CHAPTER

Logic for quantum programs 4

A simple quantum programming language was defined in Chapter 3 to write quantum programs with classical control. It was shown by several examples to be convenient to program some quantum algorithms.

As is well-known, programming is error-prone. It is even worse when programming a quantum computer, because human intuition is much better adapted to the classical world than to the quantum world. Thus, it is critical to develop methodologies and techniques for verification of quantum programs.

In this chapter, we build logical foundations for reasoning about correctness of quantum programs. This chapter consists of the following parts:

- The first step in developing a logic for quantum programs is to define the notion of quantum predicate, which can properly describe properties of quantum systems. We introduce the notion of quantum predicate as a physical observable in Section 4.1. Moreover, the notion of weakest precondition is generalized to the case of quantum programs.
- Floyd-Hoare logic is an effective proof system for correctness of classical programs. Based on Section 4.1, we develop a logic of the Floyd-Hoare style for quantum programs in Section 4.2, where soundness and (relative) completeness of such a logic are proved, and an example is given to show how this logic can be used in verification of quantum programs.
- A logic for quantum programs is not a straightforward extension of the corresponding logic for classical programs. We have to carefully consider how various quantum features can be incorporated into a logical system. It is well-known that a distinctive feature between classical and quantum systems is non-commutativity of observables about quantum systems. Section 4.3 is devoted to examining (non-)commutativity of the quantum weakest preconditions.

4.1 QUANTUM PREDICATES

In classical logic, predicates are used to describe properties of individuals or systems. Then what is a quantum predicate? A natural idea is that a quantum predicate should

Foundations of Quantum Programming.http://dx.doi.org/10.1016/B978-0-12-802306-8.00004-5

be a physical observable. Recall from Section 2.1.4 that an observable of a quantum system is expressed by a Hermitian operator M in its state Hilbert space $\mathcal{H}$. At this moment, for simplicity, we assume that $\mathcal{H}$ is finite-dimensional. If $\lambda \in \mathbb{C}$ and a nonzero vector $|\psi\rangle \in \mathcal{H}$ satisfy

$$M|\psi\rangle = \lambda|\psi\rangle,$$

then λ is called an eigenvalue of M and $|\psi\rangle$ the eigenvector of M corresponding to λ. It turns out that all eigenvalues of M are real numbers. We write $spec(M)$ for the set of eigenvalues of M – the (point) spectrum of M. For each eigenvalue $\lambda \in spec(M)$, the eigenspace of M corresponding to λ is the (closed) subspace

$$X_\lambda = \{|\psi\rangle \in \mathcal{H} : A|\psi\rangle = \lambda|\psi\rangle\}.$$

In order to see what a quantum predicate should be, let us first consider a special class of quantum observables (Hermitian operators), namely projections. Historically, Birkhoff-von Neumann quantum logic is the first logic for reasoning about the properties of quantum systems. One of its basic ideas is that a proposition about a quantum system can be modelled by a (closed) subspace X of the system's state Hilbert space $\mathcal{H}$. The subspace X can be seen as the eigenspace of the projection P_X (see Definition 2.1.10) corresponding to eigenvalue 1, and eigenvalue 1 can be understood as the truth value of the proposition modelled by X.

Extending this idea, whenever an observable (a Hermitian operator) M is considered as a quantum predicate, its eigenvalue λ should be understood as the truth value of the proposition described by the eigenspace X_λ. Note that the truth value of a classical proposition is either 0 (false) or 1 (true), and the truth value of a probabilistic proposition is given as a real number between 0 and 1. This observation leads to the following:

Definition 4.1.1. *A quantum predicate in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval* $[0, 1]$.

The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$. The state space $\mathcal{H}$ in the preceding definition and the following development can be infinite-dimensional unless it is explicitly stated to be finite-dimensional, although for simplicity, we assumed it is finite-dimensional in the discussion at the beginning of this section.

Satisfaction of Quantum Predicates:

Now we consider how a quantum state can satisfy a quantum predicate. Recall from Exercise 2.1.8 that $tr(M\rho)$ is the expectation value of measurement outcomes when a quantum system is in the mixed state ρ and we perform the projective measurement determined by observable M on it. Now if M is seen as a quantum predicate, then $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M, or more precisely the average truth value of the proposition represented by M in a quantum system of the state ρ. The reasonableness of the previous definition is further indicated by the following fact:

Lemma 4.1.1. *Let M be a Hermitian operator in $\mathcal{H}$. Then the following statements are equivalent:*

(i) *$M \in \mathcal{P}(\mathcal{H})$ is a quantum predicate.*
(ii) *$0_{\mathcal{H}} \sqsubseteq M \sqsubseteq I_{\mathcal{H}}$, where $0_{\mathcal{H}}, I_{\mathcal{H}}$ are the zero and identity operators in $\mathcal{H}$, respectively.*
(iii) *$0 \leq tr(M\rho) \leq 1$ for all density operators ρ in $\mathcal{H}$.*

An operator M satisfying $0_{\mathcal{H}} \sqsubseteq M \sqsubseteq I_{\mathcal{H}}$ is commonly called an effect in the literature of quantum logic and quantum foundations. Intuitively, clause (iii) in the previous lemma means that the satisfaction degree of a quantum predicate M by a quantum state ρ is always in the unit interval.

Exercise 4.1.1. *Prove Lemma 4.1.1.*

The following two lemmas show some basic properties of quantum predicates that will be frequently used in this chapter. The first one gives a characterization of the Löwner order between quantum predicates in terms of satisfaction degrees.

Lemma 4.1.2. *For any observables M, N, the following two statements are equivalent:*

(i) *$M \sqsubseteq N$;*
(ii) *for all density operators ρ, $tr(M\rho) \leq tr(N\rho)$.*

Exercise 4.1.2. *Prove Lemma 4.1.2.*

Furthermore, the next lemma examines the lattice-theoretic structure of quantum predicates with respect to the Löwner partial order.

Lemma 4.1.3. *The set $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ of quantum predicates with the Löwner partial order is a complete partial order (CPO) (see Definition 3.3.4).*

Proof. Similar to the proof of Proposition 3.3.2. □

It is worthwhile to point out that $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ is not a lattice except in the trivial case of one-dimensional state space $\mathcal{H}$; that is, the greatest lower bound and least upper bound of elements in $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ are not always defined.

4.1.1 QUANTUM WEAKEST PRECONDITIONS

Quantum predicates as defined previously can be used to describe the properties of quantum states. The next question that we need to answer in developing a logic for reasoning about quantum programs is: How do we describe the properties of quantum programs that transform a quantum state into another quantum state?

In classical programming theory, the notion of weakest precondition was extensively used for specifying the properties of programs. The weakest precondition describes a program in a backward way; that is, it determines the weakest property that the input must satisfy in order to achieve a given property of the output. This notion can be generalized to the quantum case. Actually, the quantum generalization of weakest precondition will play a key role in logics for quantum programs. In this subsection, we introduce a purely semantic (syntax-independent) notion of quantum weakest precondition. We saw that the denotational semantics of a quantum

program is usually represented by a quantum operation in the last chapter. So, in this subsection, a quantum program is simply abstracted as a quantum operation.

Definition 4.1.2. *Let $M, N \in \mathcal{P}(\mathcal{H})$ be quantum predicates, and let $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ be a quantum operation (see Definition 2.1.25). Then M is called a precondition of N with respect to $\mathcal{E}$, written $\{M\}\mathcal{E}\{N\}$, if*

$$tr(M\rho) \leq tr(N\mathcal{E}(\rho)) \tag{4.1}$$

for all density operators ρ in $\mathcal{H}$.

The intuitive meaning of condition (4.1) comes immediately from the interpretation of satisfaction relation between quantum states and quantum predicates: $tr(M\rho)$ is the expectation of truth value of predicate M in state ρ. More explicitly, inequality (4.1) can be seen as a probabilistic version of the statement: if state ρ satisfies predicate M, then the state after transformation $\mathcal{E}$ from ρ satisfies predicate N.

Definition 4.1.3. *Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate and $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ a quantum operation. Then the weakest precondition of M with respect to $\mathcal{E}$ is a quantum predicate $wp(\mathcal{E})(M)$ satisfying the following conditions:*

(i) *$\{wp(\mathcal{E})(M)\}\mathcal{E}\{M\}$;*
(ii) *for all quantum predicates N, $\{N\}\mathcal{E}\{M\}$ implies $N \sqsubseteq wp(\mathcal{E})(M)$, where $\sqsubseteq$ stands for the Löwner order.*

Intuitively, condition (i) indicates that $wp(\mathcal{E})(M)$ is a precondition of M with respect to $\mathcal{E}$, and condition (ii) means that whenever N is also a precondition of M, then $wp(\mathcal{E})(M)$ is weaker than N.

The preceding abstract definition of quantum weakest precondition is often not easy to use in applications. So, it is desirable to find an explicit representation of quantum weakest precondition. We learned from Theorem 2.1.1 that there are two convenient representations of a quantum operation, namely the Kraus operator-sum representation and the system-environment model. If (the denotational) semantics of a quantum program is represented in one of these two forms, its weakest precondition also enjoys an elegant representation. Let us first consider the Kraus operator-sum representation.

Proposition 4.1.1. *Suppose that quantum operation $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ is represented by the set $\{E_i\}$ of operators; that is,*

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

for every density operator ρ. Then for each predicate $M \in \mathcal{P}(\mathcal{H})$, we have:

$$wp(\mathcal{E})(M) = \sum_i E_i^\dagger M E_i. \tag{4.2}$$

Proof. We see from condition (ii) in Definition 4.1.3 that weakest precondition $wp(\mathcal{E})(M)$ is unique when it exists. Then we only need to check that $wp(\mathcal{E})(M)$ given by equation (4.2) satisfies the two conditions in Definition 4.1.3.

(i) Since $tr(AB) = tr(BA)$ for any operators A, B in $\mathcal{H}$, we have:

$$\begin{aligned} tr(wp(\mathcal{E})(M)\rho) &= tr\left(\left(\sum_i E_i^\dagger M E_i\right)\rho\right) \\ &= \sum_i tr\left(E_i^\dagger M E_i \rho\right) \\ &= \sum_i tr\left(M E_i \rho E_i^\dagger\right) \\ &= tr\left(M\left(\sum_i E_i \rho E_i^\dagger\right)\right) \\ &= tr(M\mathcal{E}(\rho)) \end{aligned} \tag{4.3}$$

for each density operator ρ in $\mathcal{H}$. Thus, $\{wp(\mathcal{E})(M)\}\mathcal{E}\{M\}$.

(ii) It is known that $M \sqsubseteq N$ if and only if $tr(M\rho) \leq tr(N\rho)$ for all ρ. Thus, if $\{N\}\mathcal{E}\{M\}$, then for any density operator ρ we have:

$$tr(N\rho) \leq tr(M\mathcal{E}(\rho)) = tr(wp(\mathcal{E})(M)\rho).$$

Therefore, it follows immediately that $N \sqsubseteq wp(\mathcal{E})(M)$. □

We can also give an intrinsic characterization of $wp(\mathcal{E})$ in the case that the denotational semantics $\mathcal{E}$ of a quantum program is given in a system-environment model:

$$\mathcal{E}(\rho) = tr_E\left[PU(|e_0\rangle\langle e_0| \otimes \rho)U^\dagger P\right] \tag{4.4}$$

for all density operator ρ in $\mathcal{H}$, where E is an environment system with state Hilbert space $\mathcal{H}_E$, U is a unitary transformation in $\mathcal{H}_E \otimes \mathcal{H}$, P is a projector onto some closed subspace of $\mathcal{H}_E \otimes \mathcal{H}$, and $|e_0\rangle$ is a fixed state in $\mathcal{H}_E$.

Proposition 4.1.2. *If quantum operation $\mathcal{E}$ is given by equation (4.4), then we have:*

$$wp(\mathcal{E})(M) = \langle e_0|U^\dagger P(M \otimes I_E)PU|e_0\rangle$$

for each $M \in \mathcal{P}(\mathcal{H})$, where I_E is the identity operator in the environment system's state space $\mathcal{H}_E$.

Proof. Let $\{|e_k\rangle\}$ be an orthonormal basis of $\mathcal{H}_E$. Then

$$\mathcal{E}(\rho) = \sum_k \langle e_k|PU|e_0\rangle\, \rho\, \langle e_0|U^\dagger P|e_k\rangle,$$

and using Proposition 4.1.1 we obtain:

$$wp(\mathcal{E})(M) = \sum_k \langle e_0|U^\dagger P|e_k\rangle M \langle e_k|PU|e_0\rangle$$
$$= \langle e_0|U^\dagger P \left(\sum_k |e_k\rangle M \langle e_k|\right) PU|e_0\rangle.$$

Note that

$$\sum_k |e_k\rangle M\langle e_k| = M \otimes \left(\sum_k |e_k\rangle\langle e_k|\right) = M \otimes I_E$$

because $\{|e_k\rangle\}$ is an orthonormal basis of $\mathcal{H}_E$, and M is an operator in $\mathcal{H}$. This completes the proof. □

Schrödinger-Heisenberg Duality:

As in classical programming theory, the denotational semantics $\mathcal{E}$ of a quantum program is a forward state transformer:

$$\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}),$$
$$\rho \mapsto \mathcal{E}(\rho) \text{ for each } \rho \in \mathcal{D}(\mathcal{H})$$

where $\mathcal{D}(\mathcal{H})$ stands for the set of partial density operators in $\mathcal{H}$: i.e., positive operators with traces ≤ 1. On the other hand, the notion of weakest precondition defines a backward quantum predicate transformer:

$$wp(\mathcal{E}) : \mathcal{P}(\mathcal{H}) \to \mathcal{P}(\mathcal{H}),$$
$$M \mapsto wp(\mathcal{E})(M) \text{ for each } M \in \mathcal{P}(\mathcal{M}).$$

They provide us with two complementary ways to look at a quantum program.

The duality between forward and backward semantics has been extensively exploited to cope with classical programs. It will be equally useful for the studies of quantum programs. Moreover, the relationship between a quantum program and its weakest precondition can even be considered from a physics point of view – the Schrödinger-Heisenberg duality (Figure 4.1) between quantum states (described as density operators) and quantum observables (described as Hermitian operators).

Definition 4.1.4. *Let $\mathcal{E}$ be a quantum operation mapping (partial) density operators to (partial) density operators, and let $\mathcal{E}^*$ be an operator mapping Hermitian operators to Hermitian operators. If we have*

$$\text{(Duality)} \qquad tr[M\mathcal{E}(\rho)] = tr[\mathcal{E}^*(M)\rho] \tag{4.5}$$

for any (partial) density operator ρ, and for any Hermitian operator M, then we say that $\mathcal{E}$ and $\mathcal{E}^*$ are (Schrödinger-Heisenberg) dual.

It follows from the definition that the dual $\mathcal{E}^*$ of a quantum operation $\mathcal{E}$ is unique whenever it exists.

$$\begin{array}{ccc} \rho & \models & \mathcal{E}^*(M) \\ \mathcal{E}\downarrow & & \uparrow \mathcal{E}^* \\ \mathcal{E}(\rho) & \models & M \end{array}$$

The mapping $\rho \mapsto \mathcal{E}(\rho)$ is the Schrödinger picture, and the mapping $M \mapsto \mathcal{E}^*(M)$ is the Heisenberg picture. The symbol $\models$ stands for satisfaction relation; that is, $tr(M\rho) = \Pr\{\rho \models M\}$ (the probability that ρ satisfies M).

FIGURE 4.1

Schrödinger-Heisenberg duality.

The following proposition indicates that the notion of weakest precondition in programming theory coincides with the notion of Schrödinger-Heisenberg duality in physics.

Proposition 4.1.3. *Any quantum operation $\mathcal{E}\in\mathcal{QO}(\mathcal{H})$ and its weakest precondition $wp(\mathcal{E})$ are dual to each other.*

Proof. Immediate from equation (4.3). □

To conclude this section, we collect several basic algebraic properties of quantum weakest preconditions in the following proposition.

Proposition 4.1.4. *Let $\lambda \geq 0$ and $\mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$, and let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{QO}(\mathcal{H})$. Then*

(i) *$wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{QO}(\mathcal{H})$;*
(ii) *$wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in \mathcal{QO}(\mathcal{H})$;*
(iii) *$wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$;*
(iv) *$wp\left(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n\right) = \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)$, where $\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)$ is defined by*

$$\left(\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)\right)(M) \stackrel{\triangle}{=} \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)$$

for any $M \in \mathcal{P}(\mathcal{H})$.

Proof. **(i)** and **(ii)** are immediately from Proposition 4.1.1.

(iii) It is easy to see that $\{L\}\mathcal{E}\{M\}$ and $\{M\}\mathcal{F}\{N\}$ implies $\{L\}\mathcal{E} \circ \mathcal{F}\{N\}$. Thus, we have:

$$\{wp(\mathcal{E})(wp(\mathcal{F})(M))\}\mathcal{E} \circ \mathcal{F}\{M\}.$$

On the other hand, we need to show that $N \sqsubseteq wp(\mathcal{E})(wp(\mathcal{F})(M))$ whenever $\{N\}\mathcal{E} \circ \mathcal{F}\{M\}$. In fact, for any density operator ρ, it follows from equation (4.3) that

$$\begin{aligned} tr(N\rho) &\leq tr(M(\mathcal{E}\circ\mathcal{F})(\rho)) \\ &= tr(M\mathcal{F}(\mathcal{E}(\rho))) \\ &= tr(wp(\mathcal{F})(M)\mathcal{E}(\rho)) \\ &= tr(wp(\mathcal{E})(wp(\mathcal{F})(M))\rho). \end{aligned}$$

Therefore, we obtain

$$wp(\mathcal{E}\circ\mathcal{F})(M) = wp(\mathcal{E})(wp(\mathcal{F})(M)) = (wp(\mathcal{F})\circ wp(\mathcal{E}))(M).$$

(iv) First, we note that the following two equalities follow immediately from the definition of $\bigsqcup$ in CPO $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$:

$$M\left(\bigsqcup_{n=0}^{\infty} M_n\right) = \lim_{n\to\infty} MM_n,$$

$$tr\left(\bigsqcup_{n=0}^{\infty} M_n\right) = \bigsqcup_{n=0}^{\infty} tr(M_n).$$

Then we can prove that

$$\left\{\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)\right\} \bigsqcup_{n=0}^{\infty} \mathcal{E}_n\{M\}.$$

Indeed, for any $\rho \in \mathcal{D}(\mathcal{H})$, we have:

$$\begin{aligned} tr\left(\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)\rho\right) &= \bigsqcup_{n=0}^{\infty} tr(wp(\mathcal{E}_n)(M)\rho) \\ &\leq \bigsqcup_{n=0}^{\infty} tr(M\mathcal{E}_n(\rho)) \\ &= tr\left(\lim_{n\to\infty} M\mathcal{E}_n(\rho)\right) \\ &= tr\left(M\left(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n\right)(\rho)\right). \end{aligned}$$

Second, we show that $\{N\} \bigsqcup_{n=0}^{\infty} \mathcal{E}_n\{M\}$ implies $N \sqsubseteq \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)$. It suffices to note that

$$\begin{aligned} tr(N\rho) &\leq tr\left(M\left(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n\right)(\rho)\right) \\ &= tr\left(\lim_{n\to\infty} M\mathcal{E}_n(\rho)\right) \\ &= \bigsqcup_{n=0}^{\infty} tr(M\mathcal{E}_n(\rho)) \end{aligned}$$

$$= \bigsqcup_{n=0}^{\infty} tr(wp(\mathcal{E}_n)(M)\rho)$$
$$= tr\left(\left(\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)\right)(M)\rho\right)$$

for all density operators ρ. Thus, it holds that

$$wp\left(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n\right)(M) = \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M).$$

□

4.2 FLOYD-HOARE LOGIC FOR QUANTUM PROGRAMS

Floyd-Hoare logic is a logical system widely used in classical programming methodology for reasoning about correctness of programs. It consists of a set of inference rules defined in terms of preconditions and postconditions.

The notions of quantum predicate and weakest precondition were introduced in the last section for abstract quantum programs modelled by quantum operations. Based on them, in this section, we present a logic of the Floyd-Hoare style for reasoning about correctness of quantum programs in the **while**-language introduced in Section 3.1.

4.2.1 CORRECTNESS FORMULAS

In the classical Floyd-Hoare logic, correctness of a program is expressed by a Hoare triple which consists of a predicate describing the input state and a predicate describing the output states of the program. The notion of Hoare triple can be directly generalized into the quantum setting.

Let $qVar$ be the set of quantum variables in the **while**-language defined in Section 3.1. For any set $X \subseteq qVar$, we write

$$\mathcal{H}_X = \bigotimes_{q \in X} \mathcal{H}_q$$

for the state Hilbert space of the system consisting of quantum variables in X, where $\mathcal{H}_q$ is the state space of quantum variable q. In particular, we set

$$\mathcal{H}_{all} = \bigotimes_{q \in qVar} \mathcal{H}_q.$$

Recall from the last section, a quantum predicate in $\mathcal{H}_X$ is a Hermitian operator P in $\mathcal{H}_X$ such that $0_{\mathcal{H}_X} \sqsubseteq P \sqsubseteq I_{\mathcal{H}_X}$. We write $\mathcal{P}(\mathcal{H}_X)$ for the set of quantum predicates in $\mathcal{H}_X$.

Definition 4.2.1. *A correctness formula is a statement of the form:*

$$\{P\}S\{Q\}$$

where S is a quantum program, and both $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$. The quantum predicate P is called the precondition of the correctness formula and Q the postcondition.

In the Floyd-Hoare logic for classical programs, P and Q in a Hoare triple $\{P\}S\{Q\}$ are two first-order logical formulas. The Hoare logical formula $\{P\}S\{Q\}$ can be used to describe two different kinds of correctness of programs:

- *Partial correctness*: If an input to program S satisfies the precondition P, then either S does not terminate, or it terminates in a state satisfying the postcondition Q.
- *Total correctness*: If an input to program S satisfies the precondition P, then S must terminate and it terminates in a state satisfying the postcondition Q.

Although the appearance of a Hoare triple $\{P\}S\{Q\}$ in the quantum case is the same as that in the classical case, precondition P and postcondition Q in the former are two quantum predicates, i.e. observables represented by Hermitian operators. We write $\mathcal{D}(\mathcal{H}_X)$ for the set of partial density operators, i.e. positive operators with traces ≤ 1, in $\mathcal{H}_X$. Intuitively, for any quantum predicate $P \in \mathcal{P}(\mathcal{H}_X)$ and state $\rho \in \mathcal{D}(\mathcal{H}_X)$, $tr(P\rho)$ stands for the probability that predicate P is satisfied in state ρ. As in the classical programming theory, a correctness formula can also be interpreted in two different ways:

Definition 4.2.2

(i) *The correctness formula $\{P\}S\{Q\}$ is true in the sense of total correctness, written*

$$\models_{tot} \{P\}S\{Q\},$$

if we have:

$$tr(P\rho) \leq tr(Q[\![S]\!](\rho)) \tag{4.6}$$

for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, where $[\![S]\!]$ is the semantic function of S (see Definition 3.3.1).

(ii) *The correctness formula $\{P\}S\{Q\}$ is true in the sense of partial correctness, written*

$$\models_{par} \{P\}S\{Q\},$$

if we have:

$$tr(P\rho) \leq tr(Q[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))] \tag{4.7}$$

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

The intuitive meaning of the defining inequality (4.6) of total correctness is:

- The probability that input ρ satisfies quantum predicate P is not greater than the probability that quantum program S terminates on ρ and its output $[\![S]\!](\rho)$ satisfies quantum predicate Q.

It is obvious from Definition 4.1.2 that $\models_{tot} \{P\}S\{Q\}$ is a restatement of the fact that P is a precondition of Q with respect to quantum operation $[\![S]\!]$, i.e.,

$$\{P\}[\![S]\!]\{Q\}.$$

Recall that $tr(\rho)-tr([\![S]\!](\rho))$ is the probability that quantum program S diverges from input ρ. Thus, the defining inequality (4.7) of partial correctness intuitively means:

- If input ρ satisfies predicate P, then either program S terminates on it and its output $[\![S]\!](\rho)$ satisfies Q, or S diverges from it.

To better understand this definition, let us see a simple example. This example clearly illustrates the difference between total correctness and partial correctness.

Example 4.2.1. *Assume that type*$(q) =$ **Boolean**. *Consider the program:*

$$S \equiv \textbf{ while } M[q] = 1 \textbf{ do } q := \sigma_z[q] \textbf{ od}$$

where $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$, *and* σ_z *is the Pauli matrix. Let*

$$P = |\psi\rangle_q\langle\psi| \otimes P'$$

where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}_2$, *and* $P' \in \mathcal{P}\left(\mathcal{H}_{qVar\setminus\{q\}}\right)$. *Then*

(i) *We see that the total correctness*

$$\models_{tot} \{P\}S\{|0\rangle_q\langle 0| \otimes P'\}$$

does not hold if $\beta \neq 0$ *and* $P' \neq 0_{\mathcal{H}_{qVar\setminus\{q\}}}$. *In fact, put*

$$\rho = |\psi\rangle_q\langle\psi| \otimes I_{\mathcal{H}_{qVar\setminus\{q\}}}.$$

Note that ρ *is not normalized for simplicity of presentation. Then*

$$[\![S]\!](\rho) = |\alpha|^2|0\rangle_q\langle 0| \otimes I_{\mathcal{H}_{qVar\setminus\{q\}}}$$

and

$$tr(P\rho) = tr(P') > |\alpha|^2 tr(P') = tr((|0\rangle_q\langle 0| \otimes P')[\![S]\!](\rho)).$$

(ii) *We have the partial correctness:*

$$\models_{par} \{P\}S\{|0\rangle_q\langle 0| \otimes P'\};$$

that is,

$$tr(P\rho) \leq tr((|0\rangle_q\langle 0| \otimes P')[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]. \tag{4.8}$$

Here, we only consider a special class of partial density operators in $\mathcal{H}_{Var\setminus\{q\}}$*:*

$$\rho = |\varphi\rangle_q\langle\varphi| \otimes \rho'$$

where $|\varphi\rangle = a|0\rangle + b|1\rangle \in \mathcal{H}_2$*, and* $\rho' \in \mathcal{D}\left(\mathcal{H}_{qVar\setminus\{q\}}\right)$*. A routine calculation yields:*

$$[\![S]\!](\rho) = |a|^2|0\rangle_q\langle 0| \otimes \rho'$$

and

$$\begin{aligned} tr(P\rho) &= |\langle\varphi|\varphi\rangle|^2 tr(P'\rho') \\ &\leq |a|^2 tr(P'\rho') + [tr(\rho') - |a|^2 tr(\rho')] \\ &= tr((|0\rangle_q\langle 0| \otimes P')[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]. \end{aligned}$$

Exercise 4.2.1. *Prove inequality* (4.8) *for all* $\rho \in \mathcal{D}(\mathcal{H}_{all})$.

The following proposition presents several basic properties of total and partial correctness formulas.

Proposition 4.2.1

(i) *If* $\models_{tot} \{P\}S\{Q\}$*, then* $\models_{par} \{P\}S\{Q\}$.

(ii) *For any quantum program* S*, and for any* $P, Q \in \mathcal{P}(\mathcal{H}_{all})$*, we have:*

$$\models_{tot} \{0_{\mathcal{H}_{all}}\}S\{Q\}, \quad \models_{par} \{P\}S\{I_{\mathcal{H}_{all}}\}.$$

(iii) *(Linearity) For any* $P_1, P_2, Q_1, Q_2 \in \mathcal{P}(\mathcal{H}_{all})$ *and* $\lambda_1, \lambda_2 \geq 0$ *with* $\lambda_1 P_1 + \lambda_2 P_2, \lambda_1 Q_1 + \lambda_2 Q_2 \in \mathcal{P}(\mathcal{H}_{all})$*, if*

$$\models_{tot} \{P_i\}S\{Q_i\} \ (i = 1, 2),$$

then

$$\models_{tot} \{\lambda_1 P_1 + \lambda_2 P_2\}S\{\lambda_1 Q_1 + \lambda_2 Q_2\}.$$

The same conclusion holds for partial correctness if $\lambda_1 + \lambda_2 = 1$.

Proof. Immediate from definition. □

4.2.2 WEAKEST PRECONDITIONS OF QUANTUM PROGRAMS

In Subsection 4.1.1, we already defined the notion of weakest precondition for a general quantum operation (thought of as the denotational semantics of a quantum program). In this subsection, we consider its syntactic counterpart, namely weakest precondition for a quantum program written in the **while**-language defined in Section 3.1. As in the case of classical Floyd-Hoare logic, weakest preconditions and weakest liberal preconditions can be defined for quantum programs corresponding

to total correctness and partial correctness, respectively. They will play a key role in establishing the (relative) completeness of Floyd-Hoare logic for quantum programs.

Definition 4.2.3. *Let S be a quantum **while**-program and $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate in $\mathcal{H}_{all}$.*

(i) *The weakest precondition of S with respect to P is defined to be the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying the following conditions:*
  (a) $\models_{tot} \{wp.S.P\}S\{P\}$;
  (b) *if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.*

(ii) *The weakest liberal precondition of S with respect to P is defined to be the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying the following conditions:*
  (a) $\models_{par} \{wlp.S.P\}S\{P\}$;
  (b) *if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{par} \{Q\}S\{P\}$ then $Q \sqsubseteq wlp.S.P$.*

By comparing the previous definition and Definition 4.1.3, we can see that they are compatible; that is,

$$wp.S.P = wp([\![S]\!])(P). \tag{4.9}$$

Note that the left-hand side of this equality is given directly in terms of program S, whereas the right-hand side is given in terms of the semantics of S.

The next two propositions give explicit representations of weakest preconditions and weakest liberal preconditions, respectively, for programs written in the quantum **while**-language. They will be essentially used in the proof of completeness of quantum Floyd-Hoare logic for total and partial correctness. Let us first consider weakest preconditions of quantum programs.

Proposition 4.2.2

(i) $wp.\mathbf{skip}.P = P$.

(ii) **(a)** *If* $type(q) =$ **Boolean**, *then*

$$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

(b) *If* $type(q) =$ **integer**, *then*

$$wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$

(iii) $wp.\overline{q} := U[\overline{q}].P = U^\dagger PU$.

(iv) $wp.S_1; S_2.P = wp.S_1.(wp.S_2.P)$.

(v) $wp.\mathbf{if}\ (\square m \cdot M[\overline{q}] = m \to S_m)\ \mathbf{fi}.P = \sum_m M_m^\dagger (wp.S_m.P) M_m$.

(vi) $wp.\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}.P = \bigsqcup_{n=0}^{\infty} P_n$, *where*

$$\begin{cases} P_0 = 0_{\mathcal{H}_{all}}, \\ P_{n+1} = M_0^\dagger P M_0 + M_1^\dagger (wp.S.P_n) M_1 \ \text{ for all } n \geq 0. \end{cases}$$

Proof. The trick is to simultaneously prove this proposition and Corollary 4.2.1 following by induction on the structure of quantum program S.

- Case 1. $S \equiv$ **skip**. Obvious.
- Case 2. $S \equiv q := |0\rangle$. We only consider the case of $type(q) =$ **integer**, and the case of $type(q) =$ **Boolean** is similar. First, it holds that

$$tr\left(\left(\sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|\right)\rho\right) = tr\left(P\sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|\right)$$
$$= tr(P[\![q := |0\rangle]\!](\rho)).$$

On the other hand, for any quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$, if

$$\models_{tot} \{Q\}q := |0\rangle\{P\},$$

i.e.,

$$tr(Q\rho) \le tr(P[\![q := |0\rangle]\!](\rho))$$
$$= tr\left(\left(\sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|\right)\rho\right)$$

for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, then it follows from Lemma 4.1.2 that

$$Q \sqsubseteq \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$

- Case 3. $S \equiv \overline{q} := U[\overline{q}]$. Similar to Case 2.
- Case 4. $S \equiv S_1; S_2$. It follows from the induction hypothesis on S_1 and S_2 that

$$tr((wp.S_1.(wp.S_2.P))\rho) = tr((wp.S_2.P)[\![S_1]\!](\rho))$$
$$= tr(P[\![S_2]\!]([\![S_1]\!](\rho)))$$
$$= tr(P[\![S_1; S_2]\!](\rho)).$$

If $\models_{tot} \{Q\}S_1; S_2\{P\}$, then for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, we have:

$$tr(QP) \le tr(P[\![S_1; S_2]\!](\rho)) = tr((wp.S_1.(wp.S_2.P))\rho).$$

Therefore, it follows from Lemma 4.1.2 that $Q \sqsubseteq wp.S_1.(wp.S_2.P)$.

- Case 5. $S \equiv$ **if** $(\square m \cdot M[\overline{q}] = m \to S_m)$ **fi**. Applying the induction hypothesis on S_m, we obtain:

$$\begin{aligned} tr\left(\left(\sum_m M_m^\dagger (wp.S_m.P) M_m\right)\rho\right) &= \sum_m tr((wp.S_m.P) M_m \rho M_m^\dagger) \\ &= \sum_m tr(P[\![S_m]\!](M_m \rho M_m^\dagger)) \\ &= tr\left(P \sum_m [\![S_m]\!]\left(M_m \rho M_m^\dagger\right)\right) \\ &= tr(P[\![\textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}]\!](\rho)). \end{aligned}$$

  If

$$\models_{tot} \{Q\}\textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}\{P\},$$

  then

$$tr(Q\rho) \le tr\left(\left(\sum_m M_m^\dagger (wp.S_m.P) M_m\right)\rho\right)$$

  for all ρ, and it follows from Lemma 4.1.2 that

$$Q \sqsubseteq \sum_m M_m^\dagger (wlp.S_m.P) M_m.$$

- Case 6. $S \equiv$ **while** $M[\overline{q}] = 1$ **do** S' **od**. For simplicity, we write $(\textbf{while})^n$ for the nth syntactic approximation "$(\textbf{while } M[\overline{q}] = 1 \textbf{ do } S' \textbf{ od})^n$" of loop S (see Definition 3.3.6). First, we have:

$$tr(P_n \rho) = tr(P[\![(\textbf{while})^n]\!](\rho)).$$

  This claim can be proved by induction on n. The basis case of $n = 0$ is obvious. By the induction hypotheses on n and S', we obtain:

$$\begin{aligned} tr(P_{n+1}\rho) &= tr(M_0^\dagger P M_0 \rho) + tr(M_1^\dagger (wp.S'.P_n) M_1 \rho) \\ &= tr(P M_0 \rho M_0^\dagger) + tr((wp.S'.P_n) M_1 \rho M_1^\dagger) \\ &= tr(P M_0 \rho M_0^\dagger) + tr(P_n[\![S']\!](M_1 \rho M_1^\dagger)) \\ &= tr(P M_0 \rho M_0^\dagger) + tr(P[\![(\textbf{while})^n]\!]([\![S']\!](M_1 \rho M_1^\dagger))) \\ &= tr[P(M_0 \rho M_0^\dagger + [\![S'; (\textbf{while})^n]\!](M_1 \rho M_1^\dagger))] \\ &= tr(P[\![(\textbf{while})^{n+1}]\!](\rho)). \end{aligned}$$

Now continuity of trace operator yields:

$$\begin{aligned} tr\left(\left(\bigsqcup_{n=0}^{\infty} P_n\right)\rho\right) &= \bigsqcup_{n=0}^{\infty} tr(P_n\rho) \\ &= \bigsqcup_{n=0}^{\infty} tr(P[\![(\textbf{while})^n]\!](\rho)) \\ &= tr\left(P\bigsqcup_{n=0}^{\infty}[\![(\textbf{while})^n]\!](\rho)\right) \\ &= tr(P[\![\textbf{while}\, M[\overline{q}] = 1\ \textbf{do}\ S'\ \textbf{od}]\!](\rho)). \end{aligned}$$

So, if

$$\models_{tot} \{Q\}\textbf{while}\, M[\overline{q}] = 1\ \textbf{do}\ S'\ \textbf{od}\{P\},$$

then

$$tr(Q\rho) \leq tr\left(\left(\bigsqcup_{n=0}^{\infty} P_n\right)\rho\right)$$

for all ρ, and by Lemma 4.1.2 we obtain $Q \sqsubseteq \bigsqcup_{n=0}^{\infty} P_n$.

□

The following corollary shows that the probability that an initial state ρ satisfies the weakest precondition $wp.S.P$ is equal to the probability that the terminal state $[\![S]\!](\rho)$ satisfies P. It follows from the proof of the previous proposition. But it can also be derived from equations (4.3) and (4.9).

Corollary 4.2.1. *For any quantum **while**-program S, for any quantum predicate $P \in \mathcal{P}(\mathcal{H}_{all})$, and for any partial density operator $\rho \in \mathcal{D}(\mathcal{H}_{all})$, we have:*

$$tr((wp.S.P)\rho) = tr(P[\![S]\!](\rho)).$$

We can also give explicit representations of weakest liberal preconditions of quantum programs.

Proposition 4.2.3

(i) $wlp.\textbf{skip}.P = P$.

(ii) **(a)** *If* $type(q) = \textbf{Boolean}$, *then*

$$wlp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

(b) *If* $type(q) =$ **integer**, *then*

$$wlp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$

(iii) $wlp.\overline{q} := U[\overline{q}].P = U^\dagger PU.$
(iv) $wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P).$
(v) $wlp.\textbf{if}\ (\square m \cdot M[\overline{q}] := m \to S_m)\ \textbf{fi}.P = \sum_m M_m^\dagger (wlp.S_m.P) M_m.$
(vi) $wlp.\textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od}.P = \bigcap_{n=0}^{\infty} P_n$, *where*

$$\begin{cases} P_0 = I_{\mathcal{H}_{all}}, \\ P_{n+1} = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.P_n) M_1 \ \ \textit{for all } n \geq 0. \end{cases}$$

Proof. Similar to the case of weakest precondition, we prove this proposition and its corollary following simultaneously by induction on the structure of quantum program S.

- Case 1. $S \equiv$ **skip**, or $q := |0\rangle$, or $\overline{q} := U[\overline{q}]$. Similar to Cases 1, 2 and 3 in the proof of Proposition 4.2.2.
- Case 2. $S \equiv S_1; S_2$. First, with the induction hypothesis on S_1 and S_2, we have:

$$\begin{aligned} tr(wlp.S_1.(wlp.S_2.P)\rho) &= tr(wlp.S_2.P[\![S_1]\!](\rho)) + [tr(\rho) - tr([\![S_1]\!](\rho))] \\ &= tr(P[\![S_2]\!]([\![S_1]\!](\rho)) + [tr([\![S_1]\!](\rho)) - tr([\![S_2]\!]([\![S_1]\!](\rho)))] \\ &\qquad + [tr(\rho) - tr([\![S_1]\!](\rho))] \\ &= tr(P[\![S_2]\!]([\![S_1]\!](\rho)) + [tr(\rho) - tr([\![S_2]\!]([\![S_1]\!](\rho)))] \\ &= tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]. \end{aligned}$$

  If $\models_{par} \{Q\}S\{P\}$, then it holds that

$$\begin{aligned} tr(Q\rho) &\leq tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))] \\ &= tr(wlp.S_1.(wlp.S_2.P)\rho) \end{aligned}$$

  for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, and by Lemma 4.1.2 we obtain:

$$Q \sqsubseteq wlp.S_1.(wlp.S_2.P).$$

- Case 3. $S \equiv$ **if** $(\square m \cdot M[\overline{q}] = m \to S_m)$ **fi**. It can be derived by the induction hypothesis on all S_m that

$$
\begin{aligned}
tr\left(\sum_m M_m^\dagger(wlp.S_m.P)M_m\rho\right) &= \sum_m tr(M_m^\dagger(wlp.S_m.P)M_m\rho)\\
&= \sum_m tr((wlp.S_m.P)M_m\rho M_m^\dagger)\\
&= \sum_m \left\{tr(P[\![S_m]\!](M_m\rho M_m^\dagger)) + [tr(M_m\rho M_m^\dagger) - tr([\![S_m]\!](M_m\rho M_m^\dagger))]\right\}\\
&= \sum_m tr\left(P[\![S_m]\!](M_m\rho M_m^\dagger)\right) + \left[\sum_m tr(M_m\rho M_m^\dagger) - \sum_m tr([\![S_m]\!](M_m\rho M_m^\dagger))\right]\\
&= tr\left(P\sum_m [\![S_m]\!](M_m\rho M_m^\dagger)\right)\\
&\qquad + \left[tr\left(\rho\sum_m M_m^\dagger M_m\right) - tr\left(\sum_m [\![S_m]\!](M_m\rho M_m^\dagger)\right)\right]\\
&= tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]
\end{aligned}
$$

because

$$\sum_m M_m^\dagger M_m = I_{\mathcal{H}_{\overline{q}}}.$$

If $\models_{par} \{Q\}S\{P\}$, then for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, it holds that

$$
\begin{aligned}
tr(Q\rho) &\le tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]\\
&= tr\left(\sum_m M_m^\dagger(wlp.S_m.P)M_m\rho\right).
\end{aligned}
$$

This together with Lemma 4.1.2 implies

$$Q \sqsubseteq \sum_m M_m^\dagger(wlp.S_m.P)M_m.$$

- Case 4. $S \equiv$ **while** $M[\overline{q}] = 1$ **do** S' **od**. We first prove that

$$tr(P_n\rho) = tr(P[\![(\textbf{while})^n]\!](\rho)) + [tr(\rho) - tr([\![(\textbf{while})^n]\!](\rho))] \tag{4.10}$$

by induction on n, where $(\textbf{while})^n$ is an abbreviation of the syntactic approximation (**while** $M[\overline{q}] = 1$ **do** S' **od**)^n. The case of $n = 0$ is obvious.

By induction on S' and the induction hypothesis on n, we observe:

$$\begin{aligned}
tr(P_{n+1}\rho) &= tr[(M_0^\dagger P M_0) + M_1^\dagger (wlp.S'.P_n) M_1 \rho] \\
&= tr(M_0^\dagger P M_0 \rho) + tr(M_1^\dagger (wlp.S'.P_n) M_1 \rho) \\
&= tr(P M_0 \rho M_0^\dagger) + tr((wlp.S'.P_n) M_1 \rho M_1^\dagger) \\
&= tr(P M_0 \rho M_0^\dagger) + tr(P_n [\![S']\!](M_1 \rho M_1^\dagger)) + [tr(M_1 \rho M_1^\dagger) - tr([\![S']\!](M_1 \rho M_1^\dagger))] \\
&= tr(P M_0 \rho M_0^\dagger) + tr(P [\![(\textbf{while})^n]\!]([\![S]\!](M_1 \rho M_1^\dagger))) + [tr([\![S]\!](M_1 \rho M_1^\dagger)) \\
&\quad - tr([\![(\textbf{while})^n]\!]([\![S]\!](M_1 \rho M_1^\dagger)))] + [tr(M_1 \rho M_1^\dagger) - tr([\![S']\!](M_1 \rho M_1^\dagger))] \\
&= tr(P[M_0 \rho M_0^\dagger + [\![(\textbf{while})^n]\!]([\![S]\!](M_1 \rho M_1^\dagger))] \\
&\quad + [tr(\rho) - tr(M_0 \rho M_0^\dagger + [\![(\textbf{while})^n]\!]([\![S]\!](M_1 \rho M_1^\dagger)))] \\
&= tr(P[\![(\textbf{while})^{n+1}]\!](\rho)) + [tr(\rho) - tr([\![(\textbf{while})^{n+1}]\!](\rho)].
\end{aligned}$$

This completes the proof of equation (4.10). Note that quantum predicate $P \sqsubseteq I$. Then $I - P$ is positive, and by continuity of trace operator we obtain:

$$\begin{aligned}
tr\left(\left(\prod_{n=0}^{\infty} P_n\right)\rho\right) &= \prod_{n=0}^{\infty} tr\,(P_n \rho) \\
&= \prod_{n=0}^{\infty} \left\{tr\left(P[\![(\textbf{while})^n]\!]\,(\rho)\right) + \left[tr(\rho) - tr([\![(\textbf{while})^n]\!](\rho))\right]\right\} \\
&= tr(\rho) + \prod_{n=0}^{\infty} tr\left[(P-I)[\![(\textbf{while})^n]\!](\rho)\right] \\
&= tr(\rho) + tr\left[(P-I)\bigsqcup_{n=0}^{\infty} [\![(\textbf{while})^n]\!](\rho)\right] \\
&= tr(\rho) + tr[(P-I)[\![S]\!](\rho)] \\
&= tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))].
\end{aligned}$$

For any $Q \in \mathcal{P}(\mathcal{H}_{all})$, $\models_{par} \{Q\}S\{P\}$ implies:

$$\begin{aligned}
tr(Q\rho) &\leq tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho)) \\
&= tr\left(\left(\prod_{n=0}^{\infty} P_n\right)\rho\right)
\end{aligned}$$

for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$. This together with Lemma 4.1.2 leads to $Q \sqsubseteq \prod_{n=0}^{\infty} P_n$. □

Corollary 4.2.2. *For any quantum **while**-program S, for any quantum predicate $P \in \mathcal{P}(\mathcal{H}_{all})$, and for any partial density operator $\rho \in \mathcal{D}(\mathcal{H}_{all})$, we have:*

$$tr((wlp.S.P)\rho) = tr(P[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho)].$$

The previous lemma means that the probability that an initial state ρ satisfies the weakest liberal precondition $wlp.S.P$ is equal to the sum of the probability that the terminal state $[\![S]\!](\rho)$ satisfies P and the probability that S does not terminate when starting from ρ.

To conclude this subsection, we present a recursive characterization of weakest precondition and weakest liberal precondition of the quantum **while**-loop. This characterization provides a key step in the proof of completeness of quantum Floyd-Hoare logic.

Proposition 4.2.4. *We write* **while** *for quantum loop "***while** $M[\overline{q}] = 1$ **do** S **od**". Then for any $P \in \mathcal{P}(\mathcal{H}_{all})$, we have:*

(i) $wp.\mathbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wp.S.(wp.\mathbf{while}.P))M_1$.

(ii) $wlp.\mathbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\mathbf{while}.P))M_1$.

Proof. We only prove (ii), and the proof of (i) is similar and easier. For every $\rho \in \mathcal{D}(\mathcal{H}_{all})$, by Proposition 4.2.3 (iv) we observe:

$$
\begin{aligned}
&tr[(M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\mathbf{while}.P))M_1)\rho] \\
&\quad = tr(PM_0\rho M_0^\dagger) + tr[(wlp.S.(wlp.\mathbf{while}.P))M_1\rho M_1^\dagger] \\
&\quad = tr(PM_0\rho M_0^\dagger) + tr[(wlp.\mathbf{while}.P)[\![S]\!](M_1\rho M_1^\dagger)] \\
&\qquad\qquad + [tr(M_1\rho M_1^\dagger) - tr([\![S]\!](M_1\rho M_1^\dagger))] \\
&\quad = tr(PM_0\rho M_0^\dagger) + tr[P[\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger))] + [tr([\![S]\!](M_1\rho M_1^\dagger) \\
&\qquad - tr([\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger))] + [tr(M_1\rho M_1^\dagger) - tr([\![S]\!](M_1\rho M_1^\dagger))] \\
&\quad = tr[P(M_0\rho M_0^\dagger + [\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger)))] \\
&\qquad\qquad + [tr(M_1\rho M_1^\dagger) - tr([\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger))] \\
&\quad = tr(P[\![\mathbf{while}]\!](\rho)) + [tr(\rho M_1^\dagger M_1) - tr([\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger)))] \\
&\quad = tr(P[\![\mathbf{while}]\!](\rho)) + [tr(\rho(I - M_0^\dagger M_0)) - tr([\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger)))] \\
&\quad = tr(P[\![\mathbf{while}]\!](\rho)) + [tr(\rho) - tr(M_0\rho M_0^\dagger + [\![\mathbf{while}]\!]([\![S]\!](M_1\rho M_1^\dagger)))] \\
&\quad = tr(P[\![\mathbf{while}]\!](\rho)) + [tr(\rho) - tr([\![\mathbf{while}]\!](\rho))].
\end{aligned}
$$

This means that

$$\left\{M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\mathbf{while}.P))M_1\right\} \mathbf{while}\{P\},$$

and

$$Q \sqsubseteq M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\mathbf{while}.P))M_1$$

provided $\models_{par} \{Q\}\mathbf{while}\{P\}$. □

From Propositions 4.2.2 (vi) and 4.2.3 (vi) we see that the previous proposition can be actually strengthened as follows:

- $wp.\mathbf{while}.P$ and $wlp.\mathbf{while}.P$ are the least fixed point and the greatest fixed point of function:

$$X \mapsto M_0^\dagger P M_0 + M_1^\dagger (wp.S.X) M_1,$$

respectively.

4.2.3 PROOF SYSTEM FOR PARTIAL CORRECTNESS

Now we are ready to present an axiomatic system of Floyd-Hoare logic for quantum **while**-programs. The axiomatic system is given in terms of correctness formulas defined in Subsection 4.2.1. The quantum Floyd-Hoare logic can be divided into two proof systems, one for partial correctness and one for total correctness. In this subsection, we introduce the proof system *qPD* for partial correctness of quantum programs. It consists of the axioms and inference rules in Figure 4.2.

An application of the proof system *qPD* and the proof system *qTD* for total correctness presented in the next subsection will be given in Subsection 4.2.5 below where the correctness of the Grover algorithm is proved using *qPD* and *qTD*. The reader who is mainly interested in the applications of quantum Floyd-Hoare logic may first leave here to learn the rule (R-LT) of the system *qTD* in the next subsection and then directly move to Subsection 4.2.5. If she/he likes, the reader can return to this point after finishing Subsection 4.2.5.

As we know, the most important issue for any logical system is its soundness and completeness. In the remainder of this subsection, we study soundness and completeness of the proof system *qPD*. We say that a correctness formula $\{P\}S\{Q\}$ is provable in *qTD*, written

$$\vdash_{qPD} \{P\}S\{Q\}$$

if it can be derived by a finite number of applications of the axioms and inference rules given in Figure 4.2.

We first prove the soundness of *qPD* with respect to the semantics of partial correctness:

- provability of a correctness formula in the proof system *qPD* implies its truth in the sense of partial correctness.

Before doing this, let us introduce an auxiliary notation: for $i = 0, 1$, the quantum operation $\mathcal{E}_i$ is defined by

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

for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$. This notation was already used in the proof of Proposition 3.3.2. It will be frequently used in this subsection and the next as well as in Chapter 5.

(Ax-Sk) $\{P\}\mathbf{Skip}\{P\}$

(Ax-In) If $type(q) = \mathbf{Boolean}$, then

$$\{|0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|\}q := |0\rangle\{P\}$$

If $type(q) = \mathbf{integer}$, then

$$\left\{\sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|\right\} q := |0\rangle\{P\}$$

(Ax-UT) $\{U^\dagger PU\}\overline{q} := U[\overline{q}]\{P\}$

(R-SC) $$\frac{\{P\}S_1\{Q\} \quad \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}$$

(R-IF) $$\frac{\{P_m\}S_m\{Q\} \text{ for all } m}{\left\{\sum_m M_m^\dagger P_m M_m\right\} \mathbf{if}\ (\square m \cdot M[\overline{q}] = m \to S_m)\ \mathbf{fi}\{Q\}}$$

(R-LP) $$\frac{\{Q\}S\left\{M_0^\dagger PM_0 + M_1^\dagger QM_1\right\}}{\{M_0^\dagger PM_0 + M_1^\dagger QM_1\}\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}\{P\}}$$

(R-Or) $$\frac{P \sqsubseteq P' \quad \{P'\}S\{Q'\} \quad Q' \sqsubseteq Q}{\{P\}S\{Q\}}$$

FIGURE 4.2

Proof system *qPD* of partial correctness.

Theorem 4.2.1 (Soundness). *The proof system qPD is sound for partial correctness of quantum **while**-programs; that is, for any quantum **while**-program S and quantum predicates $P, Q \in \mathcal{P}(\mathcal{H}_{all})$, we have:*

$$\vdash_{qPD} \{P\}S\{Q\} \ \textit{implies}\ \models_{par} \{P\}S\{Q\}.$$

Proof. We only need to show that the axioms of *qPD* are valid in the sense of partial correctness and inference rules of *qPD* preserve partial correctness.

- (Ax-Sk) It is obvious that $\models_{par} \{P\}\mathbf{skip}\{P\}$.
- (Ax-In) We only prove the case of $type(q) = \mathbf{integer}$, and the case of $type(q) = \mathbf{Boolean}$ is similar. For any $\rho \in \mathcal{D}(\mathcal{H}_{all})$, it follows from Proposition 3.3.1 (ii) that

$$\begin{aligned} tr\left[\left(\sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|\right)\rho\right] &= \sum_{n=-\infty}^{\infty} tr(|n\rangle_q\langle 0|P|0\rangle_q\langle n|\rho) \\ &= \sum_{n=-\infty}^{\infty} tr(P|0\rangle_q\langle n|\rho|n\rangle_q\langle 0|) \\ &= tr\left(P\sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|\right) \\ &= tr(P[\![q := |0\rangle]\!](\rho)). \end{aligned}$$

  Therefore, we have:

$$\models_{par} \left\{\sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|\right\} q := |0\rangle \{P\}.$$

- (Ax-UT) It is easy to see that

$$\models_{par} \{U^\dagger P U\}\overline{q} := U[\overline{q}]\{P\}.$$

- (R-SC) If $\models_{par} \{P\}S_1\{Q\}$ and $\models_{par} \{Q\}S_2\{R\}$, then for any $\rho \in \mathcal{D}(\mathcal{H}_{all})$ we have:

$$\begin{aligned} tr(P\rho) &\le tr(Q[\![S_1]\!](\rho)) + [tr(\rho) - tr([\![S_1]\!](\rho))] \\ &\le tr(R[\![S_2]\!]([\![S_1]\!](\rho))) + [tr([\![S_1]\!](\rho)) - tr([\![S_2]\!]([\![S_1]\!](\rho)))] \\ &\qquad + [tr(\rho) - tr([\![S_1]\!](\rho))] \\ &= tr(R[\![S_1; S_2]\!](\rho)) + [tr(\rho) - tr([\![S_1; S_2]\!](\rho))]. \end{aligned}$$

  Therefore, $\models_{par} \{P\}S_1; S_2\{R\}$ holds as desired.
- (R-IF) Assume that $\models_{par} \{P_m\}S_m\{Q\}$ for all possible measurement outcomes m. Then for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, since

$$\sum_m M_m^\dagger M_m = I_{\mathcal{H}_{\overline{q}}},$$

it holds that

$$\begin{aligned}
&tr\left(\sum_m M_m^\dagger P_m M_m \rho\right) = \sum_m tr(M_m^\dagger P_m M_m \rho)\\
&= \sum_m tr(P_m M_m \rho M_m^\dagger)\\
&\le \sum_m \left\{ tr(Q[\![S_m]\!](M_m \rho M_m^\dagger)) + [tr(M_m \rho M_m^\dagger) - tr([\![S_m]\!](M_m \rho M_m^\dagger))] \right\}\\
&\le \sum_m tr\left(Q[\![S_m]\!](M_m \rho M_m^\dagger)\right) + \left[\sum_m tr(M_m \rho M_m^\dagger) - \sum_m tr([\![S_m]\!](M_m \rho M_m^\dagger))\right]\\
&= tr\left(Q \sum_m [\![S_m]\!](M_m \rho M_m^\dagger)\right) + \left[tr\left(\sum_m \rho M_m^\dagger M_m\right) - tr\left(\sum_m [\![S_m]\!](M_m \rho M_m^\dagger)\right)\right]\\
&= tr(Q[\![\mathbf{if}\ldots\mathbf{fi}]\!](\rho)) + [tr(\rho) - tr([\![\mathbf{if}\ldots\mathbf{fi}]\!](\rho)],
\end{aligned}$$

and

$$\models_{par} \left\{\sum_m M_m^\dagger P_m M_m\right\} \mathbf{if}\ldots\mathbf{fi}\{Q\},$$

where **if**$\ldots$**fi** is an abbreviation of statement "**if** $(\square m \cdot M[\overline{q}] = m \to S_m)$ **fi**".

- (R-LP) Suppose that

$$\models_{par} \{Q\} S \left\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\right\}.$$

Then for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, it holds that

$$tr(Q\rho) \le tr((M_0^\dagger P M_0 + M_1^\dagger Q M_1)[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]. \tag{4.11}$$

Furthermore, we have:

$$\begin{aligned}
tr\left[\left(M_0^\dagger P M_0 + M_1^\dagger Q M_1\right)\rho\right] \le &\sum_{k=0}^{n} tr\left(P\left(\mathcal{E}_0 \circ ([\![S]\!] \circ \mathcal{E}_1)^k\right)(\rho)\right)\\
&+ tr\left(Q\left(\mathcal{E}_1 \circ \left([\![S]\!] \circ \mathcal{E}_1\right)^n\right)(\rho)\right)\\
&+ \sum_{k=0}^{n-1}\left[tr(\mathcal{E}_1 \circ ([\![S]\!] \circ \mathcal{E}_1)^k(\rho)) - tr\left(([\![S]\!] \circ \mathcal{E}_1)^{k+1}(\rho)\right)\right]
\end{aligned} \tag{4.12}$$

for all $n \ge 1$. In fact, equation (4.12) may be proved by induction on n. The case of $n = 1$ is obvious. Using equation (4.11), we obtain:

$$
\begin{aligned}
tr\left(Q\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^n\right)(\rho)\right) &\le tr\left(\left(M_0^\dagger PM_0+M_1^\dagger QM_1\right)(\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}(\rho)\right)\\
&\quad+\left[tr\left(\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^n\right)(\rho)\right)-tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}(\rho)\right)\right]\\
&= tr\left(P\left(\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}\right)(\rho)\right)+tr\left(Q\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}\right)(\rho)\right)\\
&\quad+\left[tr\left(\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^n\right)(\rho)\right)-tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}(\rho)\right)\right].
\end{aligned}
\tag{4.13}
$$

Combining equations (4.12) and (4.13), we assert that

$$
\begin{aligned}
tr\left[\left(M_0^\dagger PM_0+M_1^\dagger QM_1\right)\rho\right] &\le \sum_{k=0}^{n+1} tr\left(P\left(\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k\right)(\rho)\right)\\
&\quad+tr\left(Q\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^{n+1}\right)(\rho)\right)\\
&\quad+\sum_{k=0}^{n}\left[tr\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right)-tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^{k+1}(\rho)\right)\right].
\end{aligned}
$$

Therefore, equation (4.12) holds in the case of $n+1$ provided it is true in the case of n, and we complete the proof of equation (4.12).
Now we note that

$$
\begin{aligned}
tr\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right) &= tr\left(M_1(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)M_1^\dagger\right)\\
&= tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)M_1^\dagger M_1\right)\\
&= tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\left(I-M_0^\dagger M_0\right)\right)\\
&= tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right)-tr\left((\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k)(\rho)\right).
\end{aligned}
$$

Then it follows that

$$
\begin{aligned}
\sum_{k=0}^{n-1}\left[tr\left(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right)-tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^{k+1}(\rho)\right)\right] &= \sum_{k=0}^{n-1} tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right)\\
&\quad-\sum_{k=0}^{n-1}\left[tr\left(\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right)-\sum_{k=0}^{n-1} tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^{k+1}(\rho)\right)\right]\\
&= tr(\rho)-tr\left((\llbracket S\rrbracket\circ\mathcal{E}_1)^n(\rho)\right)-\sum_{k=0}^{n-1} tr\left(\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^k(\rho)\right).
\end{aligned}
\tag{4.14}
$$

On the other hand, we have:

$$
\begin{aligned}
tr(Q(\mathcal{E}_1\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)) &= tr(QM_1(\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)M_1^\dagger)\\
&\le tr(M_1(\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)M_1^\dagger)\\
&= tr((\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)M_1^\dagger M_1)\\
&= tr((\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)(I-M_0^\dagger M_0))\\
&= tr((\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho))-tr((\mathcal{E}_0\circ(\llbracket S\rrbracket\circ\mathcal{E}_1)^n)(\rho)).
\end{aligned}
\tag{4.15}
$$

Putting equations (4.14) and (4.15) into equation (4.12), we obtain:

$$\begin{aligned} tr\left[(M_0^\dagger P M_0 + M_1^\dagger Q M_1)\rho\right] &\le \sum_{k=0}^{n} tr\left(P(\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^k)(\rho)\right) \\ &\quad + \left[tr(\rho) - \sum_{k=0}^{n} tr((\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^k)(\rho))\right] \\ &= tr\left(P \sum_{k=0}^{n} (\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^k)(\rho)\right) \\ &\quad + \left[tr(\rho) - tr\left(\sum_{k=0}^{n} (\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^k)(\rho)\right)\right]. \end{aligned}$$

Let $n \to \infty$. Then it follows that

$$tr\left[(M_0^\dagger P M_0 + M_1^\dagger Q M_1)\rho\right] \le tr(P\llbracket \textbf{while} \rrbracket(\rho) + [tr(\rho) - tr(\llbracket \textbf{while} \rrbracket(\rho))]$$

and

$$\models_{par} \{M_0^\dagger P M_0 + M_1^\dagger Q M_1\} \textbf{while} \{P\},$$

where **while** is an abbreviation of quantum loop "**while** $M[\overline{q}] = 1$ **do** S".

- (R-Or) The validity of this rule follows immediately from Lemma 4.1.2 and Definition 4.2.2. □

Now we are going to establish completeness for the proof system *qPD* with respect to the semantics of partial correctness:

- truth of a quantum program in the sense of partial correctness implies its provability in the proof system *qPD*.

Note that the Löwner ordering assertions between quantum predicates in the rule (R-Or) are statements about complex numbers. So, only a completeness of *qPD* relative to the theory of the field of complex numbers may be anticipated; more precisely, we can add all statements that are true in the field of complex numbers into *qPD* in order to make it complete. The following theorem should be understood exactly in the sense of such a relative completeness.

Theorem 4.2.2 (Completeness). *The proof system qPD is complete for partial correctness of quantum* ***while****-programs; that is, for any quantum* ***while****-program S and quantum predicates* $P, Q \in \mathcal{P}(\mathcal{H}_{all})$*, we have:*

$$\models_{par} \{P\}S\{Q\} \text{ implies } \vdash_{qPD} \{P\}S\{Q\}.$$

Proof. If $\models_{par} \{P\}S\{Q\}$, then by Definition 4.2.3 (ii) we have $P \sqsubseteq wlp.S.Q$. Therefore, by the rule (R-Or) it suffices to prove the following:

- Claim:

$$\vdash_{qPD} \{wlp.S.Q\}S\{Q\}.$$

We proceed by induction on the structure of S to prove this claim.

- Case 1. $S \equiv$ **skip**. Immediate from the axiom (Ax-Sk).
- Case 2. $S \equiv q := 0$. Immediate from the axiom (Ax-In).
- Case 3. $S \equiv \overline{q} := U[\overline{q}]$. Immediate from the axiom (Ax-UT).
- Case 4. $S \equiv S_1; S_2$. It follows from the induction hypothesis on S_1 and S_2 that

$$\vdash_{qPD} \{wlp.S_1.(wlp.S_2.Q)\}S_1\{wlp.S_2.Q\}$$

and

$$\vdash_{qPD} \{wlp.S_2.Q\}S_2\{Q\}.$$

We obtain:

$$\vdash_{qPD} \{wlp.S_1.(wlp.S_2.Q)\}S_1; S_2\{Q\}$$

by the rule (R-SC). Then with Proposition 4.2.3 (iv) we see that

$$\vdash_{qPD} \{wlp.S_1; S_2.Q\}S_1; S_2\{Q\}.$$

- Case 5. $S \equiv$ **if** $(\square m \cdot M[\overline{q}] = m \to S_m)$ **fi**. For all m, by the induction hypothesis on S_m we obtain:

$$\vdash_{qPD} \{wlp.S_m.Q\}S_m\{Q\}.$$

Then applying the rule (R-IF) yields:

$$\vdash_{qPD} \left\{\sum_m M_m^\dagger (wlp.S_m.Q)M_m\right\} \textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}\{Q\},$$

and using Proposition 4.2.3 (v) we have:

$$\vdash_{qPD} \{wlp.\textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}.Q\}\textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}\{Q\}.$$

- Case 6. $S \equiv$ **while** $M[\overline{q}] = 1$ **do** S' **od**. For simplicity, we write **while** for quantum loop "**while** $M[\overline{q}] = 1$ **do** S' **od**". The induction hypothesis on S asserts that

$$\vdash_{qPD} \{wlp.S.(wlp.\textbf{while}.P)\}S\{wlp.\textbf{while}.P\}.$$

By Proposition 4.2.4 (ii) we have:

$$wlp.\textbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\textbf{while}.P))M_1.$$

Then by the rule (R-LP) we obtain:

$$\vdash_{qPD} \{wlp.\mathbf{while}.P\}\mathbf{while}\{P\}$$

as desired. □

4.2.4 PROOF SYSTEM FOR TOTAL CORRECTNESS

We studied the proof system *qPD* for partial correctness of quantum **while**-programs in the last subsection. In this subsection, we further study a proof system *qTD* for total correctness of quantum **while**-programs. The only difference between *qTD* and *qPD* is the inference rule for quantum **while**-loops. In the system *qPD*, we do not need to consider termination of quantum loops. However, it is crucial in the system *qTD* to have a rule that can infer termination of quantum loops. To give the rule for total correctness of quantum loops, we need a notion of bound function which expresses the number of iterations of a quantum loop in its computation.

Definition 4.2.4. *Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate and a real number $\epsilon > 0$. A function*

$$t : \mathcal{D}(\mathcal{H}_{all}) \to \mathbb{N} \text{ (nonnegative integers)}$$

*is called a (P, ϵ)-bound function of quantum loop "***while** $M[\overline{q}] = 1$ **do** S **od**" *if it satisfies the following two conditions:*

(i) $t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right) \leq t(\rho)$*; and*

(ii) $tr(P\rho) \geq \epsilon$ *implies*

$$t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right) < t(\rho)$$

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

A bound function is also often called a ranking function in the programming theory literature. The purpose of a bound function of a loop is to warrant termination of the loop. The basic idea is that the value of the bound function is always nonnegative and it is decreased with each iteration of the loop, and thus the loop should terminate after a finite number of iterations. A bound function t of a classical loop "**while** B **do** S **od** " is required to satisfy the inequality

$$t(\llbracket S \rrbracket(s)) < t(s)$$

for any input state s. It is interesting to compare this inequality with conditions (i) and (ii) of the previous definition. We see that the conditions (i) and (ii) are two inequalities between

$$t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right)$$

and $t(\rho)$, but not between $t([\![S]\!](\rho))$ and $t(\rho)$. This is because in the implementation of the quantum loop "**while** $M[\overline{q}] = 1$ **do** S **od**", we need to perform the yes-no measurement M on ρ when checking the loop guard "$M[\overline{q}] = 1$", and the states of quantum variables will become $M_1 \rho M_1^\dagger$ from ρ whence the measurement outcome "yes" is observed.

The following lemma gives a characterization of the existence of a bound function of a quantum loop in terms of the limit of the state of quantum variables when the number of iterations of the loop goes to infinity. It provides a key step for the proof of soundness and completeness of the proof system *qTD*.

Lemma 4.2.1. *Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate. Then the following two statements are equivalent:*

(i) *for any $\epsilon > 0$, there exists a (P, ϵ)-bound function t_ϵ of the* **while***-loop "***while** $M[\overline{q}] = 1$ **do** S **od**";*

(ii) $\lim_{n\to\infty} tr\left(P([\![S]\!] \circ \mathcal{E}_1)^n(\rho)\right) = 0$ *for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$.*

Proof. (i) $\Rightarrow$ (ii) We prove this implication by refutation. If

$$\lim_{n\to\infty} tr\left(P([\![S]\!] \circ \mathcal{E}_1)^n(\rho)\right) \neq 0,$$

then there exist $\epsilon_0 > 0$ and a strictly increasing sequence $\{n_k\}$ of nonnegative integers such that

$$tr\left(P([\![S]\!] \circ \mathcal{E}_1)^{n_k}(\rho)\right) \geq \epsilon_0$$

for all $k \geq 0$. Thus, we have a (P, ϵ_0)-bound function of loop "**while** $M[\overline{q}] = 1$ **do** S **od**". For each $k \geq 0$, we set

$$\rho_k = ([\![S]\!] \circ \mathcal{E}_1)^{n_k}(\rho).$$

Then it holds that $tr(P\rho_k) \geq \epsilon_0$, and by conditions (i) and (ii) in Definition 4.2.4 we obtain:

$$\begin{aligned} t_{\epsilon_0}(\rho_k) &> t_{\epsilon_0}\left([\![S]\!](M_1 \rho_k M_1^\dagger)\right) \\ &= t_{\epsilon_0}\left(\left([\![S]\!] \circ \mathcal{E}_1\right)(\rho_k)\right) \\ &\geq t_{\epsilon_0}\left(\left([\![S]\!] \circ \mathcal{E}_1\right)^{n_{k+1}-n_k}(\rho_k)\right) \\ &= t_{\epsilon_0}(\rho_{k+1}). \end{aligned}$$

Consequently, we have an infinitely descending chain $\{t_{\epsilon_0}(\rho_k)\}$ in $\mathbb{N}$. This is a contradiction because $\mathbb{N}$ is a well-founded set.

(ii) $\Rightarrow$ (i) For each $\rho \in \mathcal{D}(\mathcal{H}_{all})$, if

$$\lim_{n\to\infty} tr\left(P([\![S]\!] \circ \mathcal{E}_1)^n(\rho)\right) = 0,$$

then for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) < \epsilon$$

for all $n \geq N$. We define:

$$t_\epsilon(\rho) = \min\left\{N \in \mathbb{N} : tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) < \epsilon \text{ for all } n \geq N\right\}.$$

Now it suffices to show that t_ϵ is a (P, ϵ)-bound function of loop "**while** $M[\overline{q}] = 1$ **do** S **od**". To this end. we consider the following two cases:

- Case 1. $tr(P\rho) \geq \epsilon$. Suppose that $t_\epsilon(\rho) = N$. Then $tr(P\rho) \geq \epsilon$ implies $N \geq 1$. By the definition of t_ϵ, we assert that

  $$tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) < \epsilon$$

  for all $n \geq N$. Thus, for all $n \geq N - 1 \geq 0$,

  $$tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n\left(\llbracket S \rrbracket\left(M_1^\dagger \rho M_1\right)\right)\right) = tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^{n+1}(\rho)\right) < \epsilon.$$

  Therefore, we have:

  $$t_\epsilon\left(\llbracket S \rrbracket\left(M_1^\dagger \rho M_1\right)\right) \leq N - 1 < N = t_\epsilon(\rho).$$

- Case 2. $tr(P\rho) < \epsilon$. Again, suppose that $t_\epsilon(\rho) = N$. Now we have the following two sub-cases:
  - ▶ Subcase 2.1. $N = 0$. Then for all $n \geq 0$, it holds that

    $$tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) < \epsilon.$$

    Furthermore, it is easy to see that

    $$t_\epsilon\left(\llbracket S \rrbracket\left(M_1 \rho M_1^\dagger\right)\right) = 0 = t_\epsilon(\rho).$$

  - ▶ Subcase 2.2. $N \geq 1$. We can derive that

    $$t_\epsilon(\rho) > t_\epsilon\left(\llbracket S \rrbracket\left(M_1 \rho M_1^\dagger\right)\right)$$

    in the way of Case 1. □

Now we are ready to present the proof system *qTD* for total correctness of quantum **while**-programs. As mentioned before, the system *qTD* differs from the proof system *qPD* for partial correctness of quantum programs only in the inference rule for loops. More precisely, the proof system *qTD* consists of the axioms (Ax-Sk), (Ax-In) and (Ax-UT) and inference rules (R-SC), (R-IF) and (R-Or) in Figure 4.2 as well as inference rule (R-LT) in Figure 4.3.

$$\text{(R-LT)}\quad \frac{\begin{array}{l}\bullet\ \{Q\}S\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\\ \bullet\ \text{for each } \epsilon > 0,\ t_\epsilon \text{ is a } (M_1^\dagger Q M_1, \epsilon)\text{-bound function}\\ \quad\ \text{of loop } \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od}\end{array}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od}\{P\}}$$

FIGURE 4.3

Proof system *qTD* of total correctness.

An application of the rule (R-LT) to prove total correctness of the Grover search algorithm will be presented in Subsection 4.2.5 following.

The remainder of this subsection is devoted to establishing soundness and completeness of *qTD*:

- provability of a correctness formula in the proof system *qTD* is equivalent to its truth in the sense of total correctness.

We write:

$$\vdash_{qTD} \{P\}S\{Q\}$$

whenever the correctness formula $\{P\}S\{Q\}$ can be derived by a finite number of applications of the axioms and inference rules in *qTD*.

Theorem 4.2.3 (Soundness). *The proof system qTD is sound for total correctness of quantum* ***while****-programs; that is, for any quantum program S and quantum predicates* $P, Q \in \mathcal{P}(\mathcal{H}_{all})$*, we have:*

$$\vdash_{qTD} \{P\}S\{Q\} \ \textit{implies}\ \models_{tot} \{P\}S\{Q\}.$$

Proof. It suffices to show that the axioms of *qTD* are valid in the sense of total correctness, and inference rules of *qTD* preserve total correctness.

The proof for soundness of (Ax-Sk), (Ax-In) and (Ax-UT) is similar to the case of partial correctness. The proof of the remaining inference rules are given as follows:

- (R-SC) Suppose that $\models_{tot} \{P\}S_1\{Q\}$ and $\models_{tot} \{Q\}S_2\{R\}$. Then for any $\rho \in \mathcal{D}(\mathcal{H}_{all})$, with Proposition 3.3.1 (iv) we obtain:

$$\begin{aligned} tr(P\rho) &\le tr(Q[\![S_1]\!](\rho))\\ &\le tr(R[\![S_2]\!]([\![S_1]\!](\rho)))\\ &= tr(P[\![S_1; S_2]\!](\rho)).\end{aligned}$$

  Therefore, $\models_{tot} \{P\}S_1; S_2\{R\}$.
- (R-IF) Suppose that $\models_{tot} \{P_m\}S_m\{Q\}$ for all possible measurement outcomes m. Then for any $\rho \in \mathcal{D}(\mathcal{H}_{all})$, it holds that

$$tr\left(P_m M_m \rho M_m^\dagger\right) \leq tr\left(Q[\![S_m]\!]\left(M_m \rho M_m^\dagger\right)\right).$$

Therefore, we have:

$$\begin{aligned} tr\left(\sum_m M_m^\dagger P_m M_m \rho\right) &= \sum_m tr\left(P_m M_m \rho M_m^\dagger\right) \\ &\leq \sum_m tr\left(Q[\![S_m]\!]\left(M_m \rho M_m^\dagger\right)\right) \\ &= tr\left(Q \sum_m [\![S_m]\!]\left(M_m \rho M_m^\dagger\right)\right) \\ &= tr(Q[\![\textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}]\!](\rho)), \end{aligned}$$

and it follows that

$$\models_{tot} \left\{\sum_m M_m^\dagger P M_m\right\} \textbf{if } (\square m \cdot M[\overline{q}] = m \to S_m) \textbf{ fi}\{Q\}.$$

- (R-LT) We assume that

$$\models_{tot} \{Q\} S \left\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\right\}.$$

Then for any $\rho \in \mathcal{D}(\mathcal{H}_{all})$, we have:

$$tr(Q\rho) \leq tr\left((M_0^\dagger P M_0 + M_1^\dagger Q M_1)[\![S]\!](\rho)\right). \tag{4.16}$$

We first prove the following inequality:

$$\begin{aligned} &tr\left[\left(M_0^\dagger P M_0 + M_1^\dagger Q M_1\right)\rho\right] \\ &\leq \sum_{k=0}^{n} tr\left(P[\mathcal{E}_0 \circ ([\![S]\!] \circ \mathcal{E}_1)]^k(\rho)\right) + tr\left(Q\left[\mathcal{E}_1 \circ ([\![S]\!] \circ \mathcal{E}_1)^n\right](\rho)\right) \end{aligned} \tag{4.17}$$

by induction on n. Indeed, it holds that

$$\begin{aligned} tr\left[\left(M_0^\dagger P M_0 + M_1^\dagger Q M_1\right)\rho\right] &= tr\left(P M_0 \rho M_0^\dagger\right) + tr\left(Q M_1 \rho M_1^\dagger\right) \\ &= tr(P\mathcal{E}_0(\rho)) + tr(Q\mathcal{E}_1(\rho)). \end{aligned}$$

So, equation (4.17) is correct for the base case of $n = 0$. Assume that equation (4.17) is correct for the case of $n = m$. Then applying equation (4.16), we obtain:

$$\begin{aligned}
tr\left[\left(M_0^\dagger P M_0 + M_1^\dagger Q M_1\right)\rho\right] &= tr(P\mathcal{E}_0(\rho)) + tr\left(QM_1\rho M_1^\dagger\right) \\
&\le \sum_{k=0}^{m} tr\left(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^k(\rho)\right) + tr\left(Q\left[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^m\right](\rho)\right) \\
&\le \sum_{k=0}^{m} tr\left(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^k(\rho)\right) \\
&\qquad + tr\left(\left(M_0^\dagger P M_0 + M_1^\dagger Q M_1\right)\llbracket S \rrbracket\left(\left[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^m\right](\rho)\right)\right) \\
&= \sum_{k=0}^{m} tr\left(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^k(\rho)\right) + tr\left(PM_0\llbracket S \rrbracket\left(\left[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^m\right](\rho)\right)M_0^\dagger\right) \\
&\qquad + tr\left(QM_1\llbracket S \rrbracket\left(\left[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^m\right](\rho)\right)M_1^\dagger\right) \\
&= \sum_{k=0}^{m+1} tr\left(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^k(\rho)\right) + tr\left(Q\left[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^{m+1}\right](\rho)\right).
\end{aligned}$$

Therefore, equation (4.17) also holds for the case of $n = m + 1$. This completes the proof of equation (4.17).

Now, since for any $\epsilon > 0$, there exists $(M_1^\dagger Q M_1, \epsilon)$-bound function t_ϵ of quantum loop "**while** $M[\overline{q}] = 1$ **do** S **od**", by Lemma 4.2.1 we obtain:

$$\begin{aligned}
\lim_{n\to\infty} tr(Q[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)) &= \lim_{n\to\infty} tr(QM_1(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)M_1^\dagger) \\
&= \lim_{n\to\infty} tr(M_1^\dagger Q M_1(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)) \\
&= 0.
\end{aligned}$$

Consequently, it holds that

$$\begin{aligned}
tr[(M_0^\dagger P M_0 + M_1^\dagger Q M_1)\rho] &\le \lim_{n\to\infty} \sum_{k=0}^{n} tr(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^k(\rho)) \\
&\qquad + \lim_{n\to\infty} tr(Q[\mathcal{E}_1 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^n](\rho)) \\
&= \sum_{n=0}^{\infty} tr(P[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)]^n(\rho)) \\
&= tr\left(P\sum_{n=0}^{\infty}[\mathcal{E}_0 \circ (\llbracket S \rrbracket \circ \mathcal{E}_1)^n](\rho)\right) \\
&= tr\left(P\llbracket \textbf{while } M[\overline{q}] = 1 \textbf{ do } S \textbf{ od} \rrbracket(\rho)\right).
\end{aligned}$$

□

Theorem 4.2.4 (Completeness). *The proof system qTD is complete for total correctness of quantum **while**-programs; that is, for any quantum program S and quantum predicates $P, Q \in \mathcal{P}(\mathcal{H}_{all})$, we have:*

$$\models_{tot} \{P\}S\{Q\} \text{ implies } \vdash_{qTD} \{P\}S\{Q\}.$$

Proof. Similar to the case of partial correctness, it suffices to prove the following:

- Claim:

$$\vdash_{qTD} \{wp.S.Q\}S\{Q\}$$

for any quantum program S and quantum predicate $P \in \mathcal{P}(\mathcal{H}_{all})$, because by Definition 4.2.3 (i) we have $P \sqsubseteq wp.S.Q$ when $\models_{tot} \{P\}S\{Q\}$. This claim can be proved by induction on the structure of S. We only consider the case of $S \equiv$ **while** $M[\overline{q}] = 1$ **do** S' **od**. The other cases are similar to the proof of Theorem 4.2.2.

We write **while** for quantum loop "**while** $M[\overline{q}] = 1$ **do** S' **od**". It follows from Proposition 4.2.4(i) that

$$wp.\mathbf{while}.Q = M_0^\dagger Q M_0 + M_1^\dagger (wp.S'.(wp.\mathbf{while}.Q))M_1.$$

So, our aim is to derive that

$$\vdash_{qTD} \left\{M_0^\dagger Q M_0 + M_1^\dagger (wp.S'.(wp.\mathbf{while}.Q))M_1\right\} \mathbf{while}\{Q\}.$$

By the induction hypothesis on S' we get:

$$\vdash_{qTD} \left\{wp.S'.(wp.\mathbf{while}.Q)\right\} S'\{wp.\mathbf{while}.Q\}.$$

Then by the rule (R-LT) it suffices to show that for any $\epsilon > 0$, there exists a $(M_1^\dagger (wp.S'.(wp.\mathbf{while}.Q))M_1, \epsilon)$-bound function of the quantum loop **while**. Applying Lemma 4.2.1, we only need to prove:

$$\lim_{n\to\infty} tr\left(M_1^\dagger (wp.S'.(wp.\mathbf{while}.Q))M_1 (\llbracket S' \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) = 0. \tag{4.18}$$

The proof of equation (4.18) is carried out in two steps. First, by Propositions 4.2.2 (iv) and 3.3.1 (iv) we observe:

$$\begin{aligned} & tr\left(M_1^\dagger(wp.S'.(wp.\mathbf{while}.Q))M_1([\![S']\!]\circ\mathcal{E}_1)^n(\rho)\right) \\ &= tr\left(wp.S'.(wp.\mathbf{while}.Q)M_1([\![S']\!]\circ\mathcal{E}_1)^n(\rho)M_1^\dagger\right) \\ &= tr\left(wp.\mathbf{while}.Q[\![S']\!]\left(M_1([\![S']\!]\circ\mathcal{E}_1)^n(\rho)M_1^\dagger\right)\right) \\ &= tr\left(wp.\mathbf{while}.Q([\![S']\!]\circ\mathcal{E}_1)^{n+1}(\rho)\right) \\ &= tr\left(Q[\![\mathbf{while}]\!]([\![S']\!]\circ\mathcal{E}_1)^{n+1}(\rho)\right) \\ &= \sum_{k=n+1}^{\infty} tr\left(Q\left[\mathcal{E}_0\circ([\![S']\!]\circ\mathcal{E}_1)^k\right](\rho)\right). \end{aligned} \tag{4.19}$$

Secondly, we consider the following infinite series of nonnegative real numbers:

$$\sum_{n=0}^{\infty} tr\left(Q\left[\mathcal{E}_0\circ([\![S']\!]\circ\mathcal{E}_1)^k\right](\rho)\right) = tr\left(Q\sum_{n=0}^{\infty}\left[\mathcal{E}_0\circ([\![S']\!]\circ\mathcal{E}_1)^k\right](\rho)\right). \tag{4.20}$$

Since $Q \sqsubseteq I_{\mathcal{H}_{all}}$, it follows from Propositions 3.3.1 (iv) and 3.3.4 that

$$\begin{aligned} tr\left(Q\sum_{n=0}^{\infty}\left[\mathcal{E}_0\circ([\![S']\!]\circ\mathcal{E}_1)^k\right](\rho)\right) &= tr(Q[\![\mathbf{while}]\!](\rho)) \\ &\le tr([\![\mathbf{while}]\!](\rho)) \\ &\le tr(\rho) \le 1. \end{aligned}$$

Therefore, the infinite series in equation (4.20) converges. Note that equation (4.19) is the sum of the remaining terms of the infinite series in equation (4.20) after the nth term. Then convergence of the infinite series in equation (4.20) implies equation (4.18), and we complete the proof. □

It should be pointed out that, as remarked for Theorem 4.2.2, the preceding theorem is also merely a relative completeness of the proof system *qTD* with respect to the theory of the fields of complex numbers because, except that the rule (R-Or) is employed in *qTD*, the existence of bound functions in the rule (R-LT) is a statement about complex numbers too.

4.2.5 AN ILLUSTRATIVE EXAMPLE: REASONING ABOUT THE GROVER ALGORITHM

In the last two subsections, we developed the proof system *qPD* for partial correctness and *qTD* for total correctness of quantum **while**-programs, and established their soundness and (relative) completeness. The purpose of this subsection is to show how

the proof systems *qPD* and *qTD* can actually be used to verify correctness of quantum programs. We consider the Grover quantum search algorithm as an example.

Recall from Subsection 2.3.3 and Section 3.5 the search problem can be stated as follows. The search space consists of $N = 2^n$ elements, indexed by numbers $0, 1, \ldots, N-1$. It is assumed that the search problem has exactly L solutions with $1 \leq L \leq \frac{N}{2}$, and we are supplied with an oracle – a black box with the ability to recognize solutions to the search problem. Each element $x \in \{0, 1, \ldots, N-1\}$ is identified with its binary representation $x \in \{0,1\}^n$. In the quantum **while**-language, the Grover algorithm solving this problem can be written as the program *Grover* in Figure 4.4, where:

- **Program:**

1. $q_0 := |0\rangle;\ q_1 := |0\rangle;\ \ldots\ldots;\ q_{n-1} := |0\rangle;$
2. $q := |0\rangle;$
3. $r := |0\rangle;$
4. $q := X[q];$
5. $q_0 := H[q_0];\ q_1 := H[q_1];\ \ldots\ldots;\ q_{n-1} := H[q_{n-1}];$
6. $q := H[q];$
7. **while** $M[r] = 1$ **do** D **od**;
8. **if** $(\square x \cdot M'[q_0, q_1, \ldots, q_{n-1}] = x \rightarrow$ **skip**$)$ **fi**

FIGURE 4.4

Quantum search program *grover*.

- $q_0, q_1, \ldots, q_{n-1}, q$ are quantum variables with type **Boolean** and r with type **integer**;
- X is the NOT gate and H the Hadamard gate;
- $M = \{M_0, M_1\}$ is a measurement with

$$M_0 = \sum_{l \geq k} |l\rangle_r \langle l|, \quad M_1 = \sum_{l < k} |l\rangle_r \langle l|,$$

and k being a positive integer in the interval $\left[\frac{\pi}{2\theta} - 1, \frac{\pi}{2\theta}\right]$ with θ being determined by the equation

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-L}{2}}\ (0 \leq \theta \leq \frac{\pi}{2});$$

- M' is the measurement in the computational basis of n qubits; that is,

$$M' = \{M'_x : x \in \{0,1\}^n\}$$

with $M'_x = |x\rangle\langle x|$ for every x;

- D is the subprogram given in Figure 4.5.

- **Loop Body:**

1. $q_0, q_1, \ldots, q_{n-1}, q := O[q_0, q_1, \ldots, q_{n-1}, q]$;
2. $q_0 := H[q_0]$; $q_1 := H[q_1]$; $\ldots\ldots$; $q_{n-1} := H[q_{n-1}]$;
3. $q_0, q_1, \ldots, q_{n-1} := Ph[q_0, q_1, \ldots, q_{n-1}]$;
4. $q_0 := H[q_0]$; $q_1 := H[q_1]$; $\ldots\ldots$; $q_{n-1} := H[q_{n-1}]$;
5. $r := r + 1$

FIGURE 4.5

Loop body D.

In Figure 4.5, O is the oracle represented by the unitary operator on $n+1$ qubits:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

for all $x \in \{0,1\}^n$ and $q \in \{0,1\}$, where $f : \{0,1\}^n \to \{0,1\}$ defined by

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution,} \\ 0 & \text{otherwise} \end{cases}$$

is the characteristic function of solutions. The gate Ph is a conditional phase shift:

$$|0\rangle \to |0\rangle, \quad |x\rangle \to -|x\rangle \text{ for all } x \neq 0;$$

that is, $Ph = 2|0\rangle\langle 0| - I$.

Correctness Formula for Grover Search:

It was shown in Subsection 2.3.3 that the Grover algorithm can achieve success probability

$$\Pr(\text{success}) = \sin^2\left(\frac{2k+1}{2}\theta\right) \geq \frac{N-L}{N}$$

where k is the integer closest to the real number

$$\frac{\arccos\sqrt{\frac{L}{N}}}{\theta};$$

that is, k is an integer in the interval $\left[\frac{\pi}{2\theta} - 1, \frac{\pi}{2\theta}\right]$. The success probability is at least one-half because $L \leq \frac{N}{2}$. In particular, if $L \ll N$, then it is very high. Using the ideas introduced in the previous subsections, this fact can be expressed by the total correctness of the program *Grover*:

$$\models_{tot} \{p_{succ} I\} Grover \{P\},$$

where the precondition is the product of the success probability $p_{succ} \stackrel{\triangle}{=} \Pr(\text{success})$ and the identity operator:

$$I = \bigotimes_{i=0}^{n-1} I_{q_i} \otimes I_q \otimes I_r,$$

and the postcondition is defined by

$$P = \left(\sum_{t \text{ solution}} |t\rangle_{\overline{q}}\langle t| \right) \otimes I_q \otimes I_r,$$

I_{q_i} $(i = 0, 1, \ldots, n-1)$ and I_q are the identity operator in $\mathcal{H}_2$ (type **Boolean**), I_r is the identity operator in $\mathcal{H}_\infty$ (type **integer**) and $\overline{q} = q_0, q_1, \ldots, q_{n-1}$.

To avoid an overly complicated calculation, we choose to consider a very special case: $L = 1$ and $k = \frac{\pi}{2\theta} - \frac{1}{2}$ is the midpoint of the interval $\left[\frac{\pi}{2\theta} - 1, \frac{\pi}{2\theta}\right]$. In this case, there is a unique solution, say s, and the postcondition

$$P = |s\rangle_{\overline{q}}\langle s| \otimes I_q \otimes I_r.$$

Also, we have $p_{succ} = 1$. So, what we need to prove is then simply

$$\models_{tot} \{I\} Grover \{P\}.$$

By the soundness of *qTD* (Theorem 4.2.3), it suffices to show that

$$\vdash_{qTD} \{I\} Grover \{P\}. \tag{4.21}$$

We can prove it by using the proof rules presented in Figures 4.2 and 4.3.

Verification of Loop Body D:

For better understanding, we divide the proof of equation (4.21) into several steps. First, we verify the loop body D given in Figure 4.5. For this purpose, the following simple lemma is useful.

Lemma 4.2.2. *For each $i = 1, 2, \ldots, n$, suppose that $\overline{q}_i$ is a quantum register and U_i is a unitary operator in $\mathcal{H}_{\overline{q}_i}$. Let $U = U_n \ldots U_2 U_1$, where U_i actually stands for its cylinder extension in $\bigotimes_{i=1}^{n} \mathcal{H}_{\overline{q}_i}$ for every $i \leq n$. Then for any quantum predicate P, we have:*

$$\vdash_{qPD} \{U^\dagger P U\} \overline{q}_1 := U_1[\overline{q}_1]; \overline{q}_2 := U_2[\overline{q}_2]; \ldots; \overline{q}_n := U_n[\overline{q}_n] \{P\}.$$

Proof. By repeatedly using the axiom (Ax-UT). □

With the previous lemma, we can prove the correctness of loop body D. First, it is easy to see that

$$\sum_{t \in \{0,q\}^n} {M'_t}^\dagger P M'_t = P.$$

By the axiom (Ax-Sk) and the rule (R-IF) we obtain:

$$\vdash_{qTD} \{P\}\textbf{if } (\square x \cdot M'[q_0, q_1, \ldots, q_{n-1}] = x \rightarrow \textbf{skip}) \textbf{ fi}\{P\} \tag{4.22}$$

We put:

$$P' = |s\rangle_{\overline{q}}\langle s| \otimes |-\rangle_q\langle -| \otimes |k\rangle_r\langle k|,$$

$$|\psi_l\rangle = \cos\left[\frac{\pi}{2} + (l-k)\theta\right]|\alpha\rangle + \sin\left[\frac{\pi}{2} + (l-k)\theta\right]|s\rangle$$

for every integer l, and

$$Q = \sum_{l<k}(|\psi_l\rangle_{\overline{q}}\langle\psi_l| \otimes |-\rangle_q\langle -| \otimes |l\rangle_r\langle l|).$$

Then we have:

$$M_0^\dagger P' M_0 + M_1^\dagger Q M_1 = \sum_{l\leq k}(|\psi_l\rangle_{\overline{q}}\langle\psi_l| \otimes |-\rangle_q\langle -| \otimes |l\rangle_r\langle l|),$$

$$\begin{aligned}(G^\dagger \otimes I_q \otimes U_{+1}^\dagger)(M_0^\dagger P' M_0 + M_1^\dagger Q M_1)(G \otimes I_q \otimes U_{+1}) \\ = \sum_{l\leq k}(|\psi_{l-1}\rangle_{\overline{q}}\langle\psi_{l-1}| \otimes |-\rangle_q\langle -| \otimes |l-1\rangle_r\langle l-1|) \\ = Q\end{aligned}$$

where G is the Grover rotation defined in Figure 2.2 (see Subsection 2.3.3). Thus, it follows from Lemma 4.2.2 that

$$\vdash_{qTD} \{Q\}D\{M_0^\dagger P' M_0 + M_1^\dagger Q M_1\}.$$

Termination of Loop "while $M[r] = 1$ do D od":

A key step in proving the correctness of the Grover algorithm is to show termination of the loop in line 8 of Figure 4.4. We define a bound function

$$t : \mathcal{D}(\mathcal{H}_{\overline{q}} \otimes \mathcal{H}_q \otimes \mathcal{H}_r) \rightarrow \mathbb{N}$$

as follows:

- if $\rho \in \mathcal{D}(\mathcal{H}_{\overline{q}} \otimes \mathcal{H}_q \otimes \mathcal{H}_r)$ can be written as

$$\rho = \sum_{l,t=-\infty}^{\infty} \rho_{lt} \otimes |l\rangle\langle t|$$

with ρ_{lt} being an operator (but not necessarily a partial density operator) in $\mathcal{H}_{\overline{q}} \otimes \mathcal{H}_q$ for all $-\infty \leq l, t \leq \infty$, then

$$t(\rho) = k - \max\{\max(l,t)|\rho_{lt} \neq 0 \text{ and } l, t \leq k\}.$$

Then we have:

$$[\![D]\!](M_1\rho M_1^\dagger) = [\![D]\!]\left(\sum_{l,t<k}\rho_{l,t}\otimes|l\rangle_r\langle t|\right)$$
$$= \sum_{l,t<k}\left[\left(G\otimes I_q\right)\rho_{lt}\left(G^\dagger\otimes I_q\right)\otimes|l+1\rangle_r\langle t+1|\right],$$

and it follows that

$$t([\![D]\!](M_1\rho M_1^\dagger)) < t(\rho),$$

where G is the Grover rotation. So, t is a $(M_1^\dagger Q M_1, \epsilon)$-bound function for any ϵ. By the rule (R-LT) we assert that

$$\vdash_{qTD} \{M_0^\dagger P' M_0 + M_1^\dagger Q M_1\}\textbf{while } M[r]=1 \textbf{ do } D \textbf{ od}\{P'\}. \tag{4.23}$$

Correctness of the Grover Algorithm:

Finally, we can assemble all the ingredients prepared before to prove the correctness of the Grover algorithm. Using the axiom (Ax-In) we obtain:

$$\left\{\bigotimes_{i=0}^{m-1}|0\rangle_{q_i}\langle 0|\otimes\bigotimes_{i=m}^{n-1}I_{q_i}\otimes I_q\otimes I_r\right\}q_m := |0\rangle\left\{\bigotimes_{i=0}^{m}|0\rangle_{q_i}\langle 0|\otimes\bigotimes_{i=m+1}^{n-1}I_{q_i}\otimes I_q\otimes I_r\right\}$$

for $m = 0, 1, \ldots n-1$, and they can be combined by the rule (R-SC) to yield:

$$\{I\}q_0 := |0\rangle; q_1 := |0\rangle; \ldots; q_{n-1} := |0\rangle\left\{\bigotimes_{i=0}^{n-1}|0\rangle_{q_i}\langle 0|\otimes I_q\otimes I_r\right\}$$
$$q := |0\rangle\left\{\bigotimes_{i=0}^{n-1}|0\rangle_{q_i}\langle 0|\otimes|0\rangle_q\langle 0|\otimes I_r\right\}$$
$$r := |0\rangle\left\{\bigotimes_{i=0}^{n-1}|0\rangle_{q_i}\langle 0|\otimes|0\rangle_q\langle 0|\otimes|0\rangle_r\langle 0|\right\}$$
$$q := X[q]; q_0 := H[q_0]; q_1 := H[q_1]; \ldots;$$
$$q_{n-1} := H[q_{n-1}]; q := H[q]\left\{|\psi\rangle_{\overline{q}}\langle\psi|\otimes|-\rangle_q\langle -|\otimes|0\rangle_r\langle -|\right\}, \tag{4.24}$$

where

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

is the equal superposition. Note that the last part of equation (4.24) is derived by Lemma 4.2.2 and the following equality:

$$\left[\left(H^{\dagger}\right)^{\otimes n}\otimes X^{\dagger}H^{\dagger}\otimes I_r\right]\left(|\psi\rangle_{\overline{q}}\langle\psi|\otimes|-\rangle_q\langle-|\otimes|0\rangle_r\langle 0|\right)\left(H^{\otimes n}\otimes HX\otimes I_r\right)$$
$$=\bigotimes_{i=0}^{n-1}|0\rangle_{q_i}\langle 0|\otimes|0\rangle_q\langle 0|\otimes|0\rangle_r\langle 0|.$$

It is obvious that $P'\sqsubseteq P$. On the other hand, it follows from the assumption $k=\frac{\pi}{2\theta}-\frac{1}{2}$ that $|\psi\rangle=|\psi_0\rangle$. Then we obtain:

$$|\psi\rangle_{\overline{q}}\langle\psi|\otimes|-\rangle_q\langle-|\otimes|0\rangle_r\langle 0|=|\psi_0\rangle_{\overline{q}}\langle\psi_0|\otimes|-\rangle_q\langle-|\otimes|0\rangle_r\langle 0|$$
$$\sqsubseteq M_0^{\dagger}P'M_0+M_1^{\dagger}QM_1.$$

We complete the proof by using the rules (R-Or) and (R-SC) to combine equations (4.22), (4.23) and (4.24).

4.3 COMMUTATIVITY OF QUANTUM WEAKEST PRECONDITIONS

In the previous sections of this chapter, we have built a logical foundation for reasoning about correctness of quantum programs, including the quantum weakest precondition semantics and the Floyd-Hoare logic for quantum **while**-programs. This logical foundation is, of course, a generalization of the corresponding theories for classical and probabilistic programs, but it is certainly not a simple generalization. Indeed, it has to answer some problems that would not arise in the realm of classical and probabilistic programming. This section deals with one of these problems, namely (non-)commutativity of quantum predicates. The influence of other fundamental differences between quantum systems and classical systems on quantum programming will be revealed in Chapters 6 and 7 and discussed in Sections 8.5 and 8.6.

The significance of the (non-)commutativity problem of quantum predicates comes from the following observation that more than one predicate may be involved in specifying and reasoning about a complicated property of a quantum program, but:

- quantum predicates are observables, and their physical simultaneous verifiability depends on commutativity between them, according to the Heisenberg uncertainty principle (see [174], page 89).
- mathematically, a logical combination like conjunction and disjunction of two quantum predicates is well-defined only when they commute.

We consider the (non-)commutativity problem of quantum weakest preconditions defined in Section 4.1.1. For any two operators A and B in a Hilbert space $\mathcal{H}$, it is said that A and B commute if

$$AB=BA.$$

So, what concerns us is the question:

- Given a quantum operation $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ (as the denotational semantics of a quantum program). For two quantum predicates $M, N \in \mathcal{P}(\mathcal{H})$, when do $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute?

This question is interesting because one might need to deal with logical combinations of quantum predicates when reasoning about complicated quantum programs. For example, one might like to know whether the conjunction "M and N" is satisfied after a quantum program $\mathcal{E}$ is executed. Then she/he would consider whether the conjunction "$wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$" of weakest preconditions is satisfied before the program is executed. However, as pointed out previously, these conjunctions are well-defined only if the involved quantum predicates commute. (A further discussion about related issues is left as Problem 4.3.2 at the end of this section.)

Now we start to address this question. To warm up, we first see a simple example.

Example 4.3.1 (Bit flip and phase flip channels). *Bit flip and phase flip are quantum operations on a single qubit, and they are widely used in the theory of quantum error-correction. Let X, Y, Z stand for the Pauli matrices (see Example 2.2.2).*

- *The bit flip is defined by*

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger, \tag{4.25}$$

  where $E_0 = \sqrt{p} I$ and $E_1 = \sqrt{1-p} X$. It is easy to see that $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute when $MN = NM$ and $MXN = NXM$.
- *If E_1 in equation (4.25) is replaced by $\sqrt{1-p} Z$ (respectively $\sqrt{1-p} Y$), then $\mathcal{E}$ is the phase flip (respectively bit-phase flip), and $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute when $MN = NM$ and $MZN = NZM$ (respectively $MYN = NYM$).*

Secondly, we consider two simplest classes of quantum operations: unitary transformations and projective measurements.

Proposition 4.3.1

(i) *Let $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ be a unitary transformation; that is,*

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

for any $\rho \in \mathcal{D}(\mathcal{H})$, where U is a unitary operator in $\mathcal{H}$. Then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute if and only if M and N commute.

(ii) *Let $\{P_k\}$ be a projective measurement in $\mathcal{H}$; that is, $P_{k_1} P_{k_2} = \delta_{k_1 k_2} P_{k_1}$ and $\sum_k P_k = I_{\mathcal{H}}$, where*

$$\delta_{k_1 k_2} = \begin{cases} 1, & \text{if } k_1 = k_2, \\ 0, & \text{otherwise.} \end{cases}$$

If $\mathcal{E}$ is given by this measurement, with the result of the measurement unknown:

$$\mathcal{E}(\rho) = \sum_k P_k \rho P_k$$

for each $\rho \in \mathcal{D}(\mathcal{H})$, then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute if and only if $P_k M P_k$ and $P_k N P_k$ commute for all indices k.
In particular, let $\{|i\rangle\}$ be an orthonormal basis of $\mathcal{H}$. If $\mathcal{E}$ is given by the measurement in the basis $\{|i\rangle\}$:

$$\mathcal{E}(\rho) = \sum_i P_i \rho P_i,$$

where $P_i = |i\rangle\langle i|$ for each basis state $|i\rangle$, then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute for any $M, N \in \mathcal{P}(\mathcal{H})$.

Exercise 4.3.1. *Prove Proposition 4.3.1.*

After dealing with the previous example and special case, we now consider the weakest preconditions with respect to a general quantum operation $\mathcal{E}$. Unfortunately, we are only able to give some useful sufficient (but not necessary) conditions for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$.

As usual, we consider two representations of $\mathcal{E}$, namely the Kraus operator-sum representation and the system-environment model. Let us first work in the case where quantum operation $\mathcal{E}$ is given in the Kraus operator-sum form. The following proposition presents a sufficient condition for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ in the case where M and N already commute.

Proposition 4.3.2. *Suppose that $\mathcal{H}$ is finite-dimensional. Let $M, N \in \mathcal{P}(\mathcal{H})$ and they commute, i.e., there exists an orthonormal basis $\{|\psi_i\rangle\}$ of $\mathcal{H}$ such that*

$$M = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|, \quad N = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$$

where λ_i, μ_i are reals for each i ([174], Theorem 2.2), and let quantum operation $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$ be represented by the set $\{E_i\}$ of operators, i.e. $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$. If for any i, j, k, l, we have either $\lambda_k \mu_l = \lambda_l \mu_k$ or

$$\sum_m \langle\psi_k|E_i|\psi_m\rangle\langle\psi_l|E_j|\psi_m\rangle = 0,$$

then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute.

Exercise 4.3.2. *Prove Proposition 4.3.2.*

To present another sufficient condition for commutativity of quantum weakest preconditions, we need to introduce commutativity between a quantum operation and a quantum predicate.

Definition 4.3.1. *Let quantum operation $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ be represented by the set $\{E_i\}$ of operators, i.e., $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$, and let quantum predicate $M \in \mathcal{P}(\mathcal{H})$. Then we say that M and $\mathcal{E}$ commute if M and E_i commute for each i.*

It seems that in this definition commutativity between quantum predicate M and quantum program $\mathcal{E}$ depends on the choice of operators E_i in the Kraus representation of $\mathcal{E}$. Thus, one may wonder if this definition is intrinsic because the Kraus operators E_i are not unique. To address this problem, we need the following:

Lemma 4.3.1 ([174], Theorem 8.2). *(Unitary freedom in the operator-sum representation) Suppose that $\{E_i\}$ and $\{F_j\}$ are operator elements giving rise to quantum operations $\mathcal{E}$ and $\mathcal{F}$, respectively; that is,*

$$\mathcal{E} = \sum_i E_i \circ E_i^\dagger, \quad \mathcal{F} = \sum_j F_j \circ F_j^\dagger.$$

By appending zero operators to the shortest list of operation elements we may ensure that the numbers of E_i and F_j are the same. Then $\mathcal{E} = \mathcal{F}$ if and only if there exist complex numbers u_{ij} such that

$$E_i = \sum_j u_{ij} F_j$$

for all i, and $U = (u_{ij})$ is (the matrix representation of) a unitary operator.

As a simple corollary, we can see that the definition of commutativity between a quantum predicate M and a quantum operation $\mathcal{E}$ does not depend on the choice of the Kraus representation operators of $\mathcal{E}$.

Lemma 4.3.2. *The notion of commutativity between observables and quantum operations is well-defined. More precisely, suppose that $\mathcal{E}$ is represented by both $\{E_i\}$ and $\{F_j\}$:*

$$\mathcal{E} = \sum_i E_i \circ E_i^\dagger = \sum_j F_j \circ F_j^\dagger.$$

Then M and E_i commute for all i if and only if M and F_j commute for all j.

Furthermore, commutativity between observables and quantum operations is preserved by composition of quantum operations.

Proposition 4.3.3. *Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate, and let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{QO}(\mathcal{H})$ be two quantum operations. If M and $\mathcal{E}_i$ commute for $i = 1, 2$, then M commutes with the composition $\mathcal{E}_1 \circ \mathcal{E}_2$ of $\mathcal{E}_1$ and $\mathcal{E}_2$.*

Exercise 4.3.3. *Prove Proposition 4.3.3.*

The following proposition gives another sufficient condition for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ also in the case where M and N commute. This condition is presented in terms of commutativity of quantum operations and quantum predicates.

Proposition 4.3.4. *Let $M, N \in \mathcal{P}(\mathcal{H})$ be two quantum predicates, and let $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ be a quantum operation. If M and N commute, M and $\mathcal{E}$ commute, and N and $\mathcal{E}$ commute, then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute.*

Exercise 4.3.4. *Prove Proposition 4.3.4.*

Now we turn to consider the system-environment model of quantum operation:

$$\mathcal{E}(\rho) = tr_E\left[PU\left(|e_0\rangle\langle e_0| \otimes \rho\right)U^\dagger P\right] \tag{4.26}$$

for all density operators ρ in $\mathcal{H}$, where E is an environment system of which the state Hilbert space is $\mathcal{H}_E$, U is a unitary operator in $\mathcal{H}_E \otimes \mathcal{H}$, P is a projector onto a closed subspace of $\mathcal{H}_E \otimes \mathcal{H}$, and $|e_0\rangle$ is a given state in $\mathcal{H}_E$. To this end, we need two generalized notions of commutativity between linear operators.

Definition 4.3.2. *Let $M, N, A, B, C \in \mathcal{L}(\mathcal{H})$ be operators in $\mathcal{H}$. Then:*

(i) *We say that M and N (A, B, C)-commute if*

$$AMBNC = ANBMC.$$

In particular, it is simply said that M and N A-commute when M and N (A, A, A)-commute;

(ii) *We say that A and B conjugate-commute if*

$$AB^\dagger = BA^\dagger.$$

Obviously, commutativity is exactly $I_{\mathcal{H}}$-commutativity.

The next two propositions present several sufficient conditions for commutativity of quantum weakest preconditions when quantum operation $\mathcal{E}$ is given in the system-environment model.

Proposition 4.3.5. *Let quantum operation $\mathcal{E}$ be given by equation (4.26), and we write $A = PU|e_0\rangle$. Then:*

(i) *$wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute if and only if $M \otimes I_E$ and $N \otimes I_E$ $(A^\dagger, AA^\dagger, A)$-commute;*

(ii) *$wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute whenever $(M \otimes I_E)A$ and $(N \otimes I_E)A$ conjugate-commute,*

where $I_E = I_{\mathcal{H}_E}$ is the identity operator in $\mathcal{H}_E$.

Proposition 4.3.6. *Suppose that $\mathcal{H}$ is finite-dimensional. Let $\mathcal{E}$ be given by equation (4.26), and let $M, N \in \mathcal{P}(\mathcal{H})$ be quantum predicates and they commute, i.e., there exists an orthonormal basis $\{|\psi_i\rangle\}$ of $\mathcal{H}$ such that*

$$M = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|, \quad N = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$$

where λ_i, μ_i are reals for each i. If for any i, j, k, l, we have $\lambda_i\mu_j = \lambda_j\mu_i$ or

$$\langle e_0|U^\dagger P|\psi_i e_k\rangle \perp \langle e_0|U^\dagger P|\psi_j e_l\rangle,$$

then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute.

Exercise 4.3.5. *Prove Propositions 4.3.5 and 4.3.6.*

Obviously, (non-)commutativity of quantum weakest preconditions is still not fully understood. To conclude this section, we propose two problems for further studies.

Problem 4.3.1. *The main results obtained in this section for commutativity of the weakest preconditions $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ (Propositions 4.3.2, 4.3.4 and 4.3.6) deal with the special case where M and N commute. So, an interesting problem is to find a sufficient and necessary condition for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ of a general quantum operation $\mathcal{E}$ in the case where M and N may not commute.*

An even more general problem would be: How to characterize $[wp(\mathcal{E})(M), wp(\mathcal{E})(N)]$ in terms of $[M, N]$, where for any operators X and Y, $[X, Y]$ stands for their commutator, i.e., $[X, Y] = XY - YX$?

Problem 4.3.2. *Various healthiness conditions for predicate transformer semantics of classical programs were introduced by Dijkstra [75], e.g., conjunctivity and disjunctivity. These conditions were also carefully examined for probabilistic predicate transformers [166]. An interesting problem is to study healthiness conditions for quantum predicate transformers in the light of noncommutativity of quantum predicates. Note that this problem was considered in [225] for a special class of quantum predicates, namely projection operators.*

4.4 BIBLIOGRAPHIC REMARKS

Birkhoff-von Neumann quantum logic mentioned in Section 4.1 was first introduced in [42]. After development over 80 years, it has become a rich subject at the intersection of logic and quantum foundations; for a systematic exposition, see book [62].

The notion of quantum predicate as a Hermitian operator was conceived by D'Hondt and Panangaden, and the notion of quantum weakest precondition was first introduced by them in the seminal paper [70].

The exposition of Floyd-Hoare logic for quantum programs in Section 4.2 is based on [221]. Several other approaches to quantum Floyd-Hoare logic were briefly discussed in Subsection 1.1.3. In addition, Kakutani [132] proposed an extension of Hartog's probabilistic Hoare logic [114] for reasoning about quantum programs written in Selinger's language QPL [194]. Adams [8] defined a logic QPEL (Quantum Program and Effect Language) and its categorical semantics in terms of state-and-effect triangles.

The discussion about (non-)commutativity of quantum weakest preconditions given in Section 4.3 is based on [224]. A basis for solving Problem 4.3.2 is lattice-theoretic operations of quantum predicates (i.e., quantum effects), which have been widely studied in the mathematical literature since the 1950s; see for example [110,131].