operations.

Lemma 5.1.11. *Let R be defined by equation (5.14), and let*

$$|\Phi\rangle = \sum_j |jj\rangle$$

be the (unnormalized) maximally entangled state in $\mathcal{H} \otimes \mathcal{H}$. Then we have:

(i) *Quantum loop* (5.9) *terminates from input ρ if and only if*

$$R^n(\rho \otimes I)|\Phi\rangle = \mathbf{0}$$

for some integer $n \geq 0$;
(ii) *Quantum loop* (5.9) *almost surely terminates from input ρ if and only if*

$$\lim_{n\to\infty} R^n(\rho \otimes I)|\Phi\rangle = \mathbf{0},$$

Proof. We only prove part (i), as the proof of part (ii) is similar. First, it follows from Lemma 5.1.9 that

$$[\mathcal{G}(\rho) \otimes I]|\Phi\rangle = R(\rho \otimes I)|\Phi\rangle.$$

Repeated applications of this equality yield:

$$[\mathcal{G}^n(\rho) \otimes I]|\Phi\rangle = R^n(\rho \otimes I)|\Phi\rangle.$$

On the other hand, it holds that

$$tr(A) = \langle\Phi|A \otimes I|\Phi\rangle$$

for any matrix A. Therefore, since $\mathcal{E}$ is trace-preserving, we obtain:

$$\begin{aligned} tr\left(\left[\mathcal{E}_1 \circ (\mathcal{E} \circ \mathcal{E}_1)^{n-1}\right](\rho)\right) &= tr\left((\mathcal{E} \circ \mathcal{E}_1)^n(\rho)\right) \\ &= tr(\mathcal{G}^n(\rho)) \\ &= \langle\Phi|R^n(\rho \otimes I)|\Phi\rangle. \end{aligned}$$

Moreover, it is clear that $\langle\Phi|R^n(\rho \otimes I)|\Phi\rangle = 0$ if and only if $R^n(\rho \otimes I)|\Phi\rangle = \mathbf{0}$. □

As a direct application of the preceding lemma, we have:

Lemma 5.1.12. *Let R and $|\Phi\rangle$ be as in Lemma 5.1.11.*

(i) *Quantum loop (5.9) is terminating if and only if $R^n|\Phi\rangle = \mathbf{0}$ for some integer $n \geq 0$;*

(ii) *Quantum loop (5.9) is almost surely terminating if and only if $\lim_{n\to\infty} R^n|\Phi\rangle = \mathbf{0}$.*

Proof. Notice that a quantum loop is terminating if and only if it terminates from a special input (mixed) state:

$$\rho_0 = \frac{1}{d} \cdot I,$$

where $d = \dim \mathcal{H}$ and I is the identity operator in $\mathcal{H}$. Then this lemma follows immediately from Lemma 5.1.11. □

We can now present one of the main results of this subsection, which gives a necessary and sufficient terminating condition for a quantum loop in terms of the eigenvalues of the matrix representations of the quantum operations involved in the loop.

Theorem 5.1.3. *Let R and $|\Phi\rangle$ be as in Lemma 5.1.11. Then we have:*

(i) *If $R^k|\Phi\rangle = \mathbf{0}$ for some integer $k \geq 0$, then quantum loop (5.9) is terminating. Conversely, if loop (5.9) is terminating, then $R^k|\Phi\rangle = \mathbf{0}$ for all integer $k \geq k_0$, where k_0 is the maximal size of Jordan blocks of R corresponding to eigenvalue 0.*

(ii) *Quantum loop* (5.9) *is almost surely terminating if and only if* $|\Phi\rangle$ *is orthogonal to all eigenvectors of* $R^\dagger$ *corresponding to eigenvalues* λ *with* $|\lambda| = 1$, *where* $R^\dagger$ *is the transpose conjugate of* R.

Proof. We first prove part (i). If $R^k|\Phi\rangle = 0$ for some $k \geq 0$, then by Lemma 5.1.12 we conclude that loop (5.9) is terminating. Conversely, suppose that loop (5.9) is terminating. Again by Lemma 5.1.12, there exists some integer $n \geq 0$ such that $R^n|\Phi\rangle = 0$. For any integer $k \geq$ the maximal size of Jordan blocks of R corresponding to eigenvalue 0, we want to show that $R^k|\Phi\rangle = 0$. Without any loss of generality, we assume the Jordan decomposition of R:

$$R = SJ(R)S^{-1}$$

where

$$J(R) = \bigoplus_{i=1}^{l} J_{k_i}(\lambda_i) = diag(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \cdots, J_{k_l}(\lambda_l))$$

with $|\lambda_1| \geq \cdots \geq |\lambda_s| > 0$ and $\lambda_{s+1} = \cdots = \lambda_l = 0$. Observe that

$$R^n = SJ(R)^n S^{-1}.$$

Since S is nonsingular, it follows immediately from $R^n|\Phi\rangle = 0$ that

$$J(R)^n S^{-1}|\Phi\rangle = \mathbf{0}.$$

We can divide both matrix $J(R)$ and vector $S^{-1}|\Phi\rangle$ into two parts:

$$J(R) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad S^{-1}|\Phi\rangle = \begin{pmatrix} |x\rangle \\ |y\rangle \end{pmatrix},$$

where

$$A = \bigoplus_{i=1}^{s} J_{k_i}(\lambda_i) = diag(J_{k_1}(\lambda_1), \ldots, J_{k_s}(\lambda_s)),$$

$$B = \bigoplus_{i=s+1}^{l} J_{k_i}(\lambda_i) = diag(J_{k_{s+1}}(0), \ldots, J_{k_l}(0)),$$

$|x\rangle$ is a t-dimensional vector, $|y\rangle$ is a $(d^2 - t)$-dimensional vector, and $t = \sum_{j=1}^{s} k_j$. Then it holds that

$$J(R)^n S^{-1}|\Phi\rangle = \begin{pmatrix} A^n|x\rangle \\ B^n|y\rangle \end{pmatrix}.$$

Note that $\lambda_1, \ldots, \lambda_s \neq 0$. So, $J_{k_1}(\lambda_1), \ldots, J_{k_s}(\lambda_s)$ are nonsingular, and A is nonsingular too. Thus, $J(R)^n S^{-1}|\Phi\rangle = \mathbf{0}$ implies $A^n|x\rangle = \mathbf{0}$ and furthermore $|x\rangle = \mathbf{0}$. On the other hand, for each j with $s+1 \leq j \leq l$, since $k \geq k_j$, it holds that $J_{k_j}(0)^k = \mathbf{0}$. Consequently, $B^k = \mathbf{0}$. This together with $|x\rangle = \mathbf{0}$ implies

$$J(R)^k S^{-1}|\Phi\rangle = \mathbf{0}$$

and

$$R^k|\Phi\rangle = SJ(R)^k S^{-1}|\Phi\rangle = \mathbf{0}.$$

Now we prove part (ii). First, we know by Lemma 5.1.12 that program (5.9) is almost terminating if and only if

$$\lim_{n\to\infty} J(R)^n S^{-1}|\Phi\rangle = \mathbf{0}.$$

We assume that

$$1 = |\lambda_1| = \cdots = |\lambda_r| > |\lambda_{r+1}| \geq \cdots \geq |\lambda_l|$$

in the Jordan decomposition of R, and we write:

$$J(R) = \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}, \quad S^{-1}|\Phi\rangle = \begin{pmatrix} |u\rangle \\ |v\rangle \end{pmatrix}$$

where

$$C = diag(\lambda_1, \ldots, \lambda_r),$$
$$D = diag(J_{k_{r+1}}(\lambda_{r+1}), \ldots, J_{k_l}(\lambda_l)),$$

$|u\rangle$ is an r-dimensional vector, and $|v\rangle$ is a $(d^2 - r)$-dimensional vector. (Note that $J_{k_1}(\lambda_1), \ldots, J_{k_r}(\lambda_r)$ are all 1×1 matrices because $|\lambda_1| = \ldots = |\lambda_r| = 1$; see Lemma 5.1.10.)

If $|\Phi\rangle$ is orthogonal to all the eigenvectors of $R^\dagger$ corresponding to the eigenvalue with module 1, then by definition we have $|u\rangle = \mathbf{0}$. On the other hand, for each j with $r+1 \leq j \leq l$, since $|\lambda_j| < 1$, we have

$$\lim_{n\to\infty} J_{k_j}(\lambda_j)^n = \mathbf{0}.$$

Thus, $\lim_{n\to\infty} D^n = \mathbf{0}$. So, it follows that

$$\lim_{n\to\infty} J(R)^n S^{-1}|\Phi\rangle = \lim_{n\to\infty} \begin{pmatrix} C^n|u\rangle \\ D^n|v\rangle \end{pmatrix} = \mathbf{0}.$$

Conversely, if

$$\lim_{n\to\infty} J(R)^n S^{-1}|\Phi\rangle = \mathbf{0},$$

then $\lim_{n\to\infty} C^n|u\rangle = \mathbf{0}$. This implies $|u\rangle = \mathbf{0}$ because C is a diagonal unitary. Consequently, $|\Phi\rangle$ is orthogonal to all the eigenvectors of $R^\dagger$ corresponding to the eigenvalue with module 1. □

Expectation of Observables at the Outputs:

In addition to program termination, which we've already discussed, computing the expected value of a program variable is another important problem in classical program analysis. We now consider its quantum counterpart – computing the expectation of an observable at the output of a quantum program.

Recall from Exercise 2.1.8 that an observable is modelled by a Hermitian operator P, and the expectation (average value) of P in a state σ is $tr(P\sigma)$. In particular, whenever P is a quantum predicate, i.e., $0_{\mathcal{H}} \sqsubseteq P \sqsubseteq I_{\mathcal{H}}$, then the expectation $tr(P\sigma)$ can be understood as the probability that predicate P is satisfied in state σ. Actually, for a given input state ρ, many interesting properties of the quantum loop (5.9) can be expressed in terms of the expectation $tr(P\mathcal{F}(\rho))$ of observable P in the output state $\mathcal{F}(\rho)$. Thus, analysis of quantum programs can often be reduced to the problem of computing expectation $tr(P\mathcal{F}(\rho))$.

Now we develop a method for computing the expectation $tr(P\mathcal{F}(\rho))$. As will be seen in the proof of Theorem 5.1.4 following, our method depends on the convergence of power series

$$\sum_n R^n$$

where R is the matrix representation of $\mathcal{G} = \mathcal{E} \circ \mathcal{E}_1$ given by equation (5.14). But this series may not converge when some eigenvalues of R have module 1. A natural idea for overcoming this objection is to modify the Jordan normal form $J(R)$ of R by vanishing the Jordan blocks corresponding to those eigenvalues with module 1, which are all 1-dimensional according to Lemma 5.1.10. This yields the matrix:

$$N = SJ(N)S^{-1} \tag{5.15}$$

where $J(N)$ is obtained by modifying $J(R)$ as follows:

$$J(N) = diag(J'_1, J'_2, \cdots, J'_3), \tag{5.16}$$

$$J'_s = \begin{cases} 0 & \text{if } |\lambda_s| = 1, \\ J_{k_s}(\lambda_s) & \text{otherwise,} \end{cases}$$

for each $1 \le s \le l$.

Fortunately, as shown in the following lemma, such a modification of the matrix representation R of $\mathcal{G}$ does not change the behavior of its powers when combined with the measurement operator M_0 in the loop guard.

Lemma 5.1.13. *For any integer $n \ge 0$, we have:*

$$N_0 R^n = N_0 N^n,$$

where $N_0 = M_0 \otimes M_0^*$ is the matrix representation of $\mathcal{E}_0$.

The proof of this lemma is quite involved and thus also postponed to Section 5.4.

Now we are ready to present another main result of this subsection, which gives an explicit formula for computing the expected value of an observable at the output of a quantum loop.

Theorem 5.1.4. *The expectation of observable P in the output state $\mathcal{F}(\rho)$ of quantum loop (5.9) with input state ρ is*

$$tr(P\mathcal{F}(\rho)) = \langle\Phi|(P \otimes I)N_0(I \otimes I - N)^{-1}(\rho \otimes I)|\Phi\rangle,$$

where symbol I stands for the identity operator in $\mathcal{H}$, and

$$|\Phi\rangle = \sum_j |jj\rangle$$

is the (unnormalized) maximally entangled state in $\mathcal{H} \otimes \mathcal{H}$, with $\{|j\rangle\}$ being an orthonormal basis of $\mathcal{H}$.

Proof. With the previous preparations, this proof is more or less a straightforward calculation based on Definition 5.1.6. First, it follows from Lemma 5.1.9 together with the defining equations of quantum operations $\mathcal{E}_0$ and $\mathcal{G}$ that

$$[\mathcal{E}_0(\rho) \otimes I]|\Phi\rangle = N_0(\rho \otimes I)|\Phi\rangle, \tag{5.17}$$

$$[\mathcal{G}(\rho) \otimes I]|\Phi\rangle = R(\rho \otimes I)|\Phi\rangle. \tag{5.18}$$

By first applying equation (5.17) and then repeatedly applying equation (5.18), we obtain:

$$\begin{aligned}
[\mathcal{F}(\rho) \otimes I]|\Phi\rangle &= \left[\sum_{n=0}^{\infty} \mathcal{E}_0\left(\mathcal{G}^n(\rho)\right) \otimes I\right]|\Phi\rangle \\
&= \sum_{n=0}^{\infty} \left[\mathcal{E}_0\left(\mathcal{G}^n(\rho)\right) \otimes I\right]|\Phi\rangle \\
&= \sum_{n=0}^{\infty} N_0\left(\mathcal{G}^n(\rho) \otimes I\right)|\Phi\rangle \\
&= \sum_{n=0}^{\infty} N_0 R^n(\rho \otimes I)|\Phi\rangle
\end{aligned}$$

$$\begin{aligned}
&\overset{(a)}{=} \sum_{n=0}^{\infty} N_0 N^n (\rho \otimes I) |\Phi\rangle \\
&= N_0 \left(\sum_{n=0}^{\infty} N^n \right) (\rho \otimes I) |\Phi\rangle \\
&= N_0 (I \otimes I - N)^{-1} (\rho \otimes I) |\Phi\rangle.
\end{aligned}$$

The equality labeled by (a) follows from Lemma 5.1.13. Finally, a routine calculation yields $tr(\rho) = \langle \Phi | \rho \otimes I | \Phi \rangle$, and thus we have:

$$\begin{aligned}
tr(P\mathcal{F}(\rho)) &= \langle \Phi | P\mathcal{F}(\rho) \otimes I | \Phi \rangle \\
&= \langle \Phi | (P \otimes I)(\mathcal{F}(\rho) \otimes I) | \Phi \rangle \\
&= \langle \Phi | (P \otimes I) N_0 (I \otimes I - N)^{-1} (\rho \otimes I) | \Phi \rangle.
\end{aligned}$$

□

Average Running Time:

We already studied two program analysis problems, namely termination and expected value, for quantum loop (5.9) using matrix representation of quantum operations. To further illustrate the power of the method just introduced, we compute the average running time of loop (5.9) with input state ρ:

$$\sum_{n=1}^{\infty} n p_T^{(n)}$$

where for each $n \geq 1$,

$$p_T^{(n)} = tr\left[\left(\mathcal{E}_0 \circ (\mathcal{E} \circ \mathcal{E}_1)^{n-1} \right) (\rho) \right] = tr\left[\left(\mathcal{E}_0 \circ \mathcal{G}^{n-1} \right) (\rho) \right]$$

is the probability that the loop (5.9) terminates at the nth step. It is clear that this cannot be done by a direct application of Theorem 5.1.4. But a procedure similar to the proof of Theorem 5.1.4 leads to:

Proposition 5.1.2. *The average running time of quantum loop* (5.9) *with input state* ρ *is*

$$\langle \Phi | N_0 (I \otimes I - N)^{-2} (\rho \otimes I) | \Phi \rangle.$$

Proof. This proof is also a straightforward calculation based on Definition 5.1.6. Using equations (5.17) and (5.18) and Lemma 5.1.13, we have:

$$\begin{aligned}\sum_{n=1}^{\infty} np_n &= \sum_{n=1}^{\infty} n \cdot tr\left[\left(\mathcal{E}_0 \circ \mathcal{G}^{n-1}\right)(\rho)\right] \\ &= \sum_{n=1}^{\infty} n\langle\Phi|\left(\mathcal{E}_0 \circ \mathcal{G}^{n-1}\right)(\rho) \otimes I|\Phi\rangle \\ &= \sum_{n=1}^{\infty} n\langle\Phi|N_0 R^{n-1}(\rho \otimes I)|\Phi\rangle \\ &= \sum_{n=1}^{\infty} n\langle\Phi|N_0 N^{n-1}(\rho \otimes I)|\Phi\rangle \\ &= \langle\Phi|N_0\left(\sum_{n=1}^{\infty} nN^{n-1}\right)(\rho \otimes I)|\Phi\rangle \\ &= \langle\Phi|N_0(I \otimes I - N)^{-2}(\rho \otimes I)|\Phi\rangle.\end{aligned}$$

□

5.1.3 AN EXAMPLE

We now give an example to show how Proposition 5.1.2 can be applied to quantum walks in order to compute their average running time. We consider a quantum walk on an n-circle. It can be seen as a variant of a one-dimensional quantum walk, and it is also a special case of quantum walk on a graph defined in Subsection 2.3.4.

Let $\mathcal{H}_d$ be the direction space, which is a 2-dimensional Hilbert space with orthonormal basis state $|L\rangle$ and $|R\rangle$, indicating directions Left and Right, respectively. Assume that the n different positions on the n-circle are labelled by numbers $0, 1, \ldots, n-1$. Let $\mathcal{H}_p$ be an n-dimensional Hilbert space with orthonormal basis states $|0\rangle, |1\rangle, \ldots, |n-1\rangle$, where for each $0 \leq i \leq n-1$, the basis vector $|i\rangle$ corresponds to position i on the n-circle. Thus, the state space of the quantum walk is $\mathcal{H} = \mathcal{H}_d \otimes \mathcal{H}_p$. The initial state is assumed to be $|L\rangle|0\rangle$. Different from the quantum walks considered in Subsection 2.3.4, this walk has an absorbing boundary at position 1. So, each step of the walk consists of:

(i) Measure the position of the system to see whether the current position is 1. If the outcome is "yes", then the walk terminates; otherwise, it continues. This measurement is used to model the absorbing boundary. It can be described by

$$M = \{M_{yes} = I_d \otimes |1\rangle\langle 1|, M_{no} = I - M_{yes}\},$$

where I_d and I are the identity operators in $\mathcal{H}_d$ and $\mathcal{H}$, respectively;

(ii) A " coin-tossing" operator

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is applied in the direction space $\mathcal{H}_d$. Here, the Hadamard gate is chosen to model the "coin-tossing";

(iii) A shift operator

$$S = \sum_{i=0}^{n-1} |L\rangle\langle L| \otimes |i \ominus 1\rangle\langle i| + \sum_{i=0}^{n-1} |R\rangle\langle R| \otimes |i \oplus 1\rangle\langle i|$$

is performed in the space $\mathcal{H}$. The intuitive meaning of the operator S is that the system walks one step left or right according to the direction state. Here, $\oplus$ and $\ominus$ stand for addition and subtraction modulo n, respectively.

Using the quantum **while**-language defined in Section 3.1, this quantum walk can be written as quantum loop:

$$\textbf{while } M[d,p] = yes \textbf{ do } d,p := W[d,p] \textbf{ od}$$

where the quantum variables d, p are used to denote direction and position, respectively,

$$W = S(H \otimes I_p)$$

is the single-step walk operator, and I_p is the identity operator in $\mathcal{H}_p$.

We now compute the average running time of the quantum walk. A direct application of Proposition 5.1.2 tells us that the average running time of this walk is

$$\langle\Phi|N_0(I \otimes I - N)^{-2}(\rho \otimes I)|\Phi\rangle, \tag{5.19}$$

where

$$N_0 = M_{no} \otimes M_{no}, \quad N = (WM_{yes}) \otimes (WM_{yes})^*,$$

I is the identity matrix in $\mathcal{H} = \mathcal{H}_d \otimes \mathcal{H}_p$, and $\rho = |L\rangle\langle L| \otimes |0\rangle\langle 0|$. Note that here we do not need to use the modification procedure given by equations (5.15) and (5.16). A MATLAB program is developed to compute (5.19); see Algorithm 1. This algorithm was run on a laptop for $n < 30$, and the computational result showed that the average running time of the quantum walk on an n-circle is n.

Problem 5.1.1. *Prove or disprove that the average running time of the quantum walk on an n-circle is n for all* $n \geq 30$.

Algorithm 1 COMPUTE AVERAGE RUNNING TIME OF QUANTUM WALK ON *n*-CIRCLE

input : integer n
output: b (the average running time of quantum walk on a n-circle)
$n \times n$ **matrix** $I \leftarrow E(n)$; (*n-dimensional identity*)
integer $m \leftarrow 2n$;
$m \times m$ **matrix** $I_2 \leftarrow E(m)$; (*m-dimensional identity*)
m^2**-dimensional vector** $|\Phi\rangle \leftarrow \vec{I_2}$; (*maximally entangled state*)
$m \times m$ **matrix** $\rho \leftarrow |1\rangle\langle 1|$; (*initial state*)
2×2 **matrix** $H \leftarrow [1\ 1; 1\ -1]/\sqrt{2}$; (*Hadamard matrix*)
$m \times m$ **matrix** $M_0 \leftarrow |0\rangle\langle 0| \otimes E(2)$; (*termination test measurement*)
$m \times m$ **matrix** $M_1 \leftarrow I_2 - M_0$;
$n \times n$ **matrix** $X \leftarrow I * 0$; (*shift unitary*)
for $j = 1 : n - 1$ **do**
  $X(j, j+1) \leftarrow 1$;
end
$X(n, 1) \leftarrow 1$;
$C \leftarrow X^\dagger$;
$m \times m$ **matrix** $S \leftarrow X \otimes |0\rangle\langle 0| + C \otimes |1\rangle\langle 1|$; (*shift operator*)
$m \times m$ **matrix** $W \leftarrow S(I \otimes H)M_1$;
$m^2 \times m^2$ **matrix** $M_T \leftarrow M_0 \otimes M_0$;
$m^2 \times m^2$ **matrix** $N_T \leftarrow W_1 \otimes W_1$;
$m^2 \times m^2$ **matrix** $I_3 \leftarrow E(m^2)$; (*m^2-dimensional identity*)
real number $b \leftarrow \langle\Phi|M_T(I_3 - N_T)^{-2}(\rho \otimes I_2)|\Phi\rangle$; (*calculate the average running time*)
return b

5.2 QUANTUM GRAPH THEORY

We carefully studied termination and almost termination for quantum **while**-loops in the last section. As we will see later in the next section, the termination problem for quantum loops is a special case of reachability problem for quantum Markov chains. Indeed, classical Markov chains have been widely used in verification and analysis of randomized algorithms and probabilistic programs. So, this and the next sections are devoted to developing a theoretical framework and several algorithms for reachability analysis of quantum Markov chains. Hopefully, this will pave the way toward further research on algorithmic analysis of quantum programs.

Reachability analysis techniques for classical Markov chains heavily rely on algorithms for graph-reachability problems. Similarly, a kind of graph structures in Hilbert spaces, called quantum graphs, play a crucial role in the reachability analysis of quantum Markov chains. Therefore, in this section, we present a brief introduction to the theory of quantum graphs.

This section and the next one can be seen as the quantum generalization of reachability analysis of classical Markov chains; the reader should consult Chapter 10 of book [29] for their classical counterparts in case she/he finds some parts of these two sections hard to understand.

5.2.1 BASIC DEFINITIONS

A quantum graph structure naturally resides in a quantum Markov chain. So, let us start from the definition of quantum Markov chain. Recall that a classical Markov chain is a pair $\langle S, P\rangle$, where S is a finite set of states, and P is a matrix of transition probabilities, i.e., a mapping $P : S \times S \to [0, 1]$ such that

$$\sum_{t\in S} P(s,t) = 1$$

for every $s \in S$, where $P(s,t)$ is the probability of the system going from s to t. There is a directed graph underlying a Markov chain $\langle S, P\rangle$. The elements of S are vertices of the graph. The adjacency relation of this graph is defined as follows: for any $s, t \in S$, if $P(s,t) > 0$, then the graph has an edge from s to t. Understanding the structure of this graph is often very helpful for analysis of Markov chain $\langle S, P\rangle$ itself.

A quantum Markov chain is a quantum generalization of a Markov chain where the state space of a Markov chain is replaced by a Hilbert space and its transition matrix is replaced by a quantum operation which, as we saw in Subsection 2.1.7, is a mathematical formalism of the discrete-time evolution of (open) quantum systems.

Definition 5.2.1. *A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$, where:*

(i) *$\mathcal{H}$ is a finite-dimensional Hilbert space;*
(ii) *$\mathcal{E}$ is a quantum operation (or super-operator) in $\mathcal{H}$.*

The behavior of a quantum Markov chain can be roughly described as follows: if currently the process is in a mixed state ρ, then it will be in state $\mathcal{E}(\rho)$ in the next step. So, a quantum Markov chain $\langle \mathcal{H}, \mathcal{E}\rangle$ is a discrete-time quantum system of which the state space is $\mathcal{H}$ and the dynamics is described by quantum operation $\mathcal{E}$. From the viewpoint of quantum programming, it can be used to model the body of quantum loop (5.9).

Now we examine the graph structure underlying a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$. First of all, we introduce the adjacency relation between quantum states in $\mathcal{H}$ induced by the quantum operation $\mathcal{E}$. To this end, we need several auxiliary notions. Recall that $\mathcal{D}(\mathcal{H})$ denotes the set of partial density operators in $\mathcal{H}$, that is, positive operators ρ with trace $tr(\rho) \leq 1$. For any subset X of $\mathcal{H}$, we write $spanX$ for the subspace of $\mathcal{H}$ spanned by X, that is, it consists of all finite linear combinations of vectors in X.

Definition 5.2.2. *The support $supp(\rho)$ of a partial density operator $\rho \in \mathcal{D}(\mathcal{H})$ is the subspace of $\mathcal{H}$ spanned by the eigenvectors of ρ with nonzero eigenvalues.*

Definition 5.2.3. *Let $\{X_k\}$ be a family of subspaces of $\mathcal{H}$. Then the join of $\{X_k\}$ is defined by*

$$\bigvee_k X_k = span\left(\bigcup_k X_k\right).$$

In particular, we write $X \vee Y$ for the join of two subspaces X and Y. It is easy to see that $\bigvee_k X_k$ is the smallest subspace of $\mathcal{H}$ that contains all X_k.

Definition 5.2.4. *The image of a subspace X of $\mathcal{H}$ under a quantum operation $\mathcal{E}$ is*

$$\mathcal{E}(X) = \bigvee_{|\psi\rangle \in X} supp(\mathcal{E}(|\psi\rangle\langle\psi|)).$$

Intuitively, $\mathcal{E}(X)$ is the subspace of $\mathcal{H}$ spanned by the images under $\mathcal{E}$ of all states in X. Note that in the defining equation of $\mathcal{E}(X)$, $|\psi\rangle\langle\psi|$ is the density operator of pure state $|\psi\rangle$.

We collect several simple properties of the supports of density operators and images of quantum operations for later use.

Proposition 5.2.1

(i) *If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;*

(ii) *$supp(\rho + \sigma) = supp(\rho) \vee supp(\sigma)$;*

(iii) *If $\mathcal{E}$ has the Kraus operator-sum representation $\mathcal{E} = \sum_{i\in I} E_i \circ E_i^\dagger$, then*

$$\mathcal{E}(X) = span\{E_i|\psi\rangle : i \in I \text{ and } |\psi\rangle \in X\};$$

(iv) *$\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$. Thus, $X \subseteq Y \Rightarrow \mathcal{E}(X) \subseteq \mathcal{E}(Y)$;*

(v) *$\mathcal{E}(supp(\rho)) = supp(\mathcal{E}(\rho))$.*

Exercise 5.2.1. *Prove Proposition 5.2.1.*

Based on Definitions 5.2.2 and 5.2.4, we can define the adjacency relation between (pure and mixed) states in a quantum Markov chain.

Definition 5.2.5. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain, and let $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ be pure states and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ be mixed states in $\mathcal{H}$. Then*

(i) *$|\varphi\rangle$ is adjacent to $|\psi\rangle$ in $\mathcal{C}$, written $|\psi\rangle \to |\varphi\rangle$, if $|\varphi\rangle \in supp(\mathcal{E}(|\psi\rangle\langle\psi|))$.*

(ii) *$|\varphi\rangle$ is adjacent to ρ, written $\rho \to |\varphi\rangle$, if $|\varphi\rangle \in \mathcal{E}(supp(\rho))$.*

(iii) *σ is adjacent to ρ, written $\rho \to \sigma$, if $supp(\sigma) \subseteq \mathcal{E}(supp(\rho))$.*

Intuitively, $\langle \mathcal{H}, \to\rangle$ can be imagined as a "directed graph." However, there are two major differences between this graph and a classical graph:

- The set of vertices of a classical graph is usually finite, whereas the state Hilbert space $\mathcal{H}$ is a continuum;
- A classical graph has no mathematical structure other than the adjacency relation, but the space $\mathcal{H}$ possesses a linear algebraic structure that must be preserved by an algorithm searching through the graph $\langle \mathcal{H}, \to\rangle$.

As we will see in the following, these differences between a quantum graph and a classical graph make analysis of the former much harder than that of the latter.

We now can define the core notion of this section, namely reachability in a quantum graph, based on the adjacency relation in the same way as in the classical graph theory.

Definition 5.2.6

(i) *A path from ρ to σ in a quantum Markov chain $\mathcal{C}$ is a sequence*

$$\pi = \rho_0 \to \rho_1 \to \cdots \to \rho_n \ (n \geq 0)$$

of adjacent density operators in $\mathcal{C}$ such that $supp(\rho_0) \subseteq supp(\rho)$ and $\rho_n = \sigma$.

(ii) *For any density operators ρ and σ, if there is a path from ρ to σ then we say that σ is reachable from ρ in $\mathcal{C}$.*

Definition 5.2.7. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. For any $\rho \in \mathcal{D}(\mathcal{H})$, its reachable space in $\mathcal{C}$ is the subspace of $\mathcal{H}$ spanned by the states reachable from ρ:*

$$\mathcal{R}_{\mathcal{C}}(\rho) = span\{|\psi\rangle \in \mathcal{H} : |\psi\rangle \ \text{is reachable from} \ \rho \ \text{in} \ \mathcal{C}\}. \tag{5.20}$$

Note that in equation (5.20), $|\psi\rangle$ is identified with its density operator $|\psi\rangle\langle\psi|$.

Reachability in classical graph theory is transitive: that is, if a vertex v is reachable from u, and w is reachable from v, then w is also reachable from u. As expected, the following lemma shows that reachability in a quantum Markov chain is transitive too.

Lemma 5.2.1. *(Transitivity of reachability) For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, if $supp(\rho) \subseteq \mathcal{R}_{\mathcal{C}}(\sigma)$, then $\mathcal{R}_{\mathcal{C}}(\rho) \subseteq \mathcal{R}_{\mathcal{C}}(\sigma)$.*

Exercise 5.2.2. *Prove Lemma 5.2.1.*

We now consider how to compute the reachable space of a state in a quantum Markov chain. To motivate our method, let us consider a classical directed graph $\langle V, E \rangle$, where V is the set of vertices and $E \subseteq V \times V$ is the adjacency relation. The transitive closure of E is defined as follows:

$$t(E) = \bigcup_{n=0}^{\infty} E^n = \{\langle v, v' \rangle : v' \ \text{is reachable from} \ v \ \text{in} \ \langle V, E \rangle\}.$$

It is well-known that the transitive closure can be computed as follows:

$$t(E) = \bigcup_{n=0}^{|V|-1} E^n$$

where $|V|$ is the number of vertices. As a quantum generalization of this fact, we have:

Theorem 5.2.1. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. If $d = \dim \mathcal{H}$, then for any $\rho \in \mathcal{D}(\mathcal{H})$, we have*

$$\mathcal{R}_{\mathcal{C}}(\rho) = \bigvee_{i=0}^{d-1} supp\left(\mathcal{E}^i(\rho)\right) \tag{5.21}$$

where $\mathcal{E}^i$ is the ith power of $\mathcal{E}$; that is, $\mathcal{E}^0 = \mathcal{I}$ (the identity operation in $\mathcal{H}$) and

$$\mathcal{E}^{i+1} = \mathcal{E} \circ \mathcal{E}^i$$

for $i \geq 0$.

Proof. We first show that $|\psi\rangle$ is reachable from ρ if and only if $|\psi\rangle \in supp\left(\mathcal{E}^i(\rho)\right)$ for some $i \geq 0$. In fact, if $|\psi\rangle$ is reachable from ρ, then there exist $\rho_1, \ldots, \rho_{i-1}$ such that

$$\rho \to \rho_1 \to \ldots \to \rho_{i-1} \to |\psi\rangle.$$

Using Proposition 5.2.1 (v), we obtain:

$$\begin{aligned} |\psi\rangle \in supp(\mathcal{E}(\rho_{i-1})) &= \mathcal{E}(supp(\rho_{i-1})) \\ &\subseteq \mathcal{E}(supp(\mathcal{E}(\rho_{i-2})) \\ &= supp\left(\mathcal{E}^2(\rho_{i-2})\right) \subseteq \ldots \subseteq supp\left(\mathcal{E}^i(\rho)\right). \end{aligned}$$

Conversely, if $|\psi\rangle \in supp(\mathcal{E}^i(\rho))$, then

$$\rho \to \mathcal{E}(\rho) \to \ldots \to \mathcal{E}^{i-1}(\rho) \to |\psi\rangle$$

and $|\psi\rangle$ is reachable from ρ. Therefore, it holds that

$$\begin{aligned} \mathcal{R}_{\mathcal{C}}(\rho) &= span\{|\psi\rangle : |\psi\rangle \text{ is reachable from } \rho\} \\ &= span\left[\bigcup_{i=0}^{\infty} supp\left(\mathcal{E}^i(\rho)\right)\right] \\ &= \bigvee_{i=0}^{\infty} supp\left(\mathcal{E}^i(\rho)\right). \end{aligned}$$

Now for each $n \geq 0$, we put

$$X_n = \bigvee_{i=0}^{n} supp\left(\mathcal{E}^i(\rho)\right).$$

Then we obtain an increasing sequence

$$X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq X_{n+1} \subseteq \ldots$$

of subspaces of $\mathcal{H}$. Let $d_n = \dim X_n$ for every $n \geq 0$. Then

$$d_0 \leq d_1 \leq \ldots \leq d_n \leq d_{n+1} \leq \ldots.$$

Note that $d_n \leq d$ for all n. Thus, there must be some n such that $d_n = d_{n+1}$. Assume that N is the smallest integer n such that $d_n = d_{n+1}$. Then we have

$$0 < \dim supp(\rho) = d_0 < d_1 < \ldots < d_{N-1} < d_N \leq d$$

and $N \leq d-1$. On the other hand, both X_N and X_{N+1} are subspaces of $\mathcal{H}$, $X_N \subseteq X_{N+1}$ and $\dim X_N = \dim X_{N+1}$. Thus, $X_N = X_{N+1}$. We can prove that

$$supp\left(\mathcal{E}^{N+k}(\rho)\right) \subseteq X_N$$

for all $k \geq 1$ by induction on k. So, $\mathcal{R}_{\mathcal{C}}(\rho) = X_N$. □

5.2.2 BOTTOM STRONGLY CONNECTED COMPONENTS

We carefully defined the graph underlying a quantum Markov chain in the previous subsection. Now we move forward to examine its mathematical structure. In classical graph theory, the notion of bottom strongly connected component (BSCC) is an important tool in the studies of reachability problems. It has also been extensively applied in analysis of probabilistic programs modelled by Markov chains. In this subsection, we extend this notion to the quantum case. The quantum version of BSCC will be a basis of the reachability analysis algorithms for quantum Markov chains given in the next section.

We first introduce an auxiliary notation. Let X be a subspace of $\mathcal{H}$ and $\mathcal{E}$ a quantum operation in $\mathcal{H}$. Then the restriction of $\mathcal{E}$ on X is the quantum operation $\mathcal{E}_X$ in X defined by

$$\mathcal{E}_X(\rho) = P_X \mathcal{E}(\rho) P_X$$

for all $\rho \in \mathcal{D}(X)$, where P_X is the projection onto X. With this notation, we are able to define strong connectivity in a quantum Markov chain.

Definition 5.2.8. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. A subspace X of $\mathcal{H}$ is called strongly connected in $\mathcal{C}$ if for any $|\varphi\rangle, |\psi\rangle \in X$, we have:*

$$|\varphi\rangle \in \mathcal{R}_{\mathcal{C}_X}(\psi) \text{ and } |\psi\rangle \in \mathcal{R}_{\mathcal{C}_X}(\varphi) \tag{5.22}$$

where $\varphi = |\varphi\rangle\langle\varphi|$ and $\psi = |\psi\rangle\langle\psi|$ are the density operators corresponding to pure states $|\varphi\rangle$ and $\psi\rangle$, respectively, quantum Markov chain $\mathcal{C}_X = \langle X, \mathcal{E}_X \rangle$ is the restriction of $\mathcal{C}$ on X, and $\mathcal{R}_{\mathcal{C}_X}(\cdot)$ denotes a reachable subspace in $\mathcal{C}_X$.

Intuitively, condition (5.22) means that for any two states $|\varphi\rangle, |\psi\rangle$ in X, $|\varphi\rangle$ is reachable from $|\psi\rangle$ and $|\psi\rangle$ is reachable from $|\varphi\rangle$.

We write $SC(\mathcal{C})$ for the set of all strongly connected subspaces of $\mathcal{H}$ in $\mathcal{C}$. It is clear that $SC(\mathcal{C})$ with set inclusion $\subseteq$, i.e., $(SC(\mathcal{C}), \subseteq)$ is a partial order (see Definition 3.3.2). To further examine this partial order, we recall several concepts from lattice theory. Let $(L, \sqsubseteq)$ be a partial order. If any two elements $x, y \in L$ are comparable, that is, either $x \sqsubseteq y$ or $y \sqsubseteq x$, then we say that L is linearly ordered by $\sqsubseteq$. A partial order $(L, \sqsubseteq)$ is said to be inductive if for any subset K of L that is linearly ordered by $\sqsubseteq$, the least upper bound $\bigsqcup K$ exists in L.

Lemma 5.2.2. *The partial order $(SC(\mathcal{C}), \subseteq)$ is inductive.*

Exercise 5.2.3. *Prove Lemma 5.2.2.*

Now we further consider some special elements in the partial order $(SC(\mathcal{C}), \subseteq)$. Recall that an element x of a partial order $(L, \sqsubseteq)$ is called a maximal element of L if for any $y \in L$, $x \sqsubseteq y$ implies $x = y$. The Zorn lemma in set theory asserts that every inductive partial order has (at least one) maximal elements.

Definition 5.2.9. *A maximal element of $(SC(\mathcal{C}), \subseteq)$ is called a strongly connected component (SCC) of $\mathcal{C}$.*

To define the concept of BSCC (bottom strongly connected component) in a quantum Markov chain, we need one more auxiliary notion, namely invariant subspace.

Definition 5.2.10. *We say that a subspace X of $\mathcal{H}$ is invariant under a quantum operation $\mathcal{E}$ if $\mathcal{E}(X) \subseteq X$.*

The intuition behind the inclusion $\mathcal{E}(X) \subseteq X$ is that quantum operation $\mathcal{E}$ cannot transfer a state in X into a state outside X. Suppose that quantum operation $\mathcal{E}$ has the Kraus representation $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$. Then it follows from Proposition 5.2.1 that X is invariant under $\mathcal{E}$ if and only if it is invariant under the Kraus operators E_i: $E_i X \subseteq X$ for all i.

The following theorem presents a useful property of invariant subspaces showing that a quantum operation does not decrease the probability of falling into an invariant subspace.

Theorem 5.2.2. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. If subspace X of $\mathcal{H}$ is invariant under $\mathcal{E}$, then we have:*

$$tr(P_X \mathcal{E}(\rho)) \geq tr(P_X \rho)$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Proof. It suffices to show that

$$tr(P_X \mathcal{E}(|\psi\rangle\langle\psi|)) \geq tr(P_X |\psi\rangle\langle\psi|)$$

for each $|\psi\rangle \in \mathcal{H}$. Assume that $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$, and $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$ where $|\psi_1\rangle \in X$ and $|\psi_2\rangle \in X^\perp$. Since X is invariant under $\mathcal{E}$, we have $E_i|\psi_1\rangle \in X$ and $P_X E_i |\psi_1\rangle = E_i |\psi_1\rangle$. Then

$$\begin{aligned} a &\stackrel{\triangle}{=} \sum_i tr\left(P_X E_i |\psi_2\rangle\langle\psi_1| E_i^\dagger\right) = \sum_i tr\left(E_i |\psi_2\rangle\langle\psi_1| E_i^\dagger P_X\right) \\ &= \sum_i tr\left(E_i |\psi_2\rangle\langle\psi_1| E_i^\dagger\right) = \sum_i \langle\psi_1| E_i^\dagger E_i |\psi_2\rangle = \langle\psi_1|\psi_2\rangle = 0. \end{aligned}$$

Similarly, it holds that

$$b \stackrel{\triangle}{=} \sum_i tr\left(P_X E_i |\psi_1\rangle\langle\psi_2| E_i^\dagger\right) = 0.$$

Moreover, we have:

$$c \triangleq \sum_i tr\left(P_X E_i|\psi_2\rangle\langle\psi_2|E_i^\dagger\right) \geq 0.$$

Therefore,

$$\begin{aligned} tr\left(P_X\mathcal{E}(|\psi\rangle\langle\psi|)\right) &= \sum_i tr\left(P_X E_i|\psi_1\rangle\langle\psi_1|E_i^\dagger\right) + a + b + c \\ &\geq \sum_i tr\left(P_X E_i|\psi_1\rangle\langle\psi_1|E_i^\dagger\right) = \sum_i \langle\psi_1|E_i^\dagger E_i|\psi_1\rangle \\ &= \langle\psi_1|\psi_1\rangle = tr(P_X|\psi\rangle\langle\psi|). \end{aligned}$$

□

Now we are ready to introduce the key notion of this subsection, namely bottom strongly connected component.

Definition 5.2.11. *Let $\mathcal{C} = \langle\mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain. Then a subspace X of $\mathcal{H}$ is called a bottom strongly connected component (BSCC) of $\mathcal{C}$ if it is an SCC of $\mathcal{C}$ and it is invariant under $\mathcal{E}$.*

Example 5.2.1. *Consider quantum Markov chain $\mathcal{C} = \langle\mathcal{H}, \mathcal{E}\rangle$ with state Hilbert space $\mathcal{H} = span\{|0\rangle, \cdots, |4\rangle\}$ and quantum operation $\mathcal{E} = \sum_{i=1}^5 E_i \circ E_i^\dagger$, where the Kraus operators are given by*

$$\begin{aligned} E_1 &= \frac{1}{\sqrt{2}}(|1\rangle\langle\theta_{01}^+| + |3\rangle\langle\theta_{23}^+|), \quad E_2 = \frac{1}{\sqrt{2}}(|1\rangle\langle\theta_{01}^-| + |3\rangle\langle\theta_{23}^-|), \\ E_3 &= \frac{1}{\sqrt{2}}(|0\rangle\langle\theta_{01}^+| + |2\rangle\langle\theta_{23}^+|), \quad E_4 = \frac{1}{\sqrt{2}}(|0\rangle\langle\theta_{01}^-| + |2\rangle\langle\theta_{23}^-|), \\ E_5 &= \frac{1}{10}(|0\rangle\langle 4| + |1\rangle\langle 4| + |2\rangle\langle 4| + 4|3\rangle\langle 4| + 9|4\rangle\langle 4|), \end{aligned}$$

and

$$|\theta_{ij}^\pm\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}. \tag{5.23}$$

It is easy to verify that $B = span\{|0\rangle, |1\rangle\}$ is a BSCC of quantum Markov chain $\mathcal{C}$. Indeed, for any $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in B$, we have

$$\mathcal{E}(|\psi\rangle\langle\psi|) = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2.$$

Characterizations of BSCCs:

To help the reader have a better understanding of them, we give two characterizations of BSCCs. The first characterization is simple and it is presented in terms of reachable subspaces.

Lemma 5.2.3. *A subspace X is a BSCC of quantum Markov chain $\mathcal{C}$ if and only if $\mathcal{R}_\mathcal{C}(|\varphi\rangle\langle\varphi|) = X$ for any $|\varphi\rangle \in X$.*

Proof. We only prove the "only if" part because the "if" part is obvious. Suppose X is a BSCC. By the strong connectivity of X, we have $\mathcal{R}_\mathcal{C}(|\varphi\rangle\langle\varphi|) \supseteq X$ for all

$|\varphi\rangle \in X$. On the other hand, for any vector $|\varphi\rangle$ in X, using the invariance of X, i.e., $\mathcal{E}(X) \subseteq X$, it is easy to show that if $|\psi\rangle$ is reachable from $|\varphi\rangle$ then $|\psi\rangle \in X$. So, $\mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) \subseteq X$. □

The second characterization of BSCCs is a little bit more complicated. To present it, we need the notion of fixed point of a quantum operation.

Definition 5.2.12

(i) *A density operator ρ in $\mathcal{H}$ is called a fixed point state of quantum operation $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.*

(ii) *A fixed point state ρ of quantum operation $\mathcal{E}$ is called minimal if for any fixed point state σ of $\mathcal{E}$, it holds that $supp(\sigma) \subseteq supp(\rho)$ implies $\sigma = \rho$.*

The following lemma shows a close connection between the invariant subspaces under a quantum operation $\mathcal{E}$ and the fixed point states of $\mathcal{E}$. It provides a key step in the proof of Theorem 5.2.3 to follow.

Lemma 5.2.4. *If ρ is a fixed point state of $\mathcal{E}$, then $supp(\rho)$ is invariant under $\mathcal{E}$. Conversely, if X is invariant under $\mathcal{E}$, then there exists a fixed point state ρ_X of $\mathcal{E}$ such that $supp(\rho_X) \subseteq X$.*

Exercise 5.2.4. *Prove Lemma 5.2.4.*

Now we are able to give the second characterization, which establishes a connection between BSCCs and minimal fixed point states.

Theorem 5.2.3. *A subspace X is a BSCC of quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ if and only if there exists a minimal fixed point state ρ of $\mathcal{E}$ such that $supp(\rho) = X$.*

Proof. We first prove the "if" part. Let ρ be a minimal fixed point state such that $supp(\rho) = X$. Then by Lemma 5.2.4, X is invariant under $\mathcal{E}$. To show that X is a BSCC, by Lemma 5.2.3 it suffices to prove that for any $|\varphi\rangle \in X$, $\mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) = X$. Suppose conversely that there exists $|\psi\rangle \in X$ such that $\mathcal{R}_{\mathcal{C}}(|\psi\rangle\langle\psi|) \subsetneq X$. Then by Lemma 5.2.1 we can show that $\mathcal{R}_{\mathcal{C}}(|\psi\rangle\langle\psi|)$ is invariant under $\mathcal{E}$. By Lemma 5.2.4, we can find a fixed point state ρ_ψ with

$$supp(\rho_\psi) \subseteq \mathcal{R}_{\mathcal{C}}(|\psi\rangle\langle\psi|) \subsetneq X.$$

This contradicts the assumption that ρ is minimal.

For the "only if" part, suppose that X is a BSCC. Then X is invariant under $\mathcal{E}$, and by Lemma 5.2.4, we can find a minimal fixed point state ρ_X of $\mathcal{E}$ with $supp(\rho_X) \subseteq X$. Take $|\varphi\rangle \in supp(\rho_X)$. By Lemma 5.2.5 we have $\mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) = X$. But using Lemma 5.2.4 again, we know that $supp(\rho_X)$ is invariant under $\mathcal{E}$, so $\mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) \subseteq supp(\rho_X)$. Therefore, $supp(\rho_X) = X$. □

As mentioned previously, BSCCs will play a key role in analysis of quantum Markov chains. This application of BSCCs is based on not only our understanding of their structure described in Lemma 5.2.3 and Theorem 5.2.3 but also their relationship to each other. The following lemma clarifies the relationship between two different BSCCs.

Lemma 5.2.5

(i) *For any two different BSCCs X and Y of quantum Markov chain $\mathcal{C}$, we have $X \cap Y = \{0\}$ (0-dimensional Hilbert space).*

(ii) *If X and Y are two BSCCs of $\mathcal{C}$ with $\dim X \neq \dim Y$, then they are orthogonal, i.e., $X \perp Y$.*

Proof.

(i) Suppose conversely that there exists a nonzero vector $|\varphi\rangle \in X \cap Y$. Then by Lemma 5.2.3, we have $X = \mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) = Y$, contradicting the assumption that $X \neq Y$. Therefore $X \cap Y = \{0\}$.

(ii) We postpone this part to Section 5.4 because it needs to use Theorem 5.2.5 in the following section. □

5.2.3 DECOMPOSITION OF THE STATE HILBERT SPACE

In the previous two subsections, a graph structure in a quantum Markov chain was defined, and the notion of BSCC was generalized to the quantum case. In this subsection, we further study such a graph structure in a quantum Markov chain through a decomposition of the state Hilbert space.

Recall that a state in a classical Markov chain is transient if there is a nonzero probability that the process will never return to it, and a state is recurrent if from it the returning probability is 1. It is well-known that in a finite-state Markov chain a state is recurrent if and only if it belongs to some BSCC, and thus the state space of the Markov chain can be decomposed into the union of some BSCCs and a transient subspace. The aim of this subsection is to prove a quantum generalization of this result. Such a decomposition of the state Hilbert space forms a basis of our algorithms for reachability analysis of quantum Markov chains, to be presented in the next section.

Transient Subspaces:

Let us first define the notion of a transient subspace of a quantum Markov chain. Transient states in a finite-state classical Markov chain can be equivalently characterized as follows: a state is transient if and only if the probability that the system stays at it will eventually become 0. This observation motivates the following:

Definition 5.2.13. *A subspace $X \subseteq \mathcal{H}$ is transient in a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ if*

$$\lim_{k\to\infty} tr\left(P_X \mathcal{E}^k(\rho)\right) = 0 \tag{5.24}$$

for any $\rho \in \mathcal{D}(\mathcal{H})$, where P_X is the projection onto X.

Intuitively, $tr_X\left(P_X \mathcal{E}^k(\rho)\right)$ is the probability that the system's state falls into the subspace X after executing quantum operation $\mathcal{E}$ for k times. So, equation (5.24) means that the probability that the system stays in subspace X is eventually 0.

It is obvious from this definition that if subspaces $X \subseteq Y$ and Y is transient then X is transient too. So, it is sufficient to understand the structure of the largest transient subspace. Fortunately, we have an elegant characterization of the largest transient subspace. To give such a characterization, we need the following:

Definition 5.2.14. *Let $\mathcal{E}$ be a quantum operation in $\mathcal{H}$. Then its asymptotic average is*

$$\mathcal{E}_\infty = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}^n. \tag{5.25}$$

It follows from Lemma 3.3.4 that $\mathcal{E}_\infty$ is a quantum operation as well.

The following lemma points out a link between fixed point states of a quantum operation and its asymptotic average. This link will be used in the proof of Theorem 5.2.4 following.

Lemma 5.2.6

(i) *For any density operator ρ, $\mathcal{E}_\infty(\rho)$ is a fixed point state of $\mathcal{E}$;*
(ii) *For any fixed point state σ, it holds that $supp(\sigma) \subseteq \mathcal{E}_\infty(\mathcal{H})$.*

Exercise 5.2.5. *Prove Lemma 5.2.6.*

Now we can give a characterization of the largest transient subspace in terms of asymptotic average.

Theorem 5.2.4. *Let $\mathcal{C}=\langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain. Then the orthocomplement of the image of $\mathcal{H}$ under the asymptotic average of $\mathcal{E}$:*

$$T_{\mathcal{E}} = \mathcal{E}_\infty(\mathcal{H})^\perp$$

is the largest transient subspace in $\mathcal{C}$, where $^\perp$ stands for orthocomplement (see Definition 2.1.7(ii)).

Proof. Let P be the projection onto the subspace $T_{\mathcal{E}}$. For any $\rho \in \mathcal{D}(\mathcal{H})$, we put $p_k = tr\left(P\mathcal{E}^k(\rho)\right)$ for every $k \geq 0$. Since $\mathcal{E}_\infty(\mathcal{H})$ is invariant under $\mathcal{E}$, by Theorem 5.2.2 we know that the sequence $\{p_k\}$ is non-increasing. Thus the limit $p_\infty = \lim_{k\to\infty} p_k$ does exist. Furthermore, noting that

$$supp(\mathcal{E}_\infty(\rho)) \subseteq \mathcal{E}_\infty(\mathcal{H})$$

we have

$$\begin{aligned} 0 = tr(P\mathcal{E}_\infty(\rho)) &= tr\left(P \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}^n(\rho)\right) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} tr\left(P\mathcal{E}^n(\rho)\right) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} p_n \end{aligned}$$

$$\geq \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} p_\infty = p_\infty.$$

Thus $p_\infty = 0$, and $T_{\mathcal{E}}$ is transient by the arbitrariness of ρ.

To show that $T_{\mathcal{E}}$ is the largest transient subspace of $\mathcal{C}$, we first note that

$$supp\,(\mathcal{E}_\infty(I)) = \mathcal{E}_\infty(\mathcal{H}).$$

Let $\sigma = \mathcal{E}_\infty(I/d)$. Then by Lemma 5.2.6, σ is a fixed point state with $supp(\sigma) = T_{\mathcal{E}}^{\perp}$. Suppose Y is a transient subspace. We have

$$tr(P_Y\sigma) = \lim_{i\to\infty} tr\left(P_Y\mathcal{E}^i(\sigma)\right) = 0.$$

This implies $Y \perp supp(\sigma) = T_{\mathcal{E}}^{\perp}$. So, we have $Y \subseteq T_{\mathcal{E}}$. □

BSCC Decomposition:

After introducing the notion of transient subspace, we now consider how to decompose the state Hilbert space of a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$. First, it can be simply divided into two parts:

$$\mathcal{H} = \mathcal{E}_\infty(\mathcal{H}) \oplus \mathcal{E}_\infty(\mathcal{H})^\perp$$

where $\oplus$ stands for (orthogonal) sum (see Definition 2.1.8), and $\mathcal{E}_\infty(\mathcal{H})$ is the image of the whole state Hilbert space under the asymptotic average. We already know from Theorem 5.2.4 that $\mathcal{E}_\infty(\mathcal{H})^\perp$ is the largest transient subspace. So, what we need to do next is to examine the structure of $\mathcal{E}_\infty(\mathcal{H})$.

Our procedure for decomposition of $\mathcal{E}_\infty(\mathcal{H})$ is based on the following key lemma that shows how a fixed point state can be subtracted by another.

Lemma 5.2.7. *Let ρ and σ be two fixed point states of $\mathcal{E}$, and $supp(\sigma) \subsetneq supp(\rho)$. Then there exists another fixed point state η such that*

(i) *$supp(\eta) \perp supp(\sigma)$; and*
(ii) *$supp(\rho) = supp(\eta) \oplus supp(\sigma)$.*

Intuitively, state η in the preceding lemma can be understood as the subtraction of ρ by σ. For readability, the proof of this lemma is postponed to Section 5.4.

Now the BSCC decomposition of $\mathcal{E}_\infty(\mathcal{H})$ can be derived simply by repeated applications of the preceding lemma.

Theorem 5.2.5. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain. Then $\mathcal{E}_\infty(\mathcal{H})$ can be decomposed into the direct sum of orthogonal BSCCs of $\mathcal{C}$.*

Proof. We notice that $\mathcal{E}_\infty\left(\frac{I}{d}\right)$ is a fixed point state of $\mathcal{E}$ and

$$supp\left(\mathcal{E}_\infty\left(\frac{I}{d}\right)\right) = \mathcal{E}_\infty(\mathcal{H})$$

where $d = \dim \mathcal{H}$. Then it suffices to prove the following:

- *Claim*: Let ρ be a fixed point state of $\mathcal{E}$. Then $supp(\rho)$ can be decomposed into the direct sum of some orthogonal BSCCs.

In fact, if ρ is minimal, then by Theorem 5.2.3, $supp(\rho)$ is itself a BSCC and we are done. Otherwise, we apply Lemma 5.2.7 to obtain two fixed point states of $\mathcal{E}$ with smaller orthogonal supports. Repeating this procedure, we can get a set of minimal fixed point states $\rho_1, \cdots, \rho_k$ with mutually orthogonal supports such that

$$supp(\rho) = \bigoplus_{i=1}^{k} supp(\rho_i).$$

Finally, from Lemma 5.2.4 and Theorem 5.2.3, we know that each $supp(\rho_i)$ is a BSCC. □

Now we eventually achieve the decomposition promised at the beginning of this subsection. Combining Theorems 5.2.4 and 5.2.5, we see that the state Hilbert space of a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ can be decomposed into the direct sum of a transient subspace and a family of BSCCs:

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} \tag{5.26}$$

where B_i's are orthogonal BSCCs of $\mathcal{C}$, and $T_{\mathcal{E}}$ is the largest transient subspace.

The preceding theorem shows the existence of BSCC decomposition for quantum Markov chains. Then a question immediately arises: is such a decomposition unique? It is well known that the BSCC decomposition of a classical Markov chain is unique. However, it is not the case for quantum Markov chains, as shown in the following:

Example 5.2.2. *Let quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be given as in Example 5.2.1. Then*

$$B_1 = span\{|0\rangle, |1\rangle\}, \quad B_2 = span\{|2\rangle, |3\rangle\},$$
$$D_1 = span\{|\theta_{02}^{+}\rangle, |\theta_{13}^{+}\rangle\}, \quad D_2 = span\{|\theta_{02}^{-}\rangle, |\theta_{13}^{-}\rangle\}$$

are all BSCCs, where the states $|\theta_{ij}^{\pm}\rangle$ are defined by equation (5.23). It is easy to see that $T_{\mathcal{E}} = span\{|4\rangle\}$ is the largest transient subspace. Furthermore, we have two different decompositions:

$$\mathcal{H} = B_1 \oplus B_2 \oplus T_{\mathcal{E}} = D_1 \oplus D_2 \oplus T_{\mathcal{E}}.$$

Although the BSCC decomposition of a quantum Markov chain is not unique, fortunately we have the following weak uniqueness in the sense that any two decompositions have the same number of BSCCs, and the corresponding BSCCs in them must have the same dimension.

Theorem 5.2.6. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, and let*

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} = D_1 \oplus \cdots \oplus D_v \oplus T_{\mathcal{E}}$$

be two decompositions in the form of equation (5.26), and B_is and D_is are arranged, respectively, according to the increasing order of the dimensions. Then

(i) $u = v$; *and*
(ii) $\dim B_i = \dim D_i$ *for each* $1 \leq i \leq u$.

Proof. For simplicity, we write $b_i = \dim B_i$ and $d_i = \dim D_i$. We prove by induction on i that $b_i = d_i$ for any $1 \leq i \leq \min\{u, v\}$, and thus $u = v$ as well.

First, we claim $b_1 = d_1$. Otherwise let, say, $b_1 < d_1$. Then $b_1 < d_j$ for all j. Thus by Lemma 5.2.5 (ii), we have:

$$B_1 \perp \bigoplus_{j=1}^{v} D_j.$$

But we also have $B_1 \perp T_{\mathcal{E}}$. This is a contradiction, as it holds that

$$\left(\bigoplus_{j=1}^{v} D_j \right) \oplus T_{\mathcal{E}} = \mathcal{H}.$$

Now suppose we already have $b_i = d_i$ for all $i < n$. We claim $b_n = d_n$. Otherwise let, say, $b_n < d_n$. Then from Lemma 5.2.5 (ii), we have

$$\bigoplus_{i=1}^{n} B_i \perp \bigoplus_{i=n}^{v} D_i,$$

and consequently

$$\bigoplus_{i=1}^{n} B_i \subseteq \bigoplus_{i=1}^{n-1} D_i.$$

On the other hand, we have

$$\dim \left(\bigoplus_{i=1}^{n} B_i \right) = \sum_{i=1}^{n} b_i > \sum_{i=1}^{n-1} d_i = \dim \left(\bigoplus_{i=1}^{n-1} D_i \right),$$

a contradiction. □

Decomposition Algorithm:

We have proved the existence and weak uniqueness of BSCC decomposition for quantum Markov chains. With these theoretical preparations, we can now present an algorithm for finding a BSCC and transient subspace decomposition of a quantum Markov chain; see Algorithm 2 together with the procedure Decompose(X).

To conclude this section, we consider correctness and complexity of the BSCC decomposition algorithms. The following lemma is the key in settling the complexity of Algorithm 2.

Algorithm 2 DECOMPOSE($\mathcal{C}$)

input : A quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$
output: A set of orthogonal BSCCs $\{B_i\}$ and a transient subspace $T_{\mathcal{E}}$ such that $\mathcal{H} = \left(\bigoplus_i B_i\right) \oplus T_{\mathcal{E}}$
begin
  $\mathcal{B} \leftarrow$ Decompose($\mathcal{E}_\infty(\mathcal{H})$);
  return $\mathcal{B}$, $\mathcal{E}_\infty(\mathcal{H})^\perp$;
end

Procedure Decompose(X)

input : A subspace X which is the support of a fixed point state of $\mathcal{E}$
output: A set of orthogonal BSCCs $\{B_i\}$ such that $X = \bigoplus B_i$
begin
  $\mathcal{E}' \leftarrow P_X \circ \mathcal{E}$;
  $\mathcal{B} \leftarrow$ a density operator basis of the set {operators A in $\mathcal{H} : \mathcal{E}'(A) = A$};
  if $|\mathcal{B}| = 1$ **then**
    $\rho \leftarrow$ the unique element of $\mathcal{B}$;
    return $\{supp(\rho)\}$;
  else
    $\rho_1, \rho_2 \leftarrow$ two arbitrary elements of $\mathcal{B}$;
    $\rho \leftarrow$ positive part of $\rho_1 - \rho_2$;
    $Y \leftarrow supp(\rho)^\perp$; (* the orthocomplement of $supp(\rho)$ in X*)
    return Decompose($supp(\rho)$) $\cup$ Decompose(Y);
  end
end

Lemma 5.2.8. *Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain with $d = \dim \mathcal{H}$, and $\rho \in \mathcal{D}(\mathcal{H})$. Then*

(i) *The asymptotic average state $\mathcal{E}_\infty(\rho)$ can be computed in time $O(d^8)$.*
(ii) *A density operator basis of the set of fixed points of $\mathcal{E}$:*

$$\{\text{operators } A \text{ in } \mathcal{H} : \mathcal{E}(A) = A\}$$

can be computed in time $O(d^6)$.

For readability, we postpone the proof of this lemma into Section 5.4.

Now the correctness and complexity of Algorithm 2 are shown in the following:

Theorem 5.2.7. *Given a quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$, Algorithm 2 decomposes the Hilbert space $\mathcal{H}$ into the direct sum of a family of orthogonal BSCCs and a transient subspace of $\mathcal{C}$ in time $O(d^8)$, where $d = \dim \mathcal{H}$.*

Proof. The correctness of Algorithm 2 is easy to prove. Actually, it follows immediately from Theorem 5.2.4.

For the time complexity, we first notice that the nonrecursive part of the procedure Decompose(X) runs in time $O(d^6)$. Thus, total complexity of Decompose(X) is $O(d^7)$, as the procedure calls itself at most $O(d)$ times. Algorithm 2 first computes $\mathcal{E}_\infty(\mathcal{H})$, which, as indicated by Lemma 5.2.8 (i), costs time $O(d^8)$, and then feeds it into the procedure Decompose(X). Thus the total complexity of Algorithm 2 is $O(d^8)$. □

Problem 5.2.1. *Quantum graph theory has been developed in this section merely to provide necessary mathematical tools for reachability analysis of quantum Markov chains in the next section. It is desirable to build a richer theory of quantum graphs by generalizing more results in (di-)graphs theory [33] into the quantum setting and by understanding the essential differences between classical and quantum graphs.*

Problem 5.2.2. *The notion of a noncommutative graph was introduced in [76] in order to give a characterization of channel capacity in quantum Shannon information theory. It is interesting to find some connections between non-commutative graphs and quantum graphs defined in this section.*

5.3 REACHABILITY ANALYSIS OF QUANTUM MARKOV CHAINS

The graph structures of quantum Markov chains were carefully examined in the last section. This prepares necessary mathematical tools for reachability analysis of quantum Markov chains. In this section, we study reachability and its two variants – repeated reachability and persistence – of quantum Markov chains using the quantum graph theory developed in the last section.

As will be shown in Exercise 5.3.1 following, termination of a quantum **while**-loop can be reduced to a reachability problem of a quantum Markov chain. Indeed, as in classical and probabilistic programming theory, many other behaviors of quantum programs can be described in terms of the reachability and persistence discussed in this section when their semantics are modelled as quantum Markov chains. Furthermore, this section provides a basis for further research on analysis of more complicated quantum programs such as recursive quantum programs defined in Section 3.4, as well as nondeterministic and concurrent quantum programs, because various extensions of quantum Markov chains, e.g., recursive quantum Markov chains and quantum Markov decision processes, can serve as their semantic models.

5.3.1 REACHABILITY PROBABILITY

We first consider reachability probability in a quantum Markov chain, which is formally defined in the following:

Definition 5.3.1. *Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$ an initial state, and $X \subseteq \mathcal{H}$ a subspace. Then the probability of reaching X, starting from ρ, is*

$$\Pr(\rho \vDash \Diamond X) = \lim_{i\to\infty} tr\left(P_X \widetilde{\mathcal{E}}^i(\rho)\right) \tag{5.27}$$

where $\widetilde{\mathcal{E}}^i$ is the composition of i copies of $\widetilde{\mathcal{E}}$, and $\widetilde{\mathcal{E}}$ is the quantum operation defined by

$$\widetilde{\mathcal{E}}(\sigma) = P_X \sigma P_X + \mathcal{E}\left(P_{X^\perp} \sigma P_{X^\perp}\right)$$

for all density operators σ.

Obviously, the limit in the preceding definition exists, as the probabilities $tr\left(P_X \widetilde{\mathcal{E}}^i(\rho)\right)$ are nondecreasing in number i. Intuitively, $\widetilde{\mathcal{E}}$ can be seen as a procedure that first performs the projective measurement $\{P_X, P_{X^\perp}\}$ and then applies the identity operator $\mathcal{I}$ or $\mathcal{E}$ depending on the measurement outcome.

Exercise 5.3.1

(i) *Consider the special form of quantum **while**-loop (5.9) where the measurement in the loop guard is projective:*

$$M = \{M_0 = P_X, M_1 = P_{X^\perp}\}.$$

Find a connection between the reachability probability $\Pr(\rho \vDash \Diamond X)$ in quantum Markov chain $\langle \mathcal{H}, \mathcal{E}\rangle$ and the termination probability

$$p_T(\rho) = 1 - \lim_{n\to\infty} p_{NT}^{(n)}(\rho)$$

where ρ is the initial state, $\mathcal{E}$ is the quantum operation in the loop body, and $p_{NT}^{(n)}(\rho)$ is defined by equations (5.11) and (5.12).

(ii) *Note that a general measurement can be implemented by a projective measurement together with a unitary transformation (see Subsection 2.1.5). Show how the termination problem of loop (5.9) in its full generality can be reduced to the reachability problem of a quantum Markov chain.*

Computation of Reachability Probability:

Now we see how the reachability probability (5.27) can be computed using the quantum BSCC decomposition given in the last section. We first note that the subspace X in equation (5.27) is invariant under $\widetilde{\mathcal{E}}$. Thus $\langle X, \widetilde{\mathcal{E}}\rangle$ is a quantum Markov chain. It is easy to verify that $\widetilde{\mathcal{E}}_\infty(X) = X$. Thus, we can decompose X into a set of orthogonal BSCCs according to $\widetilde{\mathcal{E}}$ by Theorem 5.2.5.

The following lemma shows a connection between the limit probability of hitting a BSCC and the probability that the asymptotic average of the initial state lies in the same BSCC.

Lemma 5.3.1. *Let $\{B_i\}$ be a BSCC decomposition of $\mathcal{E}_\infty(\mathcal{H})$, and P_{B_i} the projection onto B_i. Then for each i, we have*

$$\lim_{k\to\infty} tr\left(P_{B_i}\mathcal{E}^k(\rho)\right) = tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right) \tag{5.28}$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Proof. We write P for the projection onto $T_{\mathcal{E}} = \mathcal{E}_\infty(\mathcal{H})^\perp$. Then similar to the proof of Theorem 5.2.4, we see that the limit

$$q_i \stackrel{\triangle}{=} \lim_{k\to\infty} tr\left(P_{B_i}\mathcal{E}^k(\rho)\right)$$

does exist, and $tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right) \leq q_i$. Moreover, we have:

$$\begin{aligned} 1 = tr\left((I-P)\mathcal{E}_\infty(\rho)\right) &= \sum_i tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right) \\ &\leq \sum_i q_i \\ &= \lim_{k\to\infty} tr\left((I-P)\mathcal{E}^k(\rho)\right) = 1. \end{aligned}$$

This implies $q_i = tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right)$. □

The preceding lemma together with Theorem 5.2.4 gives us an elegant way to compute the reachability probability of a subspace in a quantum Markov chain.

Theorem 5.3.1. *Let $\langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$, and $X \subseteq \mathcal{H}$ a subspace. Then*

$$\Pr(\rho \vDash \Diamond X) = tr\left(P_X\widetilde{\mathcal{E}}_\infty(\rho)\right),$$

and this probability can be computed in time $O(d^8)$ where $d = \dim(\mathcal{H})$.

Proof. The claim that

$$\Pr(\rho \vDash \Diamond X) = tr\left(P_X\widetilde{\mathcal{E}}_\infty(\rho)\right)$$

follows directly from Lemma 5.3.1 and Theorem 5.2.4. The time complexity of computing reachability probability follows from Lemma 5.2.8 (i). □

It should be pointed out that the reachability probability $\Pr(\rho \vDash \Diamond X)$ can also be computed directly by the techniques used in the proofs of Theorem 5.1.4 and Proposition 5.1.2.

5.3.2 REPEATED REACHABILITY PROBABILITY

Reachability of quantum Markov chains was discussed in the last subsection. In this subsection, we further study repeated reachability of quantum Markov chains using the quantum BSCC decomposition. Intuitively, repeated reachability means that a system satisfies a desired condition infinitely often. Repeated reachability is particularly useful in specifying a fairness condition for a concurrent program

consisting of a group of processes, which requires that each process participates in the computation infinitely often, provided it is enabled.

A Special Case:

To warm up, let us first consider a special case of this problem: if a quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$ starts from a pure state $|\psi\rangle$, how can its evolution sequence

$$|\psi\rangle\langle\psi|, \mathcal{E}(|\psi\rangle\langle\psi|), \mathcal{E}^2(|\psi\rangle\langle\psi|), \ldots$$

reach a subspace X of $\mathcal{H}$?

Since a quantum measurement can change the state of the measured system, we have two different scenarios. The first scenario is as follows: for each $i \geq 0$, in the i steps of evolution from $|\psi\rangle\langle\psi|$ to $\mathcal{E}^i(|\psi\rangle\langle\psi|)$, the projective measurement $\{P_X, P_{X^\perp}\}$ is performed only at the end.

Lemma 5.3.2 (Measure-once). *Let B be a BSCC of quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, and X a subspace which is not orthogonal to B. Then for any $|\psi\rangle \in B$, it holds that*

$$tr\left(P_X \mathcal{E}^i(|\psi\rangle\langle\psi|)\right) > 0$$

for infinitely many i.

Proof. As X is not orthogonal to B, we can always find a pure state $|\varphi\rangle \in B$ such that $P_X|\varphi\rangle \neq 0$. Now for any $|\psi\rangle \in B$, if there exists N such that

$$tr\left(P_X \mathcal{E}^k(|\psi\rangle\langle\psi|)\right) = 0$$

for any $k > N$, then

$$|\varphi\rangle \notin \mathcal{R}_{\mathcal{C}}\left(\mathcal{E}^{N+1}(|\psi\rangle\langle\psi|)\right)$$

which means that the reachable space $\mathcal{R}_{\mathcal{C}}\left(\mathcal{E}^{N+1}(|\psi\rangle\langle\psi|)\right)$ is a proper invariant subspace of B. This contradicts the assumption that B is a BSCC. Thus we have

$$tr\left(P_X \mathcal{E}^i(|\psi\rangle\langle\psi|)\right) > 0$$

for infinitely many i. □

In the second scenario, the measurement $\{P_X, P_{X^\perp}\}$ is performed at each of the i steps of evolution from $|\psi\rangle\langle\psi|$ to $\mathcal{E}^i(|\psi\rangle\langle\psi|)$: if the outcome corresponding to P_X is observed, the process terminates immediately; otherwise, it continues with another round of applying $\mathcal{E}$.

Lemma 5.3.3 (Measure-many). *Let B be a BSCC of a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, and $X \subseteq B$ a subspace of B. Then for any $|\psi\rangle \in B$, we have*

$$\lim_{i \to \infty} tr\left(\mathcal{G}^i(|\psi\rangle\langle\psi|)\right) = 0,$$

where the quantum operation $\mathcal{G}$ is the restriction of $\mathcal{E}$ in $X^\perp$; that is,

$$\mathcal{G}(\rho) = P_{X^\perp}\mathcal{E}(\rho)P_{X^\perp}$$

for all density operators ρ, and $X^\perp$ is the orthocomplement of X in $\mathcal{H}$.

Proof. By Lemma 3.3.4 we know that the limit

$$\mathcal{G}_\infty \stackrel{\triangle}{=} \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \mathcal{G}^n$$

exists. For any $|\psi\rangle \in B$, we claim that

$$\rho_\psi \stackrel{\triangle}{=} \mathcal{G}_\infty(|\psi\rangle\langle\psi|)$$

is a zero operator. Otherwise, it is easy to check that ρ_ψ is a fixed point of $\mathcal{G}$. Furthermore, from the fact that

$$\mathcal{E}(\rho_\psi) = \mathcal{G}(\rho_\psi) + P_X\mathcal{E}(\rho_\psi)P_X = \rho_\psi + P_X\mathcal{E}(\rho_\psi)P_X,$$

we have $tr(P_X\mathcal{E}(\rho_\psi)) = 0$ as $\mathcal{E}$ is trace-preserving. Thus $P_X\mathcal{E}(\rho_\psi) = 0$, and ρ_ψ is also a fixed point of $\mathcal{E}$. Note that

$$supp(\rho_\psi) \subseteq X^\perp \cap B.$$

By Theorem 5.2.3, we see that this contradicts the assumption that B is a BSCC.

Now with the preceding claim and the fact that $tr(\mathcal{G}^i(|\psi\rangle\langle\psi|))$ is nonincreasing in i, we immediately obtain:

$$\lim_{i\to\infty} tr\left(\mathcal{G}^i(|\psi\rangle\langle\psi|)\right) = 0.$$

□

The preceding lemma actually shows that if we set X as an absorbing boundary, which is included in BSCC B, the reachability probability will be absorbed eventually.

Now we turn to consider the general case where the initial state is a mixed state expressed as a density operator ρ. First of all, the preceding lemma can be strengthened as the following:

Theorem 5.3.2. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain, and let X be a subspace of $\mathcal{H}$ and*

$$\mathcal{G}(\rho) = P_{X^\perp}\mathcal{E}(\rho)P_{X^\perp}$$

for all density operators ρ. Then the following two statements are equivalent:

(i) *The subspace $X^\perp$ contains no BSCC;*
(ii) *For any $\rho \in \mathcal{D}(\mathcal{H})$, we have*

$$\lim_{i\to\infty} tr(\mathcal{G}^i(\rho)) = 0.$$

Proof. Similar to the proof of Lemma 5.3.3. □

The following example gives a simple application of Theorem 5.3.2.

Example 5.3.1. *Consider the quantum walk on an n-cycle described in Subsection 5.1.3. Let us set an absorbing boundary at position* 0 *(rather than at position* 1 *as in Subsection 5.1.3). Then from any initial state* $|\psi\rangle$*, we know from Theorem 5.3.2 that the probability of nontermination is asymptotically* 0 *because there is no BSCC which is orthogonal to the absorbing boundaries.*

The above discussions, in particular Lemma 5.3.3 and Theorem 5.3.2, provide us with a basis for defining a general form of repeated reachability in a quantum Markov chain $\langle \mathcal{H}, \mathcal{E}\rangle$. Note that $\mathcal{E}_\infty(\mathcal{H})^\perp$ is a transient subspace. So, we can focus our attention on $\mathcal{E}_\infty(\mathcal{H})$.

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain and X a subspace of $\mathcal{E}_\infty(\mathcal{H})$. Then we define:

$$\mathcal{X}(X) = \left\{ |\psi\rangle \in \mathcal{E}_\infty(\mathcal{H}) : \lim_{k\to\infty} tr\left(\mathcal{G}^k(|\psi\rangle\langle\psi|)\right) = 0 \right\}$$

where

$$\mathcal{G}(\rho) = P_{X^\perp}\mathcal{E}(\rho)P_{X^\perp}$$

for all $\rho \in \mathcal{D}(\mathcal{H})$. Intuitively, starting from a state $|\psi\rangle$ in $\mathcal{X}(X)$, we repeatedly run quantum operation $\mathcal{E}$, and at the end of each step we perform the measurement $\{X, X^\perp\}$. The defining equation of $\mathcal{X}(X)$ means that the probability that the system always eventually falls into $X^\perp$ is 0; in other words, the system infinitely often reaches X. It is easy to see that $\mathcal{X}(X)$ is a subspace of $\mathcal{H}$. Then the repeated reachability probability can be defined based on $\mathcal{X}(X)$.

Definition 5.3.2. *Let* $\mathcal{C} = \langle \mathcal{H}, \mathcal{E}\rangle$ *be a quantum Markov chain,* X *a subspace of* $\mathcal{H}$ *and* ρ *a density operator in* $\mathcal{H}$*. Then the probability that state* ρ *satisfies the repeated reachability* $rep(X)$ *is*

$$\Pr(\rho \vDash rep(X)) = \lim_{k\to\infty} tr\left(P_{\mathcal{X}(X)}\mathcal{E}^k(\rho)\right). \tag{5.29}$$

The well-definedness of $\Pr(\rho \vDash \text{rep}(X))$ comes from the fact that $\mathcal{X}(X)$ is invariant under $\mathcal{E}$. By Theorem 5.2.2 we know that the sequences

$$\left\{ tr\left(P_{\mathcal{X}(X)}\mathcal{E}^k(\rho)\right) \right\}$$

is nondecreasing, and thus its limit exists. The preceding definition is not easy to understand. To give the reader a better understanding of this definition, let us look at the defining equation (5.29) of repeated reachability probability in the following way: First, for any $0 \le \lambda < 1$, it follows from (5.29) that $\Pr(\rho \vDash \text{rep}(X)) \ge \lambda$ if

and only if for any $\epsilon > 0$, there exists N such that for all $k \geq N$, $\mathcal{E}^k(\rho)$ falls into subspace $\mathcal{X}(X)$ with probability $\geq \lambda - \epsilon$. On the other hand, we already noticed previously that starting from any state in $\mathcal{X}(X)$, the system can infinitely often reach X. Combining these two observations gives us the intuition that starting from ρ, the system infinitely often reaches X.

The problem of computing repeated reachability probability will be discussed in the next subsection, together with the computation of persistence probability.

5.3.3 PERSISTENCE PROBABILITY

The aim of this subsection is to study another kind of reachability of quantum Markov chains, namely persistence. Intuitively, persistence means that a desired condition is always satisfied from a certain point of time. As pointed out in the last subsection, we can focus our attention on $\mathcal{E}_\infty(\mathcal{H})$ because $\mathcal{E}_\infty(\mathcal{H})^\perp$ is a transient subspace.

Definition 5.3.3. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain and X a subspace of $\mathcal{E}_\infty(\mathcal{H})$. Then the set of states in $\mathcal{E}_\infty(\mathcal{H})$ that are eventually always in X is*

$$\mathcal{Y}(X) = \left\{ |\psi\rangle \in \mathcal{E}_\infty(\mathcal{H}) : (\exists N \geq 0)(\forall k \geq N)\ supp\left(\mathcal{E}^k(|\psi\rangle\langle\psi|)\right) \subseteq X \right\}.$$

It is clear from its defining equation that $\mathcal{Y}(X)$ consists of the pure states from which the states reachable after some time point N are all in X. Here, we give a simple example to illustrate the notion $\mathcal{Y}(X)$ as well as $\mathcal{X}(X)$ defined in the last subsection.

Example 5.3.2. *Let us revisit Example 5.2.1 where*

$$\mathcal{E}_\infty(\mathcal{H}) = span\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}.$$

(i) *If $X = span\{|0\rangle, |1\rangle, |2\rangle\}$, then*

$$\mathcal{E}_\infty(X^\perp) = supp(\mathcal{E}_\infty(|3\rangle\langle 3|)) = supp((|2\rangle\langle 2| + |3\rangle\langle 3|)/2)$$

and $\mathcal{E}_\infty(X) = \mathcal{E}_\infty(\mathcal{H})$. Thus $\mathcal{Y}(X) = B_1$ and $\mathcal{X}(X) = \mathcal{E}_\infty(\mathcal{H})$.

(ii) *If $X = span\{|3\rangle\}$, then*

$$\mathcal{E}_\infty(X^\perp) = B_1 \oplus B_2$$

and $\mathcal{E}_\infty(X) = B_2$. Thus $\mathcal{Y}(X) = \{0\}$ and $\mathcal{X}(X) = B_2$.

The following lemma gives a characterization of $\mathcal{X}(X)$ and $\mathcal{Y}(X)$ and also clarifies the relationship between them.

Lemma 5.3.4. *For any subspace X of $\mathcal{E}_\infty(\mathcal{H})$, both $\mathcal{X}(X)$ and $\mathcal{Y}(X)$ are invariant subspaces of $\mathcal{H}$ under $\mathcal{E}$. Furthermore, we have:*

(i) $\mathcal{X}(X) = \mathcal{E}_\infty(X)$;

(ii) $\mathcal{Y}(X) = \bigvee_{B \subseteq X} B = \mathcal{X}(X^\perp)^\perp$, *where B ranges over all BSCCs, and the orthogonal complements are taken in $\mathcal{E}_\infty(\mathcal{H})$.*

The proof of this lemma is postponed into Section 5.4.

Now we can define persistence probability of a quantum Markov chain.

Definition 5.3.4. *Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $X \subseteq \mathcal{H}$ a subspace and ρ a density operator in $\mathcal{H}$. Then the probability that state ρ satisfies the persistence property pers(X) is*

$$\Pr(\rho \vDash pers(X)) = \lim_{k\to\infty} tr\left(P_{\mathcal{Y}(X)}\mathcal{E}^k(\rho)\right).$$

Since $\mathcal{Y}(X)$ is invariant under $\mathcal{E}$, it follows from Theorem 5.2.2 that the sequence

$$\left\{tr\left(P_{\mathcal{Y}(X)}\mathcal{E}^k(\rho)\right)\right\}$$

is nondecreasing, and thus $\Pr(\rho \vDash \text{pers}(X))$ is well-defined. The preceding definition can be understood in a way similar to that given for Definition 5.3.2. For any $0 \leq \lambda < 1$, $\Pr(\rho \models \text{pers}(X)) \geq \lambda$ if and only if for any $\epsilon > 0$, there exists integer N such that for all $k \geq N$, $\mathcal{E}^k(\rho)$ falls into subspace $\mathcal{Y}(X)$ with probability $\geq \lambda - \epsilon$. Furthermore, starting from any state in $\mathcal{Y}(X)$, all the reachable states after some time point must be in X. Therefore, Definition 5.3.4 coincides with our intuition for persistence that a desired condition always holds after a certain point of time.

Combining Theorem 5.3.1 and Lemma 5.3.4, we obtain the main result of this subsection:

Theorem 5.3.3

(i) *The repeated reachability probability is*

$$\begin{aligned}\Pr(\rho \vDash rep(X)) &= 1 - tr\left(P_{\mathcal{X}(X)^\perp}\mathcal{E}_\infty(\rho)\right)\\ &= 1 - \Pr\left(\rho \vDash pers\left(X^\perp\right)\right).\end{aligned}$$

(ii) *The persistence probability is*

$$\Pr(\rho \vDash pers(X)) = tr(P_{\mathcal{Y}(X)}\mathcal{E}_\infty(\rho)).$$

Computation of Repeated Reachability and Persistence Probabilities:

Now we consider how to compute the repeated reachability and persistence probabilities in a quantum Markov chain. Based on Theorem 5.3.3 (ii), we are able to give an algorithm for computing persistence probability; see Algorithm 3.

Theorem 5.3.4. *Give a quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$, an initial state $\rho \in \mathcal{D}(\mathcal{H})$, and a subspace $X \subseteq \mathcal{H}$, Algorithm 3 computes persistence probability* $\Pr(\rho \vDash pers(X))$ *in time $O(d^8)$, where $d = \dim \mathcal{H}$.*

Proof. The correctness of Algorithm 3 follows immediately from Theorem 5.3.3 (ii). The time complexity is again dominated by the Jordan decomposition used in computing $\mathcal{E}_\infty(\rho)$ and $\mathcal{E}_\infty(X^\perp)$, thus it is $O(d^8)$. □

Algorithm 3 PERSISTENCE(X, ρ)

input : A quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$, a subspace $X \subseteq \mathcal{H}$, and an initial state $\rho \in \mathcal{D}(\mathcal{H})$
output: The probability $\Pr(\rho \models \text{pers}(X))$
begin
  $\rho_\infty \leftarrow \mathcal{E}_\infty(\rho)$;
  $Y \leftarrow \mathcal{E}_\infty(X^\perp)$;
  $P \leftarrow$ the projection onto $Y^\perp$; (* $Y^\perp$ is the orthocomplement of Y in $\mathcal{E}_\infty(\mathcal{H})$ *)
  return $tr(P\rho_\infty)$;
end

With Theorem 5.3.3 (i), Algorithm 3 can also be used to compute repeated reachability probability $\Pr(\rho \models \text{rep}(X))$.

We conclude this section by raising a research problem:

Problem 5.3.1. *All algorithms for analysis of quantum programs presented in this chapter are classical; that is, they were developed for analysis of quantum programs using classical computers. It is desirable to develop quantum algorithms for the same purpose that can improve the complexities of the corresponding algorithms given in this chapter.*

5.4 PROOFS OF TECHNICAL LEMMAS

Several technical lemmas were used in the previous sections without proofs. For convenience of the reader, here we collect their proofs.

Proof of Lemma 5.1.10. We first give a series of lemmas that will serve as key steps in the proof of Lemma 5.1.10. Recall from Subsection 5.1.2 that $\mathcal{E}$ is a quantum operation and $M = \{M_0, M_1\}$ a quantum measurement. The quantum operations $\mathcal{E}_0, \mathcal{E}_1$ are defined by the measurement operators M_0, M_1, respectively; that is,

$$\mathcal{E}_i(\rho) = M_i \rho M_i^\dagger$$

for all density operators ρ and $i = 0, 1$. We write $\mathcal{G} = \mathcal{E} \circ \mathcal{E}_1$.

Lemma 5.4.1. *The quantum operation $\mathcal{G} + \mathcal{E}_0$ is trace-preserving:*

$$tr[(\mathcal{G} + \mathcal{E}_0)(\rho)] = tr(\rho) \tag{5.30}$$

for all partial density operators ρ.

Proof. It suffices to see that

$$\begin{aligned}\sum_i (E_i M_1)^\dagger E_i M_1 + {M_0}^\dagger M_0 &= {M_1}^\dagger \left(\sum_i E_i^\dagger E_i \right) M_1 + {M_0}^\dagger M_0 \\ &= {M_1}^\dagger M_1 + {M_0}^\dagger M_0 = I.\end{aligned}$$

□

The next lemma shows that every complex matrix can be represented by four positive matrices.

Lemma 5.4.2. *For any matrix A, there are positive matrices B_1, B_2, B_3, B_4 such that*

(i) $A = (B_1 - B_2) + i(B_3 - B_4)$*; and*
(ii) $trB_i^2 \leq tr(A^\dagger A)$ $(i = 1, 2, 3, 4)$.

Proof. We can take Hermitian operators

$$(A + A^\dagger)/2 = B_1 - B_2, \quad -i(A - A^\dagger)/2 = B_3 - B_4,$$

where B_1, B_2 are positive operators with orthogonal supports, and B_3, B_4 are also positive operators with orthogonal supports. Then it holds that

$$\begin{aligned}\sqrt{\mathrm{tr}{B_1}^2} &= \sqrt{\mathrm{tr}({B_1}^\dagger B_1)} \\ &\leq \sqrt{\mathrm{tr}({B_1}^\dagger B_1 + {B_2}^\dagger B_2)} \\ &= \|((A + A^\dagger)/2 \otimes I)|\Phi\rangle\| \\ &\leq (\|(A \otimes I)|\Phi\rangle\| + \|(A^\dagger \otimes I)|\Phi\rangle\|)/2 \\ &= \sqrt{\mathrm{tr}(A^\dagger A)}.\end{aligned}$$

It is similar to prove that $\mathrm{tr}{B_i}^2 \leq \mathrm{tr}(A^\dagger A)$ for $i = 2, 3, 4$. □

Let R be the matrix representation of quantum operation $\mathcal{G}$; see its defining equation (5.14). Then a bound of the powers of R is given in the following:

Lemma 5.4.3. *For any integer $n \geq 0$, and for any state $|\alpha\rangle$ in $\mathcal{H} \otimes \mathcal{H}$, we have:*

$$\|R^n|\alpha\rangle\| \leq 4\sqrt{d}\||\alpha\rangle\|$$

where $d = \dim \mathcal{H}$ is the dimension of Hilbert space $\mathcal{H}$.

Proof. Suppose that $|\alpha\rangle = \sum_{i,j} a_{ij}|ij\rangle$. Then we can write:

$$|\alpha\rangle = (A \otimes I)|\Phi\rangle$$

where $A = (a_{ij})$ is a $d \times d$ matrix. A routine calculation yields:

$$\||\alpha\rangle\| = \sqrt{\mathrm{tr}A^\dagger A}.$$

We write:

$$A = (B_1 - B_2) + i(B_3 - B_4)$$

according to Lemma 5.4.2. The idea behind this decomposition is that the trace-preserving property of equation (5.30) only applies to positive operators. Put

$$|\beta_i\rangle = (B_i \otimes I)|\Phi\rangle$$

for $i = 1, 2, 3, 4$. Using the triangle inequality, we obtain:

$$\|R^n|\alpha\rangle\| \leq \sum_{i=1}^{4} \|R^n|\beta_i\rangle\| = \sum_{i=1}^{4} \|(\mathcal{G}^n(B_i) \otimes I)|\Phi\rangle\|.$$

Note that

$$\|(\mathcal{G}^n(B_i) \otimes I)|\Phi\rangle\| = \sqrt{\mathrm{tr}(\mathcal{G}^n(B_i))^2}, \tag{5.31}$$

$$\mathrm{tr}B_i^2 \leq (\mathrm{tr}B_i)^2. \tag{5.32}$$

Moreover, we know from Lemma 5.4.1 that

$$\mathrm{tr}[\mathcal{G}^n(B_i)] \leq \mathrm{tr}[(\mathcal{G} + \mathcal{E}_0)^n(B_i)] = \mathrm{tr}B_i. \tag{5.33}$$

Combining equations (5.31), (5.32) and (5.33) yields

$$\sqrt{\mathrm{tr}(\mathcal{G}^n(B_i))^2} \leq \sqrt{(\mathrm{tr}\mathcal{G}^n(B_i))^2} \leq \sqrt{(\mathrm{tr}B_i)^2}.$$

Furthermore, by the Cauchy inequality we have

$$(\mathrm{tr}B_i)^2 \leq d \cdot (\mathrm{tr}B_i^2).$$

Therefore, it follows from Lemma 5.4.2 that

$$\|R^n|\alpha\rangle\| \leq \sum_{i=1}^{4} \sqrt{d \cdot \mathrm{tr}B_i^2} \leq 4\sqrt{d \cdot \mathrm{tr}(A^\dagger A)} = 4\sqrt{d}\||\alpha\rangle\|.$$

□

Now we are ready to prove Lemma 5.1.10. We prove part (i) by refutation. If there is some eigenvalue λ of R with $|\lambda| > 1$, suppose the corresponding normalized eigenvector is $|x\rangle$: $R|x\rangle = \lambda|x\rangle$. Choose integer n such that $|\lambda|^n > 4\sqrt{d}$. Then

$$\|R^n|x\rangle\| = \|\lambda^n|x\rangle\| = |\lambda|^n > 4\sqrt{d}\||x\rangle\|.$$

This contradicts Lemma 5.4.3.

Part (ii) can also be proved by refutation. Without any loss of generality, we assume that $|\lambda_1| = 1$ with $k_1 > 1$ in the Jordan decomposition of R: $R = SJ(R)S^{-1}$. Suppose that $\{|i\rangle\}_{i=1}^{d^2}$ is the orthonormal basis of $\mathcal{H} \otimes \mathcal{H}$ compatible with the numbering of the columns and rows of R. Take an unnormalized vector $|y\rangle = S|k_1\rangle$, where $|k_1\rangle$ is the k_1th state in the basis $\{|i\rangle\}_{i=1}^{d^2}$. Since S is nonsingular, there are real numbers $L, r > 0$ such that

$$r \cdot \||x\rangle\| \leq \|S|x\rangle\| \leq L \cdot \||x\rangle\|$$

for any vector $|x\rangle$ in $\mathcal{H} \otimes \mathcal{H}$. By definition, it holds that $\||y\rangle\| \leq L$. We can choose integer n such that $nr > L \cdot 4\sqrt{d}$ because $r > 0$. Then a routine calculation yields:

$$R^n|y\rangle = L \cdot \sum_{t=0}^{k_1-1} \begin{pmatrix} n \\ t \end{pmatrix} {\lambda_1}^{n-t} |k_1 - t\rangle,$$

Consequently, we have:

$$\begin{aligned} \|R^n|y\rangle\| &\geq r \cdot \sum_{t=1}^{k_1} \begin{pmatrix} n \\ t \end{pmatrix} |\lambda_1|^{n-t} \\ &\geq nr > L \cdot 4\sqrt{d} \geq 4\sqrt{d}\||y\rangle\|. \end{aligned}$$

This contradicts Lemma 5.4.3 again, and we complete the proof.

Proof of Lemma 5.1.13. Recall from Subsection 5.1.2 that $J(N)$ is the matrix obtained from the Jordan normal form $J(R)$ of R through replacing the 1-dimensional Jordan blocks corresponding to the eigenvalues with module 1 by number 0. Without any loss of generality, we assume that the eigenvalues of R satisfy:

$$1 = |\lambda_1| = \cdots = |\lambda_s| > |\lambda_{s+1}| \geq \cdots \geq |\lambda_l|.$$

Then

$$J(R) = \begin{pmatrix} U & 0 \\ 0 & J_1 \end{pmatrix}$$

where $U = diag(\lambda_1, \cdots, \lambda_s)$ is an $s \times s$ diagonal unitary, and

$$J_1 = diag\left(J_{k_{s+1}}(\lambda_{s+1}), \cdots, J_{k_l}(\lambda_l)\right).$$

Moreover, we have:

$$J(N) = \begin{pmatrix} 0 & 0 \\ 0 & J_1 \end{pmatrix}.$$

The convergence of

$$\sum_{n=0}^{\infty} \left(\mathcal{E}_0 \circ \mathcal{G}^n\right)$$

follows immediately from Lemma 3.3.4, and it in turn implies the convergence of $\sum_{n=0}^{\infty} N_0 R^n$. It is clear that

$$\sum_{n=0}^{\infty} N_0 R^n = \sum_{n=0}^{\infty} N_0 S J(R)^n S^{-1}.$$

Since S is nonsingular, we see that

$$\sum_{n=0}^{\infty} N_0 SJ(R)^n$$

converges. This implies that

$$\lim_{n\to\infty} N_0 SJ(R)^n = 0.$$

Now we write:

$$N_0 S = \begin{pmatrix} Q & P \\ V & T \end{pmatrix},$$

where Q is an $s \times s$ matrix, T is a $(d^2 - s) \times (d^2 - s)$ matrix, and $d = \dim \mathcal{H}$ is the dimension of the state space $\mathcal{H}$. Then

$$N_0 SJ(R)^n = \begin{pmatrix} QU^n & PJ_1{}^n \\ VU^n & TJ_1{}^n \end{pmatrix},$$

and it follows that $\lim_{n\to\infty} QU^n = 0$ and $\lim_{n\to\infty} VU^n = 0$. So, we have:

$$\begin{aligned} tr(Q^\dagger Q) &= \lim_{n\to\infty} \mathrm{tr}(QU^n)^\dagger QU^n = 0, \\ tr(V^\dagger V) &= \lim_{n\to\infty} \mathrm{tr}(VU^n)^\dagger VU^n = 0. \end{aligned}$$

This yields $Q = 0$ and $V = 0$, and it follows immediately that $N_0 R^n = N_0 N^n$.

Proof of Lemma 5.2.5 (ii). We are going to show that any two BSCCs X, Y of a quantum Markov chain are orthogonal provided $\dim X \neq \dim Y$. This proof requires a technical preparation. An operator A (not necessarily a partial density operator as in Definition 5.2.12 (i)) in $\mathcal{H}$ is called a fixed point of quantum operation $\mathcal{E}$ if $\mathcal{E}(A) = A$. The following lemma shows that fixed points can be preserved by the positive matrix decomposition given in Lemma 5.4.2.

Lemma 5.4.4. *Let $\mathcal{E}$ be a quantum operation in $\mathcal{H}$ and A a fixed point of $\mathcal{E}$. If we have:*

(i) $A = (X_+ - X_-) + i(Y_+ - Y_-)$;
(ii) X_+, X_-, Y_+, Y_- *are all positive matrices; and*
(iii) $supp(X_+) \perp supp(X_-)$ *and* $supp(Y_+) \perp supp(Y_-)$,

then X_+, X_-, Y_+, Y_- are all fixed points of $\mathcal{E}$.

Exercise 5.4.1. *Prove Lemma 5.4.4.*

Now we are ready to prove Lemma 5.2.5 (ii). Suppose without any loss of generality that $\dim X < \dim Y$. By Theorem 5.2.3, we know that there are two minimal fixed point states ρ and σ with $supp(\rho) = X$ and $supp(\sigma) = Y$. Note that for any $\lambda > 0$, $\rho - \lambda\sigma$ is also a fixed point of $\mathcal{E}$. We can take λ sufficiently large such that

$$\rho - \lambda\sigma = \Delta_+ - \Delta_-$$

with $\Delta_\pm$ being positive, $supp(\Delta_-) = supp(\sigma)$, and $supp(\Delta_+) \perp supp(\Delta_-)$. Let P be the projection onto Y. It follows from Lemma 5.4.4 that both Δ_+ and Δ_- are fixed points of $\mathcal{E}$. Then

$$P\rho P = \lambda P\sigma P + P\Delta_+ P - P\Delta_- P = \lambda\sigma - \Delta_-$$

is a fixed point state of $\mathcal{E}$ too. Note that $supp(P\rho P) \subseteq Y$, σ is the minimal fixed point state and $supp(\sigma) = Y$. Therefore, we have $P\rho P = p\sigma$ for some $p \geq 0$. Now if $p > 0$, then by Proposition 5.2.1 (iii) we obtain:

$$Y = supp(\sigma) = supp(P\rho P) = span\{P|\psi\rangle : |\psi\rangle \in X\}.$$

This implies $\dim Y \leq \dim X$, contradicting our assumption. Thus we have $P\rho P = 0$, which implies $X \perp Y$.

Proof of Lemma 5.2.7. Roughly speaking, this lemma asserts that a fixed point state of $\mathcal{E}$ can be decomposed into two orthogonal fixed point states. The proof technique for Lemma 5.2.5 (ii) showing that two BSCCs are orthogonal can be used in the proof of this lemma. First, we note that for any $\lambda > 0$, $\rho - \lambda\sigma$ is also a fixed point of $\mathcal{E}$, and thus we can take λ sufficiently large such that

$$\rho - \lambda\sigma = \Delta_+ - \Delta_-$$

with $\Delta_\pm$ being positive, $supp(\Delta_-) = supp(\sigma)$, and $supp(\Delta_+)$ is the orthogonal complement of $supp(\Delta_-)$ in $supp(\rho)$. By Lemma 5.4.4, both Δ_+ and Δ_- are fixed points of $\mathcal{E}$. Let $\eta = \Delta_+$. We have:

$$supp(\rho) = supp(\rho - \lambda\sigma) = supp(\Delta_+) \oplus supp(\Delta_-) = supp(\eta) \oplus supp(\sigma).$$

Proof of Lemma 5.2.8. For part (i), we are required to figure out the complexity for computing the asymptotic average $\mathcal{E}_\infty(\rho)$ of a density operator ρ. To this end, we first present a lemma about the matrix representation of the asymptotic average of a quantum operation.

Lemma 5.4.5. *Let $M = SJS^{-1}$ be the Jordan decomposition of M where*

$$J = \bigoplus_{k=1}^{K} J_k(\lambda_k) = diag\left(J_1(\lambda_1), \ldots, J_K(\lambda_K)\right),$$

and $J_k(\lambda_k)$ is the Jordan block corresponding to the eigenvalue λ_k. Define

$$J_\infty = \bigoplus_{k \ s.t. \ \lambda_k = 1} J_k(\lambda_k)$$

and $M_\infty = SJ_\infty S^{-1}$. Then M_∞ is the matrix representation of $\mathcal{E}_\infty$.

Exercise 5.4.2. *Prove Lemma 5.4.5.*

Now we can prove part (i) of Lemma 5.2.8. We know from [61] that the time complexity of Jordan decomposition for a $d \times d$ matrix is $O(d^4)$. So, we can compute the matrix representation M_∞ of $\mathcal{E}_\infty$ in time $O(d^8)$. Furthermore, $\mathcal{E}_\infty(\rho)$ can be computed using the correspondence (Lemma 5.1.9):

$$\left(\mathcal{E}_\infty(\rho) \otimes I_{\mathcal{H}}\right)|\Psi\rangle = M_\infty(\rho \otimes I_{\mathcal{H}})|\Psi\rangle$$

where $|\Psi\rangle = \sum_{i=1}^{d} |i\rangle|i\rangle$ is the (unnormalized) maximally entangled state in $\mathcal{H} \otimes \mathcal{H}$. For part (ii), we need to settle the complexity for finding the density operator basis of the set of fixed points of $\mathcal{E}$; i.e., $\{$ matrices $A : \mathcal{E}(A) = A\}$. We first notice that this density operator basis can be computed in the following three steps:

(a) Compute the matrix representation M of $\mathcal{E}$. The time complexity is $O(md^4)$, where $m \leq d^2$ is the number of operators E_i in the Kraus representation $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$.

(b) Find a basis $\mathcal{B}$ for the null space of the matrix $M - I_{\mathcal{H}\otimes\mathcal{H}}$, and transform them into matrix forms. This can be done by Gaussian elimination with complexity being $O((d^2)^3) = O(d^6)$.

(c) For each basis matrix A in $\mathcal{B}$, compute positive matrices X_+, X_-, Y_+, Y_- such that $supp(X_+) \perp supp(X_-)$, $supp(Y_+) \perp supp(Y_-)$, and

$$A = X_+ - X_- + i(Y_+ - Y_-).$$

Let Q be the set of nonzero elements in $\{X_+, X_-, Y_+, Y_-\}$. Then by Lemma 5.4.4, every element of Q is a fixed point state of $\mathcal{E}$. Replace A by elements of Q after normalization. Then the resultant $\mathcal{B}$ is the required density operator basis. At last, we make the elements in $\mathcal{B}$ linearly independent. This can be done by removing the redundant elements in $\mathcal{B}$ using Gaussian elimination. The computational complexity of this step is $O(d^6)$.

So, we see that the total complexity for computing the density operator basis of $\{$ matrices $A : \mathcal{E}(A) = A\}$ is $O(d^6)$.

Proof of Lemma 5.3.4. We first prove the following technical lemma.

Lemma 5.4.6. *Let S be an invariant subspace of $\mathcal{E}_\infty(\mathcal{H})$ under $\mathcal{E}$. Then for any density operator ρ with $supp(\rho) \subseteq \mathcal{E}_\infty(\mathcal{H})$ and any integer k, we have*

$$tr(P_S\mathcal{E}^k(\rho)) = tr(P_S\rho)$$

where P_S is the projection onto S.

Proof. By Lemma 5.2.7, there exists an invariant subspace T such that $\mathcal{E}_\infty(\mathcal{H}) = S \oplus T$ where S and T are orthogonal. Then by Theorem 5.2.2, we have

$$tr(P_S\mathcal{E}^k(\rho)) \geq tr(P_S\rho) \text{ and } tr(P_T\mathcal{E}^k(\rho)) \geq tr(P_T\rho).$$

Furthermore, it follows that

$$\begin{aligned} 1 &\geq tr(P_S\mathcal{E}^k(\rho)) + tr(P_T\mathcal{E}^k(\rho)) \\ &\geq tr(P_S\rho) + tr(P_T\rho) = tr(\rho) = 1. \end{aligned}$$

Thus we have:

$$tr(P_S\mathcal{E}^k(\rho)) = tr(P_S\rho).$$

□

Now we can prove Lemma 5.3.4. For any pure state $|\varphi\rangle$, we write the corresponding density operator $\varphi = |\varphi\rangle\langle\varphi|$. First of all, we show that $\mathcal{Y}(X)$ is a subspace. Let $|\psi_i\rangle \in \mathcal{Y}(X)$ and α_i be complex numbers, $i = 1, 2$. Then by the definition of $\mathcal{Y}(X)$ there exists N_i such that for any $j \geq N_i$, $supp\left(\mathcal{E}^j(\psi_i)\right) \subseteq X$. Let

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle \text{ and } \rho = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|.$$

Then $|\psi\rangle \in supp(\rho)$, and from Propositions 5.2.1 (i), (ii) and (iv) we have

$$supp\left(\mathcal{E}^j(\psi)\right) \subseteq supp\left(\mathcal{E}^j(\rho)\right) = supp\left(\mathcal{E}^j(\psi_1)\right) \vee supp\left(\mathcal{E}^j(\psi_2)\right)$$

for any $j \geq 0$. So, we have $supp\left(\mathcal{E}^j(\psi)\right) \subseteq X$ for all $j \geq N \stackrel{\triangle}{=} \max\{N_1, N_2\}$, and thus $|\psi\rangle \in \mathcal{Y}(X)$.

We divide the rest of the proof into the following six claims:

- Claim 1: $\mathcal{Y}(X) \supseteq \bigvee\{B \subseteq X : B \text{ is a BSCC}\}$.
  For any BSCC $B \subseteq X$, from Lemmas 5.2.6 (ii) and 5.2.4 we have $B \subseteq \mathcal{E}_\infty(\mathcal{H})$. Furthermore, as B is a BSCC, it holds that

  $$supp\left(\mathcal{E}^i(\psi)\right) \subseteq B \subseteq X$$

  for any $|\psi\rangle \in B$ and any i. Thus $B \subseteq \mathcal{Y}(X)$, and the claim follows from the fact that $\mathcal{Y}(X)$ is a subspace.
- Claim 2: $\mathcal{Y}(X) \subseteq \bigvee\{B \subseteq X : B \text{ is a BSCC}\}$.
  For any $|\psi\rangle \in \mathcal{Y}(X)$, note that $\rho_\psi \stackrel{\triangle}{=} \mathcal{E}_\infty(\psi)$ is a fixed point state. Let $Z = supp(\rho_\psi)$. We claim that $|\psi\rangle \in Z$. This is obvious if $Z = \mathcal{E}_\infty(\mathcal{H})$. Otherwise, as $\mathcal{E}_\infty\left(\frac{I_\mathcal{H}}{d}\right)$ is a fixed point state and

  $$\mathcal{E}_\infty(\mathcal{H}) = supp\left(\mathcal{E}_\infty\left(\frac{I_\mathcal{H}}{d}\right)\right),$$

  by Lemma 5.2.7 we have $\mathcal{E}_\infty(\mathcal{H}) = Z \oplus Z^\perp$, where $Z^\perp$, the orthocomplement of Z in $\mathcal{E}_\infty(\mathcal{H})$, is also invariant. As Z is again a direct sum of some orthogonal BSCCs, by Lemma 5.3.1 we have

$$\lim_{i\to\infty} tr\left(P_Z\mathcal{E}^i(\psi)\right) = tr(P_Z\mathcal{E}_\infty(\psi)) = 1;$$

that is,

$$\lim_{i\to\infty} tr\left(P_{Z^\perp}\mathcal{E}^i(\psi)\right) = 0.$$

Together with Theorem 5.2.2, this implies $tr(P_{Z^\perp}\psi) = 0$, and so $|\psi\rangle \in Z$.
By the definition of $\mathcal{Y}(X)$, there exists $M \geq 0$, such that $supp\left(\mathcal{E}^i(\psi)\right) \subseteq X$ for all $i \geq M$. Thus

$$\begin{aligned} Z &= supp\left(\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}\mathcal{E}^i(\psi)\right) \\ &= supp\left(\lim_{N\to\infty}\frac{1}{N}\sum_{i=M}^{N}\mathcal{E}^i(\psi)\right) \subseteq X. \end{aligned}$$

Furthermore, since Z can be decomposed into the direct sum of some BSCCs, we have

$$|\psi\rangle \in Z \subseteq \bigvee\{B \subseteq X : B \text{ is a BSCC}\}.$$

Thus, Claim 2 is proved.

- Claim 3: $\mathcal{Y}(X^\perp)^\perp \subseteq \mathcal{X}(X)$.
  First, from Claims 1 and 2 previously we have $\mathcal{Y}(X^\perp) \subseteq X^\perp$, and

$$X' \triangleq \mathcal{Y}(X^\perp)^\perp$$

is invariant. Thus $X \subseteq \mathcal{Y}(X^\perp)^\perp$, and $\mathcal{E}$ is also a quantum operation in the subspace X'. We now consider the quantum Markov chain $\langle X', \mathcal{E}\rangle$. Claim 1 implies that any BSCC in $X^\perp$ is also contained in $\mathcal{Y}(X^\perp)$. Therefore, there is no BSCC in $X' \cap X^\perp$. By Theorem 5.3.2, for any $|\psi\rangle \in X'$, we obtain:

$$\lim_{i\to\infty} tr\left[(P_{X^\perp}\circ\mathcal{E})^i(\psi)\right] = 0.$$

Thus $|\psi\rangle \in \mathcal{X}(X)$ by definition, and the claim is proved.

- Claim 4: $\mathcal{X}(X) \subseteq \mathcal{Y}(X^\perp)^\perp$.
  Similar to Claim 3, we have $\mathcal{Y}(X^\perp) \subseteq X^\perp$ and $\mathcal{Y}(X^\perp)$ is invariant. Let P be the projection onto $\mathcal{Y}(X^\perp)$. Then $P_{X^\perp}PP_{X^\perp} = P$. For any $|\psi\rangle \in \mathcal{X}(X)$, we have:

$$\begin{aligned} tr\left(P\left(P_{X^\perp}\circ\mathcal{E}\right)(\psi)\right) &= tr\left(P_{X^\perp}PP_{X^\perp}\mathcal{E}(\psi)\right) \\ &= tr(P\mathcal{E}(\psi)) \geq tr(P\psi), \end{aligned}$$

where the last inequality is derived by Theorem 5.2.2. Therefore

$$0 = \lim_{i\to\infty} tr\left(\left(P_{X^\perp}\circ\mathcal{E}\right)^i(\psi)\right)$$
$$\geq \lim_{i\to\infty} tr\left(P\left(P_{X^\perp}\circ\mathcal{E}\right)^i(\psi)\right) \geq tr(P\psi),$$

and so $|\psi\rangle \in \mathcal{Y}(X^\perp)^\perp$.

- Claim 5: $\bigvee\{B \subseteq X : B \text{ is a BSCC}\} \subseteq \mathcal{E}_\infty(X^\perp)^\perp$.
  Suppose that $B \subseteq X$ is a BSCC. Then we have $tr(P_B I_{X^\perp}) = 0$. It follows from Lemma 5.4.6 that

$$tr\left(P_B\mathcal{E}^i(I_{X^\perp})\right) = 0$$

  for any $i \geq 0$. Thus

$$tr(P_B\mathcal{E}_\infty(I_{X^\perp})) = 0.$$

  This implies $B \perp \mathcal{E}_\infty(X^\perp)$. Therefore, $B \subseteq \mathcal{E}_\infty(X^\perp)^\perp$. Then the claim follows from the fact that $\mathcal{E}_\infty(X^\perp)^\perp$ is a subspace.
- Claim 6: $\mathcal{E}_\infty(X^\perp)^\perp \subseteq \bigvee\{B \subseteq X : B \text{ is a BSCC}\}$.
  We first note that $\mathcal{E}_\infty(X^\perp)^\perp$ can be decomposed into the direct sum of BSCCs B_i. For any B_i, we have

$$tr(P_{B_i}\mathcal{E}_\infty(I_{X^\perp})) = 0.$$

  Thus, $tr(P_{B_i} I_{X^\perp}) = 0$ and $B_i \perp X^\perp$. Therefore, $B_i \subseteq X$, and the claim is proved.

Finally, we observe that the invariance of $\mathcal{X}(X)$ and $\mathcal{Y}(X)$ is already included in Claims 1 and 2. This completes the proof.

5.5 BIBLIOGRAPHIC REMARKS

The studies of quantum program analysis presented in this chapter were initiated in [227], where termination of a quantum **while**-loop with a unitary transformation as the loop body was considered. In [234], the verification method for probabilistic programs developed by Sharir, Pnueli and Hart [202] was generalized to the quantum case, termination analysis of quantum programs was carried out using a quantum Markov chain as their semantic model, and thus several major results in [227] was significantly extended. The materials presented in Subsections 5.1.1 and 5.1.2 of this chapter are taken from [227] and [234], respectively. Sections 5.2 and 5.3 are mainly based on S. G. Ying et al. [235], where reachability of quantum Markov chains was thoroughly studied; in particular, the notion of BSCC of a quantum graph was introduced. Lemmas 5.4.4 and 5.4.5 are taken from Wolf [216].

For further reading, I suggest that the reader track the following three lines:

(i) *Perturbation of quantum programs*: Although not discussed in this chapter, perturbation analysis is particularly interesting for quantum programs because of noise in the implementation of quantum logical gates. It was proved in [227] that a small disturbance either on the unitary transformation in the loop body or on the measurement in the loop guard can make a quantum loop (almost) terminate, provided that some obvious dimension restriction is satisfied.

(ii) *Analysis of recursive quantum programs*: In this chapter, we only considered analysis of quantum loop programs. In [87], Feng et al. introduced a quantum generalization of Etessami and Yannakakis's recursive Markov chains [79], namely recursive super-operator-valued Markov chains, and developed some techniques for their reachability analysis. It is obvious that these techniques can be used for analysis of recursive quantum programs defined in Section 3.4. Another class of analysis techniques for classical recursive programs is based on pushdown automata; see for example [78]. The notion of pushdown quantum automata was introduced in [103], but it still is not clear how to use pushdown quantum automata in the analysis of recursive quantum programs.

(iii) *Analysis of nondeterministic and concurrent quantum programs*: An analysis for termination of nondeterministic quantum programs was carried out by Li et al. [152], generalizing several results by Hart, Sharir and Pnueli [113] for probabilistic programs. Termination of concurrent quantum programs with fairness conditions was studied by Yu et al. [238]. It was further discussed by S. G. Ying et al. [236] in terms of reachability of quantum Markov decision processes. On the other hand, only the simplest reachability of quantum programs was examined in this chapter. Several more complicated reachability properties of quantum systems were studied by Li et al. [153].

Except the line of research described in this chapter, several other approaches to quantum program analysis have been proposed in the literature. JavadiAbhari et al. [126] present a scalable framework ScaffCC for compilation and analysis of quantum programs written in Scaffold [3]; in particular they considered timing analysis for path estimation. As already mentioned in Subsection 1.1.3, abstract interpretation was generalized by Jorrand and Perdrix [129] for analysis of quantum programs. It was further extended and refined by Honda [118] to reason about separability of quantum variables in quantum programs.