Foundations of Quantum Programming

Lecture 4: Logic for Quantum Programs

Mingsheng Ying

University of Technology Sydney, Australia

Outline

Quantum Predicates

Floyd-Hoare Logic for Quantum Programs

Outline

Quantum Predicates

Floyd-Hoare Logic for Quantum Programs

Quantum Predicates

- What is a quantum predicate?

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!

Satisfaction of Quantum Predicates

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0,1]$.

Satisfaction of Quantum Predicates

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.
- Let M be a Hermitian operator in $\mathcal{H}$. The following statements are equivalent:

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.
- Let M be a Hermitian operator in $\mathcal{H}$. The following statements are equivalent:
  1. $M \in \mathcal{P}(\mathcal{H})$ is a quantum predicate.

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.
- Let M be a Hermitian operator in $\mathcal{H}$. The following statements are equivalent:
    1. $M \in \mathcal{P}(\mathcal{H})$ is a quantum predicate.
    2. $0_{\mathcal{H}} \sqsubseteq M \sqsubseteq I_{\mathcal{H}}$.

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.
- Let M be a Hermitian operator in $\mathcal{H}$. The following statements are equivalent:
  1. $M \in \mathcal{P}(\mathcal{H})$ is a quantum predicate.
  2. $0_{\mathcal{H}} \sqsubseteq M \sqsubseteq I_{\mathcal{H}}$.
  3. $0 \leq tr(M\rho) \leq 1$ for all density operators ρ in $\mathcal{H}$.

Lemma

For any observables M, N, the following two statements are equivalent:

Lemma

For any observables M, N, the following two statements are equivalent:

1. $M \sqsubseteq N$;

Lemma

The set $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ of quantum predicates with the Löwner partial order is a complete partial order (CPO).

Lemma

For any observables M, N, the following two statements are equivalent:

1. $M \sqsubseteq N$;
2. for all density operators ρ, $tr(M\rho) \leq tr(N\rho)$.

Lemma

The set $(\mathcal{P}(\mathcal{H}), \sqsubseteq)$ of quantum predicates with the Löwner partial order is a complete partial order (CPO).

Quantum Preconditions

- Let $M, N \in \mathcal{P}(\mathcal{H})$ be quantum predicates, $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ a quantum operation. Then M is a *precondition* of N with respect to $\mathcal{E}$, written $\{M\}\mathcal{E}\{N\}$, if

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

for all density operators ρ in $\mathcal{H}$.

Quantum Preconditions

- Let $M, N \in \mathcal{P}(\mathcal{H})$ be quantum predicates, $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ a quantum operation. Then M is a *precondition* of N with respect to $\mathcal{E}$, written $\{M\}\mathcal{E}\{N\}$, if

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

  for all density operators ρ in $\mathcal{H}$.
- Intuition: a *probabilistic version* of the statement — if state ρ satisfies predicate M, then the state after transformation $\mathcal{E}$ from ρ satisfies predicate N.

Quantum Weakest Preconditions

Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate, $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ a quantum operation. The weakest precondition of M with respect to $\mathcal{E}$ is a quantum predicate $wp(\mathcal{E})(M)$ satisfying:

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

Quantum Weakest Preconditions

Let $M \in \mathcal{P}(\mathcal{H})$ be a quantum predicate, $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ a quantum operation. The weakest precondition of M with respect to $\mathcal{E}$ is a quantum predicate $wp(\mathcal{E})(M)$ satisfying:

1. $\{wp(\mathcal{E})(M)\}\mathcal{E}\{M\}$;
2. for all quantum predicates N, $\{N\}\mathcal{E}\{M\}$ implies $N \sqsubseteq wp(\mathcal{E})(M)$, where $\sqsubseteq$ stands for the Löwner order.

Characterisation of Quantum Weakest Preconditions — *Kraus Operators*

Let quantum operation $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ be represented by the set $\{E_i\}$ of operators:

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

Then for each predicate $M \in \mathcal{P}(\mathcal{H})$:

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

Characterisation of Quantum Weakest Preconditions — *System-environment Model*

If quantum operation $\mathcal{E}$ is given by

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

then:

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

Schrödinger-Heisenberg Duality

- Denotational semantics $\mathcal{E}$ of a quantum program is a forward state transformer:

$$\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}),$$
$$\rho \mapsto \mathcal{E}(\rho) \text{ for each } \rho \in \mathcal{D}(\mathcal{H})$$

Schrödinger-Heisenberg Duality

- Denotational semantics $\mathcal{E}$ of a quantum program is a forward state transformer:

$$\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}),$$
$$\rho \mapsto \mathcal{E}(\rho) \text{ for each } \rho \in \mathcal{D}(\mathcal{H})$$

- Weakest precondition defines a backward quantum predicate transformer:

$$wp(\mathcal{E}) : \mathcal{P}(\mathcal{H}) \to \mathcal{P}(\mathcal{H}),$$
$$M \mapsto wp(\mathcal{E})(M) \text{ for each } M \in \mathcal{P}(\mathcal{M}).$$

Schrödinger-Heisenberg Duality (Continued)

- Let $\mathcal{E}$ be a quantum operation mapping density operators to themselves, $\mathcal{E}^*$ an operator mapping Hermitian operators to themselves. If for any density operator ρ, Hermitian operator M:

$$\text{(Duality)} \quad tr[M\mathcal{E}(\rho)] = tr[\mathcal{E}^*(M)\rho]$$

then $\mathcal{E}$ and $\mathcal{E}^*$ are (Schrödinger-Heisenberg) dual.

$$\begin{array}{ccc} \rho & \models & \mathcal{E}^*(M) \\ \mathcal{E}\downarrow & & \uparrow\mathcal{E}^* \\ \mathcal{E}(\rho) & \models & M \end{array}$$

Schrödinger-Heisenberg Duality (Continued)

- Let $\mathcal{E}$ be a quantum operation mapping density operators to themselves, $\mathcal{E}^*$ an operator mapping Hermitian operators to themselves. If for any density operator ρ, Hermitian operator M:

$$\text{(Duality)} \quad tr[M\mathcal{E}(\rho)] = tr[\mathcal{E}^*(M)\rho]$$

then $\mathcal{E}$ and $\mathcal{E}^*$ are (Schrödinger-Heisenberg) dual.

$$\begin{array}{ccc} \rho & \models & \mathcal{E}^*(M) \\ \mathcal{E}\downarrow & & \uparrow \mathcal{E}^* \\ \mathcal{E}(\rho) & \models & M \end{array}$$

- Any quantum operation $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$ and its weakest precondition $wp(\mathcal{E})$ are dual to each other.

Basic Properties of Quantum Weakest Preconditions

Let $\lambda \geq 0, \mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$, let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{QO}(\mathcal{H})$.

1. $wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{QO}(\mathcal{H})$;

Basic Properties of Quantum Weakest Preconditions

Let $\lambda \geq 0$, $\mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$, let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{QO}(\mathcal{H})$.

1. $wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{QO}(\mathcal{H})$;
2. $wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in \mathcal{QO}(\mathcal{H})$;

Basic Properties of Quantum Weakest Preconditions

Let $\lambda \geq 0, \mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$, let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{QO}(\mathcal{H})$.

1. $wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{QO}(\mathcal{H})$;
2. $wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in \mathcal{QO}(\mathcal{H})$;
3. $wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$;

Basic Properties of Quantum Weakest Preconditions

Let $\lambda \geq 0$, $\mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$, let $\{\mathcal{E}_n\}$ be an increasing sequence in $\mathcal{QO}(\mathcal{H})$.

1. $wp(\lambda\mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda\mathcal{E} \in \mathcal{QO}(\mathcal{H})$;
2. $wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in \mathcal{QO}(\mathcal{H})$;
3. $wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$;
4. $wp\left(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n\right) = \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)$, where $\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)$ is defined by

$$\left(\bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)\right)(M) \triangleq \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)$$

Outline

Quantum Predicates

Floyd-Hoare Logic for Quantum Programs

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;

Partial Correctness, Total Correctness

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.

Partial Correctness, Total Correctness

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.
  - P is called the precondition, Q the postcondition.

Partial Correctness, Total Correctness

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.
  - P is called the precondition, Q the postcondition.

Partial Correctness, Total Correctness

- Two interpretations of Hoare logical formula $\{P\}S\{Q\}$:

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.
  - P is called the precondition, Q the postcondition.

Partial Correctness, Total Correctness

- Two interpretations of Hoare logical formula $\{P\}S\{Q\}$:
  - *Partial correctness*: If an input to program S satisfies the precondition P, then either S does not terminate, or it terminates in a state satisfying the postcondition Q.

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.
  - P is called the precondition, Q the postcondition.

Partial Correctness, Total Correctness

- Two interpretations of Hoare logical formula $\{P\}S\{Q\}$:
  - *Partial correctness*: If an input to program S satisfies the precondition P, then either S does not terminate, or it terminates in a state satisfying the postcondition Q.
  - *Total correctness*: If an input to program S satisfies the precondition P, then S must terminate and it terminates in a state satisfying the postcondition Q.

Partial Correctness, Total Correctness (Continued)

- The correctness formula $\{P\}S\{Q\}$ is true in the sense of *total correctness*, written
$$\models_{tot} \{P\}S\{Q\},$$
if:
$$tr(P\rho) \leq tr(Q[\![S]\!](\rho))$$
for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, where $[\![S]\!]$ is the semantic function of S.

Partial Correctness, Total Correctness (Continued)

- The correctness formula $\{P\}S\{Q\}$ is true in the sense of *total correctness*, written
$$\models_{tot} \{P\}S\{Q\},$$
if:
$$tr(P\rho) \leq tr(Q[\![S]\!](\rho))$$
for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, where $[\![S]\!]$ is the semantic function of S.
- The correctness formula $\{P\}S\{Q\}$ is true in the sense of *partial correctness*, written
$$\models_{par} \{P\}S\{Q\},$$
if:
$$tr(P\rho) \leq tr(Q[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]$$
for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$.

Basic Properties of Correctness

1. If $\models_{tot} \{P\}S\{Q\}$, then $\models_{par} \{P\}S\{Q\}$.

Basic Properties of Correctness

1. If $\models_{tot} \{P\}S\{Q\}$, then $\models_{par} \{P\}S\{Q\}$.
2. For any quantum program S, and for any $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

$$\models_{tot} \{0_{\mathcal{H}_{all}}\}S\{Q\}, \ \ \models_{par} \{P\}S\{I_{\mathcal{H}_{all}}\}.$$

Basic Properties of Correctness

1. If $\models_{tot} \{P\}S\{Q\}$, then $\models_{par} \{P\}S\{Q\}$.
2. For any quantum program S, and for any $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

$$\models_{tot} \{0_{\mathcal{H}_{all}}\}S\{Q\}, \ \models_{par} \{P\}S\{I_{\mathcal{H}_{all}}\}.$$

3. (Linearity) For any $P_1, P_2, Q_1, Q_2 \in \mathcal{P}(\mathcal{H}_{all})$ and $\lambda_1, \lambda_2 \geq 0$ with $\lambda_1 P_1 + \lambda_2 P_2, \lambda_1 Q_1 + \lambda_2 Q_2 \in \mathcal{P}(\mathcal{H}_{all})$, if

$$\models_{tot} \{P_i\}S\{Q_i\} \ (i = 1, 2),$$

then

$$\models_{tot} \{\lambda_1 P_1 + \lambda_2 P_2\}S\{\lambda_1 Q_1 + \lambda_2 Q_2\}.$$

Basic Properties of Correctness

1. If $\models_{tot} \{P\}S\{Q\}$, then $\models_{par} \{P\}S\{Q\}$.
2. For any quantum program S, and for any $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

$$\models_{tot} \{0_{\mathcal{H}_{all}}\}S\{Q\}, \ \models_{par} \{P\}S\{I_{\mathcal{H}_{all}}\}.$$

3. (Linearity) For any $P_1, P_2, Q_1, Q_2 \in \mathcal{P}(\mathcal{H}_{all})$ and $\lambda_1, \lambda_2 \geq 0$ with $\lambda_1 P_1 + \lambda_2 P_2, \lambda_1 Q_1 + \lambda_2 Q_2 \in \mathcal{P}(\mathcal{H}_{all})$, if

$$\models_{tot} \{P_i\}S\{Q_i\} \ (i = 1, 2),$$

then

$$\models_{tot} \{\lambda_1 P_1 + \lambda_2 P_2\}S\{\lambda_1 Q_1 + \lambda_2 Q_2\}.$$

- The same conclusion holds for partial correctness if $\lambda_1 + \lambda_2 = 1$.

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.
  2. The weakest liberal precondition of S with respect to P is the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.
  2. The weakest liberal precondition of S with respect to P is the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{par} \{wlp.S.P\}S\{P\}$;

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.
  2. The weakest liberal precondition of S with respect to P is the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{par} \{wlp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{par} \{Q\}S\{P\}$ then $Q \sqsubseteq wlp.S.P$.

Weakest (Liberal) Preconditions of Quantum Programs

- Let S be a quantum **while**-program, $P \in \mathcal{P}(\mathcal{H}_{all})$ a quantum predicate in $\mathcal{H}_{all}$.
  1. The weakest precondition of S with respect to P is the quantum predicate $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{tot} \{wp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{tot} \{Q\}S\{P\}$ then $Q \sqsubseteq wp.S.P$.
  2. The weakest liberal precondition of S with respect to P is the quantum predicate $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$ satisfying:
     - $\models_{par} \{wlp.S.P\}S\{P\}$;
     - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{par} \{Q\}S\{P\}$ then $Q \sqsubseteq wlp.S.P$.
- Equivalence of semantic and syntactic definitions:

$$wp.S.P = wp([\![S]\!])(P).$$

Structural Representation of Weakest Preconditions

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

Structural Representation of Weakest Preconditions

1. $wp.\mathbf{skip}.P = P$.
2.

Structural Representation of Weakest Preconditions

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

$$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

Structural Representation of Weakest Preconditions

1. $wp.\mathbf{skip}.P = P$.
2.
   - If $type(q) = \mathbf{Boolean}$, then
   $$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$
   - If $type(q) = \mathbf{integer}$, then
   $$wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$

Structural Representation of Weakest Preconditions

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

Structural Representation of Weakest Preconditions

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

$$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

   - If $type(q) = \mathbf{integer}$, then

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

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

Structural Representation of Weakest Preconditions

1. $wp.\mathbf{skip}.P = P$.
2.
   - If $type(q) = \mathbf{Boolean}$, then
   $$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$
   - If $type(q) = \mathbf{integer}$, then
   $$wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$
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. $wp.\mathbf{if}\ (\square m \cdot M[\overline{q}] = m \rightarrow S_m)\ \mathbf{fi}.P = \sum_m M_m^\dagger (wp.S_m.P) M_m$.

Structural Representation of Weakest Preconditions

1. $wp.\mathbf{skip}.P = P$.
2.
   - If $type(q) = \mathbf{Boolean}$, then
   $$wp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$
   - If $type(q) = \mathbf{integer}$, then
   $$wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$
3. $wp.\overline{q} := U[\overline{q}].P = U^\dagger P U$.
4. $wp.S_1; S_2.P = wp.S_1.(wp.S_2.P)$.
5. $wp.\mathbf{if}\ (\square m \cdot M[\overline{q}] = m \rightarrow S_m)\ \mathbf{fi}.P = \sum_m M_m^\dagger (wp.S_m.P) M_m$.
6. $wp.\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}.P = \bigsqcup_{n=0}^{\infty} P_n$, where
$$\begin{cases} P_0 = 0_{\mathcal{H}_{all}}, \\ P_{n+1} = M_0^\dagger P M_0 + M_1^\dagger (wp.S.P_n) M_1 \text{ for all } n \geq 0. \end{cases}$$

Structural Representation of Weakest Liberal Preconditions

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

Structural Representation of Weakest Liberal Preconditions

1. $wlp.\mathbf{skip}.P = P$.
2.

Structural Representation of Weakest Liberal Preconditions

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

$$wlp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

Structural Representation of Weakest Liberal Preconditions

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

Structural Representation of Weakest Liberal Preconditions

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

Structural Representation of Weakest Liberal Preconditions

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

     $$wlp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

   - If $type(q) = \mathbf{integer}$, then

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

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

Structural Representation of Weakest Liberal Preconditions

1. $wlp.\mathbf{skip}.P = P$.
2.
   - If $type(q) = \mathbf{Boolean}$, then
     $$wlp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$
   - If $type(q) = \mathbf{integer}$, then
     $$wlp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.$$
3. $wlp.\overline{q} := U[\overline{q}].P = U^\dagger P U$.
4. $wlp.S_1; S_2.P = wlp.S_1.(wlp.S_2.P)$.
5. $wlp.\mathbf{if}\ (\square m \cdot M[\overline{q}] := m \rightarrow S_m)\ \mathbf{fi}.P = \sum_m M_m^\dagger (wlp.S_m.P) M_m$.

Structural Representation of Weakest Liberal Preconditions

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

     $$wlp.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.$$

   - If $type(q) = \mathbf{integer}$, then

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

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. $wlp.\mathbf{if}\ (\square m \cdot M[\overline{q}] := m \rightarrow S_m)\ \mathbf{fi}.P = \sum_m M_m^{\dagger}(wlp.S_m.P)M_m$.
6. $wlp.\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}.P = \bigsqcap_{n=0}^{\infty} P_n$, where

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

Trace-Preserving Property

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

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

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

Trace-Preserving Property

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

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

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

Fixed Point Characterisation

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

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

Proof System for Partial Correctness

(Ax – Sk) $\{P\}\mathbf{Skip}\{P\}$

(Ax – In) If $type(q) = \mathbf{Boolean}$, then

$$\{|0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|\}q := |0\rangle\{P\}$$

If $type(q) = \mathbf{integer}$, then

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

(Ax – UT) $\{U^\dagger PU\}\overline{q} := U\overline{q}\{P\}$

Proof System for Partial Correctness (Continued)

$$(\mathrm{R-SC}) \qquad \frac{\{P\}S_1\{Q\} \qquad \{Q\}S_2\{R\}}{\{P\}S_1;S_2\{R\}}$$

$$(\mathrm{R-IF}) \qquad \frac{\{P_m\}S_m\{Q\} \text{ for all } m}{\left\{\sum_m M_m^\dagger P_m M_m\right\} \textbf{ if } (\square m \cdot M[\overline{q}] = m \rightarrow S_m) \textbf{ fi}\{Q\}}$$

$$(\mathrm{R-LP}) \qquad \frac{\{Q\}S\left\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\right\}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\textbf{while } M[\overline{q}] = 1 \textbf{ do } S \textbf{ od}\{P\}}$$

$$(\mathrm{R-Or}) \qquad \frac{P \sqsubseteq P' \quad \{P'\}S\{Q'\} \quad Q' \sqsubseteq Q}{\{P\}S\{Q\}}$$

Soundness Theorem

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

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

Soundness Theorem

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

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

(Relative) Completeness Theorem

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

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

Bound (Ranking) Functions

- Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate, real number $\epsilon > 0$.

Bound (Ranking) Functions

- Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate, real number $\epsilon > 0$.
- A function
$$t : \mathcal{D}(\mathcal{H}_{all}) \to \omega$$
is a (P, ϵ)-bound function of quantum loop
$$\textbf{while } M[\bar{q}] = 1 \textbf{ do } S \textbf{ od}$$
if for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$:

Bound (Ranking) Functions

- Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate, real number $\epsilon > 0$.
- A function

  $$t : \mathcal{D}(\mathcal{H}_{all}) \rightarrow \omega$$

  is a (P, ϵ)-bound function of quantum loop

  $$\textbf{while } M[\bar{q}] = 1 \textbf{ do } S \textbf{ od}$$

  if for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$:

  1. $t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right) \leq t(\rho)$;

Bound (Ranking) Functions

- Let $P \in \mathcal{P}(\mathcal{H}_{all})$ be a quantum predicate, real number $\epsilon > 0$.
- A function

$$t : \mathcal{D}(\mathcal{H}_{all}) \rightarrow \omega$$

is a (P, ϵ)-bound function of quantum loop

$$\textbf{while } M[\overline{q}] = 1 \textbf{ do } S \textbf{ od}$$

if for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$:

1. $t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right) \leq t(\rho)$;
2. $tr(P\rho) \geq \epsilon$ implies

$$t\left(\llbracket S \rrbracket \left(M_1 \rho M_1^\dagger\right)\right) < t(\rho)$$

Characterisation of Bound Functions

The following two statements are equivalent:

1. for any $\epsilon > 0$, there exists a (P, ϵ)-bound function t_ϵ of the **while**-loop "**while** $M[\overline{q}] = 1$ **do** S **od**";

Characterisation of Bound Functions

The following two statements are equivalent:

1. for any $\epsilon > 0$, there exists a (P, ϵ)-bound function t_ϵ of the **while**-loop "**while** $M[\overline{q}] = 1$ **do** S **od**";
2. $\lim_{n\to\infty} tr\left(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)\right) = 0$ for all $\rho \in \mathcal{D}(\mathcal{H}_{\text{all}})$.

Proof System for Total Correctness

$$(\mathrm{R-LT})\quad \frac{\begin{array}{l}\bullet\ \{Q\}S\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\\ \bullet\ \text{for any } \epsilon > 0,\ t_\epsilon \text{ is a } (M_1^\dagger Q M_1, \epsilon) - \text{bound function}\\ \quad \text{of loop } \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}\end{array}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}\{P\}}$$

Soundness Theorem

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

$$\vdash_{qTD} \{P\}S\{Q\} \text{ implies } \models_{tot} \{P\}S\{Q\}.$$

Soundness Theorem

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

$$\vdash_{qTD} \{P\}S\{Q\} \text{ implies } \models_{tot} \{P\}S\{Q\}.$$

(Relative) Completeness Theorem

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

$$\models_{tot} \{P\}S\{Q\} \text{ implies } \vdash_{qTD} \{P\}S\{Q\}.$$