Proof rules for the correctness of quantum programs

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

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

December 10, 2013

Abstract

We apply the notion of quantum predicate proposed by D'Hondt and Panangaden to analyze a simple language fragment which may describe the quantum part of a future quantum computer in Knill's architecture. The notion of weakest liberal precondition semantics, introduced by Dijkstra for classical deterministic programs and by McIver and Morgan for probabilistic programs, is generalized to our quantum programs. To help reasoning about the correctness of quantum programs, we extend proof rules presented by Morgan for classical probabilistic loops to quantum loops. These rules are shown to be complete in the sense that any correct assertion about quantum loops can be proved using them. Some illustrative examples are also given to demonstrate the practicality of our proof rules.

1 Introduction

The theory of quantum computing has attracted considerable research efforts in the past twenty years. Benefiting from the possibility of superposition of different states and the linearity of quantum operations, quantum computing may provide considerable speedup over its classical analogue [22, 6, 7]. The existing quantum algorithms, however, are described at a very low level: they are usually represented as quantum circuits. A few works have been done in developing quantum programming languages which identify and promote high-level abstractions. The first step of writing quantum pseudo-code was moved by Knill [11]; while the first actual quantum programming language is due to Ömer [17, 18]. After that, Sanders and Zuliani [19, 25], Bettelli et al. [2], and Selinger [21] also proposed various quantum languages each having different features. We refer to [20] for a survey of this field.

The standard weakest precondition calculus [5] and its probabilistic extension [16] have been successful in reasoning about the correctness and even the rigorous derivation of classical programs. This success motivates us to develop analogous tools for quantum programs. Sanders and Zuliani [19] have provided for their qGCL a stepwise refinement mechanism. The approach, however, is classical in the sense that they treated quantum programs as special cases of probabilistic programs. As a consequence, known results about probabilistic weakest precondition calculus can be applied directly to quantum programs. Indeed, Butler and Hartel [3] have used it to reason about Grover's algorithm.

The first step towards really *quantum* weakest precondition calculus was made by D'Hondt and Panangaden [4]. They proposed the brilliant idea that we can treat an observable, mathematically described by a Hermitian matrix, as the quantum analogue of 'predicate'. The elegant duality between state-transformer semantics and the weakest precondition semantics (*wp*-semantics for short)

of quantum programs, when described by completely positive and trace-nonincreasing linear operators, was then proven to hold in a more direct way.

In this paper, we apply the ideas in [4] to analyze a simple quantum language fragment describing the quantum part of a potential quantum computer in Knill's architecture [11]. The syntax follows Selinger's style [21] except that we are only concerned with purely quantum data. We make this limitation on our language fragment merely for the sake of simplification. The results presented in this paper can be extended easily to a general language where both classical and quantum variables are involved. The denotational semantics of our language is given and shown to be a super-operator for each program construct; the *wp*-semantics which is useful for reasoning about the total correctness of quantum programs is presented following the correspondence between denotational semantics and *wp*-semantics proposed in [4]. To reason about the partial correctness of programs written in our quantum language, we extend the notion of weakest liberal precondition semantics (*wlp*-semantics for short), first introduced by Dijkstra[5] for deterministic programs and then generalized by McIver and Morgan[13] for probabilistic programs, to our quantum language. The numerical relations between these three semantics are also discussed.

In order to help reasoning about quantum programs involving loops, we extend the notion of loop invariant which is the key in correctness proving of classical programs (see [5] for deterministic and [15] for probabilistic loop invariants) to quantum setting. Based on it, we develop some rules to reason about the partial and total correctness of quantum loops. These rules are natural quantum extensions of those for classical probabilistic programs introduced by Morgan[15]. We also show the completeness of these rules in the sense that any correct assertion about quantum loops can be proved using them. To demonstrate the practicality of our proof rules, some illustrative examples are also presented. Particularly, we consider a discrete coined quantum walk on an n-cycle with an absorbing boundary at position 1, and prove using our proof rules that this kind of walk will ultimately terminate at position 1 with unit probability.

This paper is organized as follows. Section 2 is the preliminary part where basic concepts and notations used in this paper are reviewed. In Section 3, we propose the syntax and denotational semantics of our quantum language fragment. The *wp*-semantics is also given following the correspondence presented in [4]. Our main contribution starts from Section 4, where we extend the notion of *wlp*-semantics to the quantum language we consider. The quantity relations of these three semantics presented are also discussed. In Section 5, the *wp*- and *wlp*-semantics are used to present some proof rules of reasoning about quantum loop programs. The completeness of this rules are proved and some illustrative examples are also given. Section 6 is the concluding section in which we draw the conclusion and point out some problems for further studies.

2 Preliminaries

Let $\mathcal{H}$ be the associated (finite-dimensional) Hilbert space of the quantum system we are concerned with, and $\mathcal{L}(\mathcal{H})$ the set of linear operators (or complex matrices when an orthonormal basis of $\mathcal{H}$ is given. We do not distinguish between these two notions) on $\mathcal{H}$. For any linear operator $A \in \mathcal{L}(\mathcal{H})$, we have the following definitions:

1. A is hermitian if $A^\dagger = A$ where $A^\dagger$ is the adjoint operator of A such that $\langle\psi|A^\dagger|\phi\rangle = \langle\phi|A|\psi\rangle^*$ for any states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. Here for any complex number c, c^* denotes the complex conjugate of c.

2. A is positive if $\langle\psi|A|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$; it is positive-definite if for any nonzero vector $|\psi\rangle$, $\langle\psi|A|\psi\rangle > 0$. Note that a positive operator is also hermitian.

3. The trace of A is defined as $\mathrm{tr}(A) = \sum_{i=1}^{n}\langle i|A|i\rangle$ for some given orthonormal basis $\{|i\rangle,\ i = 1,\ldots,n\}$ of $\mathcal{H}$. Note also that the trace function is actually independent of the orthonormal

basis selected. Properties of trace function that will be used in this paper are the linearity and that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any operators $A, B \in \mathcal{L}(\mathcal{H})$.

With these notations, the set of all density operators (or alternatively, density matrices) on $\mathcal{H}$ can be defined as

$$\mathcal{D}\mathcal{H} := \{\ \rho \in \mathcal{L}(\mathcal{H}) \mid \mathbf{0} \sqsubseteq \rho,\ \mathrm{tr}(\rho) \leq 1\},$$

where $\mathbf{0}$ denotes the zero operator. The partial order $\sqsubseteq$ is defined on $\mathcal{L}(\mathcal{H})$ by letting $M \sqsubseteq N$ if $N - M$ is positive. The convention of allowing the trace of a density matrix to be less than 1 makes it possible to represent both the actual state (by the normalized density matrix) and the probability with which the state is reached (by the trace of the density matrix) in a single expression[21].

Recall further that for any linear operator $\mathcal{E} \in \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, $\mathcal{E}$ is said to be

1. positive if it maps positive operators in $\mathcal{L}(\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H})$;

2. completely positive if it is positive and so is the trivially extended operator

$$\mathcal{I} \otimes \mathcal{E} \in \mathcal{L}(\mathcal{H}' \otimes \mathcal{H}) \to \mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$$

for any auxiliary Hilbert space $\mathcal{H}'$. Here $\mathcal{I}$ is the identity map in $\mathcal{L}(\mathcal{H}')$. The elegant and powerful Kraus representation[12] of completely positive operators states that a map $\mathcal{E}$ is completely positive if and only if

$$\mathcal{E}(\rho) = \sum_{i=1}^{d} E_i \rho E_i^\dagger$$

for some set of matrices $\{E_i, i = 1, \ldots, d\}$. The matrices E_i are called Kraus operators of $\mathcal{E}$.

3. trace-nonincreasing if $\mathrm{tr}\mathcal{E}(A) \leq \mathrm{tr}(A)$ for any linear operator $A \in \mathcal{L}(\mathcal{H})$; it is trace-preserving if $\mathrm{tr}\mathcal{E}(A) = \mathrm{tr}(A)$ for all $A \in \mathcal{L}(\mathcal{H})$;

4. a super-operator if it is completely positive and trace-nonincreasing. In another word, a super-operator is a just completely positive operator with its Kraus operators E_i satisfying $\sum_i E_i^\dagger E_i \sqsubseteq I$.

Then the set of quantum programs over $\mathcal{H}$ can be defined as

$$\mathcal{Q}\mathcal{H} := \{\mathcal{E} \in \mathcal{D}\mathcal{H} \to \mathcal{D}\mathcal{H} \mid \mathcal{E} \text{ is a super-operator}\}.$$

The partial order on $\mathcal{Q}\mathcal{H}$ is defined naturally by letting $\mathcal{E} \sqsubseteq \mathcal{F}$ if $\mathcal{F} - \mathcal{E}$ is completely positive. It is proved in [4] that the two sets $\mathcal{D}\mathcal{H}$ and $\mathcal{Q}\mathcal{H}$ are both CPOs.

In D'Hondt and Panangaden's approach, a quantum predicate is described by a positive matrix with the maximum eigenvalue bounded by 1. To be specific, the set of quantum predicates on Hilbert space $\mathcal{H}$ is defined by

$$\mathcal{P}\mathcal{H} := \{M \in \mathcal{L}(\mathcal{H}) \mid \mathbf{0} \sqsubseteq \mathrm{M} \sqsubseteq \mathrm{I}\}.$$

This set, when equipped with the partial order defined above for $\mathcal{L}(\mathcal{H})$, is also a CPO [4]. For any $\rho \in \mathcal{D}\mathcal{H}$ and $M \in \mathcal{P}\mathcal{H}$, the degree of ρ satisfying M is denoted by the expression $\mathrm{tr}M\rho$. It is exactly the expectation (or average value according to respective probabilities) of the measurement outcomes when measuring the observable represented by M on the state ρ.

Notice that by definition, $\mathcal{D}\mathcal{H} \subseteq \mathcal{P}\mathcal{H}$, which means that any density matrix is automatically a quantum predicate. Particularly, if $M = |\psi\rangle\langle\psi|$ for some normalized pure state $|\psi\rangle \in \mathcal{H}$, then $\mathrm{tr}M\rho = \langle\psi|\rho|\psi\rangle$ is just the fidelity[1] between ρ and $|\psi\rangle\langle\psi|$, or the probability of observing $|\psi\rangle$ when

[1]Fidelity is a kind of 'distance' between quantum states defined by $F(\rho, \sigma) = \left(\mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right)^2$.

measuring ρ according to an orthonormal basis involving $|\psi\rangle$. This observation will be used to give an explanation of $wp.S.|\psi\rangle\langle\psi|$ in Section 3.

The 'healthy' predicate transformers which exactly characterize all valid quantum programs are shown to be those who are linear and completely positive [4]. Particularly, D'Hondt and Panangaden proved that quantum weakest precondition exists for any completely positive map by exploiting Kraus representation theorem. This kind of wp-semantics indeed gives an isomorphism between the set of healthy quantum predicate transformers

$$\mathcal{TH} := \{\mathcal{T} \in \mathcal{PH} \leftarrow \mathcal{PH} \mid \mathcal{T} \text{ is linear and completely positive}\}$$

and the set of quantum programs $\mathcal{QH}$ defined above, just as the cases for classical deterministic [5] and probabilistic programs [16]. Here we write the arrow backwards in the definition of $\mathcal{TH}$ to emphasize that it is actually a backward transformation from post-conditions to preconditions, compared with the forward transformation in $\mathcal{QH}$, which is from initial states to final states. D'Hondt and Panangaden also used their weakest precondition approach to prove the correctness of Grover's search algorithm. Note that there is no loop in Grover's algorithm since the number of iterations is pre-specified. One of the main contributions of the present paper is to extend D'Hondt and Panangaden's proposal to help reasoning about the correctness of quantum loops.

3 The syntax and the denotational/weakest precondition semantics

In this paper, we concentrate our attention on the purely quantum fragment of a general quantum programming language in the sense that only quantum data but no classical data are considered. Following Knill's QRAM model [11], a quantum computer in the future possibly consists of a general-purpose classical computer which controls a special quantum hardware device. Our quantum language considered here then aims at describing the action of the special quantum device, rather than the behavior of the whole computer including the classical controller. Note that the results of this paper can be easily extended to the general programming language by, for example, presenting classical and quantum variables by tuples of density matrices, and by extending quantum predicates to tuples of quantum predicates, just as what has been done in [21] and [4].

Suppose S, S_0 and S_1 denote quantum programs, $q_1, \ldots, q_n$ and q denote qubit-typed variables, and U denotes a unitary transformation which applies on a 2^n-dimensional Hilbert space. Then the syntax of our quantum language fragment is defined as follows:

$$\begin{aligned} S \quad ::= \quad & \textbf{abort} \mid \textbf{skip} \mid q := 0 \mid q_1, q_2, \ldots, q_n *= U \mid S_0; S_1 \mid \\ & \textbf{measure } q \textbf{ then } S_1 \textbf{ else } S_0 \mid \textbf{while } q \textbf{ do } S \end{aligned}$$

Here we borrow the notations from [21] except for **abort** and the loop statements. Intuitively, **abort** is the nowhere-terminating program, and $q := 0$ initializes qubit q by setting it to the standard state $|0\rangle$. The statement $q_1, q_2, \ldots, q_n *= U$ applies the unitary transformation U on the n distinct qubits $q_1, q_2, \ldots, q_n$. We put the constraint that $q_1, q_2, \ldots, q_n$ must be distinct to avoid syntactically some no-go operations such as quantum cloning. The statement **measure** q **then** S_1 **else** S_0 first applies a measurement on qubit q according to the computational basis, then executes S_1 or S_0 depending on whether the measurement result is 1 or 0. The loop statement **while** q **do** S measures qubit q first, also according to the computational basis. If the result is 0, then it terminates; otherwise it executes S and the loop repeats.

Formally, we have the following definition of denotational semantics:

Definition 3.1 *For any quantum program S, the denotational semantics of S is a map $[\![S]\!]$ from $\mathcal{DH}$ to $\mathcal{DH}$ defined inductively in Figure 1.*

Figure 1: Denotational semantics

$$
\begin{aligned}
[\![\mathbf{abort}]\!]\rho &:= \mathbf{0} \\
[\![\mathbf{skip}]\!]\rho &:= \rho \\
[\![q := 0]\!]\rho &:= |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0| \\
[\![\bar{q} *= U]\!]\rho &:= U_{\bar{q}}\rho U_{\bar{q}}^\dagger \\
[\![S_1; S_2]\!]\rho &:= [\![S_2]\!]([\![S_1]\!]\rho) \\
[\![\mathbf{measure}\ q\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0]\!]\rho &:= [\![S_1]\!](|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1|) + [\![S_0]\!](|0\rangle_q\langle 0|\rho|0\rangle_q\langle 0|) \\
[\![\mathbf{while}\ q\ \mathbf{do}\ S]\!] &:= \mu X \cdot (\mathbf{measure}\ q\ \mathbf{then}\ S; X\ \mathbf{else}\ \mathbf{skip})
\end{aligned}
$$

In Definition 3.1 and in the rest of this paper, $\bar{q}$ denotes the abbreviation of $q_1, \ldots, q_n$, $U_{\bar{q}}$ means applying U on the Hilbert space spanned by qubits $\bar{q}$, and $|x\rangle_q\langle y|$ denotes the operator which applies $|x\rangle\langle y|$ on qubit q, leaving other qubits unchanged. That is,

$$|x\rangle_q\langle y| = I_{\mathcal{H}_1} \otimes |x\rangle\langle y| \otimes I_{\mathcal{H}_2} \tag{1}$$

for some appropriate Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$.

Notice that if a measurement according to the computational basis $\{|0\rangle, |1\rangle\}$ is applied on qubit q when the whole system is in state ρ, the probability of observing outcome i is $p_i = \mathrm{tr}|i\rangle_q\langle i|\rho|i\rangle_q\langle i|$, and the post-measurement state of the whole system when i is observed is $\rho_i = |i\rangle_q\langle i|\rho|i\rangle_q\langle i|/p_i$, $i = 0, 1$. So the final output of the statement "**measure** q **then** S_1 **else** S_0" when ρ is input is

$$\sum_{i=0}^{1} p_i [\![S_i]\!]\rho_i = \sum_{i=0}^{1} [\![S_i]\!]|i\rangle_q\langle i|\rho|i\rangle_q\langle i|.$$

That justifies the definition of this statement in Definition 3.1.

The following lemma shows that the denotational semantics of our quantum programs are all super-operators. So they can be physically implemented in a future quantum computer.

Lemma 3.2 *For any quantum program S, the denotational semantics of S is a super-operator on $\mathcal{DH}$, i.e., $[\![S]\!] \in \mathcal{QH}$.*

Proof. The only case we should prove is when $S \equiv$ **while** q **do** S' is a quantum loop. In this case, it is direct from definition that

$$[\![S]\!] = \mu X \cdot (X \circ [\![S']\!] \circ \mathcal{E}_1 + \mathcal{E}_0)$$

where $\mathcal{E}_i$ are super-operators such that for any $\rho \in \mathcal{DH}$, $\mathcal{E}_i(\rho) = |i\rangle_q\langle i|\rho|i\rangle_q\langle i|$. Now suppose inductively that $[\![S']\!] \in \mathcal{QH}$. Then the map

$$X \to X \circ [\![S']\!] \circ \mathcal{E}_1 + \mathcal{E}_0$$

is Scott-continuous on $\mathcal{QH}$. From the fact that $\mathcal{QH}$ is a CPO ([21]), we derive the desired result that $[\![S]\!] \in \mathcal{QH}$. □

Figure 2: Weakest precondition semantics

$$
\begin{aligned}
wp.\mathbf{abort}.M &:= \mathbf{0} \\
wp.\mathbf{skip}.M &:= M \\
wp.(q := 0).M &:= |0\rangle_q\langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 0|M|0\rangle_q\langle 1| \\
wp.(\bar{q} *= U).M &:= U_{\bar{q}}^\dagger M U_{\bar{q}} \\
wp.(S_1; S_2).M &:= wp.S_1.(wp.S_2.M) \\
wp.(\mathbf{measure}\ q\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0).M &:= \sum_{i=0}^{1} |i\rangle_q\langle i|wp.S_i.M|i\rangle_q\langle i| \\
wp.(\mathbf{while}\ q\ \mathbf{do}\ S).M &:= \mu X \cdot (|1\rangle_q\langle 1|wp.S.X|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0|)
\end{aligned}
$$

Recall that from [4], any super-operator $\mathcal{E}$ can be given a corresponding wp-semantics as follows: suppose

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \qquad \forall \rho \in \mathcal{DH} \tag{2}$$

with $\sum_k E_k^\dagger E_k \sqsubseteq I$ is the Kraus representation of $\mathcal{E}$. Then $wp.\mathcal{E}$ is also a completely positive operator with the Kraus representation

$$wp.\mathcal{E}.M = \sum_k E_k^\dagger M E_k, \qquad \forall M \in \mathcal{PH}. \tag{3}$$

Following this idea, we define the wp-semantics for our quantum language as follows:

Definition 3.3 *For any quantum program S, the wp-semantics of S is defined by a map $wp.S$ from $\mathcal{PH}$ to $\mathcal{PH}$ defined inductively in Figure 2.*

Lemma 3.4 *The wp-semantics defined in Figure 2 indeed gives the desired correspondence. That is, for any quantum program S, if $\{E_k, k = 1, \ldots, d\}$ are the Kraus operators of $[\![S]\!]$, then $wp.S$ is also completely positive, and has $\{E_k^\dagger, k = 1, \ldots, d\}$ as its Kraus operators.*

Proof. It is easy to check. So we omit the details here. □

The following theorem shows a quantitative relation between denotational semantics and wp-semantics. Intuitively, the average outcome when observing a quantum predicate on the output of a quantum program is equal to the average outcome when observing the weakest precondition of this predicate with respect to the program on the input state.

Theorem 3.5 *For any quantum program S, quantum predicate $M \in \mathcal{PH}$, and $\rho \in \mathcal{DH}$, we have*

$$\mathrm{tr}(wp.S.M)\rho = \mathrm{tr} M[\![S]\!]\rho \tag{4}$$

Proof. Direct from Lemma 3.4 and Proposition 3.3 of [4]. □

Corollary 3.6 *The map $wp.S$ is linear on $\mathcal{PH}$ for any quantum program S. That is, for any $\lambda, \mu \in \mathbb{R}$ and $M, N \in \mathcal{PH}$,*

$$wp.S.(\lambda M + \mu N) = \lambda(wp.S.M) + \mu(wp.S.N)$$

provided that $\lambda M + \mu N \in \mathcal{PH}$.

Taking $M = I$ in Eq.(4), we have

$$\mathrm{tr}(wp.S.I)\rho = \mathrm{tr}[\![S]\!]\rho.$$

Notice that the righthand side of the above equation is exactly the probability that the program S terminates on input state ρ. So intuitively, the quantum predicate $wp.S.I$ denotes the condition the program S terminates, in analogy with the predicate $wp.S.\mathbf{true}$ in classical deterministic setting and $wp.S.1$ in probabilistic setting.

Another special case which is also worth noting is when $M = |\psi\rangle\langle\psi|$ for some normalized pure state $|\psi\rangle$. In this case, Eq.(4) becomes

$$\mathrm{tr}(wp.S.|\psi\rangle\langle\psi|)\rho = \mathrm{tr}|\psi\rangle\langle\psi|[\![S]\!]\rho = \langle\psi|[\![S]\!]\rho|\psi\rangle.$$

The quantity $\langle\psi|[\![S]\!]\rho|\psi\rangle$ denotes either the fidelity between $[\![S]\!]\rho$ and $|\psi\rangle\langle\psi|$ or the probability of observing $|\psi\rangle$ when measuring $[\![S]\!]\rho$ according to an orthonormal basis involving $|\psi\rangle$. So intuitively, the quantum predicate $wp.S.|\psi\rangle\langle\psi|$, when performed on the initial state, gives us information about the precision of the actual output of program S to approximate the desired output $|\psi\rangle$, or the probability for S, when followed by a measurement according to an orthonormal basis involving $|\psi\rangle$, to correctly output $|\psi\rangle$.

4 The weakest liberal precondition semantics

We have so far defined the *wp*-semantics, which is useful when we consider the total correctness of quantum programs. That is, what we care is not only the correctness of the final state when the program terminates, but also the condition a quantum program can terminate. To deal with partial correctness of quantum programs, we extend the notion of *wlp*-semantics to our quantum language as follows:

Definition 4.1 *For any quantum program S, the wlp-semantics of S is defined by a map $wlp.S$ from $\mathcal{PH}$ to $\mathcal{PH}$ defined inductively in Figure 3.*

Analogous with Theorem 3.5, the following theorem shows a quantitative connection between *wp*-semantics and denotational semantics.

Theorem 4.2 *For any quantum program S, quantum predicate $M \in \mathcal{PH}$, and $\rho \in \mathcal{DH}$, we have*

$$\mathrm{tr}(wlp.S.M)\rho = \mathrm{tr}M[\![S]\!]\rho + \mathrm{tr}\rho - \mathrm{tr}[\![S]\!]\rho. \tag{5}$$

Proof. We need only to consider the case when $S \equiv \mathbf{while}\ q\ \mathbf{do}\ S'$ is a quantum loop. Other cases are easier to check.

First, from definition we have

$$[\![\mathbf{while}\ q\ \mathbf{do}\ S']\!]\rho = \bigsqcup_{i=0}^{\infty} \mathcal{E}^i(\rho) \tag{6}$$

Figure 3: Weakest liberal precondition semantics

$$
\begin{array}{rcl}
wlp.\mathbf{abort}.M & := & I \\
wlp.\mathbf{skip}.M & := & M \\
wlp.(q := 0).M & := & |0\rangle_q\langle 0|M|0\rangle_q\langle 0| + |1\rangle_q\langle 0|M|0\rangle_q\langle 1| \\
wlp.(\bar{q} *= U).M & := & U_{\bar{q}}^\dagger M U_{\bar{q}} \\
wlp.(S_1; S_2).M & := & wlp.S_1.(wlp.S_2.M) \\
wlp.(\mathbf{measure}\ q\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0).M & := & \sum_{i=0}^{1} |i\rangle_q\langle i|wlp.S_i.M|i\rangle_q\langle i| \\
wlp.(\mathbf{while}\ q\ \mathbf{do}\ S).M & := & \nu X \cdot (|1\rangle_q\langle 1|wlp.S.X|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0|)
\end{array}
$$

where for any $\rho \in \mathcal{DH}$, $\mathcal{E}^0(\rho) = \mathbf{0}$ and

$$\mathcal{E}^{i+1}(\rho) = \mathcal{E}^i([\![S']\!]|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1|) + |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0|;$$

while

$$wlp.(\mathbf{while}\ q\ \mathbf{do}\ S').M = \prod_{i=0}^{\infty} \mathcal{F}^i(M), \tag{7}$$

where for any $M \in \mathcal{PH}$, $\mathcal{F}^0(M) = I$ and

$$\mathcal{F}^{i+1}(M) = |1\rangle_q\langle 1|wlp.S'.\mathcal{F}^i(M)|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0|.$$

Suppose Eq.(5) holds for the program S', i.e.,

$$\forall M \in \mathcal{PH}, \rho \in \mathcal{DH} \cdot \mathrm{tr}(I - wlp.S'.M)\rho = \mathrm{tr}(I - M)[\![S']\!]\rho. \tag{8}$$

We now prove by induction that for any $i \geq 0$

$$\forall M \in \mathcal{PH}, \rho \in \mathcal{DH} \cdot \mathrm{tr}(I - \mathcal{F}^i(M))\rho = \mathrm{tr}(I - M)\mathcal{E}^i(\rho). \tag{9}$$

When $i = 0$, Eq.(9) holds because both sides equal to 0. Suppose now Eq.(9) holds for $i = k$. Then when $i = k + 1$, we calculate that for any $M \in \mathcal{PH}$ and $\rho \in \mathcal{DH}$,

$$
\begin{array}{rcll}
 & \mathrm{tr}(I - \mathcal{F}^{k+1}(M))\rho & & \\
= & \mathrm{tr}\rho - \mathrm{tr}wlp.S'.\mathcal{F}^k(M)|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1| - \mathrm{tr}M|0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| & & \\
= & \mathrm{tr}(I - wlp.S'.\mathcal{F}^k(M))|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1| + \mathrm{tr}(I - M)|0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| & & \\
= & \mathrm{tr}(I - \mathcal{F}^k(M))([\![S']\!]|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1|) + \mathrm{tr}(I - M)|0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| & & \text{by Eq.(8)} \\
= & \mathrm{tr}(I - M)\mathcal{E}^k([\![S']\!]|1\rangle_q\langle 1|\rho|1\rangle_q\langle 1|) + \mathrm{tr}(I - M)|0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| & & \text{by induction hypothesis} \\
= & \mathrm{tr}(I - M)\mathcal{E}^{k+1}(\rho). & &
\end{array}
$$

So we deduce that Eq.(9) holds for any $i \geq 0$. Notice that the operation $\mathrm{tr}(\cdot)$ is linear. We further calculate

$$\begin{aligned}
\mathrm{tr}(wlp.S.M)\rho &= \mathrm{tr}(\sqcap_i \mathcal{F}^i(M))\rho \\
&= \sqcap_i \mathrm{tr}\mathcal{F}^i(M)\rho \\
&= \sqcap_i(\mathrm{tr}\rho - \mathrm{tr}(I-M)\mathcal{E}^i(\rho)) \qquad \text{by Eq.(9)} \\
&= \mathrm{tr}\rho - \sqcup_i \mathrm{tr}(I-M)\mathcal{E}^i(\rho) \\
&= \mathrm{tr}\rho - \mathrm{tr}(I-M) \sqcup_i \mathcal{E}^i(\rho) \\
&= \mathrm{tr}\rho - \mathrm{tr}(I-M)[\![S]\!]\rho.
\end{aligned}$$

That completes our proof. □

Taking $M = \mathbf{0}$ in Eq.(5), we have

$$\mathrm{tr}(wlp.S.\mathbf{0})\rho = \mathrm{tr}\rho - \mathrm{tr}[\![S]\!]\rho.$$

Notice that the righthand side of the above equation is exactly the probability the program S does not terminate when the input state is ρ. So intuitively the quantum predicate $wlp.S.\mathbf{0}$ denotes the condition the program S diverges.

Corollary 4.3 *For any quantum program S and quantum predicate $M \in \mathcal{PH}$,*

$$wp.S.M \sqsubseteq wlp.S.M$$

and

$$wlp.S.M + wp.S.(I-M) = I.$$

Proof. Direct from Theorems 3.5 and 4.2.

To get a clearer picture of the connection between these two precondition semantics, let us introduce a notion which can be regarded as the analogue of conjunction $\wedge$ of classical standard predicates and probabilistic conjunction & of probabilistic predicates. Note that in [15], the conjunction & of probabilistic predicates $\alpha, \beta : \Sigma \to [0,1]$ is defined by

$$\alpha \,\&\, \beta = (\alpha + \beta) \ominus \underline{1}$$

where Σ is the state space, $\underline{1}$ is the predicate which takes value 1 everywhere, and for any state $s \in \Sigma$,

$$(\alpha \ominus \beta).s = \max\{\alpha.s - \beta.s, 0\}.$$

Definition 4.4 *Suppose M and N are two quantum predicates. We define $M\&N$ as*

$$M\&N := (M + N - I)^+,$$

where for any hermitian matrix X, if $X = \sum_i \lambda_i P_i$ is the spectrum decomposition of X, then $X^+ = \sum_i \max\{\lambda_i, 0\} P_i$.

When M and N commute, i.e. when $MN = NM$, suppose $\lambda(M)$, $\lambda(N)$, and $\lambda(M\&N)$ denote respectively the vector of the eigenvalues of M, N, and $M\&N$ arranged in some pre-specified order of their (common) eigenvectors. Then

$$\lambda(M\&N) = \lambda(M) + \lambda(N) \ominus \underline{1}$$

which coincides with the case of probabilistic setting.

Note that the quantum conjunction defined in Definition 4.4 is not monotonic in general because the operation $(\cdot)^+$ is not monotonic for hermitian matrices. A simple example is as follows. Let $M = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $N = M + |0\rangle\langle 0| \sqsupseteq M$. It is not difficult to check that $M^+ \not\sqsubseteq N^+$.

Theorem 4.5 *For any quantum predicates $M, N \in \mathcal{PH}$ and any quantum program S, if $M+N \sqsupseteq I$ then*

$$wp.S.(M\&N) = wlp.S.M \ \& \ wp.S.N \tag{10}$$

and

$$wlp.S.(M\&N) = wlp.S.M \ \& \ wlp.S.N \tag{11}$$

Proof. From the assumption that $M + N \sqsupseteq I$, we have $M\&N = M + N - I$. Then

$$\begin{array}{lll} & wlp.S.M \ \& \ wp.S.N & \\ = & (wlp.S.M + wp.S.N - I)^+ & \\ = & (wp.S.N - wp.S.(I - M))^+ & \text{Corollary 4.3} \\ = & wp.S.(M + N - I) & \text{Corollary 3.6, and the assumption that } M + N \sqsupseteq I \\ = & wp.S.(M\&N). & \end{array}$$

That proves Eq.(10). For Eq.(11), we calculate that

$$\begin{array}{lll} & wlp.S.(M \ \& \ N) & \\ = & wlp.S.(M + N - I) & \\ = & I - wp.S.(2I - M - N) & \text{Corollary 4.3} \\ = & I - wp.S.(I - M) - wp.S.(I - N) & \text{Corollary 3.6} \\ = & wlp.S.M + wlp.S.N - I. & \text{Corollary 4.3} \end{array}$$

Then we have $wlp.S.(M\&N) = wlp.S.M \ \& \ wlp.S.N$ because $wlp.S.(M\&N) \sqsupseteq \mathbf{0}$. □

It may be surprising at first glance that the operation & is not symmetric in Eq.(10). In fact, we can prove similarly that $wp.S.(M\&N) = wp.S.M \ \& \ wlp.S.N$.

When taking $N = I$ in Eq.(10), we have the following direct but useful corollary:

Corollary 4.6 *For any quantum program S and quantum predicate M,*

$$wp.S.M = wlp.S.M \ \& \ wp.S.I \tag{12}$$

Recall that $wp.S.I$ denotes the condition the program S terminates. So the intuitive meaning of Eq.(12) is that a program is totally correct (represented by *wp*-semantics) if and only if it is partially correct (represented by *wlp*-semantics) *and* it terminates. This captures exactly the intuition of total correctness and partial correctness.

To conclude this section, we present some properties of *wlp*-semantics which are useful in the next section. The proofs are direct so we omit the details here.

Lemma 4.7 *For any quantum program S and quantum predicate $M, N \in \mathcal{PH}$, we have*

1. *$wlp.S.I = I$;*
2. *(monotonicity) if $M \sqsubseteq N$ then $wlp.S.M \sqsubseteq wlp.S.N$;*
3. *if $M + N \sqsubseteq I$ then $wlp.S.(M + N) = wp.S.M + wlp.S.N$;*
4. *if $M \sqsupseteq N$ then $wlp.S.(M - N) = wlp.S.M - wp.S.N$.*

5 Proof rules for quantum loops

Proof rules for programs are important on the way to designing more general refinement techniques for programming. In this section, we derive some proof rules for reasoning about loops in our quantum language fragment. We find that almost all loop rules derived in classical probabilistic programming (see, for example, [14] or [15]) can be extended to quantum case.

In classical deterministic or probabilistic programming languages, an appropriate invariant is the key for reasoning about loops. It is also true in quantum case. So our first theorem is devote to reasoning about quantum loops within partial correctness setting using *wlp*-invariants. Recall that in classical probabilistic programming, if Inv is a *wlp*-invariant of a loop statement $loop \equiv$ "**while** b **do** S" satisfying

$$[b] * Inv \Rrightarrow wlp.S.Inv, \tag{13}$$

then

$$Inv \Rrightarrow wlp.loop.([\bar{b}] * Inv).$$

Here b is a boolean variable with $[b]$ its truth-value function over the state space and $\bar{b}$ its negative. The symbol "$\Rrightarrow$" means "everywhere no more than", which is the probabilistic analogue of the implication relation "$\Rightarrow$" in standard logic; and $*$ is the pointwise multiplication defined between two probabilistic predicates.

Theorem 5.1 *For any quantum predicate $M \in \mathcal{PH}$, if*

$$|1\rangle_q\langle 1|M|1\rangle_q\langle 1| \sqsubseteq |1\rangle_q\langle 1|wlp.S.\widetilde{M_q}|1\rangle_q\langle 1| \tag{14}$$

then

$$\widetilde{M_q} \sqsubseteq wlp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|).$$

*Here and in what follows, by qloop we denote the quantum program "***while** q **do** S*"; and for any quantum predicate M, $\widetilde{M_q}$ represents the abbreviation of $\sum_{i=0}^{1} |i\rangle_q\langle i|M|i\rangle_q\langle i|$.*

Note that by definition, $|i\rangle_q\langle i|$ denotes the projector onto the subspace $\mathcal{H}_i$ of $\mathcal{H}$ where the qubit q is in the state $|i\rangle\langle i|$. So from Theorem 5.1, if the projection of M onto the subspace $\mathcal{H}_1$ is below the projection of $wlp.S.\widetilde{M_q}$ onto $\mathcal{H}_1$, then $\widetilde{M_q}$ is a liberal precondition of $|0\rangle_q\langle 0|M|0\rangle_q\langle 0|$, the projection of M onto the subspace $\mathcal{H}_0$, with respect to *qloop*.

Proof. By definition, we have

$$wlp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|) = \prod_{i=0}^{\infty} M_i,$$

where $M_0 = I$ and for $i \geq 0$,

$$M_{i+1} = |1\rangle_q\langle 1|wlp.S.M_i|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0|.$$

In what follows, we prove by induction that for any $i \geq 0$,

$$\widetilde{M_q} \sqsubseteq M_i. \tag{15}$$

When $i = 0$, Eq.(15) holds trivially. Suppose Eq.(15) holds for $i = k$. Then when $i = k + 1$, we have

$$\begin{aligned}
M_{k+1} &= |1\rangle_q\langle 1|wlp.S.M_k|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0| \\
&\sqsupseteq |1\rangle_q\langle 1|wlp.S.\widetilde{M_q}|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0| \\
&\qquad\qquad \text{induction hypothesis and Lemma 4.7.2} \\
&\sqsupseteq |1\rangle_q\langle 1|M|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0| \qquad \text{Eq.(14)} \\
&= \widetilde{M_q}
\end{aligned}$$

With that we complete the proof of this theorem. □

In the following, we call $\widetilde{M_q}$ a *wlp*-invariant of *qloop* if Eq.(14) holds; similarly, $\widetilde{M_q}$ is said to be a *wp*-invariant of *qloop* if

$$|1\rangle_q\langle 1|M|1\rangle_q\langle 1| \sqsubseteq |1\rangle_q\langle 1|wp.S.\widetilde{M_q}|1\rangle_q\langle 1|. \tag{16}$$

Note that Eq.(13) is equivalent to

$$[b] * Inv \Rrightarrow [b] * wlp.S.Inv.$$

This justifies that Eq.(14) is indeed a quantum generalization of probabilistic *wlp*-invariant.

Lemma 5.2 *For any quantum predicate M,*

1. *the predicate $wlp.qloop.M$ is a wlp-invariant of qloop,*
2. *the predicate $wp.qloop.M$ is a wp-invariant of qloop.*

Proof. We only prove 1. The proof of 2 is similar. Let $M' = wlp.qloop.M$. By definition, we know

$$M' = |1\rangle_q\langle 1|wlp.S.M'|1\rangle_q\langle 1| + |0\rangle_q\langle 0|M|0\rangle_q\langle 0|. \tag{17}$$

It is then direct that

$$|1\rangle_q\langle 1|M'|1\rangle_q\langle 1| = |1\rangle_q\langle 1|wlp.S.M'|1\rangle_q\langle 1| \tag{18}$$

and

$$|0\rangle_q\langle 0|M'|0\rangle_q\langle 0| = |0\rangle_q\langle 0|M|0\rangle_q\langle 0|. \tag{19}$$

Thus we have $M' = \widetilde{M'_q}$, and now Eq.(18) becomes

$$|1\rangle_q\langle 1|M'|1\rangle_q\langle 1| = |1\rangle_q\langle 1|wlp.S.\widetilde{M'_q}|1\rangle_q\langle 1|,$$

which just states that $M' = \widetilde{M'_q}$ is a *wlp*-invariant of *qloop*. □

Using this lemma, we can show that the proof rule presented in Theorem 5.1 is complete for reasoning about the partial correctness of quantum loops in the sense that whenever $N \sqsubseteq wlp.qloop.N'$ holds for quantum predicates N and N', we can prove it using the proof rule in Theorem 5.1 (and the monotonicity of *wlp*).

Theorem 5.3 *(completeness for partial correctness) For any quantum predicates N and N', if $N \sqsubseteq wlp.qloop.N'$ then there exists a quantum predicate M such that $\widetilde{M_q}$ is a wlp-invariant of qloop, and*

1. *$N \sqsubseteq \widetilde{M_q}$,*
2. *$wlp.qloop.|0\rangle_q\langle 0|M|0\rangle_q\langle 0| \sqsubseteq wlp.qloop.N'$.*

Proof. Let $M = wlp.qloop.N'$. By Lemma 5.2.1 we know that $\widetilde{M_q} = M$, and it is a *wlp*-invariant of *qloop*. Then 1 holds automatically. Furthermore, we have $|0\rangle_q\langle 0|M|0\rangle_q\langle 0| = |0\rangle_q\langle 0|N'|0\rangle_q\langle 0|$ by Eq.(19). Thus 2 is satisfied by noting that

$$\begin{aligned} & wlp.qloop.|0\rangle_q\langle 0|N'|0\rangle_q\langle 0| \\ = \;& \nu X \cdot |1\rangle_q\langle 1|wlp.S.X|1\rangle_q\langle 1| + |0\rangle_q\langle 0|N'|0\rangle_q\langle 0| \\ = \;& wlp.qloop.N'. \end{aligned} \tag{20}$$

□

We now turn to reasoning about quantum loops in total correctness setting. To simplify notations, we define

$$T := wp.qloop.I.$$

Intuitively, T denotes the termination condition of *qloop*. For any quantum loop, if a *wp*-invariant implies the termination condition, then its partial correctness is sufficient to guarantee its total correctness, as the following theorem states.

Theorem 5.4 *For any quantum predicate $M \in \mathcal{PH}$, if $\widetilde{M_q}$ is a wp-invariant of qloop and $\widetilde{M_q} \sqsubseteq T$, then*

$$\widetilde{M_q} \sqsubseteq wp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|).$$

Proof. Let

$$M' = \widetilde{M_q} + I - T. \tag{21}$$

Notice that from the definition

$$T = \mu X \cdot |1\rangle_q\langle 1|wp.S.X|1\rangle_q\langle 1| + |0\rangle_q\langle 0|,$$

we have

$$|1\rangle_q\langle 1|T|1\rangle_q\langle 1| = |1\rangle_q\langle 1|wp.S.T|1\rangle_q\langle 1|, \tag{22}$$

$$|0\rangle_q\langle 0|T|0\rangle_q\langle 0| = |0\rangle_q\langle 0|, \tag{23}$$

and then $\widetilde{T_q} = T$, $\widetilde{M'_q} = M'$. Furthermore, we derive $\mathbf{0} \sqsubseteq M' \sqsubseteq I$ by the the assumption that $\widetilde{M_q} \sqsubseteq T$. So M' is also a quantum predicate. We now calculate

$$\begin{array}{lll}
& |1\rangle_q\langle 1|wlp.S.\widetilde{M'_q}|1\rangle_q\langle 1| & \\
= & |1\rangle_q\langle 1|wlp.S.(\widetilde{M_q} + I - T)|1\rangle_q\langle 1| & \\
= & |1\rangle_q\langle 1|(wp.S.\widetilde{M_q} + wlp.S.(I - T))|1\rangle_q\langle 1| & \text{Lemma 4.7.3} \\
= & |1\rangle_q\langle 1|(wp.S.\widetilde{M_q} + wlp.S.I - wp.S.T)|1\rangle_q\langle 1| & \text{Lemma 4.7.4} \\
\sqsupseteq & |1\rangle_q\langle 1|M|1\rangle_q\langle 1| + |1\rangle_q\langle 1| - |1\rangle_q\langle 1|T|1\rangle_q\langle 1| & \text{Lemma 4.7.1 and Eqs.(16), (22)} \\
= & |1\rangle_q\langle 1|M'|1\rangle_q\langle 1|. &
\end{array}$$

It then follows that $\widetilde{M'_q}$ is a *wlp*-invariant of *qloop*. We further calculate

$$\begin{array}{lll}
\widetilde{M_q} & = & \widetilde{M'_q} + T - I \\
& \sqsubseteq & wlp.qloop.(|0\rangle_q\langle 0|M'|0\rangle_q\langle 0|) + T - I \qquad \text{Theorem 5.1} \\
& = & wlp.qloop.(|0\rangle_q\langle 0|M'|0\rangle_q\langle 0|) \;\&\; T \\
& = & wp.qloop.(|0\rangle_q\langle 0|M'|0\rangle_q\langle 0|) \qquad \text{Eq. (12)} \\
& = & wp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|). \qquad \text{Eqs. (21), (23)}
\end{array}$$

That completes our proof. □

Analogue to Theorem 5.3, we can show that the proof rule presented in Theorem 5.4 is also complete for reasoning about the total correctness of quantum loops.

Theorem 5.5 *(completeness for total correctness) For any quantum predicates N and N', if $N \sqsubseteq wp.qloop.N'$ then there exists a quantum predicate M such that $\widetilde{M_q}$ is a wp-invariant of qloop, and*

1. $\widetilde{M}_q \sqsubseteq T$,

2. $N \sqsubseteq \widetilde{M}_q$,

3. $wp.qloop.|0\rangle_q\langle 0|M|0\rangle_q\langle 0| \sqsubseteq wp.qloop.N'$.

Proof. Let $M = wp.qloop.N'$. By Lemma 5.2.2, $\widetilde{M}_q = M$, and it is a wp-invariant of $qloop$. Then we have $\widetilde{M}_q \sqsubseteq T$ by the monotonicity of $wp.qloop$. The rest of the proof is similar to that of Theorem 5.3. □

To demonstrate the power of the proof rules presented so far, let us consider an interesting example. As we know, quantum walk is a natural quantum extension of classical random walk, which in turn has proved to be a fundamental tool in computer science, especially in the designing of algorithms [10]. In this example, we consider a discrete coined quantum walk on an n-cycle with an absorbing boundary at position 1, and prove the property of this kind of quantum walk using our proof rules presented in Theorems 5.1 and 5.4. For more details about quantum walk on a cycle, or more generally, on any graph, we refer to [1].

Example 5.6 *Let H_c be a 2-dimensional 'coin' space with orthonomal basis states $|0\rangle$ and $|1\rangle$, and H_p be the n-dimensional principle space spanned by the position vectors $|i\rangle : i = 0, \ldots, n-1$. Let H_q be the state space of an auxiliary qubit q which indicates whether or not the position of current walk is 1. Then each step of the quantum walk we are concerned with consists of four sub-steps:*

1. *A 'coin-tossing operator' $H = |+\rangle\langle 0| + |-\rangle\langle 1|$ is applied to the coin space, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.*

2. *A shift operator*
$$S = \sum_{i=0}^{n-1} |i \ominus 1\rangle\langle i| \otimes |0\rangle\langle 0| + \sum_{i=0}^{n-1} |i \oplus 1\rangle\langle i| \otimes |1\rangle\langle 1|$$
is performed on the space $H_p \otimes H_c$, which makes the quantum walk one step left or right according to the coin state. Here $\ominus$ and $\oplus$ denote subtraction and addition modulo n, respectively.

3. *A controlling operator*
$$V = I \otimes \sum_{i \neq 1} |i\rangle\langle i| + \sigma_1 \otimes |1\rangle\langle 1|,$$
where $\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$ is one of the pauli matrices, is applied on the space $H_q \otimes H_p$ to transfer the information about whether or not the current walk is in position 1 to the indicating qubit q.

4. *Measure the indicating qubit q to see if the current position of the walk is 1. If the answer is 'yes' then terminate the walk, otherwise the walk continues.*

Formally, we can formulate the walk described above by a quantum loop, denoted in the following by $qwalk$, as
$$\textbf{while } q \textbf{ do } \overline{q} *= U \tag{24}$$
where $U = (V_{qp} \otimes I_c)(I_q \otimes S_{pc})(I_{qp} \otimes H_c)$, and $\overline{q} = q, \overline{q'}$ is a sequence of quantum qubits in the Hilbert space $H_q \otimes H_p \otimes H_c$. We write the subscripts for each operation to indicate which subspace the operation is performed on.

We now show in the following that starting from any state with the auxiliary qubit q being in $|1\rangle\langle 1|$, this loop will terminate, and output a final state where the auxiliary qubit is in $|0\rangle\langle 0|$ and the principle system lies in $|1\rangle\langle 1|$. Using the language of wp-semantics, we need to show
$$|1\rangle_q\langle 1| \otimes I_{pc} \sqsubseteq wp.qwalk.(|01\rangle_{qp}\langle 01| \otimes I_c). \tag{25}$$

To this end, we need to find an appropriate wp-invariant since it is the key to apply the proof rule presented in Theorem 5.4. Let

$$M = |01\rangle_{qp}\langle 01| \otimes I_c + |1\rangle_q\langle 1| \otimes I_{pc}$$

We now check that the predicate $\widetilde{M_q} = M$ is indeed a wp-invariant (also a wlp-invariant because the loop body is merely a unitary transformation) of qwalk. First,

$$\begin{aligned} & (V_{qp}^\dagger \otimes I_c)\widetilde{M_q}(V_{qp} \otimes I_c) \\ = \; & (V_{qp}^\dagger \otimes I_c)\left(|01\rangle_{qp}\langle 01| \otimes I_c + |11\rangle_{qp}\langle 11| \otimes I_c + |1\rangle_q\langle 1| \otimes (I_p - |1\rangle_p\langle 1|) \otimes I_c\right)(V_{qp} \otimes I_c) \\ = \; & |11\rangle_{qp}\langle 11| \otimes I_c + |01\rangle_{qp}\langle 01| \otimes I_c + |1\rangle_q\langle 1| \otimes I_{pc} - |11\rangle_{qp}\langle 11| \otimes I_c \\ = \; & |1\rangle_q\langle 1| \otimes I_{pc} + |01\rangle_{qp}\langle 01| \otimes I_c. \end{aligned}$$

So we have

$$\begin{aligned} & |1\rangle_q\langle 1|wp.(\overline{q} *= U).\widetilde{M_q}|1\rangle_q\langle 1| \\ = \; & |1\rangle_q\langle 1|U^\dagger \widetilde{M_q} U|1\rangle_q\langle 1| \\ = \; & |1\rangle_q\langle 1|(I_{qp} \otimes H_c^\dagger)(I_q \otimes S_{pc}^\dagger)(V_{qp}^\dagger \otimes I_c)\widetilde{M_q}(V_{qp} \otimes I_c)(I_q \otimes S_{pc})(I_{qp} \otimes H_c)|1\rangle_q\langle 1| \\ = \; & |1\rangle_q\langle 1|(I_q \otimes W_{pc}^\dagger)(|1\rangle_q\langle 1| \otimes I_{pc} + |01\rangle_{qp}\langle 01| \otimes I_c)(I_q \otimes W_{pc})|1\rangle_q\langle 1| \\ = \; & |1\rangle_q\langle 1|(|1\rangle_q\langle 1| \otimes I_{pc} + |0\rangle_q\langle 0| \otimes W_{pc}^\dagger(|1\rangle_p\langle 1| \otimes I_c)W_{pc})|1\rangle_q\langle 1| \\ = \; & |1\rangle_q\langle 1| \otimes I_{pc} \\ = \; & |1\rangle_q\langle 1|M|1\rangle_q\langle 1| \end{aligned}$$

where $W_{pc} = S_{pc}(I_p \otimes H_c)$ is a unitary operator on $\mathcal{H}_p \otimes \mathcal{H}_c$.

It was shown in [24] that the quantum loop qwalk is almost terminating in the sense that for any input state, the probability of nontermination after m steps of iteration will tend to 0 when m tends to infinity. That is, it holds that $\forall \rho \in \mathcal{DH} \cdot \mathrm{tr}([\![qwalk]\!]\rho) = \mathrm{tr}\rho$. Then by Theorem 3.5 we have $wp.qwalk.I_{qpc} = I_{qpc}$.

Now applying Theorem 5.4 we have $\widetilde{M_q} \sqsubseteq wp.qwalk.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|)$. Then Eq.(25) holds by noting that $|01\rangle_{qp}\langle 01| \otimes I_c \sqsupseteq \mathbf{0}$ and $|0\rangle_q\langle 0|M|0\rangle_q\langle 0| = |01\rangle_{qp}\langle 01| \otimes I_c$. Notice that from the above argument, we have indeed proved an even stronger result

$$|01\rangle_{qp}\langle 01| \otimes I_c + |1\rangle_q\langle 1| \otimes I_{pc} \sqsubseteq wp.qwalk.(|01\rangle_{qp}\langle 01| \otimes I_c) \tag{26}$$

which states additionally that from the initial state where the auxiliary qubit is in $|0\rangle$ and the principle system is in $|1\rangle$, this loop will also terminate at a state where these two subsystems keep untouched. This coincides with our intuition since in this case, the loop body will not executed and so nothing will be changed.

To conclude this section, we generalize the 0-1 law in classical programming [15] to quantum case.

Lemma 5.7 *For any quantum predicate $M \in \mathcal{PH}$, if $\widetilde{M_q}$ is a wp-invariant of qloop, and there exists $0 < p \leq 1$ such that $p * \widetilde{M_q} \sqsubseteq T$ then $\widetilde{M_q} \sqsubseteq T$. Here we abuse the symbol $*$ as the multiplication between a number and a matrix.*

Proof. Let $M' := p * M$. Then $\widetilde{M'_q} \sqsubseteq T$ and furthermore,

$$\begin{aligned} |1\rangle_q\langle 1|M'|1\rangle_q\langle 1| &= p * |1\rangle_q\langle 1|M|1\rangle_q\langle 1| \\ &\sqsubseteq p * |1\rangle_q\langle 1|wp.S.\widetilde{M_q}|1\rangle_q\langle 1| \\ &= |1\rangle_q\langle 1|wp.S.\widetilde{M'_q}|1\rangle_q\langle 1|. \qquad \text{Corollary 3.6} \end{aligned}$$

So we can derive that

$$\begin{array}{rcll} p * \widetilde{M}_q & = & \widetilde{M}'_q & \\ & \sqsubseteq & wp.qloop.(|0\rangle_q\langle 0|M'|0\rangle_q\langle 0|) & \text{Theorem 5.4} \\ & = & p * wp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|) & \text{Corollary 3.6} \\ & \sqsubseteq & p * wp.qloop.I & \text{monotonicity of } wp.qloop \\ & = & p * T. & \end{array}$$

Dividing both sides by the positive number p, we arrive at the desired result. □

Theorem 5.8 *If T is positive-definite, then for any quantum predicate $M \in \mathcal{PH}$ such that $\widetilde{M}_q$ is a wp-invariant of qloop, we have*

$$\widetilde{M}_q \sqsubseteq wp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|).$$

Proof. From the assumption that T is positive-definite, for any wp-invariant $\widetilde{M}_q$ of *qloop* there exists a sufficiently small but positive p such that $p * \widetilde{M}_q \sqsubseteq T$. So $\widetilde{M}_q \sqsubseteq T$ from Lemma 5.7. Then the result of this theorem holds by applying Theorem 5.4. □

Example 5.9 *Suppose there is only one qubit q involved in qloop. Let $T = \alpha|1\rangle\langle 1| + |0\rangle\langle 0|$. From the fact that T is the least fixed point of the map*

$$X \to |1\rangle\langle 1|wp.S.X|1\rangle\langle 1| + |0\rangle\langle 0|, \tag{27}$$

we have

$$\begin{array}{rcl} \alpha|1\rangle\langle 1| + |0\rangle\langle 0| & = & |1\rangle\langle 1|wp.S.(\alpha|1\rangle\langle 1| + |0\rangle\langle 0|)|1\rangle\langle 1| + |0\rangle\langle 0| \\ & = & |1\rangle\langle 1|(\alpha * wp.S.|1\rangle\langle 1| + wp.S.|0\rangle\langle 0|)|1\rangle\langle 1| + |0\rangle\langle 0| \\ & = & (p\alpha + q)|1\rangle\langle 1| + |0\rangle\langle 0| \end{array}$$

where

$$p = \langle 1|(wp.S.|1\rangle\langle 1|)|1\rangle, \quad q = \langle 1|(wp.S.|0\rangle\langle 0|)|1\rangle,$$

and

$$p + q = \sum_k \langle 1|wp.S.(|k\rangle\langle k|)|1\rangle = \langle 1|wp.S.I|1\rangle \leq \langle 1|I|1\rangle = 1.$$

There are two cases we should consider.

Case 1. $q = 0$. Then we have $\alpha = 0$ because T is the 'least' fixed point of Eq.(27). Thus $T = |0\rangle\langle 0|$. Suppose now $N \sqsubseteq wp.qloop.N'$. By the monotonicity of wp.qloop, we have $wp.qloop.N' \sqsubseteq T = |0\rangle\langle 0|$, and so $\langle 1|wp.qloop.N'|1\rangle = 0$. It follows that

$$wp.qloop.N' \quad = \quad |1\rangle\langle 1|wp.qloop.N'|1\rangle\langle 1| + |0\rangle\langle 0|N'|0\rangle\langle 0| = \langle 0|N'|0\rangle|0\rangle\langle 0|.$$

Then we can derive $N = \lambda_N|0\rangle\langle 0|$ for some $\lambda_N \leq \langle 0|N'|0\rangle$ from the assumption $N \sqsubseteq wp.qloop.N'$.

Conversely, for any $N = \lambda_N|0\rangle\langle 0|$ and N' such that $\lambda_N \leq \langle 0|N'|0\rangle$, we can check easily that $N \sqsubseteq wp.qloop.N'$. So we arrive at the conclusion that in the case of $q = 0$, for any quantum predicates N and N', $N \sqsubseteq wp.qloop.N'$ if and only if $N = \lambda_N|0\rangle\langle 0|$ for some $0 \leq \lambda_N \leq \langle 0|N'|0\rangle \leq 1$.

Case 2. $q > 0$. Then from $p + q \leq 1$ we have $p < 1$. So

$$T = \frac{q}{1-p}|1\rangle\langle 1| + |0\rangle\langle 0|,$$

and T is positive-definite. By a routine calculation, for any $M = \sum_{i,j=0}^{1} m_{ij}|i\rangle\langle j| \in \mathcal{PH}_2$ satisfying $m_{11} \leq m_{11}p + m_{00}q$ we have

$$\begin{aligned} |1\rangle\langle 1|M|1\rangle\langle 1| &= m_{11}|1\rangle\langle 1| \\ &\sqsubseteq (m_{11}p + m_{00}q)|1\rangle\langle 1| \\ &= |1\rangle\langle 1|wp.S.(m_{11}|1\rangle\langle 1| + m_{00}|0\rangle\langle 0|)|1\rangle\langle 1| \\ &= |1\rangle\langle 1|wp.S.\widetilde{M}_q|1\rangle\langle 1| \end{aligned}$$

So M is a wp-invariant of qloop. By Theorem 5.8 we know that $\widetilde{M}_q \sqsubseteq wp.qloop.(|0\rangle_q\langle 0|M|0\rangle_q\langle 0|)$, i.e.

$$m_{00}|0\rangle\langle 0| + m_{11}|1\rangle\langle 1| \sqsubseteq m_{00}wp.qloop.|0\rangle\langle 0|.$$

6 Conclusion and further research

The notion of quantum predicate proposed by D'Hondt and Panangaden makes it possible to reason about quantum programs in a direct way, compared with the previous proposals in the literature where quantum programs are treated as special cases of probabilistic programs. In this paper, this notion is used to analyze a simple language fragment describing the quantum part of a future quantum computer in Knill's architecture. We also extend proof rules to quantum programs with the aim to help reasoning about the partial and the total correctness of quantum programs.

The work presented in this paper is merely a small step, based on D'Hondt and Panangaden, toward a goal-directed programming methodology for quantum computation. There are still many important problems which remain for further research. First, in classical deterministic [5] or probabilistic [8, 9] programming language, nondeterminism is introduced to specify programs' behavior before a real implementation is constructed, with which stepwise development of programs from specifications is possible. In quantum programming language, we believe that nondeterminism will also play an equally important role. A kind of nondeterministic choice has been extended to qGCL by Zuliani [26] to describe and reason about counterfactual computation and mixed-state systems. The quantum programs considered by Zuliani, however, are actually probabilistic programs with some quantum primitives such as initialization, evolution and finalization. As a consequence, the nondeterministic choice is merely presented in the classical way. So a topic for further study is to introduce nondeterminism to quantum programs in the framework of D'Hondt and Panangaden.

Second, recall that deterministic programs enjoy the important property of conjunctivity[5], that is, for any standard predicates p and q,

$$wp.S.(p \wedge q) \Leftrightarrow wp.S.p \wedge wp.S.q;$$

and probabilistic programs satisfy sub-conjunctivity[16, 14]:

$$wp.S.(\alpha \ \& \ \beta) \Leftarrow wp.S.\alpha \ \& \ wp.S.\beta$$

for probabilistic predicates α and β. With these properties, correctness assertions with post-conditions described by the conjunctivity of several predicates can be checked separately for each individual predicate. As pointed out behind Definition 4.4, however, the conjunction between quantum predicates defined in this paper is not monotonic in general, and so similar properties do not hold for quantum programs. As a result, the separating strategy does not apply for reasoning about quantum programs in our setting. Whether or not there exists a notion of conjunction for quantum predicates which have a similarly nice property deserves further research.

Finally, although the proof rule for total correctness presented in Theorem 5.4 has been proved to be complete, it is not an inductive one in the sense that $\widetilde{M}_q \sqsubseteq wp.qloop.I$ occurs in the premise, which is usually very hard to check. This limits the usefulness of this rule in practice. To find an indeed inductive one, just as in classical settings, is a great challenge.

Acknowledgement

We thank the referees for their helpful comments and suggestions, which improved the presentation and the quality of this paper. Especially, one of the referees strengthened Theorem 5.1 in an earlier manuscript, with which a redundant assumption in Theorems 5.4 and 5.8 can be removed. This makes theses proof rules more powerful in practice. The referee also suggested and gave a proof for the completeness theorem for partial correctness presented in Theorem 5.3.

The authors also thank the colleagues in the Quantum Computation and Quantum Information Research Group for useful discussion. This work was partly supported by the Natural Science Foundation of China (Grant Nos. 60503001, 60321002, and 60305005), and by Tsinghua Basic Research Foundation (Grant No. 052220204).

References

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computation*, page 50. ACM Press, New York, 2001.

[2] S. Bettelli, T. Calarco, and L. Serafini. Toward an architecture for quantum programming. *European Physical Journal D*, 25(2):181–200, 2003.

[3] M. Butler and P. Hartel. Reasoning about grover's quantum search algorithm using probabilistic wp. *ACM Transactions on Programming Languages and Systems*, 21(3):417–429, 1999.

[4] E. D'Hondt and P. Panangaden. Quantum weakest preconditions. In P. Selinger, editor, *Proceedings of the 2nd Workshop on Quantum Programming Languages (QPL04)*, Turku Centre for Computer Science, 2004. See also Mathematical Structures in Computer Science, 2006.

[5] E. W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976.

[6] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. ACM STOC*, pages 212–219, 1996.

[7] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78(2):325, 1997.

[8] C. Jones. *Probabilistic nondeterminism*. PhD thesis, Edinburgh University, NK, 1990. Monograph ECS-LFCS-90-105.

[9] C. Jones and G. Plotkin. A probabilistic powerdomain of evalutions. In *Proceeding of the 4th IEEE Annual Symposium on Logic in Computer Science*, pages 186–195, Los Alamitos, California, 1989.

[10] J. Kemeny and J. Snell. *Finite Markov Chains*. Springer-Verlag, 1983.

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

[12] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer, Berlin, 1983.

[13] A. McIver and C. Morgan. Partial correctness for probabilistic demonic programs. *Theoretical Computer Science*, 266:513–541, 2001.

[14] A. McIver and C. Morgan. *Abstraction, refinement and proof for probabilistic systems*. Springer-Verlag, 2005.

[15] C. Morgan. Proof rules for probabilistic loops. Technical Report PRG-TR-25-95, 1995. Programming Research Group, Oxford University.

[16] C. Morgan, A. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, 1996.

[17] B. Ömer. *A procedural formalism for quantum computing.* Master thesis, Department of Theoretical Physics, Technical University of Vienna, 1998. http://tph.tuwien.ac.at/oemer/qcl.html.

[18] B. Ömer. *Structured Quantum Programming.* PhD thesis, Department of Theoretical Physics, Technical University of Vienna, 2003.

[19] J. W. Sanders and P. Zuliani. Quantum programming. *Mathematics of Program Construction*, 1837:80–99, 2000.

[20] P. Selinger. A brief survey of quantum programming languages. *Functional and Logic Programming*, 2998:1–6, 2004.

[21] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[22] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of the 35th IEEE FOCS*, pages 124–134, 1994.

[23] A. van Tonder. Quantum computation, categorical semantics and linear logic, 2003. arXiv:quant-ph/0312174.

[24] M. Ying and Y. Feng. Quantum loop programs. 2006. In preparation. See also http://arxiv.org/abs/quant-ph/0605218.

[25] P. Zuliani. *Quantum Programming.* PhD thesis, Oxford University, 2001.

[26] P. Zuliani. Non-deterministic quantum programming. In *Proc. QPL 2004*, pages 179–195, 2004.