Floyd-Hoare Logic for Quantum Programs

Mingsheng Ying

University of Technology, Sydney
and
Tsinghua University

Nagoya Winter Workshop, February 14-18, 2011
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Quantum Programming

Even though quantum hardware is still in its infancy, people widely believe that building a large-scale and functional quantum computer is merely a matter of time and concentrated effort.

The history of classical computing arouses that once quantum computers come into being, quantum programming languages and quantum software development techniques will play a key role in exploiting the power of quantum computers.
Formal Semantics for Quantum Programming Languages

The fact that human intuition is much better adapted to the classical world than the quantum world is one of the major reasons it is difficult to find efficient quantum algorithms. It also implies that programmers will commit many more faults in designing programs for quantum computers than programming classical computers.

It is even more critical than in classical computing to give clear and formal semantics to quantum programming languages and to provide formal methods for reasoning about quantum programs.
Floyd-Hoare Logic


S. A. Cook, Soundness and completeness of an axiom system for program verification, *SIAM Journal on Computing*, 7(1978)70-90

Floyd-Hoare Logic for Quantum Programs


Floyd-Hoare Logic for Quantum Programs, Continued

Y. Kakutani, A logic for formal verification of quantum programs, *LNCS Proceedings of ASIAN 2009*


Full-fledged Floyd-Hoare logic for quantum programs?
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Syntax

A countably infinite set $\text{Var}$ of quantum variables.

A type $t$ is a name of a Hilbert space $\mathcal{H}_t$.

Two basic types: Boolean, integer.
Syntax, Continued

The Hilbert spaces denoted by **Boolean** and **integer** are:

\[ H_{\text{Boolean}} = H_2, \]

\[ H_{\text{integer}} = H_\infty. \]

The space \( l_2 \) of square summable sequences is

\[ H_\infty = \{ \sum_{n=-\infty}^{\infty} \alpha_n |n\rangle : \alpha_n \in \mathbb{C} \text{ for all } n \in \mathbb{Z} \text{ and } \sum_{n=-\infty}^{\infty} |\alpha_n|^2 < \infty \}, \]

where \( \mathbb{Z} \) is the set of integers.
Syntax, Continued

The state space $\mathcal{H}_q$ of a quantum variable $q$ is the Hilbert space denoted by its type:

$$\mathcal{H}_q = \mathcal{H}_{\text{type}(q)}.$$

A quantum register is a finite sequence of distinct quantum variables.

The state space of a quantum register $\bar{q} = q_1, ..., q_n$ is the tensor product of the state spaces of the quantum variables occurring in $\bar{q}$:

$$\mathcal{H}_{\bar{q}} = \bigotimes_{i=1}^{n} \mathcal{H}_{q_i}.$$
Syntax, Continued

The quantum extension of classical while-programs.

\[ S ::= \text{skip} \mid q := 0 \mid \bar{q} := U\bar{q} \mid S_1; S_2 \mid \text{measure } M[\bar{q}] : \bar{S} \]
\[ \mid \text{while } M[\bar{q}] = 1 \text{ do } S \]

- \( q \) is a quantum variable and \( \bar{q} \) a quantum register;
Syntax, Continued

The quantum extension of classical while-programs.

\[ S ::= \text{skip} \mid q := 0 \mid \bar{q} := U\bar{q} \mid S_1; S_2 \mid \text{measure } M[\bar{q}] : \bar{S} \]
\[ \mid \text{while } M[\bar{q}] = 1 \text{ do } S \]

- \( q \) is a quantum variable and \( \bar{q} \) a quantum register;
- \( U \) in the statement \( \bar{q} := U\bar{q} \) is a unitary operator on \( \mathcal{H}_{\bar{q}} \).
Syntax, Continued

The quantum extension of classical \textbf{while}-programs.

\[
S ::= \text{skip} \mid q := 0 \mid \bar{q} := U\bar{q} \mid S_1; S_2 \mid \text{measure } M[\bar{q}] : \bar{S} \\
\mid \text{while } M[\bar{q}] = 1 \text{ do } S
\]

- $q$ is a quantum variable and $\bar{q}$ a quantum register;
- $U$ in the statement "$\bar{q} := U\bar{q}$" is a unitary operator on $\mathcal{H}_q$.
- in the statement "\textbf{measure } $M[\bar{q}] : \bar{S}$", $M = \{M_m\}$ is a measurement on the state space $\mathcal{H}_{\bar{q}}$ of $\bar{q}$, and $S = \{S_m\}$ is a set of quantum programs such that each outcome $m$ of measurement $M$ corresponds to $S_m$;
The quantum extension of classical **while**-programs.

\[
S ::= \text{skip} \mid q := 0 \mid \bar{q} := U\bar{q} \mid S_1; S_2 \mid \text{measure } M[\bar{q}] : \bar{S} \\
\mid \text{while } M[\bar{q}] = 1 \text{ do } S
\]

- $q$ is a quantum variable and $\bar{q}$ a quantum register;
- $U$ in the statement "$\bar{q} := U\bar{q}$" is a unitary operator on $\mathcal{H}_{\bar{q}}$.
- in the statement "**measure** $M[\bar{q}] : \bar{S}$", $M = \{M_m\}$ is a measurement on the state space $\mathcal{H}_{\bar{q}}$ of $\bar{q}$, and $S = \{S_m\}$ is a set of quantum programs such that each outcome $m$ of measurement $M$ corresponds to $S_m$;
- $M = \{M_0, M_1\}$ in the statement "**while** $M[\bar{q}] = 1$ do $S$" is a yes-no measurement on $\mathcal{H}_{\bar{q}}$. 
Outline

Introduction

Syntax of Quantum Programs

**Operational Semantics of Quantum Programs**

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
**Notation**

\( \mathcal{H}_{\text{all}} \) for the tensor product of the state spaces of all quantum variables:

\[
\mathcal{H}_{\text{all}} = \bigotimes_{\text{all } q} \mathcal{H}_q.
\]

\( E \) denotes the empty program.

A quantum configuration is a pair \( \langle S, \rho \rangle \), where \( S \) is a quantum program or \( E \), \( \rho \in \mathcal{D}^- (\mathcal{H}_{\text{all}}) \) is a partial density operator on \( \mathcal{H}_{\text{all}} \), and it is used to indicate the (global) state of quantum variables.
Notation

Let $\bar{q} = q_1, ..., q_n$ be a quantum register. A linear operator $A$ on $\mathcal{H}_{\bar{q}}$ has a cylinder extension

$$A \otimes I_{\text{Var} - \{\bar{q}\}}$$

on $\mathcal{H}_{\text{all}}$, where $I_{\text{Var} - \{\bar{q}\}}$ is the identity operator on the Hilbert space

$$\otimes_{q \in \text{Var} - \{\bar{q}\}} \mathcal{H}_q.$$
Operational Semantics

\((\text{Skip})\)
\[
\langle \text{skip}, \rho \rangle \rightarrow \langle E, \rho \rangle
\]

\((\text{Initialization})\)
\[
\langle q := 0, \rho \rangle \rightarrow \langle E, \rho_0^q \rangle
\]

where
\[
\rho_0^q = |0\rangle_q \langle 0| \rho |0\rangle_q \langle 0| + |0\rangle_q \langle 1| \rho |1\rangle_q \langle 0|
\]

if \(\text{type}(q) = \text{Boolean}\), and
\[
\rho_0^q = \sum_{n = -\infty}^{\infty} |0\rangle_q \langle n| \rho |n\rangle_q \langle 0|
\]

if \(\text{type}(q) = \text{integer}\).
Operational Semantics, Continued

(\textit{Unitary Transformation}) \quad \langle \bar{q} := U\bar{q}, \rho \rangle \rightarrow \langle E, U\rho U^\dagger \rangle

(\textit{Sequential Composition}) \quad \frac{\langle S_1, \rho \rangle \rightarrow \langle S'_1, \rho' \rangle}{\langle S_1; S_2, \rho \rangle \rightarrow \langle S'_1; S_2, \rho' \rangle}

where we make the convention that $E; S_2 = S_2$.

(\textit{Measurement}) \quad \frac{\langle \text{measure } M[\bar{q}] : \bar{S}, \rho \rangle \rightarrow \langle S_m, M_m\rho M_m^\dagger \rangle}{\langle S_1; S_2, \rho \rangle \rightarrow \langle S'_1; S_2, \rho' \rangle}

for each outcome $m$ of measurement $M = \{M_m\}$
Operational Semantics, Continued

(Loop 0)
\[
\langle \text{while } M[\overline{q}] = 1 \text{ do } S, \rho \rangle \rightarrow \langle E, M_0 \rho M_0^\dagger \rangle
\]

(Loop 1)
\[
\langle \text{while } M[\overline{q}] = 1 \text{ do } S, \rho \rangle \rightarrow \langle S; \text{while } M[\overline{q}] = 1 \text{ do } S, M_1 \rho M_1^\dagger \rangle
\]
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Definition

Let $S$ be a quantum program. Then its semantic function

$$[|S|] : \mathcal{D}^{-} (\mathcal{H}_{\text{all}}) \rightarrow \mathcal{D}^{-} (\mathcal{H}_{\text{all}})$$

is defined by

$$[|S|](\rho) = \sum \{|\rho' : \langle S, \rho \rangle \rightarrow^* \langle E, \rho' \rangle|\}$$

for all $\rho \in \mathcal{D}^{-} (\mathcal{H}_{\text{all}})$. 
Notation

Let $\Omega$ be a quantum program such that $[\vert \Omega \vert] = 0_{\mathcal{H}_{\text{all}}}$ for all $\rho \in \mathcal{D}(\mathcal{H})$; for example,

$$\Omega = \text{while } M_{\text{trivial}}[q] = 1 \text{ do skip},$$

where $q$ is a quantum variable, and

$$M_{\text{trivial}} = \{M_0 = 0_{\mathcal{H}_q}, M_1 = I_{\mathcal{H}_q}\}$$

is a trivial measurement on $\mathcal{H}_q$. 
Notation

We set:

\[
(\text{while } M[\bar{q}] = 1 \text{ do } S)^0 = \Omega, \\
(\text{while } M[\bar{q}] = 1 \text{ do } S)^{n+1} = \text{measure } M[\bar{q}] : \bar{S},
\]

where \(\bar{S} = S_0, S_1\), and

\[
S_0 = \text{skip}, \\
S_1 = S; (\text{while } M[\bar{q}] = 1 \text{ do } S)^n
\]

for all \(n \geq 0\).
Proposition: Representation of Semantic Function

1. $[[\text{skip}]](\rho) = \rho$. 

2. If $\text{type}(q) = \text{Boolean}$, then $[|q:] = 0 \langle 0 | \rho | 0 \rangle \langle 0 | \rho | 0 \rangle$.

3. If $\text{type}(q) = \text{integer}$, then $|q:] = \sum_{n=-\infty}^{\infty} |0 \rangle q \langle n | \rho | n \rangle q \langle 0 |$.

4. $|S_1; S_2| (\rho) = |S_2| (|S_1| (\rho))$.

5. $|\text{measure} M[q]| S| (\rho) = \sum_m |S_m| (M_m \rho M_m^\dagger)$.

6. $|\text{while} M[q] = 1 \text{do} S| (\rho) = \bigvee_{n=0}^{\infty} |(\text{while} M[q] = 1 \text{do} S)|_n (\rho)$. 

Proposition: Representation of Semantic Function

1. $\text{[\text{skip}]}(\rho) = \rho$.

2. If $\text{type}(q) = \text{Boolean}$, then

$$\text{[\text{q} := 0]}(\rho) = |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0|,$$

and if $\text{type}(q) = \text{integer}$, then

$$\text{[\text{q} := 0]}(\rho) \sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|.$$
Proposition: Representation of Semantic Function

1. \([[\text{skip}]\](\rho) = \rho\).

2. If \(\text{type}(q) = \text{Boolean}\), then

\[
\[|q := 0\](\rho) = |0\rangle_q |0\rangle_q |\rho\rangle_q |0\rangle_q + |0\rangle_q |1\rangle_q |1\rangle_q |0\rangle_q,
\]

and if \(\text{type}(q) = \text{integer}\), then

\[
\[|q := 0\](\rho) = \sum_{n=-\infty}^{\infty} |0\rangle_q |n\rangle_q |\rho\rangle_q |n\rangle_q |0\rangle_q.
\]

3. \([[\overline{q} := U\overline{q}]\](\rho) = U\rho U^\dagger.\)
Proposition: Representation of Semantic Function

1. $[\text{skip}](\rho) = \rho$.
2. If $\text{type}(q) = \text{Boolean}$, then

   $$[|q := 0\rangle](\rho) = |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0|,$$

   and if $\text{type}(q) = \text{integer}$, then

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

3. $[\overline{q} := U\overline{q}](\rho) = U\rho U^\dagger$.
4. $[|S_1;S_2\rangle](\rho) = [|S_2\rangle]|(|S_1\rangle)(\rho))$. 
Proposition: Representation of Semantic Function

1. \(|\text{skip}\rangle\langle\cdot|\)(\(\rho\)) = \(\rho\).

2. If \(\text{type}(q) = \text{Boolean}\), then

\[
|q := 0\rangle\langle\cdot|\)(\(\rho\)) = |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0|,
\]

and if \(\text{type}(q) = \text{integer}\), then

\[
|q := 0\rangle\langle\cdot|\)(\(\rho\)) = \sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|.
\]

3. \(|\bar{q} := U\bar{q}\rangle\langle\cdot|\)(\(\rho\)) = U\rho U^\dagger.

4. \(|S_1;S_2\rangle\langle\cdot|\)(\(\rho\)) = |S_2\rangle\langle\cdot|\)(|S_1\rangle\langle\cdot|\)(\(\rho\))).

5. \(|\text{measure } M[\bar{q} : \bar{S}]\rangle\langle\cdot|\)(\(\rho\)) = \sum_m [|S_m\rangle\langle\cdot|\)(M_m\rho M_m^\dagger).
Proposition: Representation of Semantic Function

1. $[[\text{skip}]](\rho) = \rho$.

2. If $\text{type}(q) = \text{Boolean}$, then

$$[[q := 0]](\rho) = |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0|,$$

and if $\text{type}(q) = \text{integer}$, then

$$[[q := 0]](\rho) \sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|.$$

3. $[[\bar{q} := U\bar{q}]](\rho) = U\rho U^\dagger$.

4. $[[S_1; S_2]](\rho) = [[S_2]]([[S_1]](\rho))$.

5. $[[\text{measure } M[\bar{q}] : \bar{S}]](\rho) = \sum_m [[S_m]](M_m\rho M_m^\dagger)$.

6. $[[\text{while } M[\bar{q}] = 1 \text{ do } S]](\rho) = \bigvee_{n=0}^{\infty} [[(\text{while } M[\bar{q}] = 1 \text{ do } S)^n]](\rho)$. 

Proposition: Recursion

If we write `while` for quantum loop “`while M[\bar{q}] = 1 do S`”, then for any $\rho \in D^- (\mathcal{H}_{all})$, it holds that

$$\left[|\textbf{while}|\right](\rho) = M_0\rho M_0^\dagger + \left[|\textbf{while}|\right](\left[|S|\right](M_1\rho M_1^\dagger)).$$
Proposition

For any quantum program $S$, it holds that

$$\text{tr}(\lvert S \rvert (\rho)) \leq \text{tr}(\rho)$$

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

$\text{tr}(\rho) - \text{tr}(\lvert S \rvert (\rho))$ is the probability that program $S$ diverges from input state $\rho$. 
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Definition

For any $X \subseteq \text{Var}$, a quantum predicate on $\mathcal{H}_X$ is a Hermitian operator $P$ on $\mathcal{H}_X$ such that

$$0_{\mathcal{H}_X} \subseteq P \subseteq I_{\mathcal{H}_X}.$$ 

$\mathcal{P}(\mathcal{H}_X)$ denotes the set of quantum predicates on $\mathcal{H}_X$.

For any $\rho \in \mathcal{D}^{-}(\mathcal{H}_X)$, $\text{tr}(P\rho)$ stands for the probability that predicate $P$ is satisfied in state $\rho$. 
Definition

A correctness formula is a statement of the form:

\[ \{ P \} S \{ Q \} \]

where \( S \) is a quantum program, and both \( P \) and \( Q \) are quantum predicates on \( \mathcal{H}_{all} \).

The operator \( P \) is called the precondition of the correctness formula and \( Q \) the postcondition.
Definition

1. The correctness formula $\{P\}S\{Q\}$ is true in the sense of total correctness, written
   \[ \models_{\text{tot}} \{P\}S\{Q\}, \]
   if we have:
   \[ tr(P\rho) \leq tr(Q[S](\rho)) \]
   for all $\rho \in D^-(\mathcal{H})$. 

Definition

1. The correctness formula $\{P\}S\{Q\}$ is true in the sense of total correctness, written

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

if we have:

$$tr(P\rho) \leq tr(Q[S](\rho))$$

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

2. The correctness formula $\{P\}S\{Q\}$ is true in the sense of partial correctness, written

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

if we have:

$$tr(P\rho) \leq tr(Q[S](\rho)) + [tr(\rho) - tr([S](\rho))]$$

for all $\rho \in D^-(\mathcal{H})$. 
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Definition

Let $S$ be a quantum program and $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate on $\mathcal{H}_{all}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying the following conditions:

   1.1 $| = \text{tot} \{ wp.S.P \}$ $S \{ P \};$
   1.2 if $| = \text{par} \{ Q \}$ $S \{ P \}$ then $Q \sqsubseteq wp.S.P$.
Definition

Let $S$ be a quantum program and $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ be a quantum predicate on $\mathcal{H}_{\text{all}}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $\text{wp}.S.P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   1.1 $\models_{\text{tot}} \{\text{wp}.S.P\}S\{P\}$;
Definition

Let $S$ be a quantum program and $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ be a quantum predicate on $\mathcal{H}_{\text{all}}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   1.1 $\models_{\text{tot}} \{wp.S.P\}S\{P\}$;
   1.2 if $\models_{\text{tot}} \{Q\}S\{P\}$ then $Q \subseteq wp.S.P$.

2. The weakest liberal precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   2.1 $\models_{\text{par}} \{wlp.S.P\}S\{P\}$;
   2.2 if $\models_{\text{par}} \{Q\}S\{P\}$ then $Q \subseteq wlp.S.P$. 
Definition

Let $S$ be a quantum program and $P \in \mathcal{P} (\mathcal{H}_{\text{all}})$ be a quantum predicate on $\mathcal{H}_{\text{all}}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wp.S.P \in \mathcal{P} (\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   
   1.1 $\models_{\text{tot}} \{ \text{wp}.S.P \} S \{ P \}$;
   
   1.2 if $\models_{\text{tot}} \{ Q \} S \{ P \}$ then $Q \subseteq wp.S.P$.

2. The weakest liberal precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wlp.S.P \in \mathcal{P} (\mathcal{H}_{\text{all}})$ satisfying the following conditions:
Definition

Let $S$ be a quantum program and $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ be a quantum predicate on $\mathcal{H}_{\text{all}}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   
   1.1 $\models_{\text{tot}} \{wp.S.P\}S\{P\}$;
   1.2 if $\models_{\text{tot}} \{Q\}S\{P\}$ then $Q \subseteq wp.S.P$.

2. The weakest liberal precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ satisfying the following conditions:
   
   2.1 $\models_{\text{par}} \{wlp.S.P\}S\{P\}$;
Definition

Let $S$ be a quantum program and $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate on $\mathcal{H}_{all}$.

1. The weakest precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying the following conditions:
   
   1.1 \( \models_{\text{tot}} \{ wp.S.P \} S\{ P \} \);
   
   1.2 if \( \models_{\text{tot}} \{ Q \} S\{ P \} \) then \( Q \subseteq wp.S.P \).

2. The weakest liberal precondition of $S$ with respect to $P$ is defined to be the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying the following conditions:

   2.1 \( \models_{\text{par}} \{ wlp.S.P \} S\{ P \} \);
   
   2.2 if \( \models_{\text{par}} \{ Q \} S\{ P \} \) then \( Q \subseteq wlp.S.P \).
Proposition: Representation of Weakest Precondition

1. \( wp.\text{skip}.P = P \).
Proposition: Representation of Weakest Precondition

1. \(\text{wp.skip}.P = P\).
2. If \(\text{type}(q) = \text{Boolean}\), then
   \[
   wp.q := 0.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|,
   \]
   and if \(\text{type}(q) = \text{integer}\), then
   \[
   wp.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
   \]
Proposition: Representation of Weakest Precondition

1. \( wp.\text{skip}.P = P \).
2. If \( \text{type}(q) = \text{Boolean} \), then
   \[
   wp.q := 0.P = |0\rangle_q |0\rangle_q |P\rangle_q |0\rangle_q + |1\rangle_q |0\rangle_q |P\rangle_q |1\rangle_q,
   \]
   and if \( \text{type}(q) = \text{integer} \), then
   \[
   wp.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q |0\rangle_q |P\rangle_q |n\rangle_q.
   \]
3. \( wp.\overline{q} := U\overline{q}.P = U^\dagger PU \).
Proposition: Representation of Weakest Precondition

1. \( \text{wp.skip}.P = P \).

2. If \( \text{type}(q) = \text{Boolean} \), then

   \[
   \text{wp}.q := 0.P = |0\rangle_q \langle 0|P|0\rangle_q \langle 0| + |1\rangle_q \langle 0|P|0\rangle_q \langle 1|,
   \]

   and if \( \text{type}(q) = \text{integer} \), then

   \[
   \text{wp}.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q \langle 0|P|0\rangle_q \langle n|.
   \]

3. \( \text{wp.\bar{q}} := \text{U}\bar{q}.P = \text{U}^{\dagger}P\text{U} \).

4. \( \text{wp}.S_1;S_2.P = \text{wp}.S_1.\left(\text{wp}.S_2.P\right) \).
Proposition: Representation of Weakest Precondition

1. \( \text{wp.skip}.P = P \).

2. If \( \text{type}(q) = \text{Boolean} \), then

\[
\text{wp.q} := 0.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|,
\]

and if \( \text{type}(q) = \text{integer} \), then

\[
\text{wp.q} := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
\]

3. \( \text{wp.\bar{q}} := U\bar{q}.P = U^\dagger PU \).

4. \( \text{wp.S}_1;S_2.P = \text{wp.S}_1.(\text{wp.S}_2.P) \).

5. \( \text{wp.measure} M[\bar{q}] : \bar{S}.P = \sum_m M^\dagger_m (\text{wp.S}_m.P)M_m \).
Proposition: Representation of Weakest Precondition

1. \( \text{wp.skip}.P = P \).

2. If \( \text{type}(q) = \text{Boolean} \), then

\[
\text{wp}.q := 0.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|,
\]

and if \( \text{type}(q) = \text{integer} \), then

\[
\text{wp}.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
\]

3. \( \text{wp}.\bar{q} := U\bar{q}.P = U^\dagger PU \).

4. \( \text{wp}.S_1;S_2.P = \text{wp}.S_1.(\text{wp}.S_2.P) \).

5. \( \text{wp.measure} \ M[\bar{q}] : \bar{S}.P = \sum_m M_m^\dagger (\text{wp}.S_m.P)M_m \).

6. \( \text{wp.while} \ M[\bar{q}] = 1 \text{ do } S.P = \bigvee_{n=0}^{\infty} P_n \), where

\[
\begin{cases}
    P_0 = 0_{\mathcal{H}_{\text{all}}}, \\
    P_{n+1} = M_0^\dagger PM_0 + M_1^\dagger (\text{wp}.S.P_n)M_1 \text{ for all } n \geq 0.
\end{cases}
\]
Proposition

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

$$\text{tr}(\wp(S).P) = tr(P[|S|](\rho)).$$
Proposition: Representation of Weakest Liberal Precondition

1. \( wlp.\text{skip}.P = P \).
Proposition: Representation of Weakest Liberal Precondition

1. \texttt{wlp.skip}.P = P.

2. If \texttt{type}(q) = \texttt{Boolean}, then

\[
\text{wlp}.q := 0.P = |0_q\langle 0|P|0_q\langle 0| + |1_q\langle 0|P|0_q\langle 1|
\]

and if \texttt{type}(q) = \texttt{integer}, then

\[
\text{wlp}.q := 0.P = \sum_{n=-\infty}^{\infty} |n_q\langle 0|P|0_q\langle n|
\]
Proposition: Representation of Weakest Liberal Precondition

1. $\text{wlp.skip}.P = P$.

2. If $\text{type}(q) = \text{Boolean}$, then

   $$\text{wlp}.q := 0.P = |0\rangle_q\langle0|P|0\rangle_q\langle0| + |1\rangle_q\langle0|P|0\rangle_q\langle1|,$$

   and if $\text{type}(q) = \text{integer}$, then

   $$\text{wlp}.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle0|P|0\rangle_q\langle n|.$$

3. $\text{wlp.}\bar{q} := \mathcal{U}\bar{q}.P = \mathcal{U}^\dagger P\mathcal{U}$. 
Proposition: Representation of Weakest Liberal Precondition

1. \( wlp.\texttt{skip}.P = P \).

2. If \( \text{type}(q) = \texttt{Boolean} \), then
   \[
   wlp.q := 0.P = |0\rangle_q \langle 0| P |0\rangle_q \langle 0| + |1\rangle_q \langle 0| P |0\rangle_q \langle 1|,
   \]
   and if \( \text{type}(q) = \texttt{integer} \), then
   \[
   wlp.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q \langle 0| P |0\rangle_q \langle n|.
   \]

3. \( wlp.\overline{q} := U\overline{q}.P = U^\dagger P U \).

4. \( wlp.S_1;S_2.P = wlp.S_1.(wlp.S_2.P) \).
Proposition: Representation of Weakest Liberal

1. \texttt{wlp.skip}.P = P.
2. If \texttt{type}(q) = \texttt{Boolean}, then

   \[ \texttt{wlp}.q := 0.P = |0\rangle_q \langle 0|P|0\rangle_q \langle 0| + |1\rangle_q \langle 0|P|0\rangle_q \langle 1|, \]

   and if \texttt{type}(q) = \texttt{integer}, then

   \[ \texttt{wlp}.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q \langle 0|P|0\rangle_q \langle n|. \]

3. \texttt{wlp.\overline{q}} := U\overline{q}.P = U^\dagger PU.
4. \texttt{wlp}.S_1; S_2.P = \texttt{wlp}.S_1.(\texttt{wlp}.S_2.P).
5. \texttt{wlp.measure} \texttt{M}[\overline{q}] : \overline{S}.P = \sum_m M_m^\dagger (\texttt{wlp}.S_m.P)M_m.
Proposition: Representation of Weakest Liberal Precondition

1. \(wlp.\text{skip}.P = P\).
2. If \(\text{type}(q) = \text{Boolean}\), then
   
   \[
   wlp.q := 0.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|,
   \]
   and if \(\text{type}(q) = \text{integer}\), then
   
   \[
   wlp.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
   \]
3. \(wlp.\bar{q} := U\bar{q}.P = U^\dagger PU\).
4. \(wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P)\).
5. \(wlp.\text{measure} \ M[\bar{q}] : \bar{S}.P = \sum_m M_m^\dagger (wlp.S_m.P)M_m\).
6. \(wlp.\text{while} \ M[\bar{q}] = 1 \ \text{do} \ S.P = \bigwedge_{n=0}^{\infty} P_n\), where

   \[
   \begin{cases}
   P_0 = I_{\mathcal{H}_{\text{all}}}, \\
   P_{n+1} = M_0^\dagger PM_0 + M_1^\dagger (wlp.S.P_n)M_1 \quad \text{for all } n \geq 0.
   \end{cases}
   \]
Proposition

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

$$tr((wlp.S.P)\rho) = tr(P[|S|](\rho)) + [tr(\rho) - tr([|S|](\rho))].$$
Proposition: Recursion

We write `while` for quantum loop “`while M[\bar{q}] = 1 do S`”. Then for any $P \in \mathcal{P}(\mathcal{H}_{all})$, we have:

1. $wp.\text{while}.P = M_0^\dagger PM_0 + M_1^\dagger (wp.S.(wp.\text{while}.P))M_1$. 
Proposition: Recursion

We write `while` for quantum loop “`while M[q] = 1 do S`”. Then for any \( P \in \mathcal{P}(\mathcal{H}_{all}) \), we have:

1. \( wp.while.P = M_0^\dagger P M_0 + M_1^\dagger (wp.S.(wp.while.P)) M_1 \).
2. \( wlp.while.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.while.P)) M_1 \).
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
The Proof System $PD$ for Partial Correctness

(Axiom Skip) \[ \{ P \} \text{Skip}\{ P \} \]

(Axiom Initialization) If $type(q) = \text{Boolean}$, then

\[ \{ |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1| \} q := 0\{ P \} \]

and if $type(q) = \text{integer}$, then

\[ \{ \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n| \} q := 0\{ P \} \]

(Axiom Unitary Transformation) \[ \{ U^\dagger PU \} q := U\bar{q}\{ P \} \]
The Proof System $PD$ for Partial Correctness, Continued

(Rule Sequential Composition)

$$
\begin{align*}
\{P\} S_1 \{Q\} & \quad \{Q\} S_2 \{R\} \\
\{P\} S_1; S_2 \{R\}
\end{align*}
$$

(Rule Measurement)

$$
\begin{align*}
\{P_m\} S_m \{Q\} \text{ for all } m \\
\{ \sum_m M_m^+ P_m M_m \} \text{ measure } M[\bar{q}] : S\{Q\}
\end{align*}
$$

(Rule Loop Partial)

$$
\begin{align*}
\{Q\} S\{M_0^+ PM_0 + M_1^+ QM_1\} \\
\{M_0^+ PM_0 + M_1^+ QM_1\} \text{ while } M[\bar{q}] = 1 \text{ do } S\{P\}
\end{align*}
$$

(Rule Order)

$$
\begin{align*}
P \sqsubseteq P' \\
P' \{P'\} S\{Q'\} \\
Q' \sqsubseteq Q \\
P \{P\} S\{Q\}
\end{align*}
$$
Soundness Theorem for PD

The proof system PD is sound for partial correctness of quantum programs.

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

$$\vdash_{PD} \{P\}S\{Q\} \text{ implies } \models_{\text{par}} \{P\}S\{Q\}. $$
Completeness Theorem for PD

The proof system PD is complete for partial correctness of quantum programs.

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

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

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Definition

Let $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ and $\epsilon > 0$. A function

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

is called a $(P, \epsilon)$–bound function of quantum loop “while $M[\bar{q}] = 1$ do $S$” if it satisfies the following conditions:

1. $t(\|S\|(M_1 \rho M_1^\dagger)) \leq t(\rho)$; and

for all $\rho \in \mathcal{D}^-(\mathcal{H}_{\text{all}})$. 
Definition

Let $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ and $\epsilon > 0$. A function

$$t : \mathcal{D}^{-}(\mathcal{H}_{\text{all}}) \rightarrow \mathbb{N}$$

is called a $(P, \epsilon)$–bound function of quantum loop "while $M[\bar{q}] = 1$ do $S$" if it satisfies the following conditions:

1. $t([|S|](M_1\rho M_1^\dagger)) \leq t(\rho)$; and

2. $tr(P\rho) \geq \epsilon$ implies $t([|S|](M_1\rho M_1^\dagger)) < t(\rho)$

for all $\rho \in \mathcal{D}^{-}(\mathcal{H}_{\text{all}})$. 
Lemma

Let $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$. Then the following two statements are equivalent:

1. for any $\epsilon > 0$, there exists a $(P, \epsilon)$–bound function $t_\epsilon$ of quantum loop "\textbf{while } M[\bar{q}] = 1 \textbf{ do } S";
Lemma

Let $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$. Then the following two statements are equivalent:

1. for any $\epsilon > 0$, there exists a $(P, \epsilon)$–bound function $t_\epsilon$ of quantum loop “while $M[\bar{q}] = 1$ do $S$”;

2. $\lim_{n \to \infty} tr(P([|S|] \circ \mathcal{E}_1)^n(\rho)) = 0$ for all $\rho \in \mathcal{D}^- (\mathcal{H}_{\text{all}})$. 
The Proof System $TD$ for Total Correctness

(Axiom Skip), (Axiom Initialization), (Axiom Unitary Transformation)

(Rule Sequential Composition), (Rule Measurement), (Rule Order)

\[
\{Q\} S \{M_0^\dagger PM_0 + M_1^\dagger QM_1\}
\]

for any $\epsilon > 0$, $t_\epsilon$ is a $(M_1^\dagger QM_1, \epsilon)$-bound function of loop while $M[\bar{q}] = 1$ do $S$

\[
\{M_0^\dagger PM_0 + M_1^\dagger QM_1\} \text{while } M[\bar{q}] = 1 \text{ do } S\{P\}\]
Soundness Theorem for $TD$

The proof system $TD$ is sound for total correctness of quantum programs.

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

$$\vdash_{TD} \{P\}S\{Q\} \text{ implies } \models_{\text{tot}} \{P\}S\{Q\}.$$
Completeness Theorem

The proof system $TD$ is complete for total correctness of quantum programs.

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

$$
\models_{\text{tot}} \{P\} S \{Q\} \text{ implies } \vdash_{TD} \{P\} S \{Q\}.
$$
Proof Outline

- Claim: $\vdash_{PD} \{wp.S.Q\} S \{Q\}$ for any quantum program $S$ and quantum predicate $P \in \mathcal{P}(\mathcal{H}_{all})$.

Induction on the structure of $S$. We only consider the case of $S = \textbf{while } M[\bar{q}] = 1 \textbf{ do } S'$.

$$wp.\textbf{while}.Q = M_0^\dagger QM_0 + M_1^\dagger (wp.S.(wp.\textbf{while}.Q))M_1.$$ 

So, our aim is to derive that

$$\{M_0^\dagger QM_0 + M_1^\dagger (wp.S.(wp.\textbf{while}.Q))M_1\} \textbf{while}\{Q\}.$$
Proof Outline, Continued

By the induction hypothesis on $S'$ we get:

$$\{wp.S'.(wp.\text{while}.Q)\}S\{wp.\text{while}.Q\}.$$ 

By (Rule Loop Total) it suffices to show that for any $\epsilon > 0$, there exists a $(M_1^\dag (wp.S'.(wp.S.Q))M_1, \epsilon)$—bound function of quantum loop while.

Applying Bound Function Lemma, we only need to prove:

$$\lim_{n \to \infty} tr(M_1^\dag (wp.S'.(wp.\text{while}.Q))M_1([|S'|] \circ \mathcal{E}_1)^n(\rho)) = 0.$$
Proof Outline, Continued

We observe:

\[
\text{tr}(\mathcal{M}_1^*(\text{wp.while.Q}) \mathcal{M}_1(\|S'\| \circ \mathcal{E}_1)^n(\rho)) = \text{tr}(\text{wp.while.Q}(\mathcal{M}_1(\|S'\| \circ \mathcal{E}_1)^n(\rho) \mathcal{M}_1^*))
\]

\[
= \text{tr}(\text{wp.while.Q}(\mathcal{M}_1(\|S'\| \circ \mathcal{E}_1)^{n+1}(\rho))
\]

\[
= \text{tr}(Q[\text{while}](\|S'\| \circ \mathcal{E}_1)^{n+1}(\rho))
\]

\[
= \sum_{k=n+1}^\infty \text{tr}(Q[\mathcal{E}_0 \circ (\|S'\| \circ \mathcal{E}_1)^k](\rho)).
\]
Proof Outline, Continued

We consider the following infinite series of nonnegative real numbers:

$$\sum_{n=0}^{\infty} tr(Q[E_0 \circ ([|S'|] \circ E_1)^k](\rho)) = tr(Q \sum_{n=0}^{\infty} [E_0 \circ ([|S'|] \circ E_1)^k](\rho)).$$

Since $Q \sqsubseteq I_{H_{all}}$, it follows that

$$tr(Q \sum_{n=0}^{\infty} [E_0 \circ ([|S'|] \circ E_1)^k](\rho)) = tr(Q[while](\rho)) \leq tr(|while|(\rho)) \leq tr(\rho) \leq 1.$$
Outline

Introduction

Syntax of Quantum Programs

Operational Semantics of Quantum Programs

Denotational Semantics of Quantum Programs

Correctness Formulas

Weakest Preconditions and Weakest Liberal Preconditions

Proof System for Partial Correctness

Proof System for Total Correctness

Conclusion
Conclusion

Floyd-Hoare logic for deterministic quantum programs!

- Nondeterministic quantum programs?
Conclusion

Floyd-Hoare logic for deterministic quantum programs!

- Nondeterministic quantum programs?
- Parallel quantum programs?
Conclusion

Floyd-Hoare logic for deterministic quantum programs!

- Nondeterministic quantum programs?
- Parallel quantum programs?
- Distributed quantum programs?
Thank You!