Semantic Techniques in Quantum Computation

Edited by

SIMON GAY
IAN MACKIE
Predicate Transformer Semantics of Quantum Programs

Mingsheng Ying, Runyao Duan, Yuan Feng, and Zhengfeng Ji

Abstract

This chapter presents a systematic exposition of predicate transformer semantics for quantum programs. It is divided into two parts: The first part reviews the state transformer (forward) semantics of quantum programs according to Selinger's suggestion of representing quantum programs by superoperators and elucidates D'Hondt-Panangaden's theory of quantum weakest preconditions in detail. In the second part, we develop a quite complete predicate transformer semantics of quantum programs based on Birkhoff-von Neumann quantum logic by considering only quantum predicates expressed by projection operators. In particular, the universal conjunctivity and termination law of quantum programs are proved, and Hoare's induction rule is established in the quantum setting.

8.1 Introduction

In the mid-1990s Shor and Grover discovered, respectively, the famous quantum factoring and searching algorithms. Their discoveries indicated that in principle quantum computers offer a way to accomplish certain computational tasks much more efficiently than classical computers, and thus stimulated an intensive investigation in quantum computation. Since then a substantial effort has been made to develop the theory of quantum computation, to find new quantum algorithms, and to exploit the physical techniques needed in building functional quantum computers, including in particular fault tolerance techniques.

Currently, quantum algorithms are expressed mainly at the very low level of quantum circuits. In the history of classical computation, however, it was realised long time ago that programming languages provide a technique that allows us to think about a problem that we intend to solve in a high-level, conceptual way, rather than the details of implementation. Recently, in order to offer a similar technique in quantum computation, people began to study the principles, design and semantics of quantum programming languages; for excellent surveys see Gay (2006) and Selinger (2004).
Since it provides a goal-directed program development strategy and nondeterminacy can be accommodated well in it (Dijkstra 1976; Hesselink 1992), predicate transformer semantics has a very wide influence in classical programming methodology. With the prospect of goal-directed quantum programming, two approaches to predicate transformer semantics of quantum programs have been proposed in the literature. The first approach is to treat an observation (a measurement) procedure as a probabilistic choice. Thus, a quantum computation is naturally reduced to a probabilistic computation, and predicate transformer semantics developed for probabilistic programs (Kozen 1981; Morgan et al. 1996) can be conveniently used for quantum programs. For example, Butler and Hartel (1999) used the probabilistic weakest precondition calculus (Morgan et al. 1996) to model and reason about Grover’s algorithm. In particular, Sanders and Zuliani (2000) designed a refinement calculus supporting verification and derivation of quantum programs.

The second approach was proposed by D’Hondt and Panangaden (2006), where the notion of predicate is directly taken from quantum mechanics; that is, a quantum predicate is defined to be an observable (a Hermitian operator) with eigenvalues within the unit interval. In this approach, forward operational semantics of quantum programs is described by superoperators, as suggested by Selinger (2004), and an elegant Stone-type duality between the state-transformer (forward) semantics and the predicate-transformer (backward) semantics of quantum programs can be established by employing the Kraus representation theorem for superoperators.

A further development of the second approach requires us to tackle some problems that would not arise in the realm of classical and probabilistic programming. One of such problems is to well define various logical operations of quantum predicates, since they will be needed to combine different quantum weakest preconditions in reasoning about complicated quantum programs. For example, conjunction and disjunction are two of the most frequently used logical operations, and it is natural to define conjunction and disjunction of quantum predicates as the greatest lower bound and the least upper bound of them, respectively, according to the Löwner order. Unfortunately, it is known that the set of quantum predicates is not a lattice, and thus the greatest lower bound and the least upper bound of certain quantum predicates do not exist, except in the trivial case of one-dimensional state spaces (Kadison 1951). Moreover, the problem of finding necessary and sufficient conditions for the existence of the greatest lower bound and the least upper bound of quantum predicates is still unsolved for state spaces with dimension greater than 3 (Gudder 1996). Only some sufficient conditions have been discovered, and most of them are related to commutativity of quantum predicates (for a more general exposition on commutativity required in defining operations of quantum predicates, see Varadarajan 1985, Section 7.3.6). As noticed in Ying et al. (2007), however, the weakest preconditions of two commutative quantum predicates do not necessarily commute. This is an obvious obstacle in the further development of predicate transformer semantics for quantum programs, and it seems to be very difficult to overcome in the general setting.

A way to avoid the preceding difficulty is to focus our attention on a special class of quantum predicates, namely projection operators. There are at least two further reasons for choosing to consider only projectors as quantum predicates:

- The first one is conceptual, and it comes from the following observation: The quantum predicates dealt with in D’Hondt and Panangaden (2006) are Hermitian operators whose eigenvalues are within the unit interval, and in a sense, they can be envisaged as quantization of probabilistic predicates. On the other hand, projection operators are Hermitian operators with 0 or 1 as their eigenvalues, and they should be thought of as quantization of classical (Boolean) predicates. Physically, the simplest type of measuring instrument is one performing so-called yes-no measurement. Only a single change may be triggered on such an instrument, and it is often called an effect by physicists. Indeed, Kraus (1983) presented an elegant reformulation of quantum mechanics in terms of effects, which are represented by projection operators.

- The second reason is technical: Projection operators in a Hilbert space correspond one-to-one to closed subspaces of this space, and the Löwner order restricted on projection operators coincides with the inclusion between the corresponding subspaces. The set of closed subspaces of a Hilbert space was recognized by Birkhoff and von Neumann (1936) as (the algebraic counterpart of) the logic of quantum mechanics, and its structure has been thoroughly investigated in the development of quantum logic for over 70 years. Thus, we are able to exploit the power of quantum logic in our research on predicate transformer semantics of quantum logic. In particular, the greatest lower bound and least upper bound of projection operators always exist no matter whether they commute or not.

This chapter presents a systematic exposition of the second approach to predicate transformer semantics of quantum programs, and in particular, we try to build a theoretical foundation for it. The chapter is organized as follows: Section 8.2 reviews the state transformer (forwards) semantics of quantum programs according to Selinger’s suggestion (Selinger 2004) of representing quantum programs by super-operators. D’Hondt-Panangaden’s theory (D’Hondt and Panangaden 2006) of quantum weakest preconditions is elucidated in detail in Section 8.3, where the problem of commutativity of quantum weakest preconditions is also examined. Based on the authors’ previous work (Ying et al. 2007). In Section 8.4, we develop a quite complete predicate transformer semantics of quantum programs based on Birkhoff-von Neumann quantum logic by considering only quantum predicates expressed by projection operators. More concretely, we define the notion of projective (quantum) predicate transformer and introduce various healthiness conditions for quantum programs in Subsection 8.4.3. In Subsection 8.4.4, the notion of projective weakest precondition is proposed, and Subsection 8.4.5 is devoted to examining the relationship between the D’Hondt-Panangaden quantum predicate transformer semantics and projective predicate transformer semantics. The
8.2 Quantum State Transformers

We recall that in the state transformer semantics of a classical imperative language a state space is simply assumed to be a nonempty set of states. Then a command of the language is interpreted as a state transformer that is a mapping from the state space into itself. To define the state transformer semantics of a quantum programming language, we need to introduce the notion of quantum state space and to give suitable interpretations of the quantum commands in the language.

8.2.1 Quantum States

According to a basic postulate of quantum mechanics, the state space of an isolated quantum system is a Hilbert space. For convenience of the reader, we briefly recall some basic notions from Hilbert space theory. We write $C$ for the set of complex numbers. For each complex number $\lambda \in C$, $\lambda^*$ stands for the conjugate of $\lambda$. A (complex) vector space $\mathcal{H}$ is a nonempty set $\mathcal{H}$ together with two operations: vector addition $+: \mathcal{H} \times \mathcal{H} \to \mathcal{H}$ and scalar multiplication $\cdot: \mathbb{C} \times \mathcal{H} \to \mathcal{H}$ satisfying the following conditions:

(i) $(\mathcal{H}, +)$ is an Abelian group, its zero element $0$ is called the zero vector;
(ii) $|\lambda | |\psi \rangle = |\lambda \psi \rangle$;
(iii) $\lambda (\mu |\psi \rangle) = (\lambda \mu) |\psi \rangle$;
(iv) $(\lambda + \mu)|\psi \rangle = \lambda |\psi \rangle + \mu |\psi \rangle$; and
(v) $\lambda (\lambda |\psi \rangle + |\psi \rangle) = \lambda |\psi \rangle + \lambda |\psi \rangle$

for any $\lambda, \mu \in C$ and $|\psi \rangle \in \mathcal{H}$.

An inner product over a vector space $\mathcal{H}$ is a mapping $\langle \cdot | \cdot \rangle: \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ satisfying the following properties:

(i) $|\psi \rangle \neq 0$ with equality if and only if $|\psi \rangle = 0$;
(ii) $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$; and
(iii) $\langle \phi | (\lambda_1 |\psi_1 \rangle + \lambda_2 |\psi_2 \rangle) = \lambda_1 \langle \phi | |\psi_1 \rangle + \lambda_2 \langle \phi | |\psi_2 \rangle$

for any $|\psi \rangle, |\phi \rangle, |\psi_1 \rangle, |\psi_2 \rangle \in \mathcal{H}$ and for any $\lambda_1, \lambda_2 \in C$. Sometimes, we also write $\langle |\phi \rangle, |\psi \rangle \rangle$ for the inner product $\langle |\phi \rangle |\psi \rangle \rangle$ of $|\phi \rangle$ and $|\psi \rangle$. Two vectors $|\phi \rangle, |\psi \rangle \in \mathcal{H}$ are said to be orthogonal and we write $|\phi \rangle \perp |\psi \rangle$ if $\langle |\phi \rangle |\psi \rangle = 0$. For any vector $|\psi \rangle \in \mathcal{H}$, its length $|||\psi \rangle||$ is defined to be $\sqrt{\langle |\psi \rangle |\psi \rangle}$. A vector $|\psi \rangle$ is called a unit vector if $|||\psi \rangle|| = 1$. Let $\mathcal{H}$ be an inner product space, $\{|\psi_i \rangle \}$ a sequence of vectors in $\mathcal{H}$, and $|\psi \rangle \in \mathcal{H}$. If for any $\varepsilon > 0$ there exists a positive integer $N$ such that $|||\psi_m - |\psi \rangle|| < \varepsilon$ for all $m, n \geq N$, then $\{|\psi_i \rangle \}$ is called a Cauchy sequence. If for any $\varepsilon > 0$ there exists a positive integer $N$ such that $|||\psi_n - |\psi \rangle|| < \varepsilon$ for all $n \geq N$, then $\{|\psi_i \rangle \}$ is a Cauchy sequence.

A Hilbert space $\mathcal{H}$ is a complete inner product space; that is, an inner product space in which each Cauchy sequence of vectors has a limit. Let $X$ be a subset of a Hilbert space $\mathcal{H}$. If for any $|\psi \rangle \in X$ and any $\varepsilon > 0$, there exists $|\psi \rangle \in X$ such that $|||\psi - |\psi \rangle|| < \varepsilon$, then we say that $X$ is dense in $\mathcal{H}$. A Hilbert space $\mathcal{H}$ is said to be separable if it has a countable subset dense in $\mathcal{H}$. Each orthonormal basis of a separable Hilbert space must be countable. In this chapter, we consider only separable Hilbert spaces. If a Hilbert space $\mathcal{H}$ is the state space of a quantum system, then a pure state of the system is described by a unit vector in $\mathcal{H}$. A (linear) operator on a Hilbert space $\mathcal{H}$ is a mapping $A: \mathcal{H} \to \mathcal{H}$ satisfying the following conditions:

(i) $A(|\psi \rangle + |\phi \rangle) = A(|\psi \rangle) + A(|\phi \rangle)$;
(ii) $A(\lambda |\psi \rangle) = \lambda A(|\psi \rangle)$

for all $|\psi \rangle, |\phi \rangle \in \mathcal{H}$ and $\lambda \in C$. If $\{|\psi_i \rangle \}$ is an orthonormal basis of $\mathcal{H}$, then an operator $A$ on $\mathcal{H}$ is uniquely determined by $A(|\psi_i \rangle)$. An operator $A$ on $\mathcal{H}$ is bounded if there is a constant $C \geq 0$ such that $||A(|\psi \rangle)|| \leq C \cdot |||\psi \rangle||$ for all $|\psi \rangle \in \mathcal{H}$. We write $L(\mathcal{H})$ for the set of bounded operators on $\mathcal{H}$. In this chapter, we consider only bounded operators. The zero operator that maps every vector in $\mathcal{H}$ to the zero vector is in $L(\mathcal{H})$. It is obvious that $A, B \in L(\mathcal{H})$ implies the composition $AB \in L(\mathcal{H})$. Moreover, $L(\mathcal{H})$ is a vector space in which vector addition and scalar multiplication are defined as follows: Let $A, B \in L(\mathcal{H})$ and $\lambda \in C$. Then

\[ (A + B)|\psi \rangle = A(|\psi \rangle) + B(|\psi \rangle) \]
\[ (\lambda A)|\psi \rangle = \lambda A(|\psi \rangle) \]
for each \(|\psi\rangle \in \mathcal{H}\). For any operator \(A \in \mathcal{L}(\mathcal{H})\), there exists a unique linear operator \(A^\dagger \) on \(\mathcal{H}\) such that

\[
\langle \psi | A | \psi \rangle = (A^\dagger | \psi \rangle , | \psi \rangle )
\]

for all \(|\psi\rangle, |\psi\rangle \in \mathcal{H}\). The operator \(A^\dagger \) is called the adjoint of \(A\). Let \(A, A_i \in \mathcal{L}(\mathcal{H})\) for all real numbers \(t\). If

\[
\lim_{t \to +} \|(A - A^\dagger)(| \psi \rangle \rangle)\| = 0
\]

for all \(|\psi\rangle \in \mathcal{H}\), then \(A\) is called a (strong) limit of \(\{A_i\}\) for \(t \to b^+\) and we write \(A = \lim_{t \to b^+} A_t\). Similarly, we can define \(\lim_{t \to a^-} A\), \(\lim_{t \to +} A\), and \(\lim_{t \to +\infty} A\) for a sequence \(\{A_i\}\) of operators. The norm of a bounded operator \(A\) on \(\mathcal{H}\) is defined to be

\[
\|A\| = \sup_{|\psi\rangle \neq 0} \frac{\|A(|\psi\rangle \rangle\|}{\|\psi\rangle \rangle}\]

To describe a quantum system whose state is not completely known, we need the notion of density operator. An operator \(A\) on a Hilbert space \(\mathcal{H}\) is said to be positive if \(\langle \psi | A | \psi \rangle \geq 0\) for all states \(|\psi\rangle \in \mathcal{H}\). An operator \(A\) is said to be a positive operator if \(\{(\psi_i |A | \psi_i)\}_{i=1}^{\infty}\) is summable for any orthonormal basis \(\{\psi_i\}_{i=1}^{\infty}\) of \(\mathcal{H}\); in this case, the trace \(tr(A)\) of \(A\) is defined to be

\[
tr(A) = \sum_{i=1}^{\infty} (\psi_i |A | \psi_i)
\]

where \(\{\psi_i\}\) is an orthonormal basis of \(\mathcal{H}\). It can be shown that \(tr(A)\) is independent of the choice of \(\{\psi_i\}\). A density operator \(\rho\) on a Hilbert space \(\mathcal{H}\) is defined to be a positive operator with \(tr(\rho) = 1\). Then a mixed state of a quantum system with state space \(\mathcal{H}\) is described by a density operator on \(\mathcal{H}\). We shall take a slightly generalized notion of density operator in the sequel: A partial density operator \(\rho\) is a positive with \(tr(\rho) \leq 1\). In particular, the zero operator is a partial density operator.

We can define a partial order between operators, called the Löwner partial order: Let \(A, B \in \mathcal{L}(\mathcal{H})\). Then \(A \preceq B\) if \(B - A\) is a positive operator. Recall that a complete partial order (CPO for short) is a partially ordered set \((L, \preceq)\) such that \(\sqrt{\bigwedge_{n=0}^{\infty} x_n \in L}\) for any increasing sequence \(\{x_n\}\) in \(L\).

**Proposition 8.2.1** (Selinger 2004, Proposition 3.6). The set of partial density operators on \(\mathcal{H}\), denoted by \(\mathcal{D}(\mathcal{H})\), with the Löwner partial order is a CPO, with the zero density operator as its least element.

Selinger (2004) gave a proof of the preceding proposition in the case of finite-dimensional \(\mathcal{H}\). Here we present a proof for the general case, which is essentially a modification of the proof of Theorem III.6.2 in Prugovečki (1981). To this end, we need the notion of square root of a positive operator, which in turn requires the spectral decomposition theorem for Hermitian operators. An operator \(M \in \mathcal{L}(\mathcal{H})\) is said to be Hermitian if \(M^\dagger = M\). Hermitian operators are used to represent observables in quantum mechanics. Projectors are a special class of Hermitian operators.

**Theorem 8.2.2** (Prugovečki 1981, Theorem III.6.3) (Spectral decomposition). If \(M\) is a Hermitian operator with \(spec(M) \subseteq [a, b]\), then there is a spectral family \(\{E_i\}_{-\infty \leq a < \infty}\) of projectors on \(\mathcal{H}\) satisfying the following conditions:

(i) \(E\subseteq E_i\subseteq E\_i\_j\) whenever \(\lambda_i \leq \lambda_j\);

(ii) \(E_i = \lim_{n \to \infty} E_n\) for each \(\lambda\); and

(iii) \(\lim_{n \to \infty} E_i = 0\) if \(\lambda < a\) and \(\lim_{n \to \infty} E_i = 1\) if \(\lambda > b\).

\[
M = \int_a^b \lambda dE\_i
\]

where the integral in the right-hand side is defined to be an operator satisfying the following condition: for any \(\epsilon > 0\), there exists \(\delta > 0\) such that for any \(n \geq 1\) and \(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{n-1}\) with \(a = y_0 \leq y_1 \leq \cdots \leq y_{n-1} \leq x_{n-1} \leq y_n \leq x_n = b\), it holds that

\[
\| \int_a^b \lambda dE\_i - \sum_{n=0}^{\infty} y_i(E\_i - E\_i\_j) \| < \epsilon
\]

whenever \(\max_{i=0}^{n}(x_i - x_{i-1}) < \delta\).

Now we are able to define the square root of a positive operator \(A\). Since \(A\) is a Hermitian operator, it enjoys a spectral decomposition:

\[
A = \int \lambda dE\_i
\]

Then its square root is defined to be

\[
\sqrt{A} = \int \sqrt{\lambda} dE\_i
\]

With these preliminaries, we can give:

**Proof of Proposition 8.2.1.** For any positive operator \(A\), we get:

\[
|\langle \psi | A | \psi \rangle|^2 = (|\sqrt{A} |\psi\rangle, \sqrt{A} |\psi\rangle)^2 \leq \langle \psi | A | \psi \rangle \langle \psi | A | \psi \rangle
\]

by the Cauchy-Schwarz inequality.
Let \( \{p_n\} \) be an increasing sequence in \( D(H, \mathbb{C}) \). For any \( \langle \psi \rangle \in H \), let \( A = p_n - p_m \) and \( \langle \phi \rangle = A \langle \psi \rangle \). Then
\[
\langle \psi \rangle | A \rangle | \psi \rangle \leq \langle \psi | A \rangle | \psi \rangle \leq \| \psi \|^2 \cdot tr(p_n) \leq \| \psi \|^2.
\]
and similarly we have \( \langle \psi | A \rangle | \psi \rangle \leq \| \psi \|^2 \). Thus, it follows from Equation (8.1) that
\[
| \langle \psi | A \rangle | \psi \rangle | \leq \| \psi \|^2 \cdot tr(p)
\]
Furthermore, we obtain:
\[
| \langle \psi | A \rangle | \psi \rangle | \leq \| \psi \|^2 \cdot tr(p)
\]
and \( \| A \| \leq 1 \). This leads to
\[
\langle \psi | A \rangle | \psi \rangle = \langle A \sqrt{\langle \psi \rangle} , A \sqrt{\langle \psi \rangle} \rangle
\]
\[
= \langle \sqrt{\langle \psi \rangle} , \sqrt{\langle \psi \rangle} \rangle
\]
\[
= \langle \sqrt{\langle \psi \rangle} , \sqrt{\langle \psi \rangle} \rangle
\]
\[
= \langle \psi | A \rangle | \psi \rangle.
\]
Using Equation (8.1) once again we get:
\[
\langle \psi | A \rangle | \psi \rangle - | \langle \psi | A \rangle | \psi \rangle | \leq \langle \psi | A \rangle | \psi \rangle = (\langle \psi | A \rangle | \psi \rangle)^2 \leq (\langle \psi | A \rangle | \psi \rangle)^2 = (\langle \psi | A \rangle | \psi \rangle)^2.
\]
(8.2)
Note that \( \{ \langle \psi | p_n \rangle | \psi \rangle \} \) is an increasing sequence of real numbers bounded by \( 1 \| \psi \|^2 \), and thus it is a Cauchy sequence. This together with Equation (8.2) implies that \( \{ \langle \psi | p_n \rangle | \psi \rangle \} \) is a Cauchy sequence in \( H \). So, we can define:
\[
( \lim_{n \to \infty} p_n | \psi \rangle = \lim_{n \to \infty} p_n | \psi \rangle.
\]
For any \( \lambda, \lambda_2 \in C \) and \( \langle \psi \rangle, \langle \psi_2 \rangle \in H \), it holds that
\[
( \lim_{n \to \infty} p_n (\lambda_1 | \psi \rangle + \lambda_2 | \psi_2 \rangle) = \lim_{n \to \infty} p_n (\lambda_1 | \psi \rangle + \lambda_2 | \psi_2 \rangle)
\]
\[
= \lim_{n \to \infty} (\lambda_1 p_n | \psi \rangle + \lambda_2 p_n | \psi_2 \rangle)
\]
\[
= \lambda_1 \lim_{n \to \infty} p_n | \psi \rangle + \lambda_2 \lim_{n \to \infty} p_n | \psi_2 \rangle
\]
\[
= \lambda_1 (\lim_{n \to \infty} p_n | \psi \rangle) + \lambda_2 (\lim_{n \to \infty} p_n | \psi_2 \rangle).
\]

8.2.2 Unitary Transformations

We now turn to consider interpretations of quantum commands. There are two classes of basic quantum commands: unitary transformations and quantum measurements. An operator \( U \) on \( H \) is called a unitary transformation if \( U^* U = I_d H \), where \( I_d H \) is the identity operator on \( H \); that is, \( I_d H | \psi \rangle = | \psi \rangle \) for all \( | \psi \rangle \in H \).

The basic postulate of quantum mechanics about evolution of systems may be stated as follows: Suppose that the states of a closed quantum system at times \( t_0 \) and \( t \) are \( | \psi \rangle \) and \( | \psi \rangle \), respectively. Then they are related to each other by a unitary operator \( U \) that depends only on the times \( t_0 \) and \( t \),
\[
| \psi \rangle = U | \psi \rangle.
\]

This postulate can be reformulated in the language of density operators as follows: The state \( \rho \) of a closed quantum system at time \( t \) is related to its state \( \rho_0 \) at time \( t_0 \) by a unitary operator \( U \) that depends only on the times \( t \) and \( t_0 \),
\[
\rho = U \rho_0 U^*.
\]
8.2.3 Quantum Measurements

A quantum measurement on a system with state space $\mathcal{H}$ is described by a collection $\{M_m\}$ of operators on $\mathcal{H}$ satisfying

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

where $M_m$ are called measurement operators, and the index $m$ stands for the measurement outcomes that may occur in the experiment. If the state of a quantum system is $|\psi\rangle$ immediately before the measurement, then the probability that result $m$ occurs is

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

and the state of the system after the measurement is

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{p(m)}}.$$

We can also formulate the quantum measurement postulate in the language of density operators. If the state of a quantum system was $\rho$ immediately before measurement $\{M_m\}$ is performed on it, then the probability that result $m$ occur is

$$p(m) = tr(M_m \rho M_m^\dagger),$$

and the state of the system after the measurement is

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)}.$$

8.2.4 Superoperators

Unitary transformations are suited to describe the dynamics of closed quantum systems. For open quantum systems, however, one of the key mathematical formalisms for the description of their state transformations is the notion of superoperator. To define this notion, we need to introduce tensor product of Hilbert spaces. Let $\mathcal{H}$ be a Hilbert space with orthonormal basis $\{|\psi_i\rangle\}$ and $\mathcal{K}$ a Hilbert space with orthonormal basis $\{|\phi_j\rangle\}$. Then their tensor product is defined to be

$$\mathcal{H} \otimes \mathcal{K} = \{ \sum_{i,j} a_{ij} |\psi_i\rangle |\phi_j\rangle : a_{ij} \in \mathbb{C} \text{ with } \sum_{i,j} |a_{ij}|^2 < \infty \}.$$ 

Vector addition, scalar multiplication, and inner product are defined on $\mathcal{H} \otimes \mathcal{K}$ in a natural way: Let $|\Phi\rangle = \sum_{i,j} a_{ij} |\psi_i\rangle |\phi_j\rangle$, $|\Psi\rangle = \sum_{i,j} b_{ij} |\psi_i\rangle |\phi_j\rangle \in \mathcal{H} \otimes \mathcal{K}$ and

$$\langle \Phi | = \sum_{i,j} a_{ij}^* \langle \psi_i | \langle \phi_j |, \quad \langle \Psi | = \sum_{i,j} b_{ij}^* \langle \psi_i | \langle \phi_j |.$$ 

It is easy to show that $\mathcal{H} \otimes \mathcal{K}$ is a Hilbert space with $\{|i\rangle |\phi_j\rangle\}$ as an orthonormal basis. For any $|\psi\rangle = \sum_i a_i |\psi_i\rangle \in \mathcal{H}$ and $|\phi\rangle = \sum_j b_j |\phi_j\rangle \in \mathcal{K}$, we define:

$$|\psi\rangle \otimes |\phi\rangle = \sum_{i,j} a_i b_j |\psi_i\rangle |\phi_j\rangle.$$

If $A \in \mathcal{L}(\mathcal{H})$ and $B \in \mathcal{L}(\mathcal{K})$, then $A \otimes B \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$ is defined by

$$(A \otimes B) |\psi\rangle |\phi\rangle = A |\psi\rangle \otimes B |\phi\rangle$$

for all $i, j$. Suppose that $\mathcal{E}$ is an operator on $\mathcal{L}(\mathcal{H})$ and $\mathcal{F}$ an operator on $\mathcal{L}(\mathcal{K})$. Then $\mathcal{E} \otimes \mathcal{F}$ is defined to be an operator on $\mathcal{L}(\mathcal{H} \otimes \mathcal{K})$ and it is given as follows: For each $C \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$, we can write:

$$C = \sum_k a_k (A_k \otimes B_k),$$

where $A_k \in \mathcal{L}(\mathcal{H})$ and $B_k \in \mathcal{L}(\mathcal{K})$ for all $k$, and we define:

$$(\mathcal{E} \otimes \mathcal{F})(C) = \sum_k a_k (\mathcal{E}(A_k) \otimes \mathcal{F}(B_k)).$$

By linearity we may assert that $\mathcal{E} \otimes \mathcal{F}$ is well defined; that is, $(\mathcal{E} \otimes \mathcal{F})(C)$ is independent of the choice of $A_k$ and $B_k$.

A superoperator on $\mathcal{H}$ is a linear operator $\mathcal{E}$ from the space $\mathcal{L}(\mathcal{H})$ into itself that satisfies the following two conditions:

(i) $tr(\mathcal{E}(\rho)) \leq tr(\rho)$ for each $\rho \in \mathcal{D}(\mathcal{H})$;

(ii) (Complete positivity) For any extra Hilbert space $\mathcal{H}_E$, $(I_{\mathcal{H}_E} \otimes \mathcal{E}(A))$ is positive provided $A$ is a positive operator on $\mathcal{H}_E$, where $I_{\mathcal{H}_E}$ is the identity operator on $\mathcal{L}(\mathcal{H}_E)$; that is, $I_{\mathcal{H}_E}(A) = A$ for each operator $A$ on $\mathcal{H}_E$.

We write $SO(\mathcal{H})$ for the set of superoperators on $\mathcal{H}$. The Kraus theorem gives some useful representations of superoperators.

Theorem 8.2.3 (Kraus 1983, Theorems 3.1 and 5.2; Nielsen and Chuang 2000, Section 8.2.3, Theorem 8.1). The following statements are equivalent:

(i) $\mathcal{E}$ is a superoperator on $\mathcal{H}$;

(ii) (System-environment model) There are an environment system $E$ with state space $\mathcal{H}_E$ and a unitary transformation $U$ on $\mathcal{H} \otimes \mathcal{H}_E$ and a projector $P$
onto some closed subspace of $H \otimes H_E$ such that
\[
E(\rho) = \text{tr} \left[ P U (\rho \otimes |e_0\rangle\langle e_0|) T^F \right]
\] (8.3)
for any $\rho \in D(H)$, where $|e_0\rangle$ is a fixed state in $H_E$.

(iii) (Operator-sum representation) There exists a finite or countably infinite set of operators $\{E_i\}$ on $H$ such that $\sum_i E_i E_i^\dagger \leq 1$ and
\[
E(\rho) = \sum_i E_i \rho E_i^\dagger
\] (8.4)
for all density operators $\rho \in D(H)$. We often say that $E$ is represented by the set $\{E_i\}$ of operators, or $\{E_i\}$ are operation elements giving rise to $E$ when $E$ is given by Equation (8.4).

The proof of the foregoing theorem is omitted here, and the reader can find it in Kraus (1983), Chapters 3 and 5, or Nielsen and Chuang (2000), Chapter 8.

**Proof**

Let $\{x_n\}$ be an increasing sequence in $(D(H), \supseteq)$. Then for any $\rho \in D(H)$, $\{E(\rho)\}$ is an increasing sequence in $(D(H), \supseteq)$. With Proposition 8.2.1 we can define:
\[
\bigvee_n E_n(\rho) = \bigvee_n E_n(\rho) = \lim_{n \to \infty} E_n(\rho),
\]
and it holds that
\[
\text{tr}(\bigvee_n E_n(\rho)) = \lim_{n \to \infty} \text{tr}(E_n(\rho)) \leq 1
\]
because $\text{tr}(\cdot)$ is continuous. Furthermore, $\bigvee_n E_n$ can be defined on the whole of $L(H)$ by linearity. The defining equation of $\bigvee_n E_n$ implies: (i) $E_n \subseteq \bigvee_n E_n$ for all $m \geq 0$; and (ii) if $E_n \subseteq F$ for all $n \geq 0$ then $\bigvee_n E_n \subseteq F$. So, it suffices to show that $\bigvee_n E_n$ is completely positive. Suppose that $H_E$ is an extra Hilbert space. For any $C \in L(H_E)$ and $D \in L(H)$, we have:
\[
(I_E \otimes \bigvee_n E_n)(C \otimes D) = C \otimes \bigvee_n E_n(D)
\]
for all $n$.

Then for any $A \in L(H_E \otimes H)$ we get:
\[
(I_E \otimes \bigvee_n E_n)(A) = \lim_{n \to \infty} (I_E \otimes E_n)(A)
\]
by linearity. Thus, if $A$ is positive, then $(I_E \otimes \bigvee_n E_n)(A)$ is positive for all $n$, and $(I_E \otimes \bigvee_n E_n)(A)$ is positive.

The preceding proposition allows us to introduce recursion in the setting of superoperators. Let $F$ be a continuous function from $(SO(H), \supseteq)$ into itself. Then we define:
\[
\mu \lambda. F(X) = \bigvee_{n=0}^{\infty} F^n(0);
\]
that is, $\mu \lambda. F(X)$ is the least fixed point of $F$, where $0$ is the zero superoperator, which maps all elements of $D(H)$ to the zero density operator and corresponds to the divergent program, $F(0) = 0$, and $F^{n+1}(0) = F(F^n(0))$ for all $n \geq 0$. 

The first step to present predicate transformer semantics of a quantum language is to define the notion of quantum predicate. By a careful analysis and comparison with the classical and probabilistic cases, D'Hondt and Panangaden (2006) argued that quantum predicates should be physical observables. Their approach was originally presented in the setting of finite-dimensional state spaces, but it can be easily generalized to the case of infinite-dimensional state spaces. To motivate the definition of quantum predicate in an easier way, we first consider a finite-dimensional Hilbert space $H$. According to a basic postulate, an observable of a quantum system is described by a Hermitian operator on its state space. An eigenvector of an operator $A$ on $H$ is a nonzero vector $|\psi\rangle \in H$ such that $A|\psi\rangle = \lambda |\psi\rangle$ for some $\lambda \in \mathbb{C}$, where $\lambda$ is called the eigenvalue of $A$ corresponding to $|\psi\rangle$. It is easy to see that all eigenvalues of a Hermitian operator are real numbers. The set of eigenvalues of $A$ is called the (point) spectrum of $A$ and denoted $\text{spec}(A)$. For each eigenvalue $\lambda$ of an operator $A$, the set $\{ |\psi\rangle \in H : A|\psi\rangle = \lambda |\psi\rangle \}$ is a closed subspace of $H$ and it is called the eigenspace corresponding to $\lambda$. It is well known that an observable (a Hermitian operator) $M$ determines a so-called projective measurement $(|P_m\rangle \langle P_m|)$, where $m$ ranges over $\text{spec}(M)$, and $P_m$ is the projector onto the eigenspace of $M$ corresponding to $m$ for each eigenvalue $m$. The eigenvalues $m$ stand for the possible outcomes of the measurement. As to quantum predicates, their eigenvalues should be understood as the truth values of certain propositions about quantum systems. 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 8.3.1 (D'Hondt and Panangaden 2006, Definition 2.2).** A (quantum) predicate on $H$ is a Hermitian operator $M$ on $H$ with all its eigenvalues lying within the unit interval $[0, 1]$. The set of predicates on $H$ is denoted $\mathcal{P}(H)$. The state space $H$ in the foregoing definition and the following development can be infinite-dimensional unless it is explicitly stated to be finite-dimensional. For any $M \in \mathcal{P}(H)$, we have $0_H \subseteq M \subseteq 1_H$, where $0_H$ is the zero operator on $H$, that is, $0_H|\psi\rangle = 0$ for all $|\psi\rangle \in H$. Recall that $\text{tr}(M \rho)$ is the expectation value of measurement outcomes when a quantum system is in the mixed state $\rho$ and we perform the projective measurement determined by observable $M$ on it. Thus, if $M$ is a quantum predicate, then $\text{tr}(M \rho)$ may be interpreted as the degree to which quantum state $\rho$ satisfies quantum predicate $M$, or more precisely the average truth value of the proposition represented by $M$ in a quantum system of the state $\rho$. The reasonableness of the preceding definition is further indicated by the following fact: A Hermitian operator $M$ is a quantum predicate if and only if $0 \leq \text{tr}(M \rho) \leq 1$ for all $\rho \in D(H)$. The following proposition examines the structure of quantum predicates with respect to the Löwner partial order.

**Proposition 8.3.2 (Selinger 2004, Proposition 3.6; D'Hondt and Panangaden 2006, Proposition 2.3).** The set $(\mathcal{P}(H), \subseteq)$ of quantum predicates with the Löwner partial order is a CPO.

**Proof.** Similar to the proof of Proposition 8.2.1. □

As mentioned in the introduction, $(\mathcal{P}(H), \subseteq)$ is not a lattice except in the trivial case of one-dimensional state space; that is, the greatest lower bound and least upper bound of elements in $(\mathcal{P}(H), \subseteq)$ are not always defined.

**8.3.2 Quantum Weakest Preconditions: Definitions and Representations**

Now we are ready to define the two key notions in this section, i.e., quantum generalization of Hoare assertion and quantum weakest precondition.

**Definition 8.3.3 (D'Hondt and Panangaden 2006, Definition 3.1).** For any quantum predicates $M, N \in \mathcal{P}(H)$, and for any quantum program $E \in \mathcal{SO}(H)$, $M$ is called a precondition of $N$ with respect to $E$, written $M \vdash E \mid N$, if

$$\text{tr}(M \rho) \leq \text{tr}(N \rho)$$

for all density operators $\rho \in D(H)$.

The intuitive meaning of condition (8.5) comes immediately from the interpretation of satisfaction relation between quantum states and quantum predicates: if state $\rho$ satisfies predicate $M$ then the state after transformation $E$ from $\rho$ satisfies predicate $N$.

**Definition 8.3.4 (D'Hondt and Panangaden 2006, Definition 3.2).** Let $M \in \mathcal{P}(H)$ be a quantum predicate and $E \in \mathcal{SO}(H)$ a quantum program. Then the weakest precondition of $M$ with respect to $E$ is a quantum predicate $wp(E)(M)$ satisfying the following conditions:

(i) $wp(E)(M) \mid M$;

(ii) for all quantum predicates $N$, $N \mid M$ implies $N \equiv wp(E)(M)$.

For each $E \in \mathcal{SO}(H)$, the foregoing definition gives a quantum predicate transformer $wp(E) : \mathcal{P}(H) \rightarrow \mathcal{P}(H)$. An operator-sum representation of $wp(E)$ was found in D'Hondt and Panangaden (2006) by exploiting a Stone-type duality between forward state transformers and backward predicate transformers when $E$ is given in the form of operator-sum.
Proposition 8.3.5 (D'Hondt and Panangaden 2006, Proposition 3.3). Suppose that program $E \in \text{SCQ}(H)$ is represented by the set $\{E_i\}$ of operators. Then for each predicate $M \in \mathcal{P}(H)$, we have:

$$\text{wp}(E)(M) = \sum_i E_i^p M E_i^l.$$  

(8.6)

Proof. We see from Definition 8.3.4 that weakest precondition $\text{wp}(E)(M)$ is unique when it exists. Then we only need to check that $\text{wp}(E)(M)$ given by Equation (8.6) satisfies the two conditions in Definition 8.3.4.

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

$$\text{tr}(\text{wp}(E)(M)p) = \text{tr}(\sum_i E_i^p M E_i^l)p = \sum_i \text{tr}(E_i^p M E_i^l) = \sum_i \text{tr}(M E_i p E_i^l) = \text{tr}(M \sum_i E_i p E_i^l) = \text{tr}(M \sum_i E_i^p M E_i^l).$$

Thus, $\text{wp}(E)(M) \models \text{wp}(E)(M)$.

(ii) It is easy to show that for any $M, N \in \mathcal{P}(H)$, $M \subseteq N$ if and only if $\text{tr}(M) \leq \text{tr}(N)$ for all $\rho \in \mathcal{D}(H)$. Thus, if $N \models E$, then for any $\rho \in \mathcal{D}(H)$ we have $\text{tr}(Np) \leq \text{tr}(M E(p)) = \text{tr}(\text{wp}(E)(M)p)$. Therefore, it follows immediately that $N \models \text{wp}(E)(M)$.

We can also give an intrinsic characterization of $\text{wp}(E)$ in the case that $E$ is given by a system-environment model.

Proposition 8.3.6 (Ying et al. 2007, Proposition 2.2). If $E$ is given by Equation (8.3), then we have:

$$\text{wp}(E)(M) = \sum_k (\langle e_k | UP | e_0 \rangle \rho \langle e_0 | UP | e_k \rangle).$$

for each $M \in \mathcal{P}(H)$, where $I_e$ is the identity operator in the environment system.

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

$$E(\rho) = \sum_k (\langle e_k | PU | e_0 \rangle \rho \langle e_0 | PU | e_k \rangle),$$

and using Proposition 8.3.5 we obtain:

$$\text{wp}(E)(M) = \sum_k (\langle e_k | U^* P | e_0 \rangle M (\langle e_0 | U P | e_k \rangle).$$

Thus, $\text{wp}(E)(M) \models \text{wp}(E)(M)$. Note that $\sum_k |\langle e_k | M (\langle e_0 |) = M \otimes I_e$ because $\{\langle e_i |\}$ is an orthonormal basis of $\mathcal{H}_E$. This completes the proof.

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

Proposition 8.3.7 Let $\lambda \geq 0$ and $E, F \in \text{SCQ}(H)$, and let $\{\langle e_0 |\}$ be an increasing sequence in $\text{SCQ}(H)$. Then

(i) $\text{wp}(\lambda E) = \lambda \text{wp}(E)$ provided $\lambda E \in \text{SCQ}(H)$;

(ii) $\text{wp}(E + F) = \text{wp}(E) + \text{wp}(F)$ provided $E + F \in \text{SCQ}(H)$;

(iii) $\text{wp}(E \otimes F) = \text{wp}(E) \otimes \text{wp}(F)$;

(iv) $\text{wp}(\bigvee_{n=0}^\infty E_n) = \bigvee_{n=0}^\infty \text{wp}(E_n)$, where

$$\bigvee_{n=0}^\infty \text{wp}(E_n)(M) = \bigvee_{n=0}^\infty \text{wp}(E_n)(M)$$

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

Proof.

(i) and (ii) are immediately from Proposition 8.3.5.

(iii) It is easy to see that $L(E)M(N)$ implies $L(E \otimes F)N$. Thus, we have $\text{wp}(E)(\text{wp}(F)(M)) \models \text{wp}(E \otimes F)(M)$. On the other hand, we need to show that $N \models \text{wp}(E)(\text{wp}(F)(M))$ whenever $N \models \text{wp}(E \otimes F)(M)$. In fact, for any $\rho \in \mathcal{D}(H)$, it follows from Equation (8.7) that

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

Therefore, we obtain $\text{wp}(E \otimes F)(M) = \text{wp}(E)(\text{wp}(F)(M)) = (\text{wp}(F) \otimes \text{wp}(E))(M)$.

(iv) We note that the following two equalities follow immediately from the proof of Proposition 8.2.1:

$$M(\bigvee_{n=0}^\infty M_n) = \bigvee_{n=0}^\infty MM_n,$$

and

$$\text{tr}(\bigvee_{n=0}^\infty M_n) = \bigvee_{n=0}^\infty \text{tr}(M_n).$$
First, we prove that $\bigvee_{n=0}^{\infty} wp(E_n)(M) = \bigvee_{n=0}^{\infty} wp(E_n)(M)$. Indeed, for any $\rho \in D(H)$, we have:

$$tr(\bigvee_{n=0}^{\infty} wp(E_n)(M)\rho) = \bigvee_{n=0}^{\infty} tr(wp(E_n)(M)\rho)$$

$$\leq \bigvee_{n=0}^{\infty} tr(ME_n(\rho))$$

$$= tr(\bigvee_{n=0}^{\infty} ME_n(\rho))$$

$$= tr(M \bigvee_{n=0}^{\infty} E_n(\rho))$$

$$= tr(\bigvee_{n=0}^{\infty} wp(E_n)(M)\rho)$$

Second, we show that $N(\bigvee_{n=0}^{\infty} E_n)M$ implies $N \bigvee_{n=0}^{\infty} wp(E_n)(M)$. It suffices to note that

$$tr(N\rho) \leq tr(M \bigvee_{n=0}^{\infty} E_n(\rho))$$

$$= \bigvee_{n=0}^{\infty} tr(ME_n(\rho))$$

$$= \bigvee_{n=0}^{\infty} tr(wp(E_n)(M)\rho)$$

$$= tr(M \bigvee_{n=0}^{\infty} wp(E_n)(M)\rho)$$

for all $\rho \in D(H)$. Thus, it holds that $wp(\bigvee_{n=0}^{\infty} E_n)(M) = \bigvee_{n=0}^{\infty} wp(E_n)(M)$. $\square$

**Corollary 8.3.8.** Let $F$ be a continuous function from $(SO(H), \subseteq)$ into itself. Then

$$wp(\mu_\mu F)(X) = \bigvee_{n=0}^{\infty} wp(F^n)X(0)).$$

**Proof.** Immediate from Proposition 8.3.7(\textit{i}). $\square$

### 8.3.3 Commutativity of Quantum Weakest Preconditions

Quantum predicate transformer semantics is not a simple generalization of predicate transformer semantics for classical and probabilistic programs. It has to answer some important problems that would not arise in the realm of classical and probabilistic programming. One such problem is commutativity of quantum weakest preconditions. The significance of this problem comes from the following observation: Quantum weakest preconditions are quantum predicates and in turn they are observables on the state space. Thus, their physical simultaneous verifiability depends on commutativity between them according to the Heisenberg uncertainty principle (see Nielsen and Chuang 2000, page 89). The aim of this subsection is to find some conditions under which quantum weakest preconditions commute.

Recall that for any two operators $A$ and $B$ on $H$, it is said that $A$ and $B$ commute if $AB = BA$. What concerns us in this subsection is the following:

**Question 8.3.9.** Given a quantum program $E \in SO(H)$, When do $wp(E)(M)$ and $wp(E)(N)$ commute?

This question seems very difficult to answer for a general superoperator $E$. We first see a simple example from quantum communication.

**Example 8.3.10** (Nielsen and Chuang 2000, Section 8.3) (Bit flip and phase flip channels). A qubit is a quantum state of the form $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, where $|0\rangle$ and $|1\rangle$ are two basis states, and $a_0$ and $a_1$ are complex numbers with $|a_0|^2 + |a_1|^2 = 1$. Thus, the state space of qubits is the 2-dimensional Hilbert space $H_2 = \mathbb{C}^2$, and linear operators on $H_2$ can be represented by $2 \times 2$ matrices.

Bit flip and phase flip are quantum operations on a single qubit, and they are widely used in the theory of quantum error-correction. We write the Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

Then the bit flip is defined by

$$E(p) = E_0 p E_1 + E_1 p E_0,$$

where $E_0 = \sqrt{p} I$ and $E_1 = \sqrt{1-p} X$. It is easy to see that $E(M)$ and $E(N)$ commute when $MN = NM$ and $M$ and $N$ are unitary matrices.

If $E_1$ in Equation (8.8) is replaced by $\sqrt{1-p} Z$ (resp. $\sqrt{1-p} Y$), then $E$ is the phase flip (resp. bit-phase flip), and $E(M)$ and $E(N)$ commute when $MN = NM$ and $M$ and $N$ are unitary matrices.

Now we consider the simplest superoperators: unitary transformations and projective measurements.

**Proposition 8.3.11.**

(i) Let $E \in SO(H)$ be a unitary transformation, i.e., $E(\rho) = U\rho U^\dagger$ for any $\rho \in D(H)$, where $UU^\dagger = U^\dagger U = 1_{H}$. Then $wp(E)(M)$ and $wp(E)(N)$ commute if and only if $M$ and $N$ commute.
(i) Let \( \{P_k\} \) be a projective measurement, i.e., \( P_k P_k = \delta_{k,k} P_k \) and \( \sum_k P_k = I_{\mathcal{H}^2} \), where
\[
\delta_{k,k} = \begin{cases} 1, & \text{if } k_1 = k_2, \\ 0, & \text{otherwise}. \end{cases}
\]

If \( \mathcal{E} \) is given by this measurement, with the result of the measurement unknown, i.e.,
\[
\mathcal{E}(\rho) = \sum_k P_k \rho P_k
\]
for each \( \rho \in \mathcal{D}(\mathcal{H}) \), then \( \text{wp}(\mathcal{E})(\mathcal{M}) \) and \( \text{wp}(\mathcal{E})(\mathcal{N}) \) commute if and only if \( P_k M P_k \) and \( P_k N P_k \) commute for all \( k \). In particular, let \( \{[i]\} \) be an orthonormal basis of \( \mathcal{H} \). If \( \mathcal{E} \) is given by the measurement in the basis \( \{[i]\} \), i.e.,
\[
\mathcal{E}(\rho) = \sum_i P_i \rho P_i,
\]
where \( P_i = \ket{i}\bra{i} \) for each \( i \), then \( \text{wp}(\mathcal{E})(\mathcal{M}) \) and \( \text{wp}(\mathcal{E})(\mathcal{N}) \) commute for any \( M, N \in \mathcal{P}(\mathcal{H}) \).

Proof.

(i) From Proposition 8.3.5 we obtain:
\[
\text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) = U^\dagger M U U^\dagger N U = U^\dagger M N U
\]
Then \( MN = U^\dagger \text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) U^\dagger \), and the conclusion follows.

(ii) We first obtain:
\[
\text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) = \sum_{k,l} P_k M P_k P_l N P_l = \sum_k P_k M P_k N P_k.
\]
Similarly, it holds that
\[
\text{wp}(\mathcal{E})(\mathcal{N}) \text{wp}(\mathcal{E})(\mathcal{M}) = \sum_k P_k N P_k M P_k.
\]
It is clear that \( \text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) = \text{wp}(\mathcal{E})(\mathcal{N}) \text{wp}(\mathcal{E})(\mathcal{M}) \) if \( P_k M P_k \) and \( P_k N P_k \) commute. Conversely, if \( \text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) = \text{wp}(\mathcal{E})(\mathcal{N}) \text{wp}(\mathcal{E})(\mathcal{M}) \), then by multiplying \( P_k \) in the both sides we obtain:
\[
P_k M P_k N P_k = P_k P_k M P_k N P_k = \sum_{i,l} P_i M P_l N P_l = P_k N P_k M P_k.
\]
For the case of \( P_i = \ket{i}\bra{i} \) for each \( i \), it holds that \( P_i M P_i N P_i = \ket{i}\bra{i} \ket{i}\bra{i} = \ket{i}\bra{i} \ket{i}\bra{i} = \ket{i}\bra{i} \ket{i}\bra{i} \). Note that \( \ket{i}\bra{i} \) and \( \ket{i}\bra{i} \) are complex numbers, and they commute. Thus, \( P_i M P_i N P_i = P_i N P_i M P_i \) always holds.

8 Predicate Transformer Semantics of Quantum Programs

For a general superoperator \( \mathcal{E} \), we are only able to give some sufficient conditions for commutativity of \( \text{wp}(\mathcal{E})(\mathcal{M}) \) and \( \text{wp}(\mathcal{E})(\mathcal{N}) \). We first consider the case where \( \mathcal{E} \) is given in an operator-sum form.

Proposition 8.3.12. 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 \( \{\ket{\psi_i}\} \) of \( \mathcal{H} \) such that
\[
M = \sum_i \lambda_i \ket{\psi_i}\bra{\psi_i}, \quad N = \sum_i \mu_i \ket{\psi_i}\bra{\psi_i}
\]
where \( \lambda_i, \mu_i \) are reals for each \( i \) (Nielsen and Chuang 2000, Theorem 2.2), and let \( \mathcal{E} \in \mathcal{SO}(\mathcal{H}) \) be represented by the set \( \{E_i\} \) of operators. If for any \( i, j, k, l \), we have either \( \lambda_k \mu_j = \lambda_j \mu_k \) or
\[
\sum_i (\lambda_k \mu_j) \ket{\psi_i}\bra{\psi_i} \ket{\psi_i}\bra{\psi_i} = 0,
\]
then \( \text{wp}(\mathcal{E})(\mathcal{M}) \) and \( \text{wp}(\mathcal{E})(\mathcal{N}) \) commute.

Proof. We consider the matrix representations of the involved operators with respect to the basis \( \{\ket{\psi_i}\} \). For any \( i, j \), a routine calculation leads to
\[
ME_i E_j^\dagger N = (\lambda_k \mu_j \delta_{k,j}) E_i E_j^\dagger M \\
NE_i E_j^\dagger M = (\mu_j \lambda_k \delta_{k,j}) E_i E_j^\dagger N
\]
where
\[
\epsilon_{i,j} = \sum_{k,l} \bra{\psi_i} \bra{\psi_l} \bra{\psi_l} \bra{\psi_l}
\]
for all \( k, l \). Then the condition given in this proposition implies \( ME_i E_j^\dagger N = NE_i E_j^\dagger M \). It follows from Proposition 8.3.5 that
\[
\text{wp}(\mathcal{E})(\mathcal{M}) \cdot \text{wp}(\mathcal{E})(\mathcal{N}) = (\sum_i E_i^\dagger M E_i)(\sum_i E_i^\dagger N E_i) = \sum_i E_i^\dagger M E_i E_i^\dagger N E_i
\]
and \( \text{wp}(\mathcal{E})(\mathcal{M}) \text{wp}(\mathcal{E})(\mathcal{N}) = \text{wp}(\mathcal{E})(\mathcal{N}) \text{wp}(\mathcal{E})(\mathcal{M}) \).

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

Definition 8.3.13. Let \( \mathcal{E} \in \mathcal{SO}(\mathcal{H}) \) be represented by the set \( \{E_i\} \) of operators, and let \( M \in \mathcal{P}(\mathcal{H}) \). Then we say that quantum predicate \( \mathcal{M} \) and quantum program \( \mathcal{E} \) commute if \( M \) and \( E_i \) commute for each \( i \).

It seems that in the foregoing definition commutativity between quantum predicate \( \mathcal{M} \) 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 such operators are not unique. To address this problem, we need the following:

Lemma 8.3.14 (Nielsen and Chuang 2000, Theorem 8.2) (Unitary freedom in the operator-sum representation). Suppose that \( \{E_i\} \) and \( \{F_j\} \) are operation elements
giving rise to quantum operations $\mathcal{E}$ and $\mathcal{F}$, respectively. 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

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

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

As a simple corollary, we can see that commutativity between $M$ and $\mathcal{E}$ is irrelevant to the choice of the Kraus representation operators $\mathcal{E}$.

Lemma 8.3.15. 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 $\{F_j\}$. Then $M$ and $E_i$ commute for all $i$ if and only if $M$ and $F_j$ commute for all $j$.

Proof. Immediate from Lemma 8.3.14. □

Commutativity between observables and quantum operations is preserved by composition of quantum operations.

Proposition 8.3.16. Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate, and let $E_i, E_j \in \mathcal{SO}(\mathcal{H})$ be two quantum programs. If $M$ and $E_i$ commute for $i = 1, 2$, then $M$ commutes with the composition $E_1 \circ E_2$ of $E_1$ and $E_2$.

Proof. Suppose that $E_1$ is represented by $\{E_i\}$ and $E_2$ is represented by $\{F_j\}$. Then for any $\rho \in \mathcal{D}(\mathcal{H})$, we have:

$$\mathcal{E}_i \circ \mathcal{E}_j (\rho) = \mathcal{E}_j (\mathcal{E}_i (\rho)) = \sum_{i,j} F_j E_i \rho E_i^* F_j^*.$$ 

With Lemma 8.3.15 it suffices to note that $M(F_j E_i) = F_j M E_i = (F_j E_i) M$ for all $i, j$. □

The following proposition gives another sufficient condition for commutativity of $wp(\mathcal{E})$ and $wp(\mathcal{F})$.

Proposition 8.3.17. Let $M, N \in \mathcal{P}(\mathcal{H})$ be two quantum predicates, and let $E_i \in \mathcal{SO}(\mathcal{H})$ be a quantum program. If $M$ and $N$ commute, and $M$ and $E_i$ commute, and $N$ and $E_i$ commute, then $wp(\mathcal{E})$ and $wp(\mathcal{F})$ commute.

Proof. Since $M$ and $E_i$ commute, $N$ and $E_j$ commute for all $i, j$, and $N$ is Hermitian, i.e., $N^* = N$, we have:

$$M E_i N = E_i M E_i N = E_i M (N E_i)^* = E_i M N E_i^* = E_i M N E_i^* = E_i M N E_i^*$$

and from Equation (8.9) we obtain:

$$wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N) = \sum_{i,j} E_i^* E_i M N E_j^* E_j.$$ 

Similarly, it holds that

$$wp(\mathcal{E})(N) \cdot wp(\mathcal{E})(M) = \sum_{i,j} E_i^* E_i N M E_j^* E_j.$$ 

Then commutativity between $M$ and $N$ implies $wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N) = wp(\mathcal{E})(N) \cdot wp(\mathcal{E})(M)$. □

It is easy to see from Proposition 8.3.11 that the condition for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ given in Proposition 8.3.17 is not necessary.

Now we turn to consider the system-environment model of superoperator. To this end, we need two generalized notions of commutativity between linear operators.

Definition 8.3.18. Let $M, N, A, B, C \in \mathcal{L}(\mathcal{H})$.

(i) If $AMBNC = ANBMC$, then we say that $M$ and $N$ $(A, B, C)$-commute.

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

(ii) If $AA^* = A^* A$, then we say that $A$ and $B$ conjugate-commute.

Obviously, commutativity is exactly $I_d$-commutativity.

The next two propositions presents several conditions for commutativity of quantum weakest preconditions when quantum programs are given in the system-environment model.

Proposition 8.3.19. Let $\mathcal{E}$ be given by Equation (8.3), and we write $A = PU(e_0)$.

(i) if $wp(\mathcal{E}_1)(M)$ and $wp(\mathcal{E}_2)(N)$ commute if and only if $M \otimes I_E$ and $N \otimes I_E$ $(A_1, A_2, A)$-commute;

(ii) if $M \otimes I_E$ and $A$ and $N \otimes I_E$ and $A$ conjugate-commute, then wp(\mathcal{E}_1)(M)$ and $wp(\mathcal{E}_2)(N)$ commute.

Proof. Immediate from Proposition 8.3.6. □

Proposition 8.3.20. Suppose that $\mathcal{H}$ is finite-dimensional. Let $\mathcal{E}$ be given by Equation (8.3), and 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 $\lambda_i, \mu_i$ are reals for each $i$. If for any $i, j, k, l$, we have $\lambda_i \mu_j = \lambda_j \mu_i$ or $|\langle e_0 \rangle \langle U^T P \psi_i e_0 | = |\langle e_0 \rangle \langle U^T P \psi_j e_0 |,$

then $wp(\mathcal{E}_1)(M)$ and $wp(\mathcal{E}_2)(N)$ commute.
8.4 Quantum Predicate Transformers: Projection Operators = Predicates

The last section was devoted to an exposition of the D'Hondt-Panangaden approach to quantum weakest preconditions where quantum predicates are represented by Hermitian operators with their eigenvalues in the unit interval. This broad definition of quantum predicates allows us to establish an elegant duality between the state-transformer (forward) semantics and the predicate-transformer (backward) semantics of quantum programs. However, it also causes certain difficulties in the further development of quantum predicate-transformer semantics; for example, some logical operations of quantum predicates are not always well defined. To avoid these obstacles, we choose to consider a special class of quantum predicates, namely projection operators, in this section. Since the notion of projection operator is equivalent to that of closed subspace in a Hilbert space, we do not distinguish a closed subspace from the projector onto it, and for the most part we directly deal with closed subspaces in the sequel for simplicity of presentation.

8.4.1 Orthomodular Lattices

To describe the algebraic structure of the set of closed subspaces of a Hilbert space, we briefly recall some basic notions from the theory of orthomodular lattices; for more details we refer to Bruns and Harding (2000) and Kalmbach (1983). A complete orthomodular lattice is a 5-tuple \( L = (L, \leq, \wedge, \vee, \perp) \), where:

(i) \( (L, \leq, \wedge, \vee) \) is a complete lattice. Here, \( \leq \) is the partial ordering on \( L \), and for any \( M, N \subseteq L \), \( \wedge M \) and \( \vee M \) stand for the greatest lower bound and the least upper bound of \( M \), respectively. We use 0, 1 to denote the least and greatest elements of \( L \), respectively.

(ii) \( \perp \) is a unary operation on \( L \), called orthocomplement, and required to satisfy the following conditions:

(a) \( a \wedge a^\perp = 0 \); 
(b) \( a^\perp \perp = a \); and 
(c) \( a \leq b \) implies \( b^\perp \leq a^\perp \) for any \( a, b \in L \).

It is easy to see that the condition (ii)(c) is equivalent to one of the De Morgan laws: \( (a \wedge b)^\perp = a^\perp \vee b^\perp \) and \( (a \vee b)^\perp = a^\perp \wedge b^\perp \) for any \( a, b \in L \). A complete orthomodular lattice is a complete ortholattice \( L = (L, \leq, \wedge, \vee, \perp) \) satisfying the orthomodular law:

\[
a \leq b \implies a \vee (a^\perp \wedge b) = b
\]

for all \( a, b \in L \). The orthomodular law can be replaced by the following equation:

\[
a \vee (a^\perp \wedge (a \vee b)) = a \vee b \quad \text{for any } a, b \in L.
\]

A complete Boolean algebra is a complete ortholattice \( L = (L, \leq, \wedge, \vee, \perp) \) fulfilling the distributive law of join over meet:

\[
a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)
\]

for all \( a, b, c \in L \). With the De Morgan law it is easy to know that this condition is equivalent to the distributive law of meet over join: \( a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \) for any \( a, b, c \in L \). Obviously, the distributive law implies the orthomodular law, and so a complete Boolean algebra is a complete orthomodular lattice.

A central notion in the theory of orthomodular lattices is commutativity of elements. Let \( L = (L, \leq, \wedge, \vee, \perp) \) be a complete ortholattice, and let \( a, b \in L \). We say that \( a \) commutes with \( b \), in symbols \( a \circ b \), if we have:

\[
a = (a \wedge b) \vee (a \wedge b^\perp)
\]

The following lemma indicates that commutativity is preserved by lattice-theoretic operations.

Lemma 8.4.1 (Bruns and Harding 2000). Let \( L = (L, \leq, \wedge, \vee, \perp) \) be an orthomodular lattice, and let \( a \in L \) and \( b_i \in L \) (\( i \in I \)). If \( a \circ b_i \) for all \( i \in I \), then \( a \circ (\bigwedge_{i \in I} b_i) \) and \( a \circ (\bigvee_{i \in I} b_i) \) exist.

Proof. For any \( i, j, k, l \), it holds that

\[
(\psi, e_1)(M \otimes I_k)PU|e_0\rangle|e_0\rangle(U^\dagger P(N \otimes I_l)\psi, e_0) = h_{ijkl}(\psi, e_1)(PU|e_0\rangle|e_0\rangle(U^\dagger P)|\psi, e_0\rangle).
\]

If \( h_{ijkl} = h_{ijkl} \) or \( \langle e_0\rangle(U^\dagger P)|\psi, e_0\rangle \perp \langle e_0\rangle(U^\dagger P)|\psi, e_0\rangle \), i.e.,

\[
(\psi, e_1)(U^\dagger P|e_0\rangle|e_0\rangle(U^\dagger P)|\psi, e_0\rangle = 0,
\]

then we have:

\[
(\psi, e_1)(M \otimes I_k)PU|e_0\rangle|e_0\rangle(U^\dagger P(N \otimes I_l)\psi, e_0) = (\psi, e_1)(M \otimes I_k)PU|e_0\rangle|e_0\rangle(U^\dagger P(M \otimes I_k)\psi, e_0).
\]

This means that

\[
(M \otimes I_k)PU|e_0\rangle|e_0\rangle(U^\dagger P(N \otimes I_l) = (N \otimes I_k)PU|e_0\rangle|e_0\rangle(U^\dagger P(M \otimes I_k)\psi, e_0).
\]

Thus, the conclusion follows immediately from Proposition 8.3.19. □

To conclude this section, we would like to point out that some sufficient conditions for commutativity of quantum weakest preconditions have been presented here, but the problem of finding a sufficient and necessary condition for this commutativity for a general quantum program is still open and seems very difficult. A even more general topic for further studies would be:
The major difference between a Boolean algebra and an orthomodular lattice is that in general distributivity is not valid in the latter. However, a local distributivity can be recovered for orthomodular lattices by attaching commutativity.

**Lemma 8.4.2** (Bruns and Harding 2000). Let \( \mathcal{L} = (L, \leq, \wedge, \vee, \bot) \) be an orthomodular lattice. For any \( a \in L \) and \( b_i \in L (i \in I) \), if \( a \sqcap b_i \) for all \( i \in I \), then
\[
a \sqcup \left( \bigvee_{i \in I} b_i \right) = \bigvee_{i \in I} (a \sqcap b_i),
\]
provided \( \bigwedge_{i \in I} b_i \) and \( \bigvee_{i \in I} b_i \) exist.

Furthermore, the foregoing lemma can be generalized considerably by introducing the notion of commutator. Let \( \mathcal{L} = (L, \leq, \wedge, \vee, \bot) \) be an orthomodular lattice, and let \( A \subseteq L \). The strong commutator \( \Gamma(A) \) of \( A \) is defined by
\[
\Gamma(A) = \bigvee \{ b : a \sqcap b \text{ for all } a \in A, \text{ and } (a \wedge b)(a_k \wedge b) \text{ for all } a_k, b_k \in A \}.
\]
If \( A \) is finite, then the commutator \( \gamma(A) \) of \( A \) is defined by
\[
\gamma(A) = \bigvee \{ \bigwedge_{a \in A} a^{(a)} : f : A \rightarrow \{1, -1\} \text{ is a mapping} \},
\]
where \( a^{(a)} \) denotes \( a \) itself and \( a^{-1} \) denotes \( a^\perp \). The relation between commutator and strong commutator is clarified by the following lemma. In addition, the third item of the following lemma shows that commutator is a relativization of the notion of commutativity.

**Lemma 8.4.3** (Takeuti 1981). Let \( \mathcal{L} = (L, \leq, \wedge, \vee, \bot) \) be an orthomodular lattice and let \( A \subseteq L \). Then

(i) \( \Gamma(A) \leq \gamma(A) \).

(ii) If \( A \) is finite, then \( \Gamma(A) = \gamma(A) \).

(iii) \( \gamma(A) = 1 \) if and only if all the members of \( A \) are mutually commutable.

The following theorem clarifies algebraic structures of the set of closed subspaces of a Hilbert space.

**Theorem 8.4.6** (Sasaki) (Kalmbach 1983). \( (S(H), \sqsubseteq, \sqcap, \sqcup, \bot) \) is a complete orthomodular lattice, where the partial order \( \subseteq \) is the set inclusion, the smallest element is the 0-dimensional subspace \( \{0\} \), the largest element is \( H \), and for any \( M \subseteq S(H) \), we have:
\[
\bigwedge_{X \in M} X = \bigcap_{X \in M} X, \quad \bigvee_{X \in M} X = \bigcup_{X \in M} X.
\]

The orthocomplement of \( X \) is defined to be
\[
X^\perp = \{ \psi : X \} \forall \psi \in A \}.
\]

The orthocomplement of \( X \) is defined to be
\[
X^\perp = \{ \psi : X \} \forall \psi \in A \}.
\]

Finally, the following lemma clarifies algebraic structures of the set of closed subspaces of a Hilbert space.

**Theorem 8.4.6** (Sasaki) (Kalmbach 1983). \( (S(H), \sqsubseteq, \sqcap, \sqcup, \bot) \) is a complete orthomodular lattice, where the partial order \( \subseteq \) is the set inclusion, the smallest element is the 0-dimensional subspace \( \{0\} \), the largest element is \( H \), and for any \( M \subseteq S(H) \), we have:
\[
\bigwedge_{X \in M} X = \bigcap_{X \in M} X, \quad \bigvee_{X \in M} X = \bigcup_{X \in M} X.
\]

We shall need the following lemma, which was proved by the author in Ying (2005) and extensively used in automata theory based on quantum logic (Ying 2000, 2005, 2007).

**Lemma 8.4.5** (Ying 2005). Let \( \mathcal{L} = (L, \leq, \wedge, \vee, \bot) \) be an orthomodular lattice and let \( A \subseteq L \). Then for any \( B \subseteq [A] \) we have \( \Gamma(A) \leq \Gamma(B) \), where \( [A] \) stands for the subalgebra of \( \mathcal{L} \) generated by \( A \).

**8.4.2 Subspaces of a Hilbert Space**

We now are ready to examine the algebraic structure of closed subspaces of a Hilbert space. Let \( \mathcal{H} \) be a Hilbert space. For any \( X \subseteq \mathcal{H} \), we write:
\[
\text{span}(X) = \bigcap \{ Y \subseteq \mathcal{H} : X \subseteq Y \}
\]
Then \( \text{span}(X) \) is the smallest subspace of \( \mathcal{H} \) containing \( X \), and it is called the subspace of \( \mathcal{H} \) generated by \( X \). It is obvious that \( \text{span}(X) \) is the set of linear combinations of vectors in \( X \); that is,
\[
\text{span}(X) = \{ \sum_{i=1}^{n} \alpha_i \psi_i : n \geq 1, \alpha_i \in \mathbb{C} \text{ and } \psi_i \in X \text{ for all } 1 \leq i \leq n \}.
\]

The set of closed subspaces of \( \mathcal{H} \) is denoted by \( S(\mathcal{H}) \). If we identify each closed subspace \( X \) of \( \mathcal{H} \) with the projector \( P_X \), then \( S(\mathcal{H}) \) can be seen as a subset of \( \mathcal{P}(\mathcal{H}) \). Moreover, the inclusion relation coincides with the Löwner partial order in \( S(\mathcal{H}) \); for any \( X, Y \subseteq S(\mathcal{H}) \), \( X \subseteq Y \) if and only if \( P_Y \subseteq P_X \). For any \( X, Y \subseteq S(\mathcal{H}) \), if \( |\psi \rangle \perp \langle \psi | \) for all \( |\psi \rangle \in X \) and \( \langle \psi | \in Y \), then \( X \text{ and } Y \) are said to be orthogonal, and we write \( X \perp Y \); in particular we simply write \( \langle \psi | \perp Y \). The orthocomplement of \( X \) is defined to be
\[
X^\perp = \{ \psi : X \} \forall \psi \in X \}.
\]

The following theorem clarifies algebraic structures of the set of closed subspaces of a Hilbert space.

**Theorem 8.4.6** (Sasaki) (Kalmbach 1983). \( (S(H), \sqsubseteq, \sqcap, \sqcup, \bot) \) is a complete orthomodular lattice, where the partial order \( \subseteq \) is the set inclusion, the smallest element is the 0-dimensional subspace \( \{0\} \), the largest element is \( H \), and for any \( M \subseteq S(H) \), we have:
\[
\bigwedge_{X \in M} X = \bigcap_{X \in M} X, \quad \bigvee_{X \in M} X = \bigcup_{X \in M} X.
\]

**8.4.3 Projective Predicate Transformers**

With the preliminaries given in the previous subsections, we are able to deal with the special class of quantum predicate transformers where only projection
operators are considered as quantum predicates. Assume that $\mathcal{H}$ is a Hilbert space. Then a closed subspace of $\mathcal{H}$ is called a projective predicate on $\mathcal{H}$. A projective predicate transformer on $\mathcal{H}$ is a mapping from the set $\mathcal{S}(\mathcal{H})$ of projective predicates into itself. The set of projective predicate transformers on $\mathcal{H}$ is denoted by $\text{QPT}(\mathcal{H})$, i.e.,

$$\text{QPT}(\mathcal{H}) = \mathcal{S}(\mathcal{H})^\mathcal{S}(\mathcal{H}).$$

We may introduce a partial order on $\text{QPT}(\mathcal{H})$ in a pointwise way: for any quantum predicate transformers $f, g \in \text{QPT}(\mathcal{H})$, $f \leq g$ if $f(X) \leq g(X)$ for all $X \in \mathcal{S}(\mathcal{H})$.

The next lemma follows immediately from Theorem 8.4.6.

**Lemma 8.4.7.** The set $(\text{QPT}(\mathcal{H}), \leq)$ of quantum predicate transformers on $\mathcal{H}$ is a complete orthomodular lattice.

(i) Its smallest and largest elements are denoted by $\mathbf{0}, \mathbf{1}$, respectively, and they are defined by $\mathbf{0}(X) = \{\emptyset\}$ (the 0-dimensional subspace of $\mathcal{H}$), and $\mathbf{1}(X) = \mathcal{H}$ for each $X \in \mathcal{S}(\mathcal{H})$.

(ii) For any $\mathcal{F} \subseteq \text{QPT}(\mathcal{H})$ and $X \in \mathcal{S}(\mathcal{H})$, we have:

$$\bigwedge_{f \in \mathcal{F}} f(X) = \bigwedge_{f \in \mathcal{F}} f(X),$$

$$\bigvee_{f \in \mathcal{F}} f(X) = \bigvee_{f \in \mathcal{F}} f(X).$$

A reward of focusing our attention on projection operators is that quantum predicates constitute a lattice in a natural way. Thus, various healthiness conditions (Dijkstra 1976; Hesselink 1992) can be easily generalized to the case of quantum predicate transformers.

**Definition 8.4.8.** Let $f$ be a projective predicate transformer on $\mathcal{H}$. Then

(i) $f$ is said to be monotone if $X \subseteq Y$ implies $f(X) \leq f(Y)$ for any $X, Y \in \mathcal{S}(\mathcal{H})$.

(ii) $f$ is said to be finitely conjunctive if $f(X \land Y) = f(X) \land f(Y)$ for any $X, Y \in \mathcal{S}(\mathcal{H})$.

(iii) $f$ is said to be positively conjunctive if

$$f(\bigvee_{\mu \in \mathcal{M}} \mu) = \bigvee_{\mu \in \mathcal{M}} f(\mu) \quad (8.10)$$

for any nonempty $\mathcal{M} \subseteq \mathcal{S}(\mathcal{H})$.

(iv) $f$ is said to be universally conjunctive if it is positively conjunctive and $f(\mathbf{1}) = \mathbf{1}$.

(v) $f$ is said to be finitely disjunctive if $f(X \lor Y) = f(X) \lor f(Y)$ for any $X, Y \in \mathcal{S}(\mathcal{H})$.

(vi) $f$ is said to be positively disjunctive if

$$f(\bigvee_{\mu \in \mathcal{M}} \mu) = \bigvee_{\mu \in \mathcal{M}} f(\mu) \quad (8.11)$$

for any nonempty $\mathcal{M} \subseteq \mathcal{S}(\mathcal{H})$.

(vii) $f$ is said to be universally disjunctive if it is positively disjunctive and $f(\mathbf{1}) = \mathbf{1}$.

(viii) $f$ is said to be upper-continuous if Equation (8.10) holds whenever $\emptyset \neq \mathcal{M} \subseteq \mathcal{S}(\mathcal{H})$ is a chain, i.e., it always holds that $X \subseteq Y$ or $Y \subseteq X$ for any $X, Y \in \mathcal{M}$.

(ix) $f$ is said to be lower-continuous if Equation (8.11) holds whenever $\emptyset \neq \mathcal{M} \subseteq \mathcal{S}(\mathcal{H})$ is a chain.

We write $\text{QMT}(\mathcal{H}), \text{QMC}(\mathcal{H}), \text{QMP}(\mathcal{H})$, and $\text{QMU}(\mathcal{H})$ for the sets of monotone, finitely conjunctive, positively conjunctive, and universally conjunctive projective predicate transformers on $\mathcal{H}$, respectively. In addition, we write $\text{QMP}(\mathcal{H}), \text{QMC}(\mathcal{H}), \text{QMP}(\mathcal{H}), \text{QMP}(\mathcal{H})$, and $\text{QMP}(\mathcal{H})$ for the sets of finitely disjunctive, upper-continuous, lower-continuous, positively disjunctive, and universally disjunctive projective predicate transformers on $\mathcal{H}$, respectively. Obviously, we have:

- $\text{QMC}(\mathcal{H}) \subseteq \text{QMP}(\mathcal{H}) \subseteq \text{QMC}(\mathcal{H})$;
- $\text{QMP}(\mathcal{H}) \subseteq \text{QMD}(\mathcal{H}) \subseteq \text{QMD}(\mathcal{H})$;
- $\text{QMC}(\mathcal{H}) \subseteq \text{QMD}(\mathcal{H})$;
- $\text{QMC}(\mathcal{H}) \subseteq \text{QCC}(\mathcal{H}) \subseteq \text{QMT}(\mathcal{H})$.

The following lemma clarifies further the relationship among the preceding spaces of projective predicate transformers.

**Lemma 8.4.9.**

(i) $\text{QMT}(\mathcal{H})$ is a complete sublattice of $\text{QPT}(\mathcal{H})$.

(ii) $\text{QMC}(\mathcal{H}), \text{QMP}(\mathcal{H}), \text{QCC}(\mathcal{H})$ and $\text{QMC}(\mathcal{H})$ are all inf-closed in $\text{QPT}(\mathcal{H})$.

(iii) $\text{QMP}(\mathcal{H}), \text{QMD}(\mathcal{H}), \text{QMC}(\mathcal{H})$ and $\text{QMD}(\mathcal{H})$ are all sup-closed in $\text{QPT}(\mathcal{H})$.

We now present a simple example to illustrate the notions previously introduced.

**Example 8.4.10.** Let $A : \mathcal{H} \to \mathcal{H}$ be a bounded linear operator. We define mapping $A^{-1} : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ by

$$A^{-1}(X) = \{\psi \in \mathcal{H} : A(\psi) \in X\}$$

for each $X \in \mathcal{S}(\mathcal{H})$. For any $X \in \mathcal{S}(\mathcal{H})$, it is easy to check that $A^{-1}(X)$ is a subspace of $\mathcal{H}$, and closeness of $A^{-1}(X)$ follows immediately from continuity of $A$. Thus, $A^{-1}$ is a projective predicate transformer. It is easy to see that $A^{-1}$ is
universally conjunctive. At the same time, $A^{-1}$ is universally disjunctive, i.e.,

$$A^{-1}(\bigvee_i X_i) = \bigvee_i A^{-1}(X_i)$$

for any $X_i \in S(\mathcal{H})$. In fact,

$$A^{-1}(\bigvee_i X_i) = A^{-1}\left(\bigcup_i Y \in S(\mathcal{H}) : X_i \subseteq Y \text{ for all } i\right)$$

$$= \bigcup_i A^{-1}(Y) : X_i \subseteq Y \in S(\mathcal{H}) \text{ for all } i.$$ 

Note that $Y \in S(\mathcal{H})$ implies $A^{-1}(Y) \in S(\mathcal{H})$, and $X_i \subseteq Y$ implies $A^{-1}(X_i) \subseteq A^{-1}(Y)$. Thus, we have:

$$A^{-1}(\bigvee_i X_i) \subseteq \bigvee_i A^{-1}(X_i) \quad \text{for all } i.$$ 

(i) For any unitary operator $U$, we have:

$$U^{-1}(X) = (U^{-1} \rho) : |\psi\rangle \in X.$$ 

In particular, we consider some single qubit gates. Let $\mathcal{H}_2$ be the 2-dimensional Hilbert space. Then

$$S(\mathcal{H}_2) = \{|0\rangle, \langle 1| \}$$

where $\mathcal{H}(\alpha, \beta) = \{|\gamma(\alpha i \theta)\rangle : \gamma \in C\}$ is a 1-dimensional subspace of $\mathcal{H}_2$ for each $\alpha, \beta$. We first look at the most frequently used single qubit gates, Pauli matrices $X, Y,$ and $Z$, the Hadamard gate:

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

the phase gate:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

and the gate:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$ 

The predicate transformers $X^{-1}, Y^{-1}, Z^{-1}, H^{-1}, S^{-1}$ and $T^{-1}$ are given by

$$X^{-1}(\mathcal{H}(\alpha, \beta)) = X(\mathcal{H}(\alpha, \beta)) = \mathcal{H}(\beta, \alpha),$$

$$Y^{-1}(\mathcal{H}(\alpha, \beta)) = Y(\mathcal{H}(\alpha, \beta)) = \mathcal{H}(\beta, \alpha),$$

$$Z^{-1}(\mathcal{H}(\alpha, \beta)) = Z(\mathcal{H}(\alpha, \beta)) = \mathcal{H}(\alpha, -\beta),$$

$$S^{-1}(\mathcal{H}(\alpha, \beta)) = \mathcal{H}(\alpha, -i\beta),$$

$$T^{-1}(\mathcal{H}(\alpha, \beta)) = \mathcal{H}(\alpha, e^{-i\pi/4} \beta).$$

for all $\alpha, \beta$. In general, each unitary operation on a single qubit can be written in the form of $U = e^{i\theta} R_z(\phi) R_y(\psi) R_x(\delta)$, where $\lambda, \mu, \nu,$ and $\delta$ are real numbers,

$$R_z(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}, \quad R_y(\psi) = \begin{pmatrix} \cos \frac{\psi}{2} & -\sin \frac{\psi}{2} \\ \sin \frac{\psi}{2} & \cos \frac{\psi}{2} \end{pmatrix}$$

are the rotation operators about y and z axes, respectively (Nielsen and Chuang 2000). Then the predicate transformer $U^{-1}$ is given by

$$U^{-1}(\mathcal{H}(\alpha, \beta)) = H(\alpha \cos \frac{\psi}{2} + \beta e^{i\phi} \sin \frac{\theta}{2}, \beta e^{i\phi} \cos \frac{\psi}{2} - \alpha e^{i\phi} \sin \frac{\theta}{2}).$$

(ii) For any quantum measurement $\{M_\alpha \}$, if $X \in S(\mathcal{H})$, then

$$M_\alpha^{-1}(X) = \{ |\psi\rangle \in \mathcal{H} : |\rho_\alpha\rangle \in X \}$$

is the set of quantum states such that the postmeasurement states will lie in $X$ whenever we perform measurement $\{M_\alpha \}$ on them and the outcome $m$ is reported. In particular, we consider the computational basis measurement

$$\{ p_0 = |0\rangle \langle 0|, p_1 = |1\rangle \langle 1| \}$$

on the first qubit of a 2-qubit system. For $i = 0, 1$, if we hope that the measurement outcome is $i$ and the postmeasurement state is in the 1-dimensional space $\mathcal{H}_1(\alpha, \beta)$, then the state of the system before the measurement should be in

$$P_i^{-1}(\mathcal{H}_1(\alpha, \beta)) = \{ |\gamma(\alpha i \theta)\rangle : \gamma \in C\}.$$ 

8.4.4 Projective Weakest Preconditions

In Section 8.3 the forward semantics of quantum programs is given in terms of superoperators. The backward semantics of a quantum program is defined to be a mapping from the set of Hermitian operators bounded by $0_\mathcal{H}$ and $I_\mathcal{H}$ into itself. In particular, it follows from Proposition 8.3.5 that the weakest precondition of a quantum program is also a superoperator. In the present section, we decided to consider only projective predicates, and then backward semantics of quantum programs is represented by mappings from the set of closed subspaces of the state space into itself. What is the corresponding forward semantics of quantum programs? Quantum programs are constructed from two kinds of quantum commands: unitary transformations and quantum measurements. A unitary transformation is a bijection from the state space onto itself. On the other hand, a quantum measurement introduces certain probabilism. Roughly speaking, a quantum measurement transforms a quantum state to a set of quantum states, namely the postmeasurement states. Thus, a measurement can be seen as a one-to-many mapping from the state space into itself if the vectors used to represent the postmeasurement states are allowed to be not normalized and the probabilities of measurement outcomes are encoded into the lengths of these vectors. Furthermore, nondeterminate choice is a basic program constructor, and we hope it can
be accommodated well in the forward semantics of quantum programs. Again, nondeterministic choice leads us to consider one-to-many mappings from the state space into itself. Note that a one-to-many mapping from a set $X$ into itself can be equivalently treated as a mapping from the power set of $X$ into itself. This, together with the consideration of preserving algebraic and topological structures in the state space, motivates us to define (the forward semantics of) a quantum program as a mapping from the set of closed subspaces of the state space into itself.

**Definition 8.4.11.** A mapping $t$ from $S(H)$ into itself is called a quantum program if it is lower-continuous, i.e., for any increasing sequences $\{X_n\}_{n=0}^{\infty}$ of closed subspaces of $H$,

$$t(\bigvee_{n=0}^{\infty} X_n) = \bigvee_{n=0}^{\infty} t(X_n).$$

At first glance, the foregoing definition coincides with the definition of lower-continuous projective predicate transformer (see Definition 8.4.8(ix)). However, an essential difference exists between them: a quantum program in Definition 8.4.11 is forward, whereas a projective predicate transformer is backward. More precisely, let $H_0 = H_1 = H$. Then a mapping $t : S(H_0) \to S(H_1)$ is seen as a quantum program from $H_0$ to $H_1$, but a mapping $f : S(H_1) \to S(H_0)$ is treated as a predicate transformer from $H_1$ to $H_0$. This is similar to the case of classical programs.

The notions of Hoare assertion and weakest precondition can be defined in the setting of projective predicates in a familiar way.

**Definition 8.4.12.** Let $t$ be a mapping from $S(H)$ into itself:

(i) For any $X, Y \in S(H)$, we write $X(t)Y$ if $t(X) \subseteq Y$.

(ii) For any $X \in S(H)$, the weakest precondition of $X$ with respect to $t$ is defined to be a closed subspace $wp(t)(X)$ of $H$ satisfying the following conditions:

(a) $wp(t)(X) \subseteq X$;

(b) for any $Y \in S(H)$, $Y(t)X$ implies $Y \subseteq wp(t)(X)$.

### 8.4.5 The D'Hondt-Panangaden Weakest Preconditions versus Projective Weakest Preconditions

In this subsection we deviate from the right path to examine the relationship between projective weakest preconditions and the D'Hondt and Panangaden weakest preconditions defined in Section 8.3. We first consider a special class of quantum programs that are represented by superoperators preserving projectors.

**Definition 8.4.13.**

(i) Let $E \in SO(H)$. If for any $X \in S(H)$, there exists $Y \in S(H)$ such that $E(P_x) = \lambda P_y$ for some $0 < \lambda \leq 1$, then we say that $E$ preserves projectors.

(ii) Let $E \in SO(H)$ preserves projectors. Then the restriction $t_E$ of $E$ on $S(H)$ is defined as follows: For each $X \in S(H)$, if $E(P_x) = \lambda P_y$, then $t_E(X) = Y$.

We note that if $E(P_x) = \lambda P_y$ and $E(P_y) = \mu P_z$ then $Y = Z$. So, $t_E$ is well-defined.

To simplify the presentation, we introduce an auxiliary notion. For any $X, Y \in S(H)$, we define the cosine of the angle between $X$ and $Y$ as follows:

$$\cos(X, Y) = \frac{\dim X \dim Y}{\sum_{i=1}^{\dim X} \sum_{j=1}^{\dim Y} |\langle \psi_i | \psi_j \rangle|^2},$$

where $\{|\psi_i\rangle\}_{i=1}^{\dim H}$ is an orthonormal basis of $H$ such that $|\psi_i\rangle \in X$ for all $i \leq \dim X$ and $|\psi_j\rangle \in Y$ for all $j \leq \dim Y$ and $|\langle \psi_i | \psi_j \rangle|_{i<j}^{\dim H}$ is an orthonormal basis of $H$ such that $|\psi_j\rangle \in Y$ for all $j \leq \dim Y$ and $|\psi_i\rangle \in X$ for all $i \leq \dim X$. It is easy to show that $\cos(X, Y)$ does not depend on the choices of $\{|\psi_i\rangle\}$ and $\{|\psi_j\rangle\}$.

The following technical lemmas will be used in the proofs of the main results in this subsection.

**Lemma 8.4.14.** Let $X, X_1, X_2, Y \in S(H)$. Then we have:

(i) $\cos(X, Y) = \cos(Y, X) = \sqrt{tr(P_x P_y)}$, 

(ii) $X_1 \subseteq X_2$ implies $\cos(X_1, Y) \leq \cos(X_2, Y)$, 

(iii) $\cos(X, Y) \leq \min(\dim X, \sqrt{\dim Y})$, and $\cos(X, Y) = \sqrt{\dim X}$ if and only if $X \subseteq Y$.

**Proof.** Suppose that both $\{|\psi_i\rangle\}$ and $\{|\psi_j\rangle\}$ are orthonormal bases of $H$, $|\psi_i\rangle \in X$ for all $i \leq \dim X$, $|\psi_j\rangle \in X^2$ for all $i > \dim X$, $|\psi_j\rangle \in Y$ for all $j \leq \dim Y$, and $|\psi_j\rangle \in Y^2$ for all $j > \dim Y$. Then

$$tr(P_x P_y) = tr(\sum_{i=1}^{\dim X} |\psi_i\rangle \langle \psi_i|) \cdot \sum_{j=1}^{\dim Y} |\psi_j\rangle \langle \psi_j|)$$

$$= \sum_{i=1}^{\dim X} \sum_{j=1}^{\dim Y} tr(|\psi_i\rangle \langle \psi_i| |\psi_j\rangle \langle \psi_j|)$$

$$= \sum_{i=1}^{\dim X} \sum_{j=1}^{\dim Y} |\langle \psi_i | \psi_j \rangle|^2$$

$$= \cos(X, Y)^2$$

$$\leq \dim X \dim Y$$

$$\leq \sum_{i=1}^{\dim X} \sum_{j=1}^{\dim Y} |\langle \psi_i | \psi_j \rangle|^2$$

$$= \sum_{i=1}^{\dim X} ||\psi_i||^2$$

$$= \dim X.$$

If $\cos(X, Y) = \sqrt{\dim X}$, then

$$\sum_{i=1}^{\dim X} ||\psi_i||^2 = 1$$

for all $i \leq \dim X$. This implies $|\psi_i\rangle \in Y$ for all $i \leq \dim X$, and $X \subseteq Y$. \qed
Lemma 8.4.15. Let \( \mathcal{E} \in SO(H) \) preserve projectors, let \( X, Y \in \mathcal{S}(H) \), and let \( X \) be finite-dimensional. If for all \( \rho \in D(H) \), we have:
\[
\text{tr}(P_{\lambda} \rho) \leq \text{tr}(P_{\lambda} \mathcal{E}(\rho)),
\]
then \( t_\mathcal{E}(X) \subseteq Y \).

Proof. \((\Leftarrow)\) Suppose that \( \mathcal{E}(P_{\lambda}) = \lambda P_{\lambda} \). Since \( X \) is a finite-dimensional subspace of \( H \), we have:
\[
\frac{1}{\dim(X)} P_{\lambda} \in D(H),
\]
where \( \dim(X) \) is the dimension of \( X \). Then we obtain:
\[
\text{tr}(\frac{\lambda}{\dim(X)} P_{\lambda}) = \text{tr}(\frac{\lambda}{\dim(X)} \mathcal{E}(P_{\lambda})) \leq \text{tr}(\frac{1}{\dim(X)} P_{\lambda}) = 1
\]
from the definition of superoperator. This implies that \( Z \) is finite-dimensional.

Thus, it follows that
\[
\frac{\lambda \dim(Z)}{\dim(X)} = \text{tr}(\frac{\lambda}{\dim(X)} P_{\lambda}) \leq 1
\]
and
\[
\lambda \leq \frac{\dim(X)}{\dim(Z)}
\]

Putting
\[
\rho = \frac{1}{\dim(X)} P_{\lambda},
\]
we get:
\[
1 = \frac{1}{\dim(X)} \text{tr}(P_{\lambda})
= \frac{1}{\dim(X)} \text{tr}(P_{\lambda} P_{\lambda})
= \text{tr}(P_{\lambda} P_{\lambda})
\leq \text{tr}(P_{\lambda} \mathcal{E}(\rho))
= \frac{\lambda}{\dim(X)} \text{tr}(P_{\lambda} \mathcal{E}(P_{\lambda}))
= \frac{\lambda}{\dim(X)} \text{tr}(P_{\lambda} P_{\lambda})
\leq \frac{1}{\dim(Z)} \text{tr}(P_{\lambda} P_{\lambda})
\]
and \( \dim(Z) \leq \text{tr}(P_{\lambda} P_{\lambda}) \). Therefore, using Lemma 8.4.14 we obtain \( t_\mathcal{E}(X) = Z \subseteq Y \). \(\Box\)

Suppose that \( \mathcal{E} \in SO(H) \) is a quantum program preserving projectors. Of course, the D'Hondt-Panangaden weakest precondition \( wp(\mathcal{E}) \) of \( \mathcal{E} \) can be defined in \( (P(H), \subseteq) \) according to Definition 8.3.4. On the other hand, the weakest precondition \( wp(t_\mathcal{E}) \) can be defined in \( (S(H), \subseteq) \) according to Definition 8.4.12. An interesting problem is to compare the restriction of \( wp(\mathcal{E}) \) on \( S(H) \) with \( wp(t_\mathcal{E}) \).

Proposition 8.4.16. Let \( \mathcal{E} \in SO(H) \) preserve projectors.

(i) For any \( X \in S(H) \), if \( Z \) is a finite-dimensional subspace of \( H \) and \( P_{\lambda} \subseteq wp(\mathcal{E}(P_{\lambda})) \), then \( Z \subseteq wp(t_\mathcal{E}(X)) \) for all \( \rho \in D(H) \).

(ii) If \( \mathcal{E} \) satisfies the condition: \( \rho \subseteq wp(\mathcal{E}(\rho)) \) for all \( \rho \in D(H) \), then for any \( X \in S(H) \), we have:
\[
P_{\mathcal{E}(X)} \subseteq wp(\mathcal{E}(P_{\lambda})).
\]

Proof.

(i) For any \( \rho \in D(H) \), we have:
\[
\text{tr}(P_{\lambda} \rho) \leq \text{tr}(wp(\mathcal{E}(P_{\lambda} \rho))) \leq \text{tr}(P_{\lambda} \mathcal{E}(\rho)).
\]

Then it follows from Lemma 8.4.15 that \( t_\mathcal{E}(Z) \subseteq X \), and by definition we obtain \( Z \subseteq wp(t_\mathcal{E}(X)) \).

(ii) Assume that \( Y = wp(t_\mathcal{E}(X)) \). Then \( t_\mathcal{E}(Y) \subseteq X \), i.e., \( \mathcal{E}(P_{\lambda}) = \lambda P_{\lambda} \) for some \( \lambda \) and \( Z \) with \( 0 < \lambda \leq 1 \) and \( X \supseteq Z \subseteq S(H) \). Now for any \( \rho \in D(H) \), by Proposition 8.3.5 we obtain:
\[
\text{tr}(P_{\lambda} \rho) \leq \text{tr}(\mathcal{E}(P_{\lambda} \rho)) \leq \text{tr}(P_{\lambda} \mathcal{E}(\rho)).
\]

Now we consider a partial inverse of the problem dealt with in the above proposition. Let \( i \) be a mapping from \( S(H) \) into itself satisfying the upper continuity:
\[
t\left( \bigcap_{\lambda \in \mu} E_\lambda \right) = \bigcap_{\lambda \in \mu} t(E_\lambda)
\]

Therefore, it holds that \( P_{\lambda} E_\lambda \subseteq wp(E_\lambda P_{\lambda}) \) follows. \(\Box\)
for any family \( \{E_n\}_{n \in \mathbb{N}} \) of closed subspaces of \( H \) with \( E_n \subseteq E_m \) whenever \( n \leq m \). Then \( t \) induces an operator \( E_t \) on \( \mathcal{L}(H) \) in the following way: Each bounded positive operator \( A \) can be written in the form of

\[
A = \int_0^b \lambda dE_{\lambda},
\]

by the spectral decomposition theorem, where \( b \geq 0 \), and \( E_{\lambda} \in \mathcal{S}(H) \) for any \( 0 \leq \lambda \leq b \). Then it follows from the upper continuity of \( t \) that \( |t(E_{\lambda})| \) is a spectral family, and we can define

\[
E_t(A) = \int_0^b \lambda dt(E_{\lambda}).
\]

Furthermore, \( E_t(A) \) can be defined for all \( A \in \mathcal{L}(H) \) by linearity. It is easy to check that \( E_t \) is a superoperator if \( \dim(t(X)) < \dim(X) \) for any \( X \in \mathcal{S}(H) \). On the other hand, if \( f \in \mathcal{Q}(\mathcal{L}(H)) \) is an upper-continuous projective predicate transformer, then we can define the extension \( f^* : \mathcal{P}(H) \to \mathcal{P}(H) \) of \( f \) in a similar way: for any \( M \in \mathcal{P}(H) \),

\[
f^*(M) = \int_0^1 \lambda dF_{\lambda} \tag{8.12}
\]

where \( M = \int_0^1 \lambda dF_{\lambda} \) is the spectral decomposition of \( M \).

**Proposition 8.4.17.** Let \( t \) be a mapping from \( \mathcal{S}(H) \) into itself satisfying the upper continuity and preserving the cosine of the angle between two closed subspaces of \( H \):

\[
\cos(X, Y) \leq \cos(t(X), t(Y))
\]

for any \( X, Y \in \mathcal{S}(H) \). Then we have \( wp(t)^*(M) \subseteq wp(E_t)(M) \), where \( wp(-) \) in the left-hand side and \( wp(-) \) in the right-hand side are given according to Definitions 8.4.12 and 8.3.4, respectively, and the extension \( * \) in the left-hand side is defined according to Equation (8.12).

**Proof (Outline).** The theory of spectral measures and integrals (see Prugovečki 1981, Chapter III.5) can be generalized to the case of positive operator-valued measures and integrals (Diestel and Uhl 1977) so that

\[
\int \lambda dA_{\lambda}
\]

is well defined, where \( \{A_{\lambda}\} \) is a family of positive operators. Furthermore, we have:

\[
A \cdot (\int \lambda dA_{\lambda}) = \int \lambda d(A_{\lambda}A), \tag{8.13}
\]

\[
(\int \lambda dA_{\lambda}) \cdot A = \int \lambda d(A_{\lambda}A), \tag{8.14}
\]

\[
tr(\int \lambda dA_{\lambda}) = \int \lambda dtr(A_{\lambda}), \tag{8.15}
\]

Thus, for any \( M \in \mathcal{P}(H) \), we show that \( wp(t)^*(M) \subseteq wp(E_t)(M) \). To this end, we only need to prove that \( wp(t)^*(M)(E_{\lambda})M, i.e.,

\[
tr(wp(t)^*(M)(E_{\lambda})M) \leq tr(wp(E_t)(M)(F_{\lambda})M)
\]

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

\[
M = \int_0^1 \lambda dE_{\lambda}, \quad \rho = \int_0^1 \mu dF_{\mu}
\]

are the spectral decompositions of \( M \) and \( \rho \), respectively. Then with Equations (8.13) and (8.14) we obtain:

\[
wp(t)^*(M)\rho = \left[ \int_0^1 \lambda dwp(t)(E_{\lambda}) \right] \cdot \rho
\]

\[
= \int_0^1 \lambda d\left[wwp(t)(E_{\lambda}) \cdot \rho \right]
\]

\[
= \int_0^1 \lambda d\left(wwp(t)(E_{\lambda}) \cdot \int_0^1 \mu dF_{\mu} \right]
\]

\[
= \int_0^1 \lambda d\left(\int_0^1 \mu dwp(t)(E_{\lambda}) \cdot F_{\mu} \right].
\]

Similarly, we have:

\[
wp(E_t)^*(M)\rho = \int_0^1 \lambda d\left(\int_0^1 \mu d(E_{\lambda} \cdot t(F_{\mu})) \right].
\]

Therefore, it follows from Equation (8.15) that

\[
tr(wp(t)^*(M)(E_{\lambda})M) \leq tr(wp(E_t)(M)(E_{\lambda})M).
\]

Consequently, it suffices to show that

\[
tr(wp(t)(E_{\lambda}) \cdot F_{\lambda}) \leq tr(E_{\lambda} \cdot t(F_{\lambda})).
\]

In fact, since \( wp(t)(E_{\lambda})t(E_{\lambda}) \), we have \( tr(wp(t)(E_{\lambda})t(E_{\lambda})) \leq E_{\lambda} \). Then by Lemma 8.4.14 and the assumption that \( t \) preserves the cosine of the angle between closed subspaces of \( H \), we obtain:

\[
tr(wp(t)(E_{\lambda}) \cdot F_{\lambda}) = \cos(wp(t)(E_{\lambda}), F_{\lambda})^2
\]

\[
\leq \cos(t(wp(t)(E_{\lambda})), t(F_{\lambda}))^2
\]

\[
\leq \cos(E_{\lambda}, t(F_{\lambda}))^2
\]

\[
\leq tr(E_{\lambda} \cdot t(F_{\lambda})).
\]

\(\square\)
8.4.6 Quantum Commands

The remaining part of this section is mainly devoted to defining the semantics of recursive procedures in the setting of projective predicates and to establish some of the fundamental properties of recursive procedures. We adopt the abstract syntax of commands with procedures and unbounded choices used in Hesselink (1992). The results obtained in the following subsections generalize the main results in Hesselink (1992) to the case of quantum programs by replacing classical predicates with projective predicates in the semantics of commands. This can be clearly seen from a comparison between the results presented later and the corresponding ones in Hesselink (1992). Following Hesselink (1992), let $S$ and $H$ be two sets of symbols. It is required that $S \cap H = \emptyset$. The elements of $S$ are called simple commands, and the elements of $H$ are called procedure names. We put $A = S \cup H$ and assume that $A$ does not contain the symbol $\epsilon$ and $\lambda$. The set of strings over $A$ is denoted by $A^\omega$. We shall use $\epsilon$ to denote the empty string, and concatenation of strings will be expressed by the infix operator $\cdot$. Intuitively, the concatenation $\cdot$ is used to denote sequential composition of commands. Furthermore, we write $A^0$ for the set of nonempty subsets of $A$, i.e., $A^0 = P(A^*) - \{ \emptyset \}$, where $P(\cdot)$ stands for power set. The elements of $A^0$ are called commands. A command $C \in A^0$ stands for the choice among the elements of $C$, which are also commands, whenever $C$ contains more than one element.

The recursive procedures are declared by a function

$$\text{body} : H \rightarrow A^0.$$ 

For each procedure name $h \in H$, the body function $\text{body}$ associates it to its body $\text{body}(h)$, which is a command expression that may contain occurrences of $h$ or other procedure names. Intuitively, the behavior of procedure $h$ is given by the defining equation $h = \text{body}(h)$. It is worth noting that recursive calls may happen because $h$ is allowed to appear in $\text{body}(h)$.

We can define two operations of commands. The sequential composition of two commands $C, D \in A^0$ is defined to be

$$C; D = \{ s; t : s \in C \text{ and } t \in D \},$$

and the (unbounded) choice of a nonempty family $C \subseteq A^0$ of commands is defined to be

$$\bigcup C \subseteq C = \bigcup_{C \subseteq C} C.$$

Semantics of commands is given in terms of homomorphisms from commands to quantum predicate transformers.

**Definition 8.4.18.** A homomorphism is a mapping $\varphi : A^0 \rightarrow \mathcal{QPT}(H)$ satisfying the following conditions:

(i) $\varphi(\epsilon) = 1_{\mathcal{QPT}(H)}$ (the identity mapping on $\mathcal{QPT}(H)$);
(ii) $\varphi(C; D) = \varphi(C) \circ \varphi(D)$;
(iii) $\varphi(\bigcup C \subseteq C) = \bigcup_{C \subseteq C} \varphi(C)$

for any $C, D \in A^0$ and $C \subseteq A^0$.

A homomorphism can be obtained by extending a mapping from simple commands and procedure names to projective predicate transformers in a natural way.

**Definition 8.4.19.** Let $\psi : A \rightarrow \mathcal{QPT}(H)$ be a mapping. Then:

(i) The extension $\psi^0$ of $\psi$ on $A^0$ is defined inductively as follows:
$$\psi^0(\epsilon) = 1_{\mathcal{QPT}(H)}$$
and $\psi^0(A) = \psi^0(A_1; A_2)$ for each $A_1 \in A$ and $A_2 \in A^0$.

(ii) The extension $\psi^\omega$ of $\psi$ on $A^\omega$ is defined by
$$\psi^\omega(C) = \bigcup_{C \subseteq C} \psi^0(C),$$
for any $C \in A^\omega$.

Some basic properties of the preceding extension are presented in the following lemma, and their routine proofs are omitted.

**Lemma 8.4.20.**

(i) If $\text{range}(\psi) \subseteq \mathcal{QMC}(H)$, then $\text{range}(\psi^0) \subseteq \mathcal{QMC}(H)$.

(ii) If $\text{range}(\psi) \subseteq \mathcal{QMU}(H)$, then $\psi^\omega$ is a homomorphism.

8.4.7 Knaster-Tarski Fixed Point Theorem

To define semantics of quantum procedures, we need the Knaster-Tarski fixed point theorem. For convenience of the reader, we briefly review it in this subsection. Let $L$ be a lattice and $D$ a mapping from $L$ into itself. If

$$D(U) = \{ D(w) : w \in U \} \subseteq U,$$
then $U$ is said to be $D$-invariant.

**Theorem 8.4.21 (Knaster-Tarski) (Hesselink 1992).** Let $L$ be a complete lattice, and let $D : L \rightarrow L$ be a monotone function. Then

(i) $D$ has a least fixed point $\text{lp}(D)$ and a greatest fixed point $\text{gfp}(D)$.

(ii) For any $D$-invariant subset $U$ of $L$, we have:

(a) $\text{lp}(D) \in U$ if $U$ is sup-closed, i.e., $\bigvee V \in U$ for all $V \subseteq U$;
(b) $\text{gfp}(D) \in U$ if $U$ is inf-closed, i.e., $\bigwedge V \in U$ for all $V \subseteq U$.

The upper and lower ordinal powers of a mapping $D : L \rightarrow L$ are defined as follows:
The next proposition gives an explicit representation of fixed points in terms of ordinal powers.

Proposition 8.4.22 (Lloyd 1987). Let \( L \) be a complete lattice, and let \( D : L \to L \) be monotone. Then

(i) \( D \uparrow \alpha \leq \text{lfp}(D) \) and \( \text{gfp}(D) \leq D \downarrow \alpha \) for any ordinal number \( \alpha \);
(ii) There exist ordinal numbers \( \alpha_0 \) and \( \alpha_1 \) such that \( D \uparrow \alpha = \text{lfp}(D) \) for all \( \alpha \geq \alpha_0 \), and \( D \downarrow \alpha = \text{gfp}(D) \) for all \( \alpha \geq \alpha_1 \).

The following proposition will be used in proving the termination law of quantum programs.

Proposition 8.4.23 (Hesselink 1992). Let \( L \) be a complete lattice and \( K \) a complete sublattice of \( L \), let \( f, g : \text{L} \to L \) be monotone mappings, and let \( f \downarrow K \) be the restriction of \( f \) on \( K \). Then

(i) \( D \uparrow \alpha \leq \text{lfp}(D) \) and \( \text{gfp}(D) \leq D \downarrow \alpha \) for any ordinal number \( \alpha \);
(ii) \( D \uparrow \alpha = \text{lfp}(D) \) if \( \alpha \) is a limit ordinal.

Theorem 8.4.27 (Universal conjunctivity of weakest liberal precondition).

Definition 8.4.25. Let \( w : S \to QMT(\mathcal{H}) \). Then:

(i) The weakest precondition function generated by \( w \) is defined to be \( \text{wlp}[w] = (w \cup \text{lfp}(D[w]))^\mathbb{N} \).

(ii) The weakest liberal precondition function generated by \( w \) is defined to be \( \text{wp}[w] = (w \cup \text{gfp}(D[w]))^\mathbb{N} \).

Lemma 8.4.26. For any \( w : S \to QMT(\mathcal{H}) \) and \( h \in H \), we have:

(i) \( \text{wp}[w](h) = \text{wp}[w](\text{body}(h)) \) and \( \text{wp}[w](h) = \text{wp}[w](\text{body}(h)) \);
(ii) If \( \text{range}(w) \subseteq QMU(\mathcal{H}), \text{then wp}[w] \) is a homomorphism.

Proof.

(i) is obvious from the definition of \( D[w] \) and Definition 8.4.25.

(ii) It follows from Lemma 8.4.4(ii) that \( QMU(\mathcal{H})^H \) is inf-closed. On the other hand, we see that \( D[w] \) is \( QMU(\mathcal{H})^H \)-invariant by a routine calculation. Then we have \( \text{gfp}(D[w]) \in QMU(\mathcal{H})^H \) by Theorem 8.4.22(i), and it follows from Definition 8.4.25(ii) and Lemma 8.4.26(ii) that \( \text{wp}[w] \) is a homomorphism. \( \square \)
Another important healthiness condition is termination law, which asserts that the total correctness of a program is the conjunction of the termination and the partial correctness of the program. It has been widely used in reasoning about total correctness of classical programs. The quantum version of termination law is not a straightforward generalization of the classical termination law. It requires some new insights from quantum logic, and its proof is much more skillful than that for classical programs (Hesselink 1992). To establish the quantum termination law, we first need to give two technical lemmas:

**Lemma 8.4.28.** Let \( X \in S(\mathcal{H}) \), and let \( w : S \to \mathcal{QM}T(\mathcal{H}) \) and \( u : H \to \mathcal{QM}T(\mathcal{H}) \). If for all \( a \in S \) and \( h \in H \), we have \( X \subseteq w(a)(X) \) and \( X \subseteq u(h)(X) \), then for all \( C \in A^\mathcal{H} \), it holds that

\[
X \subseteq (w \cup u)^\mathcal{H}(C)(X).
\]

**Proof.** We proceed by induction on the structure of \( C \). For the case of \( C = a \), it is obvious. If \( C = a \cup s \), where \( a \in A \) and \( s \in A^* \), then we obtain:

\[
(w \cup u)^\mathcal{H}(C)(X) = (w \cup u)^\mathcal{H}(a)(X) \\
= (w \cup u)^\mathcal{H}(a)(w \cup u)^\mathcal{H}(s)(X)) \\
\supseteq (w \cup u)^\mathcal{H}(a)(X) \\
\supseteq X
\]

from the induction hypothesis: \( X \subseteq (w \cup u)^\mathcal{H}(a)(X) \). In general, it follows that

\[
(w \cup u)^\mathcal{H}(C)(X) = \bigvee_{s \in C} (w \cup u)^\mathcal{H}(s)(X) \supseteq X
\]

from the induction hypothesis that \( X \subseteq (w \cup u)^\mathcal{H}(s)(X) \) for all \( s \in A^* \). \( \square \)

**Lemma 8.4.29.** Let \( X \in S(\mathcal{H}) \). If \( X \subseteq w(a)(X) \) for all \( a \in S \), then for all \( a \in A \) we have:

\[
X \subseteq w\{w[a](X).
\]

**Proof.** From Definition 8.4.25 we obtain:

\[
w\{w[a](X) = \begin{cases} 
    w(a)(X) & \text{if } a \in S, \\
    gfp(D[w])(a)(X) & \text{if } a \in H.
\end{cases}
\]

Therefore, it suffices to show that \( X \subseteq gfp(D[w])(h)(X) \). By Theorem 8.4.27, we only need to prove \( X \subseteq (D[w]) \downarrow a(h)(X) \) for all ordinal numbers \( a \), where \( D[w] \downarrow a \) is an ordinal power of \( D[w] \).

We proceed by transfinite induction on \( a \). If \( a = 0 \), then

\[
(D[w] \downarrow a)(h)(X) = H
\]

and the conclusion holds. Now assume that \( X \subseteq (D[w] \downarrow a)(h)(X) \). Then

\[
(D[w] \downarrow (a + 1))(h)(X) = D[w](D[w] \downarrow a)(h)(X) = (w \cup (D[w] \downarrow a))^{\mathcal{H}}(body(h))(X)
\]

and it follows from Lemma 8.4.28 that

\[
X \subseteq (D[w] \downarrow (a + 1))(h)(X).
\]

Finally, if \( a \) is a limit ordinal and \( X \subseteq (D[w] \downarrow \beta)(h)(X) \) for all \( \beta < a \), then

\[
X \subseteq \bigvee_{\beta < a}(D[w] \downarrow \beta)(h)(X) = (D[w] \downarrow a)(h)(X).
\]

To present the quantum termination law in a compact way, we need to introduce an auxiliary notation. For any \( w : S \to \mathcal{QM}T(\mathcal{H}) \), we write:

\[
\text{Range}(w) = \bigcup_{a \in S} w(a)(X) : X \in S(\mathcal{H}).
\]

**Theorem 8.4.30 (Termination law).** Suppose that \( w_1, w_2 : S \to \mathcal{QM}T(\mathcal{H}) \) satisfy the following condition:

\[
w_1(a)(X) = w_1(a)(\mathcal{H}) \land w_2(a)(X)
\]

for any \( a \in S \) and \( X \in S(\mathcal{H}) \). Then

(i) For any \( C \subseteq A^\mathcal{H} \) and \( X \in S(\mathcal{H}) \), we have:

\[
w_1(C)(X) \subseteq w_1(w_2)(C)(\gamma(M)) \land w_2(w_1)(C)(X).
\]

(ii) Let \( M \subseteq S(\mathcal{H}) \). If

(a) \( \text{Range}(w_1), \text{Range}(w_2) \subseteq M \),
(b) \( \Gamma(M) \subseteq w_1(a)(\Gamma(M)) \) for all \( a \in S \), and
(c) \( w_2(a) \) is universally conjunctive for all \( a \in S \),

then we have:

\[
w_1(w_2(C)(\gamma(M)) \land w_2(w_1)(C)(X) \land \Gamma(M) \subseteq w_1:w_2)(C)(X),
\]

where \( \Gamma(M) \) stands for the strong commutator of \( M \).

Note that if all the elements of \( M \) commute mutually then \( \Gamma(M) = H \), and condition (ii)(b) becomes a part of condition (ii)(c). Furthermore, we have:

\[
w_1(w_2(C)(\gamma(M)) \land w_1:w_2)(C)(X) = w_1:w_2)(C)(X)
\]

by combining the two parts of the theorem.

**Proof.**

(i) It is obvious that \( w_1(w_2(C)(\gamma(M)) \land w_1:w_2)(C)(X) \). So, we only need to show that

\[
w_1(w_2(C)(\gamma(M)) \land w_1:w_2)(C)(X).
\]
Since $w_1 \subseteq w_2$, we have $D[w_1] \subseteq D[w_2]$. Then we obtain:

$$\text{lfp}(D[w_1]) \leq \text{gfp}(D[w_1]) \leq \text{gfp}(D[w_2])$$

by Proposition 8.4.23, and it follows that

$$w_1 \subseteq (w_1 \cup \text{lfp}(D[w_1])) \subseteq (w_1 \cup \text{gfp}(D[w_1])) = w_2.$$

(ii) The proof of part (ii) consists of five claims. First, we write $[M]$ for the complete lattice of $S(\mathcal{H})$ generated by $M$. Put

$$W = \{u \in QM(\mathcal{H})^H : u(\mathcal{H}) \in [M] \text{ for all } h \in H \text{ and } X \in S(\mathcal{H})\}.$$

It is easy to see that $W$ is a complete lattice of $QM(\mathcal{H})^H$.

- **Claim 1.** $D[w_1] \uparrow \alpha, D[w_2] \downarrow \alpha \in W$ for all ordinal numbers $\alpha$, where $D[w_1] \uparrow \alpha, D[w_2] \downarrow \alpha$ are ordinal powers of $D[w_1]$ and $D[w_2]$, respectively.

The proof of this claim can be carried out by transfinite induction on $\alpha$, and it is routine and so omitted here. We only need to note that here the condition $\text{Range}(w_1), \text{Range}(w_2) \subseteq M$ is required.

Let $\text{lfp}(D[w_1])$ and $\text{gfp}(D[w_2])$ stand for the least fixed points of $D[w_1]$ in $QM(\mathcal{H})^H$ and $W$, respectively. In addition, let $\text{gfp}(D[w_1])$ and $\text{gfp}(D[w_2])$ be the greatest fixed points of $D[w_2]$ in $QM(\mathcal{H})^H$ and $W$, respectively. Then we have:

- **Claim 2.** $\text{lfp}(D[w_1]) = \text{gfp}(D[w_1]) = \text{gfp}(D[w_2])$.

In fact, we see that $\text{lfp}(D[w_1]), \text{gfp}(D[w_2]) \in W$ by combining claim 1 and Proposition 8.4.22. Then claim 2 follows immediately from Proposition 8.4.23.

Now we set

$$U = \{u \in W : u(\mathcal{H}) \leq \text{wlp}[w_2](u(\mathcal{H})) \leq \Gamma(M) \leq u(\mathcal{H}) \text{ for all } h \in H \text{ and } X \in S(\mathcal{H})\}.$$

- **Claim 3.** For each $u \in U$, we have:

$$(w_1 \cup u)^\ominus(C(X)) \leq \text{wlp}[w_2](u(C)(X)) \leq \Gamma(M) \leq (w_1 \cup u)^\ominus(C(X))$$

for all $C \in \mathcal{A}^0$ and $X \in S(\mathcal{H})$.

The proof of this claim is carried out by induction on the structure of $C$.

- **Case 1.** $C = a \in S$. Then we have:

$$(w_1 \cup u)^\ominus(C(X)) = w_1(a)(X),$$

$$(w_1 \cup u)^\ominus(C(\mathcal{H})) = w_1(a)(\mathcal{H}).$$

Thus, claim 3 follows from the assumption about $w_1$ and $w_2$.

- **Claim 4.** $U$ is $D[w_1]$-invariant.

- **Case 2.** $C = h \in H$. Then

$$(w_1 \cup u)^\ominus(C(\mathcal{H})) = u(h)(\mathcal{H}),$$

$$(w_1 \cup u)^\ominus(C(X)) = u(h)(X),$$

and claim 3 follows from the fact that $u \not\in U$.

- **Case 3.** $C = a \cup s$, where $a \in A$ and $s \in A^*$. For simplicity, we write:

$$LHS = (w_1 \cup u)^\ominus(C(\mathcal{H})) \land \text{wlp}[w_2](C(X)) \land \Gamma(M).$$

Then by using Lemma 8.4.29 we assert that $\Gamma(M) \subseteq \text{wlp}[w_2](a)(\Gamma(M))$, and it follows that

$$LHS \leq (w_1 \cup u)^\ominus(C(\mathcal{H})) \land \text{wlp}[w_2](a(C)(X)) \land \Gamma(M) \land \text{wlp}[w_2](a)(\text{wlp}[w_2](a)(X)) \land \Gamma(M).$$

Since $w_2(a)$ is universally conjunctive, we have:

$$LHS \leq (w_1 \cup u)^\ominus(C(\mathcal{H})) \land \text{wlp}[w_2](a)(w_1 \cup u)^\ominus(C(X)) \land \text{wlp}[w_2](a)(X) \land \Gamma(M).$$

by using Theorem 8.4.27 and the induction hypothesis on $s$ and $a$.

In general, the induction hypothesis on $s \in A^*$ leads to

$$LHS = \bigwedge_{s \in C} (w_1 \cup u)^\ominus(s)(\mathcal{H}) \land \bigwedge_{s \in C} \text{wlp}[w_2](s)(X) \land \Gamma(M)$$

$$= \bigwedge_{s \in C} (w_1 \cup u)^\ominus(s)(\mathcal{H}) \land \text{wlp}[w_2](s)(X) \land \Gamma(M)$$

and this completes the proof of claim 3.

- **Claim 4.** $U$ is $D[w_1]$-invariant.
In fact, for any \( u \in \mathcal{U} \), claim 3, together with Lemma 8.4.26, yields:

\[
D[w_1](u)(h)(X) = (w_1 \cup u)^\circ (\text{body}(h))(X) \leq D[w_1,\mathcal{U}](h)(X)
\]

This means \( D[w_1](u) \in \mathcal{U} \).  

Claim 5. \( \mathcal{U} \) is sup-closed.

It follows from Theorem 8.4.27 that

\[
wlp[w_2] = (w_2 \cup \text{gfp}(D[w_2]))^\circ \circ \text{body} = (w_2 \cup (D[w_2] \downarrow \alpha))^{\circ} \circ \text{body}
\]

for some ordinal number \( \alpha \). Then claim 1 implies \( wlp[w_2](h)(X) \in [\mathcal{M}] \) for all \( h \in \mathcal{H} \) and \( X \in \mathcal{S}(\mathcal{H}) \).

For any \( u \in \mathcal{U} \), we obtain:

\[
\bigwedge_{i \in I} w_2(h)(X) \land wlp[w_2](h)(X) \land \Gamma(M) = (w_2 \cup u)^\circ \circ (\text{body}(h))(X) \leq D[w_1,\mathcal{U}](h)(X)
\]

by Lemmas 8.4.4 and 8.4.5. Thus, \( \bigvee_{i \in I} u_i \in \mathcal{U} \).

Finally, combining claims 3, 4 and 5 and Theorem 8.4.27 we assert that \( \text{lfp}(D[w_1]) = \text{gfp}(D[w_1]) \in \mathcal{U} \), and we complete the proof by using Claim 3 once again and by noting that

\[
wp[w_1] = (w_1 \cup \text{gfp}(D[w_1]))^\circ.
\]

A weak version of universal conjunctivity of quantum weakest preconditions can be derived from universal conjunctivity of quantum weakest liberal preconditions and termination law.

Corollary 8.4.31. Let \( w_1, w_2 \) and \( M \) be as in Theorem 8.4.30. Then for each \( C \in \mathcal{A}^\circ \) we have:

(i) \( wp[w](C)(\bigvee_{i \in I} X_i) \leq \bigwedge_{i \in I} wp[w](C)(X_i) \).

(ii) If \( I \neq \emptyset \) then it holds that

\[
\bigwedge_{i \in I} wp[w](C)(X_i) \land \Gamma(M) \leq wp[w](C)(\bigwedge_{i \in I} X_i).
\]

8.4.10 Induction Rules

Hoare's induction rule (Hoare 1971) is a basic tool of establishing partial correctness of recursive procedures. It may be easily generalized to quantum programs with the projective predicate transformer semantics.

Theorem 8.4.32 (Hoare's induction rule). Let \( h_i \in \mathcal{H} \) \( (i \in I) \), let \( w : \mathcal{S} \rightarrow \text{QMT}(\mathcal{H}) \), and let \( X_i, Y_i \in \mathcal{S}(\mathcal{H}) \) \( (i \in I) \). Suppose that for all homomorphisms \( \varphi \) with \( \varphi[S] = w \),

\[
X_i \leq \varphi(h_i)(Y_i) \text{ for every } i \in I.
\]

implies

\[
X_i \leq \varphi(\text{body}(h_i))(Y_i) \text{ for every } i \in I.
\]

Then \( X_i \leq wlp[w](h_i)(Y_i) \) for every \( i \in I \).

Proof. Put

\[
\mathcal{U} = \{ u : \text{QMT}(\mathcal{H})^\circ : X_i \leq u(h_i)(Y_i) \text{ for all } i \in I \}.
\]

It is obvious that \( \mathcal{U} \) is inf-closed. For any \( u \in \mathcal{U} \), we see from Lemma 8.4.20 that \( (w \cup u)^\circ \) is a homomorphism. In addition, we have:

\[
(w \cup u)^\circ (h_i)(Y_i) = u(h_i)(Y_i) \supseteq X_i
\]

for all \( i \in I \), and \( (w \cup u)^\circ [S] = w \). Then the assumption yields:

\[
D[w](u)(h_i)(Y_i) = (w \cup u)^\circ (\text{body}(h_i))(Y_i) \supseteq X_i
\]

for all \( i \in I \). Hence, \( \mathcal{U} \) is \( D[w] \)-invariant. With Theorem 8.4.21 we obtain \( \text{gfp}(D[w]) \in \mathcal{U} \); that is,

\[
wp[w](h_i)(Y_i) = \text{gfp}(D[w])(h_i)(Y_i) \supseteq X_i
\]

for all \( i \in I \). □

Similarly, we are able to prove the following quantum generalization of Hesselink's necessity rule, which is useful for proving that a recursive procedure does not satisfy a specification (see Hesselink 1992, Section 2.7).

Theorem 8.4.33 (Hesselink's necessity rule). Let \( h_i \in \mathcal{H} \) \( (i \in I) \), let \( w : \mathcal{S} \rightarrow \text{QMT}(\mathcal{H}) \), and let \( X_i, Y_i \in \mathcal{S}(\mathcal{H}) \) \( (i \in I) \). Suppose that for all homomorphisms \( \varphi \) with \( \varphi[S] = w \),

\[
\varphi(h_i)(Y_i) \subseteq X_i \text{ for every } i \in I.
\]
implies
\[ \psi(\text{body}(h_i))(Y) \subseteq X, \text{ for every } i \in I. \]

Then \[ \text{wp}[u](h_i)(Y) \subseteq X, \text{ for every } i \in I. \]

8.5 Conclusion

This chapter presents a systematic exposition of predicate transformer semantics of quantum programs. The chapter is divided into two main parts. The first part is devoted to a thorough review of the D'Hondt-Panangaden approach to quantum predicate transformer semantics where quantum predicates are treated as observables with their eigenvalues within the unit interval. In the second part, we choose to deal with a special class of quantum predicates, namely projection operators. This allows us to establish a quite complete predicate transformer semantics for quantum programs by employing some powerful mathematical tools from Birkhoff-von Neumann quantum logic. In particular, various healthiness conditions are introduced, and the universal conjunctivity, termination law, and Hoare's induction rule are generalized into the quantum setting. The relationship between projective weakest preconditions and the D'Hondt-Panangaden quantum predicate transformer semantics and Kozen's probabilistic predicate transformer semantics. Furthermore, we believe that quantum backward semantic techniques and quantum refinement calculus will even find their applications in quantum engineering design, an area much wider than quantum programming.

Acknowledgment

The authors are very grateful to the anonymous referees for their invaluable comments and suggestions, which helped to improve considerably the presentation of this paper. The first three authors would also like to express their sincere thanks to Professor Chengqi Zhang, Director of the Center of Quantum Computation and Intelligent Systems, University of Technology, Sydney, for providing the excellent working environment. This work was partly supported by the National Foundation of Natural Sciences of China (Grant No: 60736011, 60621062) and the National Key Project for Fundamental Research of China (Grant No: 2007CB807901).

Bibliography

Abstract

It is well known that the "quantum logic" approach to the foundations of quantum mechanics is based on the subspace ordering of projectors on a Hilbert space. In this paper, we show that this is a special case of an ordering on partial isometries, introduced by Halmos and McLaughlin. Partial isometries have a natural physical interpretation, however, they are notoriously not closed under composition. In order to take a categorical approach, we demonstrate that the Halmos-McLaughlin partial ordering, together with tools from both categorical logic and inverse categories, allows us to form a category of partial isometries.

This category can reasonably be considered a "categorification" of quantum logic - we therefore compare this category with Abramsky and Coecke's "compact closed categories" approach to foundations and with the "monoidal closed categories" view of categorical logic. This comparison illustrates a fundamental incompatibility between these two distinct approaches to the foundations of quantum mechanics.

9.1 Introduction

As early as 1936, von Neumann and Birkhoff proposed treating projectors on Hilbert space as propositions about quantum systems (Birkhoff and von Neumann 1936), by direct analogy with classical order-theoretic approaches to logic. Boolean lattices arise as the Lindenbaum-Tarski algebras of propositional logics, and as the set of all projectors on a Hilbert space also forms an orthocomplemented lattice, the operations meet, join, and complement were analogously interpreted as the logical connectives conjunction, disjunction, and negation.

However, the lattice of projectors is not a Boolean lattice, so this interpretation requires modifications to the rules of propositional logic (notably the distributive law, $A \land (B \lor C) = (A \land B) \lor (A \land C)$ fails and is replaced by the weaker condition $A \leq C \Rightarrow A \land (A^\perp \lor C) = C$. The resulting system of orthomodular lattices has become known as quantum logic, and a number of authors (Finkelstein...