Commutativity of Quantum Weakest Preconditions*

Mingsheng Ying[†], Jianxin Chen, Yuan Feng and Runyao Duan

State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology,
Tsinghua University, Beijing 100084, China

Abstract

The notion of quantum weakest precondition was introduced by D'Hondt and P. Panangaden (*Mathematical Structures in Computer Science* 16(2006)429-451), and they presented a representation of weakest precondition of a quantum program in the operator-sum form. In this letter, we give an intrinsic characterization of the weakest precondition of a quantum program given in a system-environment model. Furthermore, some sufficient conditions for commutativity of quantum weakest preconditions are presented.

Key Words: Formal Semantics; Quantum program; Hermitian matrix; Super-operator; Weakest precondition

1 Introduction

In the middle of 1990's Shor [14] and Grover [5] discovered, respectively, the famous quantum factoring and searching algorithms. These indicate that quantum computation offers a way to accomplish certain computational tasks much more efficiently than classical 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 techniques needed in building functional quantum computers.

Currently, quantum algorithms are expressed at the very low level of quantum circuits. Recently, however, some authors [1, 2, 7, 10, 12, 13] begun to study the design and semantics of quantum programming languages. In particular, a notion of quantum weakest precondition is introduced and a Stone-type duality between the state transition semantics and the predicate transformer semantics for quantum programs is established by D'Hondt and Panangaden [3].

Following Selinger [13], quantum programs may be represented by super-operators. In D'Hondt and Panangaden's approach [3], a quantum predicate is then defined to be an observable, namely, a Hermitian operator on the state space. This is a natural generalization of Kozen's probabilistic predicate as a measurable function [8].

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 of such problems is commutativity of quantum weakest preconditions. The significance of this problem comes from the following two observations. First, 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 [9], page 89). Sec-

*This work was partly supported by the National Foundation of Natural Sciences of China (Grant No: 60621062) and the National Key Project for Fundamental Research of China (Grant No: 2007CB807901).

[†]Email: yingmsh@tsinghua.edu.cn

ond, various logical operations of quantum weakest preconditions such as conjunction and disjunction will be needed in reasoning about complicated quantum programs, but defining these operations requires commutativity between the involved quantum predicates (see [6], Section 3.6).

The aim of this letter is to find some conditions under which quantum weakest preconditions commute. This letter is organized as follows: Some basic notions of quantum programs and quantum weakest preconditions are reviewed in Section 2. At the end of Section 2, a characterization of quantum weakest precondition is presented for the case that quantum programs are given in a system-environment model. In Section 3, we give some sufficient conditions under which quantum weakest preconditions commute. We then consider the problem of commutativity of weakest preconditions for quantum programs written in a fragment of Selinger's quantum programming language QPL in Section 4. A short conclusion is drawn in Section 5.

2 Quantum Weakest Preconditions

We first recall from [3] some basic notions needed in the sequel. Let $\mathcal{H}$ be a Hilbert space. Two vectors $|\varphi\rangle$ and $|\psi\rangle$ in $\mathcal{H}$ are said to be orthogonal and we write $|\varphi\rangle\perp|\psi\rangle$ if $\langle\varphi|\psi\rangle = 0$. The set of linear operators on $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. An operator A on $\mathcal{H}$ is said to be Hermitian if $M^\dagger = M$, and an operator A is positive if $\langle x|A|x\rangle \geq 0$ for all states $|x\rangle \in \mathcal{H}$. The trace $tr(A)$ of A is defined to be

$$tr(A) = \sum_i \langle i|A|i\rangle,$$

where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}$. A density matrix ρ on a Hilbert space $\mathcal{H}$ is a positive operator with $tr(\rho) \leq 1$. Here, following [13], the trace of a density operator is allowed to be smaller than 1 so that non-normalized quantum states can be dealt with in a convenient way. The set of density operators on $\mathcal{H}$ is denoted $\mathcal{D}(\mathcal{H})$. Let A and B be two operators on $\mathcal{H}$. Then the Löwner ordering between them is defined as follows: $A \sqsubseteq B$ if $B - A$ is a positive operator.

A super-operator on $\mathcal{H}$ is a linear operator $\mathcal{E}$ from the space $\mathcal{L}(\mathcal{H})$ into itself which 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 operation on $\mathcal{H}_R$.

We write $\mathcal{CP}(\mathcal{H})$ for the set of super-operators on $\mathcal{H}$. Super-operators are used to represent quantum programs (see [13, 3] for details). The following theorem gives two representations of super-operators, which are needed in the sequel.

Theorem 2.1 *([9], Section 8.2.3; Theorem 8.1) The following statements are equivalent:*

(1) $\mathcal{E}$ is a super-operator on $\mathcal{H}$;

(2) (System-environment model) There are an environment system E with state space $\mathcal{H}_E$, and a unitary transformation U and a projector P on $\mathcal{H} \otimes \mathcal{H}_E$ such that

$$\mathcal{E}(\rho) = tr_E[PU(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P] \qquad (1)$$

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

(3) (Kraus operator-sum representation) There exists a set of operators $\{E_i\}$ on $\mathcal{H}$ such that $\sum_i E_i^\dagger E_i \sqsubseteq I$ and

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \qquad (2)$$

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 Eq.(2).

A (quantum) predicate on $\mathcal{H}$ is defined to be a Hermitian operator M with $0 \sqsubseteq M \sqsubseteq I$. The set of predicates on $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Definition 2.1 *([3], Definition 3.1) For any quantum predicates $M, N \in \mathcal{P}(\mathcal{H})$, and for* *any quantum program $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$, M is called a precondition of N with respect to $\mathcal{E}$, written $M\{\mathcal{E}\}N$, if*

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

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

Definition 2.2 *([3], Definition 3.2) Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate and $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ 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 $N \sqsubseteq wp(\mathcal{E})(M)$.

An operator-sum representation of $wp(\mathcal{E})$ was found in [3] by exploiting a Stone-type duality when $\mathcal{E}$ is given in the form of operator-sum.

Proposition 2.1 *([3], Proposition 3.3) Suppose that $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ is represented by the set $\{E_i\}$ of operators. Then for each $M \in \mathcal{D}(\mathcal{H})$, we have:*

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

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 2.2 *If $\mathcal{E}$ is given by Eq. 1, 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 2.2 we obtain:

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

$$= \langle e_0|U^\dagger P(\sum_k |e_k\rangle M\langle e_k|)PU|e_0\rangle.$$

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. □

3 Commutativity

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 paper is the following:

Question 1: *Given a quantum program $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$. When do $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute?*

We first see a simple example.

Example 3.1 *(Bit flip and phase flip) Bit flip and phase flip are quantum operations on single qubits, and they are widely used in the theory of quantum error-correction. We write the Pauli matrices:*

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

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

Then the bit flip is given by

$$\mathcal{E}(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger, \qquad (3)$$

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

If E_1 in Eq. 3 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 super-operators: unitary transformations and quantum measurements.

Proposition 3.1 *(1) Let $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ be a unitary transformation, i.e., $\mathcal{E}(\rho) = U\rho U^\dagger$ for any $\rho \in \mathcal{D}(\mathcal{H})$, where $UU^\dagger = U^\dagger U = I$.*

Then $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ commute if and only if M and N commute.

(2) Let $\{P_k\}$ be a projective measurement, i.e., $P_{k_1}P_{k_2} = \delta_{k_1k_2}P_{k_1}$ and $\sum_k P_k = I$, 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. (1) From Proposition 2.1 we obtain:

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

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

(2) We obtain:

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

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:

$$\begin{aligned} P_kMP_kNP_k &= P_k(\sum_l P_lMP_lNP_l) \\ &= P_k(\sum_l P_lNP_lMP_l) = P_kNP_kMP_k. \end{aligned}$$

For the case of $P_i = |i\rangle\langle i|$ for each i, $P_iMP_iNP_i = |i\rangle\langle i|M|i\rangle\langle i|N|i\rangle\langle i|$. 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. □

The question about commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ seems very difficult to answer for a general super-operator. We are only able to give some sufficient conditions for such a commutativity. We first consider the operator-sum form of super-operator.

Proposition 3.2 *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*

$$M = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \text{ and } N = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$$

where λ_i, μ_i are reals for each i ([9], Theorem 2.2), and let $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ 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 $ME_iE_j^\dagger N = (\lambda_k\mu_l e_{kl})_{k,l}$ and $NE_iE_j^\dagger M = (\mu_k\lambda_l e_{kl})_{k,l}$ 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 2.1 that

$$\begin{aligned} &wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N) \\ &= (\sum_i E_i^\dagger ME_i)(\sum_i E_i^\dagger NE_i) \\ &= \sum_{i,j} E_i^\dagger ME_iE_j^\dagger NE_j, \end{aligned} \tag{4}$$

and

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

Definition 3.1 *Let $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ 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.*

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

Lemma 3.1 *(Unitary freedom in the operator-sum representation; [9], Theorem 8.2) Suppose that $\{E_1, ...E_m\}$ and $\{F_1, ..., F_n\}$ 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 $m = n$. Then $\mathcal{E} = \mathcal{F}$ if and only if there exist complex numbers u_{ij} such that $E_i = \sum_j u_{ij} F_j$, and $(u_{ij})_{m\times m}$ is a unitary matrix.*

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 3.2 *The notion of commutativity between observables and quantum operations is well-defined. Suppose that $\mathcal{E}$ is represented by both $\{E_1, ...E_m\}$ and $\{F_1, ..., F_n\}$. Then M and E_i commute for all $i = 1, 2, ..., m$ if and only if M and F_j commute for all $j = 1, 2, ..., n$.*

Proof. Immediate from Lemma 3.1. □

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

Proposition 3.3 *Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate, and let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{CP}(\mathcal{H})$ be two quantum programs. If M and $\mathcal{E}_i$ commute for $i = 1, 2$, then M and $\mathcal{E}_1; \mathcal{E}_2$ commute.*

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:

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

With Lemma 3.2 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 3.4 *Let $M, N \in \mathcal{P}(\mathcal{H})$ be two quantum predicates, and let $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$ 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:

$$\begin{aligned} &ME_iE_j^\dagger N = E_iME_j^\dagger N^\dagger = E_iM(NE_j)^\dagger \\ &= E_iM(E_jN)^\dagger = E_iMN^\dagger E_j^\dagger = E_iMNE_j^\dagger \end{aligned}$$

and from Eq. 4 we obtain:

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

Similarly, it holds that

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

Then commutativity between M and N implies

$$wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N) = wp(\mathcal{E})(M) \cdot wp(\mathcal{E})(N). \square$$

It is easy to see from Proposition 3.1 that the condition for commutativity of $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ given in Proposition 3.4 is not necessary.

We now turn to consider the system-environment model of super-operator. To this end, we need a generalization of commutativity between linear operators.

Definition 3.2 *Let $M, N, A, B, C \in \mathcal{L}(\mathcal{H})$.*

(1) 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;

(2) If $AB^\dagger = BA^\dagger$, then we say that A and B conjugate-commute.

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

Proposition 3.5 *Let $\mathcal{E}$ be given by Eq. 1, and we write $A = PU|e_0\rangle$.*

(1) $wp(\mathcal{E})(M)$ 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;

(2) 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 2.2. □

Proposition 3.6 *Let $\mathcal{E}$ be given by Eq. 1, 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*

$$M = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \text{ and } N = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$$

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

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

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

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

$$\langle\psi_i e_k|(M\otimes I_E)PU|e_0\rangle\langle e_0|U^\dagger P(N\otimes I_E)|\psi_j e_l\rangle$$
$$= \lambda_i\mu_j\langle\psi_i e_k|PU|e_0\rangle\langle e_0|U^\dagger P|\psi_j e_l\rangle.$$

If $\lambda_i\mu_j = \lambda_j\mu_i$ or

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

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

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

This means that

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

Then the conclusion follows immediately from Proposition 3.6. □

4 Commutativity in a Fragment of Quantum Programming Language

In this section, we consider the problem of commutativity of quantum weakest preconditions in the purely quantum fragment of Selinger's quantum programming language QPL. The syntax of this fragment is given by

$$S ::= \textbf{abort}|\textbf{skip}|q := 0|\overline{q}* = U|S;S|$$
$$\textbf{measure } q \textbf{ then } S \textbf{ else } S|\textbf{while } q \textbf{ do } S$$

For simplicity, we identify a quantum program written in QPL and its denotation in $\mathcal{CP}(\mathcal{H})$. D'Hondt and Panangaden's quantum weakest precondition calculus was used by Feng et al. [4] in reasoning about (total and partial) correctness of quantum programs written in the above fragment of QPL. In particular, they gave the following:

Lemma 4.1 *([4], Figure 2) For any $M \in \mathcal{M}(\mathcal{H})$, we have:*

$wp(\textbf{abort})(M) = \mathbf{0}$,
$wp(\textbf{skip})(M) = M$,
$wp(q := 0)(M) = |0\rangle_q\langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 0|M|0\rangle_q\langle 1|$,
$wp(\overline{q}* = U)(M) = U_{\overline{q}}^\dagger M U_{\overline{q}}$,
$wp(S_1; S_2)(M) = wp(S_1)(wp(S_2)(M))$,
$wp(\textbf{measure } q \textbf{ then } S_1 \textbf{ else } S_0)(M) = |0\rangle_q\langle 0|wp(S_0)(M)|0\rangle_q\langle 0| + |1\rangle_q\langle 1|wp(S_1)(M)|1\rangle_q\langle 1|$,
$wp(\textbf{while } q \textbf{ do } S)(M) = \mu X.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 1|wp(S)(X)|1\rangle_q\langle 1|)$,

where $|i\rangle_q\langle j|$ denotes the operator which applies $|i\rangle\langle j|$ on qubit q, leaving other qubits unchanged, i.e., $|i\rangle_q\langle j| = I_{\mathcal{H}_1} \otimes |i\rangle\langle j| \otimes I_{\mathcal{H}_2}$ for some appropriate Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, and $\mu X.\mathcal{F}(X)$ stands for the least fixed point of $\mathcal{F}(X)$.

To present the main result of this section, we introduce a notion of commutativity-reflectance.

Definition 4.1 *Let $A, B, C \in \mathcal{L}(\mathcal{H})$ and $\mathcal{E} \in \mathcal{CP}(\mathcal{H})$. We say that $\mathcal{E}$ reflects $(A, B, C)-$commutativity if $wp(\mathcal{E})(M)$ and $wp(\mathcal{E})(N)$ $(A, B, C)-$commute whenever M and N $(A, B, C)-$commute. In particular, it is said that $\mathcal{E}$ reflects $A-$commutativity if it reflects $(A, A, A)-$commutativity, and we simply say that $\mathcal{E}$ reflects commutativity if it reflects $I_{\mathcal{H}}-$commutativity, where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$.*

Proposition 4.1 *(1) For any $M, N \in \mathcal{P}(\mathcal{H})$, $wp(\mathbf{abort})(M)$ and $wp(\mathbf{abort})(N)$ commute.*

(2) $wp(\mathbf{skip})(M)$ and $wp(\mathbf{skip})(N)$ commute if and only if M and N commute.

(3) $wp(q := 0)(M)$ and $wp(q := 0)(N)$ commute if and only if M and N $|0\rangle_q\langle 0|-$commute and $(|1\rangle_q\langle 0|, |0\rangle_q\langle 0|, |0\rangle_q\langle 1|)-$commute.

(4) $wp(\overline{q}* = U)(M)$ and $wp(\overline{q}* = U)(N)$ commute if and only if M and N commute.

(5) If both S_1 and S_2 reflects commutativity, so do $S_1; S_2$.

(6) $wp(\mathbf{measure}\ q\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0)(M)$ and $wp(\mathbf{measure}\ q\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0)(N)$ commute if and only if $wp(S_i)(M)$ and $wp(S_i)(N)$ $|i\rangle_q\langle i|-$commute for $i = 0, 1$.

(7) If M and N $|0\rangle_q\langle 0|-$commute, and S reflects $|1\rangle_q\langle 1|-$commutativity, then $wp(\mathbf{while}\ q\ \mathbf{do}\ S)(M)$ and $wp(\mathbf{while}\ q\ \mathbf{do}\ S)(N)$ commute. Conversely, if $wp(\mathbf{while}\ q\ \mathbf{do}\ S)(M)$ and $wp(\mathbf{while}\ q\ \mathbf{do}\ S)(N)$ commute, then M and N $|0\rangle_q\langle 0|-$commute.

Proof. (1), (2) and (5) are immediate from Lemma 4.1, and (4) from Proposition 3.1(1).

(3) From Lemma 4.1 we obtain:

$$wp(q := 0)(M)wp(q := 0)(N) = |0\rangle_q\langle 0|M|0\rangle_q \langle 0|N|0\rangle_q\langle 0| + |1\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 1|,$$

$$wp(q := 0)(N)wp(q := 0)(M) = |0\rangle_q\langle 0|N|0\rangle_q \langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 1|.$$

If M and N $|0\rangle_q\langle 0|-$commute and $(|1\rangle_q\langle 0|, |0\rangle_q\langle 0|, |0\rangle_q\langle 1|)-$commute, it is clear that

$$wp(q := 0)(M)wp(q := 0)(N) = wp(q := 0)(N)wp(q := 0)(M).$$

Conversely, if $wp(q := 0)(M)$ and $wp(q := 0)(N)$ commute, then

$$\begin{aligned}|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0| &= |0\rangle_q\langle 0|wp(q := 0)(M)wp(q := 0)(N)\\ &= |0\rangle_q\langle 0|wp(q := 0)(N)wp(q := 0)(M)\\ &= |0\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 0|.\end{aligned}$$

Similarly, we have:

$$|1\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 1| = |1\rangle_q\langle 0|N|0\rangle_q\langle 0|M|0\rangle_q\langle 1|.$$

(6) Similar to (3).

(7) We put

$$\begin{aligned}\mathcal{F}^{(0)}(M) &= |0\rangle_q\langle 0|M|0\rangle_q\langle 0|,\\ \mathcal{F}^{(n+1)}(M) &= |0\rangle_q\langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 1|wp(S)(\mathcal{F}^{(n)}(M))|1\rangle_q\langle 1|\end{aligned}$$

for all $n \geq 0$. Note that

$$\begin{aligned}&|1\rangle_q\langle 1|\mathcal{F}^{(0)}(M)|1\rangle_q\langle 1|\mathcal{F}^{(0)}(N)|1\rangle_q\langle 1|\\ &\quad = |1\rangle_q\langle 1|\mathcal{F}^{(0)}(N)|1\rangle_q\langle 1|\mathcal{F}^{(0)}(M)|1\rangle_q\langle 1| = \mathbf{0}.\end{aligned}$$

Then it is easy to show that $\mathcal{F}^{(n)}(M)\mathcal{F}^{(n)}(N) = \mathcal{F}^{(n)}(N)\mathcal{F}^{(n)}(M)$ by induction on n. We write $qloop = \mathbf{while}\ q\ \mathbf{do}\ S$ for short. It follows that

$$\begin{aligned}&wp(qloop)(M)wp(qloop)(N)\\ &= \sqcup_{n\geq 0}\mathcal{F}^{(n)}(M) \sqcup_{n\geq 0} \mathcal{F}^{(n)}(N)\\ &= \sqcup_{n\geq 0}\mathcal{F}^{(n)}(M)\mathcal{F}^{(n)}(N)\\ &= \sqcup_{n\geq 0}\mathcal{F}^{(n)}(N)\mathcal{F}^{(n)}(M)\\ &= wp(qloop)(N)wp(qloop)(M).\end{aligned}$$

Conversely, by induction we have

$$|0\rangle_q\langle 0|\mathcal{F}^{(n)}(M)\mathcal{F}^{(n)}(N) = |0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|.$$

Then

$$\begin{aligned}&|0\rangle_q\langle 0|wp(qloop)(M)wp(qloop)(N)\\&=\sqcup_{n\geq 0}|0\rangle_q\langle 0|\mathcal{F}^{(n)}(M)\mathcal{F}^{(n)}(N)\\&=|0\rangle_q\langle 0|M|0\rangle_q\langle 0|N|0\rangle_q\langle 0|,\end{aligned}$$

and

$$\begin{aligned}&wp(qloop)(M)wp(qloop)(N)\\&\qquad=wp(qloop)(N)wp(qloop)(M)\end{aligned}$$

implies that M and N $|0\rangle_q\langle 0|$−commute. □

5 Conclusion

Some sufficient conditions for commutativity of quantum weakest preconditions are presented in this letter, 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 general topic for further studies would be:

Question 2. 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., $[X,Y]=XY-YX$?

Note that in this letter we works in finite-dimensional Hilbert spaces. The infinite-dimensional counterpart of the above question might interest mathematicians working in the area of operator algebras [11].

References

[1] S. Betteli, T. Calarco and L. Serafini, Toward an architecture for quantum programming, arXiv:cs.PL/0103009 v2, Nov. 2001.

[2] R. Chadha, P. Mateus, and A. Sernadas, Reasoning about quantum imperative programs, *Electronic Notes in Theoretical Computer Science*, 158(2006)19–40.

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

[4] Y. Feng, R. Y. Duan, Z. F. Ji and M. S. Ying, Proof rules for correctness of quantum programs, *Theoretical Computer Science* (to appear)

[5] L. Grover, A fast quantum mechanical algorithm for database search, in: *Proceedings, 28th Annual ACM Symposium on the Theory of Computing,* pages 212-219, ACM Press, New York, 1996.

[6] V. S. Varadarajan, *Geometry of Quantum Theory*, Springer-Verlag, New York, 1985 (Second Edition).

[7] E. H. Knill, Conventions for quantum pseudocode, LANL report LAUR-96-2724, 1996.

[8] D. Kozen, Semantics of probabilistic programs, *Journal of Computer and System Science* 22(1981)328-350.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[10] B. *Ö*mer, A procedural formalism for quantum computing, Master's thesis, Department of theoretical Physics, Technical University of Vienna, July 1998. http://tph.tuwien.ac.at/ oemer/qcl.html.

[11] C. R. Putnam, *Commutation Properties of Hilbert Space Operators and Related Topics*, Springer-Verlag, New York, 1967.

[12] J. W. Sanders and P. Zuliani, Quantum programming, in: *Proceedings, Mathematics of Program Construction 2000*, LNCS 1837, pages 80-99, 2000.

[13] P. Selinger, Towards a quantum programming language, *Mathematical Structures in Computer Science* 14(2004)527-586.

[14] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, pages 124-134, IEEE Press, Los Alamitos, CA, 1994.