Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Copyright Information
More information

Semantic Techniques in Quantum Computation

Edited by

SIMON GAY

IAN MACKIE

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521513746

First published 2010

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data

Semantic techniques in quantum computation / edited by Simon Gay, Ian Mackie.
p. cm.
Includes index.
ISBN 978-0-521-51374-6 (hardback)
1. Quantum computers. 2. Programming languages (Electronic computers) – Semantics.
3. Quantum theory. I. Gay, Simon, 1969– II. Mackie, I. (Ian)
QA76.889.S36 2009
004.1–dc22 2009032804

ISBN 978-0-521-51374-6 Hardback

Raussendorf, R., and Briegel, H. J. (2001) A one-way quantum computer. *Physical Review Letters* **86**.

Raussendorf, R., and Briegel, H. J. (2002) Computational model underlying the one-way quantum computer. *Quantum Information & Computation* **2**. Quant-ph/0108067.

Raussendorf, R., Browne, D. E., and Briegel, H. J. (2003) Measurement-based quantum computation on cluster states. *Physical Review A* **68**.

Schlingemann, D. (2003) Cluster states, algorithms and graphs. Quant-ph/0305170.

Schumacher, B., and Werner, R. F. (2004) Reversible quantum cellular automata. Quant-ph/0405174.

Selinger, P. (2004) Towards a quantum programming language. *Mathematical Structures in Computer Science* **14**(4).

Selinger, P. (2005a) Dagger compact closed categories and completely positive maps. In Selinger (2005b).

Selinger, P., editor (2005b) *Proceedings of the 3nd International Workshop on Quantum Programming Languages, Electronic Notes in Theoretical Computer Science*.

Tame, M. S., Paternostro, M., Kim, M. S., and Vedral, V. (2004) Toward a more economical cluster state quantum computation. Quant-ph/0412156.

Tame, M. S., Paternostro, M., Kim, M. S., and Vedral, V. (2006) Natural three-qubit interactions in one-way quantum computing. *Physical Review A* **73**. Quant-ph/0507173.

Unruh, D. (2005) Quantum programs with classical output streams. In Selinger (2005b).

van Dam, W. (1996) *Quantum cellular automata*. Master's thesis, Computer Science, Nijmegen.

Walther, P., k. J. Resch, Rudolph, T., Schenck, E., Weinfurter, H., Vedral, V., Aspelmeyer, M., and Zeilinger, A. (2005) Experimental one-way quantum computing. *Nature* **434**. Quant-ph/0503126.

Watrous, J. (1995) On one-dimensional quantum cellular automata. In *Proceedings of FOCS'95 – Symposium on Foundations of Computer Science*. LNCS.

8

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 realized 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 quantum extension qGCL of the guarded-command language GCL and established 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-onto-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 mathematical 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 syntax and semantics of quantum commands are then presented in Subsections 8.4.6 and 8.4.8. The universal conjunctivity and termination law of quantum programs are proved in Subsection 8.4.9. The termination law is one of the main results of the present paper, and its proof requires essential applications of mathematical tools developed in quantum logic, in particular, Takeuti's technique of strong commutator (Takeuti 1981). In Subsection 8.4.10, Hoare's induction rule is established in the quantum setting. The main results of Section 8.4 have not been published before. We draw a brief conclusion and point out some topics for further studies in Section 8.5. To make the chapter as self-contained as possible, we briefly present preliminaries when needed.

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 in 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 $\lambda \in \mathbf{C}$, λ^* stands for the conjugate of λ. A (complex) vector space is a nonempty set $\mathcal{H}$ together with two operations: vector addition $+ : \mathcal{H} \times \mathcal{H} \to \mathcal{H}$ and scalar multiplication $\cdot : \mathbf{C} \times \mathcal{H} \to \mathcal{H}$, satisfying the following conditions:

(i) $(\mathcal{H}, +)$ is an Abelian group, its zero element 0 is called the zero vector;
(ii) $1|\varphi\rangle = |\varphi\rangle$;
(iii) $\lambda(\mu|\varphi\rangle) = \lambda\mu|\varphi\rangle$;
(iv) $(\lambda + \mu)|\varphi\rangle = \lambda|\varphi\rangle + \mu|\varphi\rangle$; and
(v) $\lambda(|\varphi\rangle + |\psi\rangle) = \lambda|\varphi\rangle + \lambda|\psi\rangle$

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

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

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

for any $|\varphi\rangle, |\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ and for any $\lambda_1, \lambda_2 \in \mathbf{C}$. Sometimes, we also write $(|\varphi\rangle, |\psi\rangle)$ for the inner product $\langle\varphi|\psi\rangle$ of $|\varphi\rangle$ and $|\psi\rangle$. Two vectors $|\varphi\rangle, |\psi\rangle$ in $\mathcal{H}$ are said to be orthogonal and we write $|\varphi\rangle \perp |\psi\rangle$ if $\langle\varphi|\psi\rangle = 0$. For any vector $|\psi\rangle$ in $\mathcal{H}$, its length $||\psi||$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$. A vector $|\psi\rangle$ is called a unit vector if $||\psi|| = 1$. Let $\mathcal{H}$ be an inner product space, $\{|\psi_n\rangle\}$ a sequence of vectors in $\mathcal{H}$, and $|\psi\rangle \in \mathcal{H}$. If for any $\epsilon > 0$ there exists a positive integer N such that $||\psi_m - \psi_n|| < \epsilon$ for all $m, n \geq N$, then $\{|\psi_n\rangle\}$ is called a Cauchy sequence. If for any $\epsilon > 0$ there exists a positive integer N such that $||\psi_n - \psi|| < \epsilon$ for all $n \geq N$, then $|\psi\rangle$ is called a limit of $\{|\psi_n\rangle\}$ and we write $|\psi\rangle = \lim_{n\to\infty}|\psi_n\rangle$. A family $\{|\psi_i\rangle\}_{i\in I}$ of vectors in $\mathcal{H}$ is summable with the sum $|\psi\rangle$ and we write $|\psi\rangle = \sum_{i\in I}|\psi_i\rangle$ if for any $\epsilon > 0$ there is a finite subset J of I such that

$$||\psi - \sum_{i\in K}\psi_i|| < \epsilon$$

for every finite subset K of I containing J. A family $\{|\psi_i\rangle\}_{i\in I}$ of unit vectors is called an orthonormal basis of $\mathcal{H}$ if

(i) $|\psi_i\rangle \perp |\psi_j\rangle$ for any $i, j \in I$ with $i \neq j$; and
(ii) $|\psi\rangle = \sum_{i\in I}\langle\psi_i|\psi\rangle|\psi_i\rangle$ for each $|\psi\rangle \in \mathcal{H}$.

A Hilbert space 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 Hilbert space $\mathcal{H}$. If for any $|\psi\rangle \in \mathcal{H}$ and any $\epsilon > 0$, there exists $|\varphi\rangle \in X$ such that $||\psi - \varphi|| < \epsilon$, 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) $A(|\varphi\rangle + |\psi\rangle) = A|\varphi\rangle + A|\psi\rangle$;
(ii) $A(\lambda|\psi\rangle) = \lambda A|\psi\rangle$

for all $|\varphi\rangle, |\psi \in \mathcal{H}$ and $\lambda \in \mathbf{C}$. If $\{|\psi_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$, then an operator A is uniquely determined by $\{A|\psi_i\rangle\}$. An operator A on $\mathcal{H}$ is said to be bounded if there is a constant $C \geq 0$ such that $\|A|\psi\rangle\| \leq C \cdot \|\psi\|$ for all $|\psi\rangle \in \mathcal{H}$. We write $\mathcal{L}(\mathcal{H})$ 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 $\mathcal{L}(\mathcal{H})$. It is obvious that $A, B \in \mathcal{L}(\mathcal{H})$ implies the composition $AB \in \mathcal{L}(\mathcal{H})$. Moreover, $\mathcal{L}(\mathcal{H})$ is a vector space in which vector addition and scalar multiplication are defined as follows: Let $A, B \in \mathcal{L}(\mathcal{H})$ and $\lambda \in \mathbf{C}$. 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

$$(|\varphi\rangle, A|\psi\rangle) = (A^\dagger|\psi\rangle, |\varphi\rangle)$$

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

$$\lim_{t\rightarrow t_0+} \|(A_t - A)|\psi\rangle\| = 0$$

for all $|\psi\rangle \in \mathcal{H}$, then A is called a (strong) limit of $\{A_t\}$ for $t \rightarrow t_0+$ and we write $A = \lim_{t\rightarrow t_0+} A_t$. Similarly, we can define $\lim_{t\rightarrow -\infty} A_t$, $\lim_{t\rightarrow +\infty} A_t$, and $\lim_{n\rightarrow\infty} A_n$ for a sequence $\{A_n\}$ of operators. The norm of a bounded operator A on $\mathcal{H}$ is defined to be

$$\|A\| = \sup_{|\psi\rangle\neq 0} \frac{\|A|\psi\rangle\|}{\|\psi\|}.$$

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 trace operator if $\{\langle\psi_i|A|\psi_i\rangle\}_{i\in I}$ is summable for any orthonormal basis $\{|\psi_i\rangle\}_{i\in I}$ of $\mathcal{H}$; in this case, the trace $tr(A)$ of A is defined to be

$$tr(A) = \sum_i \langle\psi_i|A|\psi_i\rangle$$

where $\{|\psi_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$. It can be shown that $tr(A)$ is independent of the choice of $\{|\psi_i\rangle\}$. A density operator ρ 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 ρ 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 $A \sqsubseteq B$ if $B - A$ is a positive operator. Recall that a complete partial order (CPO for short) is a partially ordered set $(L, \leq)$ such that $\bigvee_{n=0}^{\infty} x_n \in L$ 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 $D(\mathcal{H})$, 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. Let $X \subseteq \mathcal{H}$. If we have $|\varphi\rangle + |\psi\rangle \in X$ and $\lambda|\varphi\rangle \in X$ for any $|\varphi\rangle, |\psi\rangle \in X$ and $\lambda \in \mathbf{C}$, then X is called a subspace of $\mathcal{H}$. For each $X \subseteq \mathcal{H}$, the closure $\overline{X}$ of X is defined to be the set of limits $\lim_{n\rightarrow\infty} |\psi_n\rangle$ of sequences $\{|\psi_n\rangle\}$ in X. A subspace X of a Hilbert space $\mathcal{H}$ is said to be closed if $\overline{X} = X$. Let X be a closed subspace of $\mathcal{H}$ and $|\psi\rangle \in \mathcal{H}$. Then there exist uniquely $|\psi_0\rangle \in X$ and $|\psi_1\rangle \in X^\perp$ such that $|\psi\rangle = |\psi_0\rangle + |\psi_1\rangle$. The vector $|\psi_0\rangle$ is called the projection of $|\psi\rangle$ onto X and written $|\psi_0\rangle = P_X|\psi\rangle$. Thus, an operator P_X on $\mathcal{H}$ is defined and it is called the projector onto X. A spectral family on $\mathcal{H}$ is a family $\{E_\lambda\}_{-\infty<\lambda<+\infty}$ of projectors on $\mathcal{H}$ satisfying the following conditions:

(i) $E_{\lambda_1} \sqsubseteq E_{\lambda_2}$ whenever $\lambda_1 \leq \lambda_2$;
(ii) $E_\lambda = \lim_{\mu\rightarrow\lambda+} E_\mu$ for each λ; and
(iii) $\lim_{\lambda\rightarrow-\infty} E_\lambda = 0_{\mathcal{H}}$ and $\lim_{\lambda\rightarrow+\infty} E_\lambda = Id_{\mathcal{H}}$.

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 $\{E_\lambda\}$ such that*

$$M = \int_a^b \lambda dE_\lambda,$$

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 $x_0, x_1, ..., x_{n-1}, x_n, y_1, ..., y_{n-1}, y_n$ with $a = x_0 \leq y_1 \leq x_1 \leq ... \leq y_{n-1} \leq x_{n-1} \leq y_n \leq x_n = b$, it holds that

$$\|\int_a^b \lambda dE_\lambda - \sum_{i=1}^{n} y_i(E_{x_i} - E_{x_{i-1}})\| < \epsilon$$

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

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:

$$A = \int \lambda dE_\lambda.$$

Then its square root is defined to be

$$\sqrt{A} = \int \sqrt{\lambda} dE_\lambda.$$

With these preliminaries, we can give:

Proof of Proposition 8.2.1. For any positive operator A, we get:

$$|\langle\varphi|A|\psi\rangle|^2 = |(\sqrt{A}|\varphi\rangle, \sqrt{A}|\psi\rangle)|^2 \leq \langle\varphi|A|\varphi\rangle\langle\psi|A|\psi\rangle \tag{8.1}$$

by the Cauchy-Schwarz inequality.

Let $\{\rho_n\}$ be an increasing sequence in $\mathcal{D}(\mathcal{H}, \sqsubseteq)$. For any $|\psi\rangle \in \mathcal{H}$, let $A = \rho_n - \rho_m$ and $|\varphi\rangle = A|\psi\rangle$. Then

$$\langle\psi|A|\psi\rangle \leq \langle\psi|\rho_n|\psi\rangle \leq \|\psi\|^2 \cdot tr(\rho_n) \leq \|\psi\|^2,$$

and similarly we have $\langle\varphi|A|\varphi\rangle \leq \|\varphi\|^2$. Thus, it follows from Equation (8.1) that $|\langle\varphi|A|\psi\rangle|^2 \leq \|\psi\|^2 \cdot \|\varphi\|^2$. Furthermore, we obtain:

$$\begin{aligned}
\|A\|^4 &= \sup_{|\psi\rangle\neq 0} \frac{\|A|\psi\rangle\|^4}{\|\psi\|^4} \\
&= \sup_{|\psi\rangle\neq 0} \frac{\langle\varphi|A|\psi\rangle^2}{\|\psi\|^4} \\
&\leq \sup_{|\psi\rangle\neq 0} \frac{\|\varphi\|^2}{\|\psi\|^2} \\
&= \sup_{|\psi\rangle\neq 0} \frac{\|A|\psi\rangle\|^2}{\|\psi\|^2} = \|A\|^2
\end{aligned}$$

and $\|A\| \leq 1$. This leads to

$$\begin{aligned}
\langle\varphi|A|\varphi\rangle &= (A\sqrt{A}|\psi\rangle, A\sqrt{A}|\psi\rangle) \\
&= \|A\sqrt{A}|\psi\rangle\|^2 \\
&\leq \|A\|^2\|\sqrt{A}|\psi\rangle\|^2 \\
&= (\sqrt{A}|\psi\rangle, \sqrt{A}|\psi\rangle) \\
&= \langle\psi|A|\psi\rangle.
\end{aligned}$$

Using Equation (8.1) once again we get:

$$\|\rho_n|\psi\rangle - \rho_m|\psi\rangle\|^4 = |\langle\varphi|A|\psi\rangle|^2 \leq \langle\psi|A|\psi\rangle^2 = |\langle\psi|\rho_n|\psi\rangle - \langle\psi|\rho_m|\psi\rangle|^2. \tag{8.2}$$

Note that $\{\langle\psi|\rho_n|\psi\rangle\}$ is an increasing sequence of real numbers bounded by $\|\psi\|^2$, and thus it is a Cauchy sequence. This together with Equation (8.2) implies that $\{\rho_n|\psi\rangle\}$ is a Cauchy sequence in $\mathcal{H}$. So, we can define:

$$(\lim_{n\rightarrow\infty} \rho_n)|\psi\rangle = \lim_{n\rightarrow\infty} \rho_n|\psi\rangle.$$

For any $\lambda_1, \lambda_2 \in \mathbf{C}$ and $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$, it holds that

$$\begin{aligned}
(\lim_{n\rightarrow\infty} \rho_n)(\lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle) &= \lim_{n\rightarrow\infty} \rho_n(\lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle) \\
&= \lim_{n\rightarrow\infty} (\lambda_1\rho_n|\psi_1\rangle + \lambda_2\rho_n|\psi_2\rangle) \\
&= \lambda_1 \lim_{n\rightarrow\infty} \rho_n|\psi_1\rangle + \lambda_2 \lim_{n\rightarrow\infty} \rho_n|\psi_2\rangle \\
&= \lambda_1(\lim_{n\rightarrow\infty} \rho_n)|\psi_1\rangle + \lambda_2(\lim_{n\rightarrow\infty} \rho_n)|\psi_2\rangle,
\end{aligned}$$

and $\lim_{n\rightarrow\infty} \rho_n$ is a linear operator. For any $|\psi\rangle \in \mathcal{H}$, we have:

$$\langle\psi| \lim_{n\rightarrow\infty} \rho_n|\psi\rangle = (|\psi\rangle, \lim_{n\rightarrow\infty} \rho_n|\psi\rangle) = \lim_{n\rightarrow\infty} \langle\psi|\rho_n|\psi\rangle \geq 0.$$

Thus, $\lim_{n\rightarrow\infty} \rho_n$ is positive. Let $\{|\psi_i\rangle\}$ be an orthonormal basis of $\mathcal{H}$. Then

$$\begin{aligned}
tr(\lim_{n\rightarrow\infty} \rho_n) &= \sum_i \langle\psi_i| \lim_{n\rightarrow\infty} \rho_n|\psi_i\rangle \\
&= \sum_i (|\psi_i\rangle, \lim_{n\rightarrow\infty} \rho_n|\psi_i\rangle) \\
&= \lim_{n\rightarrow\infty} \sum_i \langle\psi_i|\rho_n|\psi_i\rangle \\
&= \lim_{n\rightarrow\infty} tr(\rho_n) \leq 1,
\end{aligned}$$

and $\lim_{n\rightarrow\infty} \rho_n \in \mathcal{D}(\mathcal{H})$. So, it suffices to show that $\lim_{n\rightarrow\infty} \rho_n = \bigvee_{n=0}^{\infty} \rho_n$; that is, (i) $\rho_m \sqsubseteq \lim_{n\rightarrow\infty} \rho_n$ for all $m \geq 0$; and (ii) if $\rho_m \sqsubseteq \rho$ for all $m \geq 0$, then $\lim_{n\rightarrow\infty} \rho_n \sqsubseteq \rho$. Note that for any positive operators B and C, $B \sqsubseteq C$ if and only if $\langle\psi|B|\psi\rangle \leq \langle\psi|C|\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$. Then both (i) and (ii) follow immediately from $\langle\psi| \lim_{n\rightarrow\infty} \rho_n|\psi\rangle = \lim_{n\rightarrow\infty} \langle\psi|\rho_n|\psi\rangle$. □

Intuitively, each $\rho \in \mathcal{D}(\mathcal{H})$ may be interpreted as a partially computed result, and thus $1 - tr(\rho)$ is the probability that the result is still not computed at the stage represented by ρ. Note that if $\rho_1 \sqsubseteq \rho_2$ then $tr(\rho_1) \leq tr(\rho_2)$. This fact fits Scott's interpretation (Scott 1970) of the partial order in a computational domain very well: $\rho_1 \sqsubseteq \rho_2$ means that more computation might improve ρ_1 to a possibly better-computed result ρ_2.

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 $\mathcal{H}$ is called a unitary transformation if $U^\dagger U = Id_{\mathcal{H}}$, where $Id_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$; that is, $Id_{\mathcal{H}}|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$.

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 $|\psi_0\rangle$ 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,

$$|\psi\rangle = U|\psi_0\rangle.$$

This postulate can be reformulated in the language of density operators as follows: The state ρ of a closed quantum system at time t is related to its state ρ_0 at time t_0 by a unitary operator U that depends only on the times t and t_0,

$$\rho = U\rho_0U^\dagger.$$

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

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

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 ρ immediately before measurement $\{M_m\}$ is performed on it, then the probability that result m occur is

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

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 $\{|\varphi_i\rangle\}$ and $\mathcal{K}$ a Hilbert space with orthonormal basis $\{|\psi_j\rangle\}$. Then their tensor product is defined to be

$$\mathcal{H}\otimes\mathcal{K} = \{\sum_{i,j}\alpha_{ij}|\varphi_i\psi_j\rangle : \alpha_{ij}\in\mathbf{C} \text{ with } \sum_{i,j}|\alpha_{ij}|^2 < \infty\}.$$

Vector addition, scalar multiplication, and inner product are defined on $\mathcal{H}\otimes\mathcal{K}$ in a natural way: Let $|\Phi\rangle = \sum_{i,j}\alpha_{ij}|\varphi_i\psi_j\rangle$, $|\Psi\rangle = \sum_{i,j}\beta_{ij}|\varphi_i\psi_j\rangle \in \mathcal{H}\otimes\mathcal{K}$ and $\lambda\in\mathbf{C}$. Then

$$|\Phi\rangle + |\Psi\rangle = \sum_{i,j}(\alpha_{ij}+\beta_{ij})|\varphi_i\psi_j\rangle,$$
$$\lambda|\Phi\rangle = \sum_{i,j}\lambda\alpha_{ij}|\varphi_i\psi_j\rangle,$$
$$\langle\Phi|\Psi\rangle = \sum_{i,j}\alpha_{ij}^*\beta_{ij}.$$

It is easy to show that $\mathcal{H}\otimes\mathcal{K}$ is a Hilbert space with $\{|\varphi_i\psi_j\rangle\}$ as an orthonormal basis. For any $|\varphi\rangle = \sum_i\alpha_i|\varphi_i\rangle\in\mathcal{H}$ and $|\psi\rangle = \sum_j\beta_j|\psi_j\rangle\in\mathcal{K}$, we define:

$$|\varphi\rangle\otimes|\psi\rangle = \sum_{i,j}\alpha_i\beta_j|\varphi_i\psi_j\rangle.$$

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

$$(A\otimes B)|\varphi_i\psi_j\rangle = A|\varphi_i\rangle\otimes B|\psi_j\rangle$$

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:

$$C = \sum_k\alpha_k(A_k\otimes B_k)$$

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

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

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 $\mathcal{H}_R$, $(\mathcal{I}_R\otimes\mathcal{E})(A)$ is positive provided A is a positive operator on $\mathcal{H}_R\otimes\mathcal{H}$, where $\mathcal{I}_R$ is the identity operator on $\mathcal{L}(\mathcal{H}_R)$; that is, $\mathcal{I}_R(A) = A$ for each operator A on $\mathcal{H}_R$.

We write $\mathcal{SO}(\mathcal{H})$ 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 $\mathcal{H}\otimes\mathcal{H}_E$ *such that*

$$\mathcal{E}(\rho) = tr_E[PU(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P] \tag{8.3}$$

for any $\rho\in\mathcal{D}(\mathcal{H})$*, where* $|e_0\rangle$ *is a fixed state in* $\mathcal{H}_E$*.*

(iii) *(Operator-sum representation) There exists a finite or countably infinite set of operators* $\{E_i\}$ *on* $\mathcal{H}$ *such that* $\sum_i E_i^\dagger E_i \sqsubseteq I$ *and*

$$\mathcal{E}(\rho) = \sum_i E_i\rho E_i^\dagger \tag{8.4}$$

for all density operators $\rho\in\mathcal{D}(\mathcal{H})$*. We often say that* $\mathcal{E}$ *is represented by the set* $\{E_i\}$ *of operators, or* $\{E_i\}$ *are operation elements giving rise to* $\mathcal{E}$ *when* $\mathcal{E}$ *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.

A basic principle of Scott's theory of computation (Scott 1970) is that computable functions on domains are continuous. Let $(L,\leq)$ be a CPO. Then a function f from L into itself is said to be continuous if

$$f(\bigvee_n x_n) = \bigvee_n f(x_n)$$

for any increasing sequence $\{x_n\}$ in L.

Proposition 8.2.4 *Each superoperator is a continuous function from* $(\mathcal{D}(\mathcal{H}),\sqsubseteq)$ *into itself.*

Proof. Suppose that $\mathcal{E}$ is a superoperator whose operation elements are $\{E_i\}$, and $\{\rho_n\}$ is an increasing sequence in $\mathcal{D}(\mathcal{H})$. Then by Proposition 8.2.1 we obtain:

$$\begin{aligned}\mathcal{E}(\bigvee_n \rho_n) &= \mathcal{E}(\lim_{n\to\infty}\rho_n)\\ &= \sum_i E_i(\lim_{n\to\infty}\rho_n)E_i^\dagger\\ &= \lim_{n\to\infty}\sum_i E_i\rho_n E_i^\dagger\\ &= \lim_{n\to\infty}\mathcal{E}(\rho_n)\\ &= \bigvee_n \mathcal{E}(\rho_n).\end{aligned}$$

□

The preceding lemma guarantees that it is reasonable to interpret a program as a superoperator in the state transformer (forward) semantics of a quantum programming language.

For any real number $\lambda\geq 0$, and $\mathcal{E},\mathcal{F}\in\mathcal{SO}(\mathcal{H})$, $\lambda\mathcal{E}$ and $\mathcal{E}+\mathcal{F}$ are completely positive, but they may not be superoperators because they do not necessarily satisfy the first condition in the definition of superoperator. On the other hand, it is easy to see that $\mathcal{E}\circ\mathcal{F}$ is a superoperator. The Löwner partial order induces a partial order between superoperators in a natural way: Let $\mathcal{E},\mathcal{F}\in\mathcal{SO}(\mathcal{H})$. Then $\mathcal{E}\sqsubseteq\mathcal{F}$ if $\mathcal{E}(\rho)\sqsubseteq\mathcal{F}(\rho)$ for all $\rho\in\mathcal{D}(\mathcal{H})$.

Proposition 8.2.5 (Selinger 2004, Lemma 6.4). *The set* $(\mathcal{SO}(\mathcal{H}),\sqsubseteq)$ *of superoperators on* $\mathcal{H}$ *is a CPO.*

Proof. Let $\{\mathcal{E}_n\}$ be an increasing sequence in $(\mathcal{SO}(\mathcal{H}),\sqsubseteq)$. Then for any $\rho\in\mathcal{D}(\mathcal{H})$, $\{\mathcal{E}_n(\rho)\}$ is an increasing sequence in $(\mathcal{D}(\mathcal{H}),\sqsubseteq)$. With Proposition 8.2.1 we can define:

$$(\bigvee_n\mathcal{E}_n)(\rho) = \bigvee_n\mathcal{E}_n(\rho) = \lim_{n\to\infty}\mathcal{E}_n(\rho),$$

and it holds that

$$tr((\bigvee_n\mathcal{E}_n)(\rho)) = tr(\lim_{n\to\infty}\mathcal{E}_n(\rho)) = \lim_{n\to\infty}tr(\mathcal{E}_n(\rho))\leq 1$$

because $tr(\cdot)$ is continuous. Furthermore, $\bigvee_n\mathcal{E}_n$ can be defined on the whole of $\mathcal{L}(\mathcal{H})$ by linearity. The defining equation of $\bigvee_n\mathcal{E}_n$ implies: (i) $\mathcal{E}_m\sqsubseteq\bigvee_n\mathcal{E}_n$ for all $m\geq 0$; and (ii) if $\mathcal{E}_m\sqsubseteq\mathcal{F}$ for all $m\geq 0$ then $\bigvee_n\mathcal{E}_n\sqsubseteq\mathcal{F}$. So, it suffices to show that $\bigvee_n\mathcal{E}_n$ is completely positive. Suppose that $\mathcal{H}_R$ is an extra Hilbert space. For any $C\in\mathcal{L}(\mathcal{H}_R)$ and $D\in\mathcal{L}(\mathcal{H})$, we have:

$$\begin{aligned}(\mathcal{I}_R\otimes\bigvee_n\mathcal{E}_n)(C\otimes D) &= C\otimes(\bigvee_n\mathcal{E}_n)(D)\\ &= C\otimes\lim_{n\to\infty}\mathcal{E}_n(D)\\ &= \lim_{n\to\infty}(C\otimes\mathcal{E}_n(D))\\ &= \lim_{n\to\infty}(\mathcal{I}_R\otimes\mathcal{E}_n)(C\otimes D).\end{aligned}$$

Then for any $A\in\mathcal{L}(\mathcal{H}_R\otimes\mathcal{H})$ we get:

$$(\mathcal{I}_R\otimes\bigvee_n\mathcal{E}_n)(A) = \lim_{n\to\infty}(\mathcal{I}_R\otimes\mathcal{E}_n)(A)$$

by linearity. Thus, if A is positive, then $(\mathcal{I}_R\otimes\mathcal{E}_n)(A)$ is positive for all n, and $(\mathcal{I}_R\otimes\bigvee_n\mathcal{E}_n)(A)$ is positive. □

The preceding proposition allows us to introduce recursion in the setting of superoperators. Let $\mathbf{F}$ be a continuous function from $(\mathcal{SO}(\mathcal{H}),\sqsubseteq)$ into itself. Then we define:

$$\mu\mathcal{X}.\mathbf{F}(\mathcal{X}) = \bigvee_{n=0}^{\infty}\mathbf{F}^{(n)}(0);$$

that is, $\mu\mathcal{X}.\mathbf{F}(\mathcal{X})$ is the least fixed point of $\mathbf{F}$, where 0 is the zero superoperator, which maps all elements of $\mathcal{D}(\mathcal{H})$ to the zero density operator and corresponds to the divergent program, $\mathbf{F}(0)=0$, and $\mathbf{F}^{(n+1)}(0)=\mathbf{F}(\mathbf{F}^{(n)}(0))$ for all $n\geq 0$.

8.3 Quantum Weakest Preconditions: D'Hondt-Panangaden Approach

8.3.1 Hermitian Operators as Quantum Predicates

The first step to present predicate transformer semantics of a quantum programming 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 $\mathcal{H}$. 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 $\mathcal{H}$ is a nonzero vector $|\psi\rangle \in \mathcal{H}$ such that $A|\psi\rangle = \lambda|\psi\rangle$ for some $\lambda \in \mathbf{C}$, where λ 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 $spec(A)$. For each eigenvalue λ of an operator A, the set $\{|\psi\rangle \in \mathcal{H} : A|\psi\rangle = \lambda|\psi\rangle\}$ is a closed subspace of $\mathcal{H}$ and it is called the eigenspace corresponding to λ. It is well known that an observable (a Hermitian operator) M determines a so-called projective measurement $\{P_m\}$, where m ranges over $spec(M)$, 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 $\mathcal{H}$ is a Hermitian operator M on $\mathcal{H}$ with all its eigenvalues lying within the unit interval* [0, 1].

The set of predicates on $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$. The state space $\mathcal{H}$ in the foregoing definition and the following development can be infinite-dimensional unless it is explicitly stated to be finite-dimensional. For any $M \in \mathcal{P}(\mathcal{H})$, we have $0_{\mathcal{H}} \sqsubseteq M \sqsubseteq Id_{\mathcal{H}}$, where $0_{\mathcal{H}}$ is the zero operator on $\mathcal{H}$; that is, $0_{\mathcal{H}}|\psi\rangle = 0$ for all $|\psi\rangle \in \mathcal{H}$. Recall that $tr(M\rho)$ is the expectation value of measurement outcomes when a quantum system is in the mixed state ρ and we perform the projective measurement determined by observable M on it. Thus, if M is a quantum predicate, then $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M, or more precisely the average truth value of the proposition represented by M in a quantum system of the state ρ. The reasonableness of the preceding definition is further indicated by the following fact: A Hermitian operator M is a quantum predicate if and only if $0 \leq tr(M\rho) \leq 1$ for all $\rho \in \mathcal{D}(\mathcal{H})$.

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 $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ 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, $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ 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 $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ 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 $M, N \in \mathcal{P}(\mathcal{H})$, and for any quantum program $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$, M is called a precondition of N with respect to $\mathcal{E}$, written $M\{\mathcal{E}\}N$, if*

$$tr(M\rho) \leq tr(N\mathcal{E}(\rho)) \tag{8.5}$$

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

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

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

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

For each $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$, the foregoing definition gives a quantum predicate transformer $wp(\mathcal{E}) : \mathcal{P}(\mathcal{H}) \rightarrow \mathcal{P}(\mathcal{H})$. An operator-sum representation of $wp(\mathcal{E})$ was found in D'Hondt and Panangaden (2006) by exploiting a Stone-type duality between forward state transformers and backward predicate transformers when $\mathcal{E}$ is given in the form of operator-sum.

Proposition 8.3.5 (D'Hondt and Panangaden 2006, Proposition 3.3). *Suppose that program $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$ is represented by the set $\{E_i\}$ of operators. Then for each predicate $M \in \mathcal{P}(\mathcal{H})$, we have:*

$$wp(\mathcal{E})(M) = \sum_i E_i^\dagger M E_i. \tag{8.6}$$

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

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

$$\begin{aligned} tr(wp(\mathcal{E})(M)\rho) &= tr((\sum_i E_i^\dagger M E_i)\rho) \\ &= \sum_i tr(E_i^\dagger M E_i \rho) \\ &= \sum_i tr(M E_i \rho E_i^\dagger) \qquad (8.7) \\ &= tr(M(\sum_i E_i \rho E_i^\dagger)) \\ &= tr(M\mathcal{E}(\rho)) \end{aligned}$$

for each $\rho \in \mathcal{D}(\mathcal{H})$. Thus, $wp(\mathcal{E})(M)\{\mathcal{E}\}M$.

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

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

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

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

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

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

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

and using Proposition 8.3.5 we obtain:

$$\begin{aligned} wp(\mathcal{E})(M) &= \sum_k \langle e_0|U^\dagger P|e_k\rangle M \langle e_k|PU|e_0\rangle \\ &= \langle e_0|U^\dagger P(\sum_k |e_k\rangle M \langle e_k|)PU|e_0\rangle. \end{aligned}$$

Note that $\sum_k |e_k\rangle M \langle e_k| = M \otimes I_E$ because $\{|e_k\rangle\}$ is an orthonormal basis of $\mathcal{H}_k$. 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 $\mathcal{E}, \mathcal{F} \in \mathcal{SO}(\mathcal{H})$, and let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{SO}(\mathcal{H})$. Then*

(i) *$wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{SO}(\mathcal{H})$;*
(ii) *$wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in \mathcal{SO}(\mathcal{H})$;*
(iii) *$wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$;*
(iv) *$wp(\bigvee_{n=0}^{\infty} \mathcal{E}_n) = \bigvee_{n=0}^{\infty} wp(\mathcal{E}_n)$, where*

$$(\bigvee_{n=0}^{\infty} wp(\mathcal{E}_n))(M) \overset{def}{=} \bigvee_{n=0}^{\infty} wp(\mathcal{E}_n)(M)$$

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

Proof.

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

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

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

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

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

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

$$tr(\bigvee_{n=0}^{\infty} M_n) = \bigvee_{n=0}^{\infty} tr(M_n).$$

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

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

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

$$\begin{aligned} tr(N\rho) &\leq tr(M(\bigvee_{n=0}^{\infty} \mathcal{E}_n)(\rho)) \\ &= tr(\bigvee_{n=0}^{\infty} M\mathcal{E}_n(\rho)) \\ &= \bigvee_{n=0}^{\infty} tr(M\mathcal{E}_n(\rho)) \\ &= \bigvee_{n=0}^{\infty} tr(wp(\mathcal{E}_n)(M)\rho) \\ &= tr((\bigvee_{n=0}^{\infty} wp(\mathcal{E}_n))(M)\rho) \end{aligned}$$

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

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

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

Proof. Immediate from Proposition 8.3.7(iv). □

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 $\mathcal{H}$, 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* $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$*. When do* $wp(\mathcal{E})(M)$ *and* $wp(\mathcal{E})(N)$ *commute?*

This question seems very difficult to answer for a general superoperator $\mathcal{E}$. 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* $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$*, where* $|0\rangle$ *and* $|1\rangle$ *are two basis states, and* α_0 *and* α_1 *are complex numbers with* $|\alpha_0|^2 + |\alpha_1|^2 = 1$*. Thus, the state space of qubits is the 2-dimensional Hilbert space* $\mathcal{H}_2 = \mathbf{C}^2$*, and linear operators on* $\mathcal{H}_2$ *can be represented by* 2×2 *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:

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

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then the bit flip is defined by

$$\mathcal{E}(\rho) = E_0\rho E_0^{\dagger} + E_1\rho E_1^{\dagger}, \tag{8.8}$$

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

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

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

Proposition 8.3.11.

(i) *Let* $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$ *be a unitary transformation, i.e.,* $\mathcal{E}(\rho) = U\rho U^{\dagger}$ *for any* $\rho \in \mathcal{D}(\mathcal{H})$*, where* $UU^{\dagger} = U^{\dagger}U = Id_{\mathcal{H}}$*. Then* $wp(\mathcal{E})(M)$ *and* $wp(\mathcal{E})(N)$ *commute if and only if* M *and* N *commute.*

(ii) *Let $\{P_k\}$ be a projective measurement, i.e., $P_{k_1}P_{k_2} = \delta_{k_1k_2}P_{k_1}$ and $\sum_k P_k = Id_{\mathcal{H}}$, where*

$$\delta_{k_1k_2} = \begin{cases} 1, & \text{if } k_1 = k_2, \\ 0, & \text{otherwise.} \end{cases}$$

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

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

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

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

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

Proof.

(i) From Proposition 8.3.5 we obtain:

$$wp(\mathcal{E})(M)wp(\mathcal{E})(N) = U^\dagger MUU^\dagger NU = U^\dagger MNU.$$

Then $MN = Uwp(\mathcal{E})(M)wp(\mathcal{E})(N)U^\dagger$, and the conclusion follows.

(ii) We first obtain:

$$wp(\mathcal{E})(M)wp(\mathcal{E})(N) = \sum_{k,l} P_kMP_kP_lNP_l = \sum_k P_kMP_kNP_k.$$

Similarly, it holds that

$$wp(\mathcal{E})(N)wp(\mathcal{E})(M) = \sum_k P_kNP_kMP_k.$$

It is clear that $wp(\mathcal{E})(M)wp(\mathcal{E})(N) = wp(\mathcal{E})(N)wp(\mathcal{E})(M)$ if P_kMP_k and P_kNP_k commute. Conversely, if $wp(\mathcal{E})(M)wp(\mathcal{E})(N) = wp(\mathcal{E})(N)wp(\mathcal{E})(M)$, then by multiplying P_k in the both sides we obtain:

$$P_kMP_kNP_k = P_k(\sum_l P_lMP_lNP_l) = P_k(\sum_l P_lNP_lMP_l) = P_kNP_kMP_k.$$

For the case of $P_i = |i\rangle\langle i|$ for each i, it holds that $P_iMP_iNP_i = |i\rangle\langle i|M|i\rangle\langle i|N|i\rangle\langle i|$. Note that $\langle i|M|i\rangle$ and $\langle i|M|i\rangle$ are complex numbers, and they commute. Thus, $P_iMP_iNP_i = P_iNP_iMP_i$ always holds. □

For a general superoperator $\mathcal{E}$, we are only able to give some sufficient conditions for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$. We first consider the case where $\mathcal{E}$ is given in a 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 $\{|\psi_i\rangle\}$ of $\mathcal{H}$ such that*

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

where λ_i, μ_i are reals for each i (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 $\lambda_k\mu_l = \lambda_l\mu_k$ or

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

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

Proof. We consider the matrix representations of the involved operators with respect to the basis $\{|\psi_i\rangle\}$. For any i, j, a routine calculation leads to

$$ME_iE_j^\dagger N = (\lambda_k\mu_le_{kl})_{k,l} \text{ and } NE_iE_j^\dagger M = (\mu_k\lambda_le_{kl})_{k,l},$$

where

$$e_{kl} = \sum_m \langle\psi_k|E_i|\psi_m\rangle\langle\psi_m|E_j^\dagger|\psi_l\rangle$$

for all k, l. Then the condition given in this proposition implies $ME_iE_j^\dagger N = NE_iE_j^\dagger M$. It follows from Proposition 8.3.5 that

$$wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N) = (\sum_i E_i^\dagger ME_i)(\sum_i E_i^\dagger NE_i) = \sum_{i,j} E_i^\dagger ME_iE_j^\dagger NE_j, \tag{8.9}$$

and $wp(\mathcal{E})(M)wp(\mathcal{E})(N) = wp(\mathcal{E})(N)wp(\mathcal{E})(M)$. □

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 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 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*

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

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

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

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 $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{SO}(\mathcal{H})$ be two quantum programs. If M and $\mathcal{E}_i$ commute for $i = 1, 2$, then M commutes with the composition $\mathcal{E}_1 \circ \mathcal{E}_2$ of $\mathcal{E}_1$ and $\mathcal{E}_2$.*

Proof. Suppose that $\mathcal{E}_1$ is represented by $\{E_i\}$ and $\mathcal{E}_2$ is represented by $\{F_j\}$. Then for any $\rho \in \mathcal{D}(\mathcal{H})$, we have:

$$(\mathcal{E}_1 \circ \mathcal{E}_2)(\rho) = \mathcal{E}_2(\mathcal{E}_1(\rho)) = \sum_{i,j} F_j E_i \rho E_i^\dagger F_j^\dagger.$$

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

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

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

$$\begin{aligned} M E_i E_j^\dagger N &= E_i M E_j^\dagger N^\dagger = E_i M (N E_j)^\dagger \\ &= E_i M (E_j N)^\dagger = E_i M N^\dagger E_j^\dagger = E_i M N E_j^\dagger \end{aligned}$$

and from Equation (8.9) we obtain:

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

Similarly, it holds that

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

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 $AB^\dagger = BA^\dagger$, then we say that A and B conjugate-commute.*

Obviously, commutativity is exactly $Id_{\mathcal{H}}$-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 $A = PU|e_0\rangle$.*

(i) *$wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute if and only if $M \otimes I_E$ and $N \otimes I_E$ $(A^\dagger, AA^\dagger, A)$–commute;*
(ii) *If $(M \otimes I_E)A$ and $(N \otimes I_E)A$ conjugate-commute, then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ 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 λ_i, μ_i are reals for each i. If for any i, j, k, l, we have $\lambda_i \mu_j = \lambda_j \mu_i$ or

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

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

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

$$\begin{aligned}&\langle\psi_i e_k|(M\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(N\otimes I_E)|\psi_j e_l\rangle\\ &\qquad=\lambda_i\mu_j\langle\psi_i e_k|PU|e_0\rangle\langle e_0|U^\dagger P|\psi_j e_l\rangle.\end{aligned}$$

If $\lambda_i\mu_j=\lambda_j\mu_i$ or $\langle e_0|U^\dagger P|\psi_i e_k\rangle\perp\langle e_0|U^\dagger P|\psi_j e_l\rangle$, *i.e.*,

$$\langle\psi_i e_i|UP|e_0\rangle\langle e_0|U^\dagger P|\psi_j e_l\rangle=0,$$

then we have:

$$\begin{aligned}&\langle\psi_i e_k|(M\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(N\otimes I_E)|\psi_j e_l\rangle\\ &\qquad=\langle\psi_i e_k|(N\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(M\otimes I_E)|\psi_j e_l\rangle.\end{aligned}$$

This means that

$$(M\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(N\otimes I_E)=(N\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(M\otimes I_E).$$

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:

Question 8.3.21. *How to characterize* $[wp(\mathcal{E})(M), wp(\mathcal{N})(N)]$ *in terms of* $[M, N]$*, where for any operators* X *and* Y*,* $[X, Y]$ *stands for their commutator, i.e.,* $[X, Y]=XY-YX$*?*

The foregoing question might interest mathematicians working in the area of operator algebras (Putnam 1967).

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 ortholattice is a 5-tuple $\mathcal{L}=\langle L,\leq,\wedge,\vee,\perp\rangle$, where:

(i) $\langle L,\leq,\wedge,\vee\rangle$ is a complete lattice. Here, $\leq$ is the partial ordering on L, and for any $M\subseteq L$, $\bigwedge M$ and $\bigvee M$ 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) $a\wedge a^\perp=0,\ a\vee a^\perp=1$;
(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 $\mathcal{L}=\langle L,\leq,\wedge,\vee,\perp\rangle$ satisfying the orthomodular law:

$$a\leq b \text{ implies } a\vee(a^\perp\wedge b)=b$$

for all $a, b\in L$. The orthomodular law can be replaced by the following equation: $a\vee(a^\perp\wedge(a\vee b))=a\vee b$ for any $a, b\in L$. A complete Boolean algebra is a complete ortholattice $\mathcal{L}=\langle L,\leq,\wedge,\vee,\perp\rangle$ 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 $\mathcal{L}=\langle L,\leq,\wedge,\vee,\perp\rangle$ be a complete ortholattice, and let $a, b\in L$. We say that a commutes with b, in symbols aCb, 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* $\mathcal{L}=\langle L,\leq,\wedge,\vee,\perp\rangle$ *be an orthomodular lattice, and let* $a\in L$ *and* $b_i\in L$ $(i\in I)$*. If* aCb_i *for all* $i\in I$*, then* $aC(\bigwedge_{i\in I}b_i)$ and $aC(\bigvee_{i\in I}b_i)$ *provided* $\bigwedge_{i\in I}b_i$ *and* $\bigvee_{i\in I}b_i$ *exist.*

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 $\mathcal{L} = \langle L, \leq, \wedge, \vee, \perp\rangle$ be an orthomodular lattice. For any $a \in L$ and $b_i \in L$ $(i \in I)$, if aCb_i for all $i \in I$, then*

$$a \wedge (\bigvee_{i\in I} b_i) = \bigvee_{i\in I}(a \wedge b_i),$$
$$a \vee (\bigwedge_{i\in I} b_i) = \bigwedge_{i\in I}(a \vee b_i)$$

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 $\mathcal{L} = \langle L, \leq, \wedge, \vee, \perp\rangle$ be an orthomodular lattice, and let $A \subseteq L$. The strong commutator $\Gamma(A)$ of A is defined by

$$\Gamma(A) = \bigvee\{b : \ aCb \text{ for all } a \in A, \text{and } (a_1 \wedge b)C(a_2 \wedge b) \text{ for all } a_1, a_2 \in A\}.$$

If A is finite, then the commutator $\gamma(A)$ of A is defined by

$$\gamma(A) = \bigvee\{\bigwedge_{a\in A} a^{f(a)} : f : A \to \{1, -1\} \text{ is a mapping}\},$$

where a^1 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 $\mathcal{L} = \langle L, \leq, \wedge, \vee, \perp\rangle$ 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 is a generalization of Lemma 8.4.2 given in terms of strong commutator.

Lemma 8.4.4 (Takeuti 1981). *Let $\mathcal{L} = \langle L, \leq, \wedge, \vee, \perp\rangle$ be an orthomodular lattice and let $A \subseteq L$. Then*

$$\Gamma(A) \wedge (a \wedge \bigvee_{i\in I} b_i) \leq \bigvee_{i\in I}(a \wedge b_i),$$
$$\Gamma(A) \wedge \bigwedge_{i\in I}(a \vee b_i) \leq a \vee \bigwedge_{i\in I} b_i$$

for any $a \in A$ and $b_i \in A$ $(i \in I)$.

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 $\mathcal{L} = \langle L, \leq, \wedge, \vee, \perp\rangle$ 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:

$$span(X) = \bigcap\{Y : X \subseteq Y \text{ is a subspace of } \mathcal{H}\}.$$

Then *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 *span(X)* is the set of linear combinations of vectors in X; that is,

$$span(X) = \{\sum_{i=1}^{n} \lambda_i|\varphi_i\rangle : n \geq 1, \lambda_i \in \mathbf{C} \text{ and } |\varphi_i\rangle \in X \text{ for all } 1 \leq i \leq n\}.$$

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

$$X^{\perp} = \{|\varphi\rangle \in \mathcal{H} : |\varphi\rangle \perp X\}.$$

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

Theorem 8.4.6 (Sasaki) (Kalmbach 1983). *$(\mathcal{S}(\mathcal{H}), \subseteq, \wedge, \vee, \perp)$ 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 $\mathcal{H}$, and for any $\mathcal{M} \subseteq \mathcal{S}(\mathcal{H})$, we have:*

$$\bigwedge \mathcal{M} = \bigcap_{X\in\mathcal{M}} X,$$
$$\bigvee \mathcal{M} = \bigcap\{Y \in \mathcal{S}(\mathcal{H}) : \ X \subseteq Y \text{ for all } X \in \mathcal{M}\} = \overline{span(\bigcup \mathcal{M})}.$$

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 $\mathcal{QPT}(\mathcal{H})$, *i.e.*,

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

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

$$f \subseteq g \text{ if } f(X) \subseteq g(X) \text{ for all } X \in \mathcal{S}(\mathcal{H}).$$

The next lemma follows immediately from Theorem 8.4.6.

Lemma 8.4.7. *The set $(\mathcal{QPT}(\mathcal{H}), \subseteq)$ 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* $\mathbf{0}(X) = \{0\}$ *(the* 0*-dimensional subspace of* $\mathcal{H}$*), and* $\mathbf{1}(X) = \mathcal{H}$ *for each* $X \in \mathcal{S}(\mathcal{H})$.

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

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

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

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 $f(X) \subseteq f(Y)$ for any $X, Y \in \mathcal{S}(\mathcal{H})$;*

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

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

$$f(\bigwedge \mathcal{M}) = \bigwedge_{X \in \mathcal{M}} f(X) \tag{8.10}$$

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

(iv) *f is said to be universally conjunctive if it is positively conjunctive and $f(\mathcal{H}) = \mathcal{H}$;*

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

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

$$f(\bigvee \mathcal{M}) = \bigvee_{X \in \mathcal{M}} f(X) \tag{8.11}$$

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

(vii) *f is said to be universally disjunctive if it is positively disjunctive and $f(\{0\}) = \{0\}$;*

(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 $\mathcal{QMT}(\mathcal{H})$, $\mathcal{QMC}(\mathcal{H})$, $\mathcal{QMP}(\mathcal{H})$, and $\mathcal{QMU}(\mathcal{H})$ for the sets of monotone, finitely conjunctive, positively conjunctive, and universally conjunctive projective predicate transformers on $\mathcal{H}$, respectively. In addition, we write $\mathcal{QMD}(\mathcal{H})$, $\mathcal{QUC}(\mathcal{H})$, $\mathcal{QLC}(\mathcal{H})$, $\mathcal{QPD}(\mathcal{H})$, and $\mathcal{QUD}(\mathcal{H})$ 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:

- $\mathcal{QMU}(\mathcal{H}) \subseteq \mathcal{QMP}(\mathcal{H}) \subseteq \mathcal{QMC}(\mathcal{H})$;
- $\mathcal{QUD}(\mathcal{H}) \subseteq \mathcal{QPD}(\mathcal{H}) \subseteq \mathcal{QMD}(\mathcal{H})$, $\mathcal{QUC}(\mathcal{H})$;
  and
- $\mathcal{QMC}(\mathcal{H})$, $\mathcal{QMD}(\mathcal{H})$, $\mathcal{QUC}(\mathcal{H})$, $\mathcal{QLC}(\mathcal{H}) \subseteq \mathcal{QMT}(\mathcal{H}) \subseteq \mathcal{QPT}(\mathcal{H})$.

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

Lemma 8.4.9.

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

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

(iii) *$\mathcal{QMD}(\mathcal{H})$, $\mathcal{QPD}(\mathcal{H})$, $\mathcal{QUC}(\mathcal{H})$ and $\mathcal{QUD}(\mathcal{H})$ are all sup-closed in $\mathcal{QPT}(\mathcal{H})$.*

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*

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

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

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

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

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

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

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

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

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

$$S(\mathcal{H}_2) = \{\{0\}, \mathcal{H}_2\} \cup \{\mathcal{H}_1(\alpha, \beta) : \alpha, \beta \in \mathbf{C}\}$$

where $\mathcal{H}_1(\alpha, \beta) = \{\gamma(\alpha|0\rangle + \beta|1\rangle) : \gamma \in \mathbf{C}\}$ is a 1-dimensional subspace of $\mathcal{H}_2$ for each α, β. 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 $\frac{\pi}{8}$ gate:

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

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

$$\begin{aligned}
X^{-1}(\mathcal{H}_1(\alpha, \beta)) &= X(\mathcal{H}_1(\alpha, \beta)) = \mathcal{H}_1(\beta, \alpha), \\
Y^{-1}(\mathcal{H}_1(\alpha, \beta)) &= Y(\mathcal{H}_1(\alpha, \beta)) = \mathcal{H}_1(-\beta, \alpha), \\
Z^{-1}(\mathcal{H}_1(\alpha, \beta)) &= Z(\mathcal{H}_1(\alpha, \beta)) = \mathcal{H}_1(\alpha, -\beta), \\
S^{-1}(\mathcal{H}_1(\alpha, \beta)) &= \mathcal{H}_1(\alpha, -i\beta), \\
T^{-1}(\mathcal{H}_1(\alpha, \beta)) &= \mathcal{H}_1(\alpha, e^{-\frac{i\pi}{4}}\beta)
\end{aligned}$$

for all α, β. In general, each unitary operation on a single qubit can be written in the form of $U = e^{i\lambda}R_z(\mu)R_y(\nu)R_z(\delta)$, where λ, μ, ν, and δ are real numbers,

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \; R_z(\theta) = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$$

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

$$U^{-1}(\mathcal{H}_1(\alpha, \beta)) = \mathcal{H}_1(\alpha\cos\frac{\nu}{2} + \beta e^{i\mu}\sin\frac{\nu}{2}, \beta e^{i(\delta+\mu)}\cos\frac{\nu}{2} - \alpha e^{i\delta}\sin\frac{\nu}{2}).$$

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

$$M_m^{-1}(X) = \{|\psi\rangle \in \mathcal{H} : |\psi_m\rangle \in X\}$$

is the set of quantum states such that the postmeasurement states will lie in X whenever we perform measurement $\{M_m\}$ 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

$$P_i^{-1}(\mathcal{H}_1(\alpha, \beta)) = \{\gamma(\alpha|i0\rangle + \beta|i1\rangle) : \gamma \in \mathbf{C}\}.$$

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 semantics 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, nondeterminate 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 $\mathcal{S}(\mathcal{H})$ 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 $\mathcal{H}$,*

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

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 $\mathcal{H}_0 = \mathcal{H}_1 = \mathcal{H}$. Then a mapping $t : \mathcal{S}(\mathcal{H}_0) \to \mathcal{S}(\mathcal{H}_1)$ is seen as a quantum program from $\mathcal{H}_0$ to $\mathcal{H}_1$, but a mapping $f : \mathcal{S}(\mathcal{H}_0) \to \mathcal{S}(\mathcal{H}_1)$ is treated as a predicate transformer from $\mathcal{H}_1$ to $\mathcal{H}_0$. 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 $\mathcal{S}(\mathcal{H})$ into itself.*

(i) *For any $X, Y \in \mathcal{S}(\mathcal{H})$, we write $X\{t\}Y$ if $t(X) \subseteq Y$.*
(ii) *For any $X \in \mathcal{S}(\mathcal{H})$, the weakest precondition of X with respect to t is defined to be a closed subspace $wp(t)(X)$ of $\mathcal{H}$ satisfying the following conditions:*
   (a) *$wp(t)(X)\{t\}X$;*
   (b) *for any $Y \in \mathcal{S}(\mathcal{H})$, $Y\{t\}X$ 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 $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$. If for any $X \in \mathcal{S}(\mathcal{H})$, there exists $Y \in \mathcal{S}(\mathcal{H})$ such that $\mathcal{E}(P_X) = \lambda P_Y$ for some $0 < \lambda \leq 1$, then we say that $\mathcal{E}$ preserves projectors.*
(ii) *Let $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$ preserves projectors. Then the restriction $t_{\mathcal{E}}$ of $\mathcal{E}$ on $\mathcal{S}(\mathcal{H})$ is defined as follows: For each $X \in \mathcal{S}(\mathcal{H})$, if $\mathcal{E}(P_X) = \lambda P_Y$, then $t_{\mathcal{E}}(X) = Y$.*

We note that if $\mathcal{E}(P_X) = \lambda P_Y$ and $\mathcal{E}(P_X) = \mu P_Z$ then $Y = Z$. So, $t_{\mathcal{E}}$ is well-defined.

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

$$\cos\langle X, Y\rangle = \sqrt{\sum_{i=1}^{\dim X}\sum_{j=1}^{\dim Y} |\langle\varphi_i|\psi_j\rangle|^2},$$

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

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

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

(i) $\cos\langle X, Y\rangle = \cos\langle Y, X\rangle = \sqrt{tr(P_X \cdot P_Y)}$.
(ii) $X_1 \subseteq X_2$ *implies* $\cos\langle X_1, Y\rangle \leq \cos\langle X_2, Y\rangle$.
(iii) $\cos\langle X, Y\rangle \leq \min(\sqrt{\dim X}, \sqrt{\dim Y})$, *and* $\cos\langle X, Y\rangle = \sqrt{\dim X}$ *if and only if* $X \subseteq Y$.

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

$$\begin{aligned}
tr(P_XP_Y) &= tr(\sum_{i=1}^{\dim X} |\varphi_i\rangle\langle\varphi_i| \cdot \sum_{j=1}^{\dim Y} |\psi_j\rangle\langle\psi_j|) \\
&= \sum_{i=1}^{\dim X}\sum_{j=1}^{\dim Y} tr(|\varphi_i\rangle\langle\varphi_i|\psi_j\rangle\langle\psi_j|) \\
&= \sum_{i=1}^{\dim X}\sum_{j=1}^{\dim Y} |\langle\varphi_i|\psi_j\rangle|^2 \\
&= \cos\langle X, Y\rangle^2 \\
&\leq \sum_{i=1}^{\dim X}\sum_{j=1}^{\dim\mathcal{H}} |\langle\varphi_i|\psi_j\rangle|^2 \\
&= \sum_{i=1}^{\dim X} ||\varphi_i||^2 \\
&= \dim X.
\end{aligned}$$

If $\cos\langle X, Y\rangle = \sqrt{\dim X}$, then

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

for all $i \leq \dim X$. This implies $|\varphi_i\rangle \in Y$ for all $i \leq \dim X$, and $X \subseteq Y$. □

Lemma 8.4.15. *Let $\mathcal{E} \in \mathcal{SO}(\mathcal{H})$ preserve projectors, let $X, Y \in \mathcal{S}(\mathcal{H})$, and let X be finite-dimensional. If for all $\rho \in \mathcal{D}(\mathcal{H})$, we have:*

$$tr(P_X\rho) \leq tr(P_Y\mathcal{E}(\rho)),$$

then $t_{\mathcal{E}}(X) \subseteq Y$.

Proof. ($\Leftarrow$) Suppose that $\mathcal{E}(P_X) = \lambda P_Z$. Since X is a finite-dimensional subspace of $\mathcal{H}$, we have:

$$\frac{1}{\dim(X)}P_X \in \mathcal{D}(\mathcal{H}),$$

where $\dim(X)$ is the dimension of X. Then we obtain:

$$tr(\frac{\lambda}{\dim(X)}P_Z) = tr(\mathcal{E}(\frac{1}{\dim(X)}P_X)) \leq tr(\frac{1}{\dim(X)}P_X) = 1$$

from the definition of superoperator. This implies that Z is finite-dimensional. Thus, it follows that

$$\frac{\lambda \dim(Z)}{\dim(X)} = tr(\frac{\lambda}{\dim(X)}P_Z) \leq 1$$

and

$$\lambda \leq \frac{\dim(X)}{\dim(Z)}.$$

Putting

$$\rho = \frac{1}{\dim(X)}P_X,$$

we get:

$$\begin{aligned} 1 &= \frac{1}{\dim(X)}tr(P_X) \\ &= \frac{1}{\dim(X)}tr(P_XP_X) \\ &= tr(P_X\rho) \\ &\leq tr(P_Y\mathcal{E}(\rho)) \\ &= \frac{1}{\dim(X)}tr(P_X\mathcal{E}(P_X)) \\ &= \frac{\lambda}{\dim(X)}tr(P_YP_Z) \\ &\leq \frac{1}{\dim(Z)}tr(P_YP_Z) \end{aligned}$$

and $\dim(Z) \leq tr(P_YP_Z)$. Therefore, using Lemma 8.4.14 we obtain $t_{\mathcal{E}}(X) = Z \subseteq Y$. □

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

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

(i) *For any $X \in \mathcal{S}(\mathcal{H})$, if Z is a finite-dimensional subspace of $\mathcal{H}$, and $P_Z \sqsubseteq wp(\mathcal{E})(P_X)$, then $Z \subseteq wp(t_{\mathcal{E}})(X)$ provided $wp(t_{\mathcal{E}})(X)$ is defined.*

(ii) *If $\mathcal{E}$ satisfies the condition: $\rho \sqsubseteq wp(\mathcal{E})(\mathcal{E}(\rho))$ for all $\rho \in \mathcal{D}(\mathcal{H})$, then for any $X \in \mathcal{S}(\mathcal{H})$, we have:*

$$P_{wp(t_{\mathcal{E}})(X)} \sqsubseteq wp(\mathcal{E})(P_X).$$

Proof.

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

$$tr(P_Z\rho) \leq tr(wp(\mathcal{E})(P_X)\rho) \leq tr(P_X\mathcal{E}(\rho)).$$

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.*, $\mathcal{E}(P_Y) = \lambda P_Z$ for some λ and Z with $0 < \lambda \leq 1$ and $X \supseteq Z \in \mathcal{S}(\mathcal{H})$. Now for any $\rho \in \mathcal{D}(\mathcal{H})$, by Proposition 8.3.5 we obtain:

$$\begin{aligned} tr(P_Y\rho) &\leq tr(P_Y wp(\mathcal{E})(\mathcal{E}(\rho))) \\ &= tr(P_Y \cdot \sum_{i,j} E_i^\dagger E_j \rho E_j^\dagger E_i) \\ &= \sum_{i,j} tr(P_Y E_i^\dagger E_j \rho E_j^\dagger E_i) \\ &= \sum_{i,j} tr(E_i P_Y E_i^\dagger E_j \rho E_j^\dagger) \\ &= tr(\sum_i E_i P_Y E_i^\dagger \cdot \sum_j E_j \rho E_j^\dagger) \\ &= tr(\mathcal{E}(P_Y)\mathcal{E}(\rho)) \\ &\leq tr(P_Z\mathcal{E}(\rho)) \\ &\leq tr(P_X\mathcal{E}(\rho)). \end{aligned}$$

Therefore, it holds that $P_Y\{\mathcal{E}\}P_X$, and $P_Y \sqsubseteq wp(\mathcal{E})(P_X)$ follows. □

Now we consider a partial inverse of the problem dealt with in the above proposition. Let t be a mapping from $\mathcal{S}(\mathcal{H})$ into itself satisfying the upper continuity:

$$t(\bigcap_{\lambda<\mu} E_\mu) = \bigcap_{\lambda<\mu} t(E_\mu)$$

for any family $\{E_\mu\}_{\lambda<\mu}$ of closed subspaces of $\mathcal{H}$ with $E_{\mu_1} \subseteq E_{\mu_2}$ whenever $\mu_1 \leq \mu_2$. Then t induces an operator $\mathcal{E}_t$ on $\mathcal{L}(\mathcal{H})$ 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 $E_\lambda \in \mathcal{S}(\mathcal{H})$ 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

$$\mathcal{E}_t(A) = \int_0^b \lambda dt(E_\lambda).$$

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

$$f^*(M) = \int_0^1 \lambda df(F_\lambda) \tag{8.12}$$

when $M = \int_0^1 \lambda dF_\lambda$ is the spectral decomposition of M.

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

$$\cos\langle X, Y\rangle \leq \cos\langle t(X), t(Y)\rangle$$

for any $X, Y \in \mathcal{S}(\mathcal{H})$. Then we have $wp(t)^* \sqsubseteq wp(\mathcal{E}_t)$, where $wp(\cdot)$ in the left-hand side and $wp(\cdot)$ 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:

$$A \cdot (\int \lambda dA_\lambda) = \int \lambda d(AA_\lambda), \tag{8.13}$$

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

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

where A is a positive operator, and the right-hand side of Equation (8.15) is the Lebesgue-Stieltjes integral.

Now for any $M \in \mathcal{P}(\mathcal{H})$, we show that $wp(t)^*(M) \sqsubseteq wp(\mathcal{E}_t)(M)$. To this end, we only need to prove that $wp(t)^*(M)\{\mathcal{E}_t\}M$, *i.e.*,

$$tr(wp(t)^*(M)\rho) \leq tr(M\mathcal{E}_t(\rho))$$

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

$$M = \int_0^1 \lambda dE_\lambda, \quad \rho = \int_0^1 \mu dF_\mu$$

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

$$\begin{aligned} wp(t)^*(M)\rho &= [\int_0^1 \lambda dwp(t)(E_\lambda)] \cdot \rho \\ &= \int_0^1 \lambda d[wp(t)(E_\lambda) \cdot \rho] \\ &= \int_0^1 \lambda d[wp(t)(E_\lambda) \cdot \int_0^1 \mu dF_\mu] \\ &= \int_0^1 \lambda d\{\int_0^1 \mu d[wp(t)(E_\lambda) \cdot F_\mu]\}. \end{aligned}$$

Similarly, we have:

$$M\mathcal{E}_t(\rho) = \int_0^1 \lambda d\{\int_0^1 \mu d[E_\lambda \cdot t(F_\mu)]\}.$$

Therefore, it follows from Equation (8.15) that

$$\begin{aligned} tr(wp(t)^*(M)\rho) &= \int_0^1 \lambda d\{\int_0^1 \mu d[tr(wp(t)(E_\lambda) \cdot F_\mu)]\}, \\ tr(M\mathcal{E}_t(\rho)) &= \int_0^1 \lambda d\{\int_0^1 \mu d[tr(E_\lambda \cdot t(F_\mu))]\}. \end{aligned}$$

Consequently, it suffices to show that

$$tr(wp(t)(E_\lambda) \cdot F_\mu) \leq tr(E_\lambda \cdot t(F_\mu)).$$

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

$$\begin{aligned} tr(wp(t)(E_\lambda) \cdot F_\mu) &= \cos\langle wp(t)(E_\lambda), F_\mu\rangle^2 \\ &\leq \cos\langle t(wp(t)(E_\lambda)), t(F_\mu)\rangle^2 \\ &\leq \cos\langle E_\lambda, t(F_\mu)\rangle^2 \\ &\leq tr(E_\lambda \cdot t(F_\mu)). \end{aligned}$$

□

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. Put $A = S \cup H$ and assume that A does not contain the symbol ϵ and ";". The set of strings over A is denoted by A^*. We shall use ϵ to denote the empty string, and concatenation of strings will be expressed by the infix operator ";". Intuitively, the concatenation ";" is used to denote sequential composition of commands. Furthermore, we write $A^{\odot}$ for the set of nonempty subsets of A^*, i.e., $A^{\odot} = \mathcal{P}(A^*) - \{\emptyset\}$, where $\mathcal{P}(\cdot)$ stands for power set. The elements of $A^{\odot}$ are called commands. A command $C \in A^{\odot}$ stands for the choice among the elements of C, which are also commands, whenever C contains more than one elements. The recursive procedures are declared by a function

$$\mathbf{body} : H \rightarrow A^{\odot}.$$

For each procedure name $h \in H$, the body function **body** associates it to its body $\mathbf{body}(h)$, 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 $h = \mathbf{body}(h)$. It is worth noting that recursive calls may happen because h is allowed to appear in $\mathbf{body}(h)$.

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

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

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

$$(\bigsqcup C \in \mathcal{C} :: C) = \bigcup_{C \in \mathcal{C}} C.$$

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

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

(i) $\varphi(\epsilon) = Id_{S(\mathcal{H})}$ (the identity mapping on $S(\mathcal{H})$);
(ii) $\varphi(C; D) = \varphi(C) \circ \varphi(D)$;
(iii) $\varphi(\bigsqcup C \in \mathcal{C} : C) = \bigwedge_{C \in \mathcal{C}} \varphi(C)$

for any $C, D \in A^{\odot}$ and $\mathcal{C} \subseteq A^{\odot}$.

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 $v : A \rightarrow \mathcal{QPT}(\mathcal{H})$ be a mapping. Then:*

(i) *The extension v^* of v on A^* is defined inductively as follows: $v^*(\epsilon) = Id_{S(\mathcal{H})}$, and $v^*(a; s) = v(a) \circ v^*(s)$ for each $a \in A$ and $s \in A^*$.*
(ii) *The extension $v^{\odot}$ of v on $A^{\odot}$ is defined by*

$$v^{\odot}(C) = \bigwedge_{s \in C} v^*(s)$$

for any $C \in A^{\odot}$.

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 range$(v) \subseteq \mathcal{QMT}(\mathcal{H})$, then range$(v^{\odot}) \subseteq \mathcal{QMT}(\mathcal{H})$. The same holds for $\mathcal{QMC}(\mathcal{H})$, $\mathcal{QMP}(\mathcal{H})$ and $\mathcal{QMU}(\mathcal{H})$.*
(ii) *If range$(v) \subseteq \mathcal{QMU}(\mathcal{H})$, then $v^{\odot}$ 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* $\text{lfp}(D)$ *and a greatest fixed point $gfp(D)$.*
(ii) *For any D-invariant subset U of L, we have:*
  (a) $\text{lfp}(D) \in U$ *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:

- $D \uparrow 0 = 0, D \downarrow 0 = 1$;
- $D \uparrow (\alpha + 1) = D(D \uparrow \alpha), D \downarrow (\alpha + 1) = D(D \downarrow \alpha)$ for each ordinal number α; and
- $D \uparrow \alpha = \bigvee\{D \uparrow \beta : \beta < \alpha\}$, $D \downarrow \alpha = \bigwedge\{D \downarrow \beta : \beta < \alpha\}$ if α is a limit ordinal number.

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) $D \uparrow \alpha \leq \mathrm{lfp}(D)$ *and* $\mathrm{gfp}(D) \leq D \downarrow \alpha$ *for any ordinal number* α*;*
(ii) *There exist ordinal numbers* α_0 *and* α_1 *such that* $D \uparrow \alpha = \mathrm{lfp}(D)$ *for all* $\alpha \geq \alpha_0$*, and* $D \downarrow \alpha = \mathrm{gfp}(D)$ *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 $f, g : L \to L$ be monotone mappings, and let $f|K$ be the restriction of f on K. Then*

(i) (a) $\mathrm{lfp}(f|K) = \mathrm{lfp}(f)$ *if* $\mathrm{lfp}(f) \in K$*;*
(b) $\mathrm{gfp}(f|K) = \mathrm{gfp}(f)$ *if* $\mathrm{gfp}(f) \in K$.
(ii) $\mathrm{lfp}(f) \leq \mathrm{lfp}(g)$, $\mathrm{gfp}(f) \leq \mathrm{gfp}(g)$ *if* $f \leq g$*, i.e.,* $f(a) \leq g(a)$ *for all* $a \in L$.

8.4.8 Semantics of Recursive Quantum Commands

Now we are able to define semantics of recursion expressed by procedure names and their declarations. Let $w : S \to \mathcal{QPT}(\mathcal{H})$ and $u : H \to \mathcal{QPT}(\mathcal{H})$. Then their merging $w \cup u : A \to \mathcal{QPT}(\mathcal{H})$ is defined by

$$(w \cup u)(a) = \begin{cases} w(a) & \text{if } a \in S, \\ u(a) & \text{if } a \in H. \end{cases}$$

Note that $w \cup u$ is well defined because it was assumed that $S \cap H = \emptyset$. As an immediate corollary of Lemma 8.4.20(i), we have:

Lemma 8.4.24. *If for any $a \in S$, $w(a)$ is universally conjunctive, and for any $a \in H$, $u(a)$ is universally conjunctive, then for any $C \in A^{\odot}$, $(w \cup u)^{\odot}(C)$ is universally conjunctive.*

For each mapping $w : S \to \mathcal{QMT}(\mathcal{H})$, it induces a mapping $D[w]$ from $\mathcal{QMT}(\mathcal{H})^H$ into itself as follows:

$$D[w](u) = (w \cup u)^{\odot} \circ \mathbf{body}$$

for any $u : H \to \mathcal{QMT}(\mathcal{H})$. It follows directly from the definition of $w \cup u$ and Lemma 8.4.20(i) that $D[w](u)(h) \in \mathcal{QMT}(\mathcal{H})$ for every $h \in H$. Then we are ready to present the key definition of this section.

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

(i) *The weakest precondition function generated by w is defined to be*

$$wp[w] = (w \cup \mathrm{lfp}(D[w]))^{\odot}.$$

(ii) *The weakest liberal precondition function generated by w is defined to be*

$$wlp[w] = (w \cup \mathrm{gfp}(D[w]))^{\odot},$$

where $\mathrm{lfp}(D[w])$ *and* $\mathrm{gfp}(D[w])$ *stand for the least and greatest fixed points of* $D[w]$*, respectively.*

It is easy to see that $D[w]$ is monotone. Then we know that $\mathrm{lfp}(D[w])$ and $glp(D[w])$ always exist from Lemma 8.4.9(i) and Theorem 8.4.21(i), and $wp[w]$ and $wlp[w]$ are well defined.

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

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

Proof.

(i) is obvious from the definition of $D[w]$ and Definition 8.4.25.
(ii) It follows from Lemma 8.4.9(ii) that $\mathcal{QMU}(\mathcal{H})^H$ is inf-closed. On the other hand, we see that $D[w]$ is $\mathcal{QMU}(\mathcal{H})^H$–invariant by a routine calculation. Then we have $\mathrm{gfp}(D[w]) \in \mathcal{QMU}(\mathcal{H})^H$ by Theorem 8.4.21(ii), and it follows from Definition 8.4.25(ii) and Lemma 8.4.20(ii) that $wlp[w]$ is a homomorphism. □

8.4.9 Healthiness Laws for Quantum Commands

Healthiness conditions were first introduced by Dijkstra (1976) and then thoroughly investigated by Dijkstra and Scholten (1990) among others, and they prescribe certain properties of predicate transformers. The aim of this section is to establish the quantum generalizations of some healthiness laws.

Universal conjunctivity is one of the most important healthiness laws for predicate transformers, and it asserts that the predicate transformers under consideration preserve arbitrary meets of predicates. Universal conjunctivity of classical weakest liberal preconditions can be generalized to the quantum case in a straightforward way.

Theorem 8.4.27 (Universal conjunctivity of weakest liberal precondition). *If $w(a)$ is universally conjunctive for all $a \in S$, then $wlp[w](C)$ is universally conjunctive for each $C \in A^{\odot}$.*

Proof. We see that $\mathrm{gfp}(D[w]) \in \mathcal{QMU}(\mathcal{H})^H$ from the proof of Lemma 8.4.26(ii). Thus, it immediately follows from Lemma 8.4.24 and Definition 8.4.25(ii) that $wlp[w]\ (C) \in \mathcal{QMU}(\mathcal{H})$ for all $C \in A^{\odot}$. □

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 $X \in \mathcal{S}(\mathcal{H})$, and let $w : S \to \mathcal{QMT}(\mathcal{H})$ and $u : H \to \mathcal{QMT}(\mathcal{H})$. 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 $C \in A^{\odot}$, it holds that*

$$X \subseteq (w \cup u)^{\odot}(C)(X).$$

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

$$\begin{aligned}(w \cup u)^{\odot}(C)(X) &= (w \cup u)^*(a; s)(X)\\ &= (w \cup u)(a)((w \cup u)^*(s)(X))\\ &\supseteq (w \cup u)(a)(X)\\ &\supseteq X\end{aligned}$$

from the induction hypothesis: $X \subseteq (w \cup u)^{\odot}(s)(X)$. In general, it follows that

$$(w \cup u)^{\odot}(C)(X) = \bigwedge_{s \in C}(w \cup u)^*(s)(X) \supseteq X$$

from the induction hypothesis that $X \subseteq (w \cup u)^{\odot}(s)(X)$ for all $s \in A^*$. □

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

$$X \subseteq wlp[w](a)(X).$$

Proof. From Definition 8.4.25 we obtain:

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

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

We proceed by transfinite induction on α. If $\alpha = 0$, then

$$(D[w] \downarrow \alpha)(h)(X) = \mathcal{H}$$

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

$$\begin{aligned}(D[w] \downarrow (\alpha + 1))(h)(X) &= D[w](D[w] \downarrow \alpha)(h)(X)\\ &= (w \cup (D[w] \downarrow \alpha))^{\odot}(\mathbf{body}(h))(X)\end{aligned}$$

and it follows from Lemma 8.4.28 that

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

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

$$X \subseteq \bigwedge_{\beta < \alpha}(D[w] \downarrow \beta)(h)(X) = (D[w] \downarrow \alpha)(h)(X).$$

□

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

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

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

$$w_1(a)(X) = w_1(a)(\mathcal{H}) \wedge w_2(a)(X)$$

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

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

$$wp[w_1](C)(X) \subseteq wp[w_1](C)(\mathcal{H}) \wedge wlp[w_2](C)(X).$$

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

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

then we have:

$$wp[w_1](C)(\mathcal{H}) \wedge wlp[w_2](C)(X) \wedge \Gamma(\mathcal{M}) \subseteq wp[w_1](C)(X),$$

where $\Gamma(\mathcal{M})$ stands for the strong commutator of $\mathcal{M}$.

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

$$wp[w_1](C)(\mathcal{H}) \wedge wlp[w_2](C)(X) = wp[w_1](C)(X)$$

by combining the two parts of the theorem.

Proof.

(i) It is obvious that $wp[w_1](C)(X) \subseteq wp[w_1](C)(\mathcal{H})$. So, we only need to show that

$$wp[w_1](C)(X) \subseteq wlp[w_2](C)(X).$$

Since $w_1 \subseteq w_2$, we have $D[w_1] \subseteq D[w_2]$. Then we obtain:

$$\mathrm{lfp}(D[w_1]) \subseteq \mathrm{gfp}(D[w_1]) \subseteq \mathrm{gfp}(D[w_2])$$

by Proposition 8.4.23, and it follows that

$$wp[w_1] = (w_1 \cup \mathrm{lfp}(D[w_1]))^{\odot} \subseteq (w_2 \cup \mathrm{gfp}(D[w_2]))^{\odot} = wlp[w_2].$$

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

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

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

- *Claim 1.* $D[w_1] \uparrow \alpha, D[w_2] \downarrow \alpha \in \mathcal{W}$ *for all ordinal numbers* α, *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 α, and it is routine and so omitted here. We only need to note that here the condition $Range(w_1), Range(w_2) \subseteq \mathcal{M}$ is required.

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

- *Claim 2.* $\mathrm{lfp}(D[w_1]) = \mathrm{Lfp}(D[w_1])$ *and* $\mathrm{gfp}(D[w_2]) = \mathrm{Gfp}(D[w_2])$.

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

Now we set

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

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

$$(w_1 \cup u)^{\odot}(C)(\mathcal{H}) \wedge wlp[w_2](C)(X) \wedge \Gamma(\mathcal{M}) \subseteq (w_1 \cup u)^{\odot}(C)(X)$$

for all $C \in A^{\odot}$ *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:

$$(w_1 \cup u)^{\odot}(C)(X) = w_1(a)(X),$$

$$(w_1 \cup u)^{\odot}(C)(\mathcal{H}) = w_1(a)(\mathcal{H}),$$

$$wlp[w_2](C)(X) = (w_2 \cup \mathrm{gfp}(D[w_2]))^{\odot}(C)(X) = w_2(a)(X).$$

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

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

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

$$(w_1 \cup u)^{\odot}(C)(X) = u(h)(X),$$

and claim 3 follows from the fact that $u \in \mathcal{U}$.

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

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

Then we obtain:

$$\begin{aligned}LHS &= (w_1 \cup u)(a)((w_1 \cup u)^*(s)(\mathcal{H})) \wedge wlp[w_2](a)(wlp[w_2](s)(X)) \wedge \Gamma(\mathcal{M}) \\ &\subseteq (w_1 \cup u)(a)(\mathcal{H}) \wedge wlp[w_2](a)((w_1 \cup u)^*(s)(\mathcal{H})) \\ &\qquad \wedge wlp[w_2](a)(wlp[w_2](s)(X)) \wedge \Gamma(\mathcal{M}).\end{aligned}$$

Using Lemma 8.4.29 we assert that $\Gamma(\mathcal{M}) \subseteq wlp[w_2](a)(\Gamma(\mathcal{M}))$, and it follows that

$$\begin{aligned}LHS &\subseteq (w_1 \cup u)(a)(\mathcal{H}) \wedge wlp[w_2](a)((w_1 \cup u)^*(s)(\mathcal{H})) \\ &\qquad \wedge wlp[w_2](a)(wlp[w_2](s)(X)) \wedge wlp[w_2](\Gamma(\mathcal{M})) \wedge \Gamma(\mathcal{M}).\end{aligned}$$

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

$$\begin{aligned}LHS &\subseteq (w_1 \cup u)(a)(\mathcal{H}) \wedge wlp[w_2](a)((w_1 \cup u)^*(s)(\mathcal{H}) \\ &\qquad \wedge wlp[w_2](s)(X) \wedge \Gamma(\mathcal{M})) \wedge \Gamma(\mathcal{M}) \\ &\subseteq (w_1 \cup u)(a)(\mathcal{H}) \wedge wlp[w_2](a)((w_1 \cup u)^*(s)(X)) \wedge \Gamma(\mathcal{M}) \\ &\subseteq (w_1 \cup u)(a)((w_1 \cup u)^*(s)(X)) \\ &= (w_1 \cup u)^*(a; s)(X) \\ &= (w_1 \cup u)^{\odot}(C)(X)\end{aligned}$$

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

$$\begin{aligned}LHS &= \bigwedge_{s \in C}(w_1 \cup u)^*(s)(\mathcal{H}) \wedge \bigwedge_{s \in C} wlp[w_2](s)(X) \wedge \Gamma(\mathcal{M}) \\ &= \bigwedge_{s \in C}[(w_1 \cup u)^*(s)(\mathcal{H}) \wedge wlp[w_2](s)(X) \wedge \Gamma(\mathcal{M})] \\ &\subseteq \bigwedge_{s \in C}(w_1 \cup u)^*(s)(X) \\ &= (w_1 \cup u)^{\odot}(C)(X)\end{aligned}$$

and this completes the proof of claim 3.

- *claim 4.* $\mathcal{U}$ *is* $D[w_1]$*-invariant.*

In fact, for any $u \in \mathcal{U}$, claim 3, together with Lemma 8.4.26, yields:

$$\begin{aligned}
D[w_1](u)(h)(\mathcal{H}) \wedge wlp[w_2](h)(X) \wedge \Gamma(\mathcal{M})\\
&= (w_1 \cup u)^{\odot}(\mathbf{body}(h))(\mathcal{H}) \wedge wlp[w_2](\mathbf{body}(h))(X) \wedge \Gamma(\mathcal{M})\\
&\leq (w_1 \cup u)^{\odot}(\mathbf{body}(h))(X)\\
&\leq D[w_1](u)(h)(X).
\end{aligned}$$

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

- *Claim 5. $\mathcal{U}$ is sup-closed.*

It follows from Theorem 8.4.27 that

$$wlp[w_2] = (w_2 \cup \mathrm{gfp}(D[w_2]))^{\odot} \circ \mathbf{body} = (w_2 \cup (D[w_2] \downarrow \alpha))^{\odot} \circ \mathbf{body}$$

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

For any $u_i \in \mathcal{U}$ $(i \in I)$, we obtain:

$$\begin{aligned}
(\bigvee_{i\in I} u_i)(h)(\mathcal{H}) \wedge wlp[w_2](h)(X) \wedge \Gamma(\mathcal{M})\\
&= (\bigvee_{i\in I} u_i(h)(\mathcal{H})) \wedge wlp[w_2](h)(X) \wedge \Gamma(\mathcal{M})\\
&\subseteq \bigvee_{i\in I}(u_i(h)(\mathcal{H}) \wedge wlp[w_2](h)(X) \wedge \Gamma(\mathcal{M}))\\
&\subseteq \bigvee_{i\in I} u_i(h)(X)\\
&= (\bigvee_{i\in I} u_i)(h)(X)
\end{aligned}$$

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 $\mathrm{lfp}(D[w_1]) = \mathrm{Lfp}(D[w_1]) \in \mathcal{U}$, and we complete the proof by using Claim 3 once again and by noting that

$$wp[w_1] = (w_1 \cup \mathrm{lfp}(D[w_1]))^{\odot}.$$

□

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 $\mathcal{M}$ be as in Theorem 8.4.30. Then for each $C \in A^{\odot}$ we have:*

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

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

$$\bigwedge_{i\in I} wp[w](C)(X_i) \wedge \Gamma(\mathcal{M}) \subseteq wp[w](C)(\bigwedge_{i\in I} X_i).$$

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 $h_i \in H$ $(i \in I)$, let $w : S \rightarrow \mathcal{QMT}(\mathcal{H})$, and let $X_i, Y_i \in S(\mathcal{H})$ $(i \in I)$. Suppose that for all homomorphisms φ with $\varphi|S = w$,*

$$X_i \subseteq \varphi(h_i)(Y_i) \text{ for every } i \in I$$

implies

$$X_i \subseteq \varphi(\mathbf{body}(h_i))(Y_i) \text{ for every } i \in I.$$

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

Proof. Put

$$\mathcal{U} = \{u : \mathcal{QMT}(\mathcal{H})^H : X_i \subseteq u(h_i)(Y_i) \text{ for all } i \in I\}.$$

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

$$(w \cup u)^{\odot}(h_i)(Y_i) = u(h_i)(Y_i) \supseteq X_i$$

for all $i \in I$, and $(w \cup u)^{\odot}|S = w$. Then the assumption yields:

$$D[w](u)(h_i)(Y_i) = (w \cup u)^{\odot}(\mathbf{body}(h_i))(Y_i) \supseteq X_i$$

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

$$wlp[w_i](h_i)(Y_i) = \mathrm{gfp}(D[w])(h_i)(Y_i) \supseteq X_i$$

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 $h_i \in H$ $(i \in I)$, let $w : S \rightarrow \mathcal{QMT}(\mathcal{H})$, and let $X_i, Y_i \in S(\mathcal{H})$ $(i \in I)$. Suppose that for all homomorphisms φ with $\varphi|S = w$,*

$$\varphi(h_i)(Y_i) \subseteq X_i \text{ for every } i \in I$$

implies

$$\varphi(\mathbf{body}(h_i))(Y_i) \subseteq X_i \text{ for every } i \in I.$$

Then $wp[w](h_i)(Y_i) \subseteq X_i$ *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 to two main parts. The first part is devoted into 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 weakest preconditions are carefully examined.

An interesting topic for further studies would be to establish a link between quantum predicate transformer semantics and Kozen's probabilistic predicate transformer semantics (Kozen 1981) through the Gleason theorem (Dvurečenskij 1993).

This chapter focuses on establishing a mathematical foundation of quantum predicate transformer semantics. So, a more important topic for further studies would be to apply the abstract mechanism developed in the present chapter to quantum program verification or development. In fact, D'Hondt and Panangaden (2006) used their approach to give a semantics of Selinger's QPL (Selinger 2004), and the D'Hondt-Panangaden approach to quantum predicate transformer semantics was also used by the authors of the present chapter (Feng et al. 2007) to give proof rules for the correctness of programs written in a simple language fragment that may describe the quantum part of a future quantum computer in Knill's architecture (Knill 1996). In a forthcoming paper, we will systematically use the projective predicate transformer semantics developed in the second part of this chapter in reasoning about programs written in the existing quantum programming languages, *e.g.*, Ömer's QCL (Ömer 2003), Sander and Zuliani's qGCL (Sanders and Zuliani 2000), and Selinger's QPL (Selinger 2004), as well as quantum loops defined in Ying and Feng (2006). In Zuliani (2004), Zuliani initiated a study of nondeterministic quantum programming. In the future studies, we hope to define the notion of refinement relation between quantum programs based on quantum predicate transformer semantics and eventually build a refinement calculus for supporting stepwise refinement strategy in quantum programs development by combining the work reported in this chapter with that of Zuliani (2004).

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

Birkhoff, G., and von Neumann, J. (1936) The logic of quantum mechanics. *Annals of Mathematics* **37**:823–843.

Bruns, G., and Harding, J. (2000) Algebraic aspects of orthomodular lattices. In Coecke, B., Moore, D., and Wilce, A., editors, *Current Research in Operational Quantum Logic: Algebras, Categories, Languages*, pages 37–65. Kluwer.

Butler, M. J., and Hartel, P. H. (1999) Reasoning about grover's quantum search algorithms using probabilistic wp. *ACM Transactions on Programming Languages and Systems* **21**:417–430.

D'Hondt, E., and Panangaden, P. (2006) Quantum weakest preconditions. *Mathematical Structures in Computer Science* **16**:429–451.

Diestel, J., and Uhl, J. J. Jr., (1977) *Vector Measures*. American Mathematical Society.

Dijkstra, E. W. (1976) *A Discipline of Programming*. Prentice-Hall.

Dijkstra, E. W., and Scholten, C. S. (1990) *Predicate Calculus and Program Semantics*. Springer-Verlag.

Dvurečenskij, A. (1993) *Gleason's Theorem and Its Applications*. Kluwer.

Feng, Y., Duan, R. Y., Ji, Z. F., and Ying, M. S. (2007) Proof rules for correctness of quantum programs. *Theoretical Computer Science* **386**:151–166.

Gay, S. J. (2006) Quantum programming languages: survey and bibliography. *Mathematical Structures in Computer Science* **16**:581–600.

Gudder, S. (1996) Lattice properties of quantum effects. *Journal of Mathematical Physics* **37**:2637–2642.

Hesselink, W. H. (1992) *Programs, Recursion and Unbounded Choice: Predicate-Transformation Semantics and Transformation Rules*. Cambridge University Press.

Hoare, C. A. R. (1971) Procedures and parameters: an axiomatic approach. In Engeler, E., editor, *Symposium on Semantics of Algorithmic Languages*, pages 102–116. *Lecture Notes in Mathematics* 188, Springer-Verlag.

Kadison, R. (1951) Order properties of bounded self-adjoint operators. *Proceedings of American Mathical Society* **34**:505–510.

Kalmbach, G. (1983) *Orthomodular Lattices*. Academic Press.

Knill, E. (1996) Conventions for quantum pseudocode. Technical Report LAUR-96-2724, Los Alamos National Laboratory.

Kozen, D. (1981) Semantics of probabilistic programs. *Journal of Computer and System Sciences* **22**:328–350.

Kraus, K. (1983) *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer-Verlag.

Lloyd, J. W. (1987) *Foundations of Logic Programming*. Springer-Verlag.

Morgan, C. C., McIver, A. K., and Seidel, K. (1996) Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems* **18**:325–353.

Nielsen, M. A., and Chuang, I. L. (2000) *Quantum Computation and Quantum Information*. Cambridge University Press.

Ömer, B. (2003) *Structured Quantum Programming*. Ph.D. thesis, Technicla Unviersity of Vienna.

Prugovečki, E. (1981) *Quantum Mechanics in Hilbert Space*. Academic Press.

Putnam, C. R. (1967) *Commutation Properties of Hilbert Space Operators and Related Topics*. Springer-Verlag.

Sanders, J. W., and Zuliani, P. (2000) Quantum programming. In *Proceedings of Mathematics of Program Construction 2000*, pages 80–99. LNCS 1837.

Scott, D. S. (1970) Outline of a mathematical theory of computation. In *Proceedings of 4th Annual Princeton Conference on Information Sciences and Systems*, pages 169–176.

Selinger, P. (2004) Towards a quantum programming language. *Mathematical Structures in Computer Science* **14**:527–586.

Takeuti, G. (1981) Quantum set theory. In Beltrametti, E., and Fraassen, B. C. v., editors, *Current Issues in Quantum Logics*, pages 303–322. Plenum.

Varadarajan, V. S. (1985) *Geometry of Quantum Theory*. Springer-Verlag.

Ying, M. S. (2000) Automata theory based on quantum logic (i), (ii). *International Journal of Theoretical Physics* **39**:985–995; 2545–2557.

Ying, M. S. (2005) A theory of computation based on quantum logic (i). *Theoretical Computer Science* **344**:134–207.

Ying, M. S. (2007) Quantum logic and automata theory. In Engesser, K., Gabbay, D., and Lehmann, D., editors, *Handbook of Quantum Logic and Quantum Structures*, pages 619–754. Elsevier.

Ying, M. S., Chen, J. X., Feng, Y., and Duan, R. Y. (2007) Commputativity of quantum weakest preconditions. *Information Processing Letters* **104**:152–158.

Ying, M. S., and Feng, Y. (2006) Quantum loop programs. *http://arxiv.org/abs/quant-ph/0605218*.

Zuliani, P. (2004) Non-deterministic quantum programming. In Selinger, P., editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages*, pages 179–195. TUCS General Publication No 33, Turku Centre for Computer Science, Turku, Finland.

9

The Structure of Partial Isometries

Peter Hines and Samuel L. Braunstein

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, $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ fails and is replaced by the weaker condition $A \leq C \Rightarrow A \wedge (A^{\perp} \vee C) = C$). The resulting system of *orthomodular lattices* has become known as *quantum logic*, and a number of authors (Finkelstein