Floyd-Hoare Logic for Quantum Programs

Article *in* ACM Transactions on Programming Languages and Systems · December 2011

DOI: 10.1145/2049706.2049708 · Source: DBLP

1 author:

Mingsheng Ying
Tsinghua University

Floyd-Hoare Logic for Quantum Programs

Mingsheng Ying

University of Technology, Sydney
and
Tsinghua University

Nagoya Winter Workshop, February 14-18, 2011

Outline

Outline

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

R. Floyd, Assigning meaning to programs, in: J. T. Schwartz (ed.) ***Proceedings of Symposium on Applied Mathematics 19, Mathematical Aspects of Computer Science,*** 1967, pp. 19-32

C. A. R. Hoare, An axiomatic basis for computer programming, ***Communication of the ACM***, 12(1969)576-580

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

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

Floyd-Hoare Logic for Quantum Programs

O. Brunet and P. Jorrand, Dynamic quantum logic for quantum programs, ***International Journal of Quantum Information*** 2(2004)45-54

A. Baltag and S. Smets, LQP: the dynamic logic of quantum information, ***Mathematical Structures in Computer Science*** 16(2006)491-525

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

Floyd-Hoare Logic for Quantum Programs, Continued

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

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

Full-fledged Floyd-Hoare logic for quantum programs?

Outline

Syntax

A countably infinite set *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:

$$\mathcal{H}_{\mathbf{Boolean}} = \mathcal{H}_2,$$

$$\mathcal{H}_{\mathbf{integer}} = \mathcal{H}_\infty.$$

The space l_2 of square summable sequences is

$$\mathcal{H}_\infty = \{ \sum_{n=-\infty}^{\infty} \alpha_n |n\rangle : \alpha_n \in \mathbb{C} \text{ for all } n \in \mathbb{Z} \text{ and } \sum_{n=-\infty}^{\infty} |\alpha_n|^2 < \infty \},$$

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:

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

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

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

$$\mathcal{H}_{\overline{q}} = \bigotimes_{i=1}^{n} \mathcal{H}_{q_i}.$$

Syntax, Continued

The quantum extension of classical **while**-programs.

$$
\begin{aligned}
S ::= {} & \textbf{skip} \mid q := 0 \mid \overline{q} := U\overline{q} \mid S_1; S_2 \mid \textbf{measure}\ M[\overline{q}] : \overline{S} \\
& \mid \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S
\end{aligned}
$$

- q is a quantum variable and $\overline{q}$ a quantum register;

Syntax, Continued

The quantum extension of classical **while**-programs.

$$
\begin{aligned}
S ::= \mathbf{skip} \mid q := 0 \mid \overline{q} := U\overline{q} \mid S_1; S_2 \mid \mathbf{measure}\ M[\overline{q}] : \overline{S} \\
\mid \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S
\end{aligned}
$$

- q is a quantum variable and $\overline{q}$ a quantum register;
- U in the statement "$\overline{q} := U\overline{q}$" is a unitary operator on $\mathcal{H}_{\overline{q}}$.

Syntax, Continued

The quantum extension of classical **while**-programs.

$$\begin{aligned} S ::= \mathbf{skip} \mid q := 0 \mid \overline{q} := U\overline{q} \mid S_1; S_2 \mid \mathbf{measure}\ M[\overline{q}] : \overline{S} \\ \mid \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S \end{aligned}$$

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

Syntax, Continued

The quantum extension of classical **while**-programs.

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

- q is a quantum variable and $\overline{q}$ a quantum register;
- U in the statement "$\overline{q} := U\overline{q}$"is a unitary operator on $\mathcal{H}_{\overline{q}}$.
- in the statement "**measure** $M[\overline{q}] : \overline{S}$", $M = \{M_m\}$ is a measurement on the state space $\mathcal{H}_{\overline{q}}$ of $\overline{q}$, 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** $M[\overline{q}] = 1$ **do** S"is a yes-no measurement on $\mathcal{H}_{\overline{q}}$.

Outline

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

$$A \otimes I_{Var-\{\overline{q}\}}$$

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

$$\bigotimes_{q \in Var-\{\overline{q}\}} \mathcal{H}_q.$$

Operational Semantics

$$(Skip) \qquad \frac{}{\langle \mathbf{skip}, \rho \rangle \rightarrow \langle E, \rho \rangle}$$

$$(Initialization) \qquad \frac{}{\langle q := 0, \rho \rangle \rightarrow \langle E, \rho_0^q \rangle}$$

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 $type(q) = \mathbf{Boolean}$, and

$$\rho_0^q = \sum_{n=-\infty}^{\infty} |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|$$

if $type(q) = \mathbf{integer}$.

Operational Semantics, Continued

$$(\textit{Unitary Transformation}) \qquad \frac{}{\langle \overline{q} := U\overline{q}, \rho\rangle \rightarrow \langle E, U\rho U^{\dagger}\rangle}$$

$$(\textit{Sequential Composition}) \qquad \frac{\langle S_1, \rho\rangle \rightarrow \langle S_1', \rho'\rangle}{\langle S_1; S_2, \rho\rangle \rightarrow \langle S_1'; S_2, \rho'\rangle}$$

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

$$(\textit{Measurement}) \qquad \frac{}{\langle \textbf{measure}\ M[\overline{q}] : \overline{S}, \rho\rangle \rightarrow \langle S_m, M_m \rho M_m^{\dagger}\rangle}$$

for each outcome m of measurement $M = \{M_m\}$

Operational Semantics, Continued

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

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

Outline

Definition

Let S be a quantum program. Then its semantic function

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

is defined by

$$[|S|](\rho) = \sum \{|\rho' : \langle S, \rho \rangle \to^* \langle E, \rho' \rangle|\} \tag{1}$$

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

Notation

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

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

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:

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

where $\overline{S} = S_0, S_1$, and

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

for all $n \geq 0$.

Proposition: Representation of Semantic Function

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

Proposition: Representation of Semantic Function

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

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

Proposition: Representation of Semantic Function

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

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

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

Proposition: Representation of Semantic Function

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

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

3. $[|\overline{q} := U\overline{q}|](\rho) = U\rho U^\dagger$.
4. $[|S_1; S_2|](\rho) = [|S_2|]([|S_1|](\rho))$.

Proposition: Representation of Semantic Function

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

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

3. $[|\overline{q} := U\overline{q}|](\rho) = U\rho U^{\dagger}$.
4. $[|S_1; S_2|](\rho) = [|S_2|]([|S_1|](\rho))$.
5. $[|\mathbf{measure}\ M[\overline{q}] : \overline{S}|](\rho) = \sum_m [|S_m|](M_m \rho M_m^{\dagger})$.

Proposition: Representation of Semantic Function

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

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

3. $[|\overline{q} := U\overline{q}|](\rho) = U\rho U^{\dagger}$.
4. $[|S_1; S_2|](\rho) = [|S_2|]([|S_1|](\rho))$.
5. $[|\mathbf{measure}\ M[\overline{q}] : \overline{S}|](\rho) = \sum_m [|S_m|](M_m \rho M_m^{\dagger})$.
6. $[|\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S|](\rho) = \bigvee_{n=0}^{\infty} [|(\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S)^n|](\rho)$.

Proposition: Recursion

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

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

Proposition

For any quantum program S, it holds that

$$tr([|S|](\rho)) \leq tr(\rho)$$

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

$tr(\rho) - tr([|S|](\rho))$ is the probability that program S diverges from input state ρ.

Outline

Definition

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

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

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

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

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

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

Outline

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:

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 $\models_{\text{tot}} \{wp.S.P\}S\{P\}$;

Definition

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

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

Proposition: Representation of Weakest Precondition

1. $wp.\mathbf{skip}.P = P$.

Proposition: Representation of Weakest Precondition

1. $wp.\mathbf{skip}.P = P$.
2. If $type(q) = \mathbf{Boolean}$, 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 $type(q) = \mathbf{integer}$, 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. $wp.\mathbf{skip}.P = P$.
2. If $type(q) = \mathbf{Boolean}$, 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 $type(q) = \mathbf{integer}$, then

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

3. $wp.\overline{q} := U\overline{q}.P = U^\dagger PU$.

Proposition: Representation of Weakest Precondition

1. $wp.\mathbf{skip}.P = P$.
2. If $type(q) = \mathbf{Boolean}$, 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 $type(q) = \mathbf{integer}$, then

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

3. $wp.\overline{q} := U\overline{q}.P = U^{\dagger}PU$.
4. $wp.S_1; S_2.P = wp.S_1.(wp.S_2.P)$.

Proposition: Representation of Weakest Precondition

1. $wp.\mathbf{skip}.P = P$.
2. If $type(q) = \mathbf{Boolean}$, 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 $type(q) = \mathbf{integer}$, then

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

3. $wp.\overline{q} := U\overline{q}.P = U^\dagger PU$.
4. $wp.S_1; S_2.P = wp.S_1.(wp.S_2.P)$.
5. $wp.\mathbf{measure}\ M[\overline{q}] : \overline{S}.P = \sum_m M_m^\dagger(wp.S_m.P)M_m$.

Proposition: Representation of Weakest Precondition

1. $wp.\textbf{skip}.P = P$.
2. If $type(q) = \textbf{Boolean}$, 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 $type(q) = \textbf{integer}$, then

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

3. $wp.\overline{q} := U\overline{q}.P = U^\dagger PU$.
4. $wp.S_1; S_2.P = wp.S_1.(wp.S_2.P)$.
5. $wp.\textbf{measure}\ M[\overline{q}] : \overline{S}.P = \sum_m M_m^\dagger(wp.S_m.P)M_m$.
6. $wp.\textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S.P = \bigvee_{n=0}^{\infty} P_n$, where

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

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:

$$tr((wp.S.P)\rho) = tr(P[|S|](\rho)).$$

Proposition: Representation of Weakest Liberal Precondition

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

Proposition: Representation of Weakest Liberal Precondition

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

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

Proposition: Representation of Weakest Liberal Precondition

1. $wlp.\mathbf{skip}.P = P$.
2. If $type(q) = \mathbf{Boolean}$, 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 $type(q) = \mathbf{integer}$, then
$$wlp.q := 0.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$
3. $wlp.\overline{q} := U\overline{q}.P = U^{\dagger}PU$.

Proposition: Representation of Weakest Liberal Precondition

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

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

3. $wlp.\overline{q} := U\overline{q}.P = U^\dagger PU$.
4. $wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P)$.

Proposition: Representation of Weakest Liberal Precondition

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

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

3. $wlp.\overline{q} := U\overline{q}.P = U^{\dagger}PU$.
4. $wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P)$.
5. $wlp.\mathbf{measure}\ M[\overline{q}] : \overline{S}.P = \sum_m M_m^{\dagger}(wlp.S_m.P)M_m$.

Proposition: Representation of Weakest Liberal Precondition

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

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

3. $wlp.\overline{q} := U\overline{q}.P = U^\dagger PU$.
4. $wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P)$.
5. $wlp.\mathbf{measure}\ M[\overline{q}] : \overline{S}.P = \sum_m M_m^\dagger(wlp.S_m.P)M_m$.
6. $wlp.\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S.P = \bigwedge_{n=0}^{\infty} P_n$, where

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

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:

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

Proposition: Recursion

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

1. $wp.\mathbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wp.S.(wp.\mathbf{while}.P)) M_1$.

Proposition: Recursion

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

1. $wp.\mathbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wp.S.(wp.\mathbf{while}.P))M_1$.
2. $wlp.\mathbf{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\mathbf{while}.P))M_1$.

Outline

The Proof System *PD* for Partial Correctness

(*Axiom Skip*) $\{P\}\mathbf{Skip}\{P\}$

(*Axiom Initialization*) If *type*$(q) = \mathbf{Boolean},$ 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*$(q) = \mathbf{integer},$ then

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

(*Axiom Unitary Transformation*) $\{U^\dagger PU\}\overline{q} := U\overline{q}\{P\}$

The Proof System PD for Partial Correctness, Continued

$$(\textit{Rule Sequential Composition}) \qquad \frac{\{P\}S_1\{Q\} \qquad \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}$$

$$(\textit{Rule Measurement}) \qquad \frac{\{P_m\}S_m\{Q\} \text{ for all } m}{\{\sum_m M_m^\dagger P_m M_m\}\textbf{measure } M[\overline{q}] : \overline{S}\{Q\}}$$

$$(\textit{Rule Loop Partial}) \qquad \frac{\{Q\}S\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\textbf{while } M[\overline{q}] = 1 \textbf{ do } S\{P\}}$$

$$(\textit{Rule Order}) \qquad \frac{P \sqsubseteq P' \quad \{P'\}S\{Q'\} \quad Q' \sqsubseteq Q}{\{P\}S\{Q\}}$$

Soundness Theorem for *PD*

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

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

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

Outline

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

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

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

is called a $(P, \epsilon)-$bound function of quantum loop "**while** $M[\overline{q}] = 1$ **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_ϵ of quantum loop "**while** $M[\overline{q}] = 1$ **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_ϵ of quantum loop "**while** $M[\overline{q}] = 1$ **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)

$$(\textit{Rule Loop Total}) \quad \frac{\begin{array}{c}\{Q\}S\{M_0^\dagger PM_0 + M_1^\dagger QM_1\} \\ \text{for any } \epsilon > 0,\, t_\epsilon \text{ is a } (M_1^\dagger QM_1, \epsilon) - \text{bound function} \\ \text{of loop } \textbf{while } M[\overline{q}] = 1 \textbf{ do } S\end{array}}{\{M_0^\dagger PM_0 + M_1^\dagger QM_1\}\textbf{while } M[\overline{q}] = 1 \textbf{ do } S\{P\}}$$

Soundness Theorem for *TD*

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

For any quantum program S and quantum predicates $P, Q \in \mathcal{P}(\mathcal{H}_{\text{all}})$, 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: $\vdash_{PD} \{wlp.S.Q\}S\{Q\}$ for any quantum program S and quantum predicate $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$.

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

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

So, our aim is to derive that

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

Proof Outline, Continued

By the induction hypothesis on S' we get:

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

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

Applying Bound Function Lemma, we only need to prove:

$$\lim_{n\to\infty} tr(M_1^\dagger(wp.S'.(wp.\textbf{while}.Q))M_1([|S'|] \circ \mathcal{E}_1)^n(\rho)) = 0.$$

Proof Outline, Continued

We observe:

$$
\begin{aligned}
tr(M_1^\dagger(wp.S'.(wp.\textbf{while}.Q))M_1([|S'|]\circ\mathcal{E}_1)^n(\rho)) \\
&= tr(wp.S'.(wp.\textbf{while}.Q)M_1([|S'|]\circ\mathcal{E}_1)^n(\rho)M_1^\dagger) \\
&= tr(wp.\textbf{while}.Q[|S'|](M_1([|S'|]\circ\mathcal{E}_1)^n(\rho)M_1^\dagger)) \\
&= tr(wp.\textbf{while}.Q([|S'|]\circ\mathcal{E}_1)^{n+1}(\rho)) \\
&= tr(Q[|\textbf{while}|]([|S'|]\circ\mathcal{E}_1)^{n+1}(\rho)) \\
&= \sum_{k=n+1}^{\infty} tr(Q[\mathcal{E}_0\circ([|S'|]\circ\mathcal{E}_1)^k](\rho)).
\end{aligned}
$$

Proof Outline, Continued

We consider the following infinite series of nonnegative real numbers:

$$\sum_{n=0}^{\infty} tr(Q[\mathcal{E}_0 \circ ([|S'|] \circ \mathcal{E}_1)^k](\rho)) = tr(Q \sum_{n=0}^{\infty} [\mathcal{E}_0 \circ ([|S'|] \circ \mathcal{E}_1)^k](\rho)).$$

Since $Q \sqsubseteq I_{\mathcal{H}_{all}}$, it follows that

$$\begin{aligned} tr(Q \sum_{n=0}^{\infty} [\mathcal{E}_0 \circ ([|S'|] \circ \mathcal{E}_1)^k](\rho)) &= tr(Q[|\textbf{while}|](\rho)) \\ &\leq tr([|\textbf{while}|](\rho)) \leq tr(\rho) \leq 1. \end{aligned}$$

Outline

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!