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?

A quantum predicate in a Hilbert space $H$ is a Hermitian operator $M$ in $H$ with all its eigenvalues lying within the unit interval $[0, 1]$.

The set of predicates in $H$ is denoted $P(H)$.

Satisfaction of Quantum Predicates

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

Let $M$ be a Hermitian operator in $H$. The following statements are equivalent:

1. $M \in P(H)$ is a quantum predicate.
2. $0 \leq M \leq I$.
3. $0 \leq \text{tr}(M \rho) \leq 1$ for all density operators $\rho$ in $H$.
Quantum Predicates

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

Satisfaction of Quantum Predicates

\[ \text{tr}(M\rho) \text{ may be interpreted as the degree to which quantum state } \rho \text{ satisfies quantum predicate } M. \]

\[ \text{Let } M \text{ be a Hermitian operator in } H. \text{ The following statements are equivalent:} \]

1. \( M \in \mathcal{P}(H) \) is a quantum predicate.
2. \( 0 \leq M \leq I \).
3. \( 0 \leq \text{tr}(M\rho) \leq 1 \) for all density operators \( \rho \) in \( H \).
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 $[0, 1]$.

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

- $\text{tr}(M \rho)$ may be interpreted as the degree to which quantum state $\rho$ 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. $0 \leq M \leq I$.
  3. $0 \leq \text{tr}(M \rho) \leq 1$ for all density operators $\rho$ in $\mathcal{H}$. 
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

- $\text{tr}(M\rho)$ may be interpreted as the degree to which quantum state $\rho$ 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

- $\text{tr}(M\rho)$ may be interpreted as the degree to which quantum state $\rho$ 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

- $\text{tr}(M \rho)$ may be interpreted as the degree to which quantum state $\rho$ 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 $\rho$ 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. $0_{\mathcal{H}} \subseteq M \subseteq I_{\mathcal{H}}$. 
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

▶ \( \text{tr}(M\rho) \) may be interpreted as the degree to which quantum state \( \rho \) 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. \( 0_{\mathcal{H}} \subseteq M \subseteq I_{\mathcal{H}} \).
  3. \( 0 \leq \text{tr}(M\rho) \leq 1 \) for all density operators \( \rho \) in \( \mathcal{H} \).
**Lemma**

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

1. $M \preceq N$;
2. for all density operators $\rho$, $\text{tr}(M\rho) \leq \text{tr}(N\rho)$. 

**Lemma**

The set $(\mathcal{P}(H), \preceq)$ 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. $M \sqsubseteq N$;

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. $M \subseteq N$;
2. for all density operators $\rho$, $\text{tr}(M\rho) \leq \text{tr}(N\rho)$.

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

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

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

Intuition: a probabilistic version of the statement — if state $\rho$ satisfies predicate $M$, then the state after transformation $\mathcal{E}$ from $\rho$ satisfies predicate $N$. 
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 \textit{precondition} of \( N \) with respect to \( \mathcal{E} \), written \( \{M\}\mathcal{E}\{N\} \), if

\[
\text{tr}(M\rho) \leq \text{tr}(N\mathcal{E}(\rho))
\]

for all density operators \( \rho \) in \( \mathcal{H} \).

- Intuition: a \textit{probabilistic version} of the statement — if state \( \rho \) satisfies predicate \( M \), then the state after transformation \( \mathcal{E} \) from \( \rho \) 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

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

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:

$$\mathcal{E} : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}),$$

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

\[
wp(\mathcal{E}) : \mathcal{P}(\mathcal{H}) \to \mathcal{P}(\mathcal{H}),
\]

\[
M \mapsto wp(\mathcal{E})(M) \text{ for each } M \in \mathcal{P}(\mathcal{M}).
\]
Let $\mathcal{E}$ be a quantum operation mapping density operators to themselves, $\mathcal{E}^\ast$ an operator mapping Hermitian operators to themselves. If for any density operator $\rho$, Hermitian operator $M$:

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

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

\[\rho \models \mathcal{E}^\ast(M)\]

\[\mathcal{E} \downarrow \quad \uparrow \mathcal{E}^\ast\]

\[\mathcal{E}(\rho) \models M\]
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 $\rho$, 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.

$$\rho \models \mathcal{E}^*(M)$$

$$\mathcal{E} \downarrow \quad \mathcal{E}^* \uparrow$$

$$\mathcal{E}(\rho) \models M$$

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

1. $wp(\lambda \mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda \mathcal{E} \in QO(\mathcal{H})$;
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 $\lambda \geq 0$, $\mathcal{E}, \mathcal{F} \in QO(\mathcal{H})$, let $\{\mathcal{E}_n\}$ be an increasing sequence in $QO(\mathcal{H})$.

1. $wp(\lambda \mathcal{E}) = \lambda wp(\mathcal{E})$ provided $\lambda \mathcal{E} \in QO(\mathcal{H})$;
2. $wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + wp(\mathcal{F})$ provided $\mathcal{E} + \mathcal{F} \in QO(\mathcal{H})$;
3. $wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$;
Basic Properties of Quantum Weakest Preconditions

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

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

- \( S \) is a quantum program;
- \( P, Q \in \mathbb{P}(\text{Hall}) \) are quantum predicates in \( \text{Hall} \);
- \( P \) 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 \( Q \).
Correctness Formulas

- A correctness formula is a statement of the form:

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

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 \( \{P\} S \{Q\} \):

  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 \( Q \).
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
  \[ \models_{\text{tot}} \{P\} S \{Q\}, \]
  if:
  \[ tr(P\rho) \leq tr(Q[S](\rho)) \]
  for all $\rho \in D(H_{all})$, 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

\[
\models_{\text{tot}} \{P\} S \{Q\},
\]

if:

\[
tr(P\rho) \leq tr(Q\llbracket S \rrbracket(\rho))
\]

for all \( \rho \in \mathcal{D}(\mathcal{H}_{\text{all}}) \), where \( \llbracket S \rrbracket \) is the semantic function of \( S \).

▷ The correctness formula \( \{P\} S \{Q\} \) is true in the sense of partial correctness, written

\[
\models_{\text{par}} \{P\} S \{Q\},
\]

if:

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

for all \( \rho \in \mathcal{D}(\mathcal{H}_{\text{all}}) \).
Basic Properties of Correctness

1. If $\mathbf{\vdash}_{\text{tot}} \{P\} S\{Q\}$, then $\mathbf{\vdash}_{\text{par}} \{P\} S\{Q\}$. 

▶ The same conclusion holds for partial correctness if $\lambda_1 + \lambda_2 = 1$. 
Basic Properties of Correctness

1. If $|\equiv_{\text{tot}} \{P\} S\{Q\}$, then $|\equiv_{\text{par}} \{P\} S\{Q\}$.

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

$$|\equiv_{\text{tot}} \{0\mathcal{H}_{\text{all}}\} S\{Q\}, \quad |\equiv_{\text{par}} \{P\} S\{I\mathcal{H}_{\text{all}}\}.$$
Basic Properties of Correctness

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

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

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

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

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

then

$$\models_{\text{tot}} \{\lambda_1 P_1 + \lambda_2 P_2\} S\{\lambda_1 Q_1 + \lambda_2 Q_2\}.$$
Basic Properties of Correctness

1. If $|=_{\text{tot}} \{P\} S\{Q\}$, then $|=_{\text{par}} \{P\} S\{Q\}$.

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

   $|=_{\text{tot}} \{0_{\mathcal{H}_{\text{all}}}\} S\{Q\}, \quad |=_{\text{par}} \{P\} S\{I_{\mathcal{H}_{\text{all}}}\}$.

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

   $|=_{\text{tot}} \{P_i\} S\{Q_i\} \ (i = 1, 2)$,

   then

   $|=_{\text{tot}} \{\lambda_1 P_1 + \lambda_2 P_2\} S\{\lambda_1 Q_1 + \lambda_2 Q_2\}$.

   ▶ The same conclusion holds for partial correctness if $\lambda_1 + \lambda_2 = 1$. 
Weakest (Liberal) Preconditions of Quantum Programs

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

Equivalence of semantic and syntactic definitions:

$$wp(S).P = wp(\llbracket S \rrbracket)(P)$$
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:

\[
\begin{align*}
\|wp.S.P\| & = \text{tot}\{wp.S.P\} \\
\|Q\| & = \text{tot}\{Q\} \\
\text{if } Q \in \mathcal{P}(\mathcal{H}_{all}) \text{ satisfies } \|Q\| = \text{tot}\{Q\} \text{ then } Q \trianglelefteq wp.S.P
\end{align*}
\]
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:
   - $\models_{\text{tot}} \{wp.S.P\}S\{P\};$
   - if quantum predicate $Q \in \mathcal{P}(\mathcal{H}_{all})$ satisfies $\models_{\text{tot}} \{Q\}S\{P\}$ 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 $\textbf{while}$-program, $P \in \mathcal{P}(\mathcal{H}_{\text{all}})$ a quantum predicate in $\mathcal{H}_{\text{all}}$.

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

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

Equivalence of semantic and syntactic definitions:

$$wp.S.P = wp(\llbracket S \rrbracket)(P).$$
Structural Representation of Weakest Preconditions

1. \( wp.\text{skip}.P = P \).
Structural Representation of Weakest Preconditions

1. \( wp.\text{skip}.P = P \).
2. 

... (continued on the next page)
Structural Representation of Weakest Preconditions

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

2.
   - If \( \text{type}(q) = \text{Boolean} \), then
     \[
     \text{wp} \cdot q := |0\rangle \cdot P = |0\rangle_q \langle 0 | P | 0 \rangle_q \langle 0 | + |1\rangle_q \langle 0 | P | 0 \rangle_q \langle 1 |.
     \]
Structural Representation of Weakest Preconditions

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

2. 
   - If \( \text{type}(q) = \text{Boolean} \), then
     \[
     \text{wp}.q := |0\rangle.P = |0\rangle_q|0\rangle_P|0\rangle_q\langle 0| + |1\rangle_q|0\rangle_P|0\rangle_q\langle 1|.
     \]
   - If \( \text{type}(q) = \text{integer} \), then
     \[
     \text{wp}.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q|0\rangle_P|0\rangle_q\langle n|.
     \]
Structural Representation of Weakest Preconditions

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

2. 
   - If \( \text{type}(q) = \text{Boolean} \), 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 \( \text{type}(q) = \text{integer} \), then
     \[
     wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
     \]

3. \( \text{wp.} \bar{q} := U[\bar{q}].P = U^\dagger PU \).
Structural Representation of Weakest Preconditions

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

2. 
   - If $\text{type}(q) = \text{Boolean}$, then
     \begin{equation}
     \text{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|.
     \end{equation}
   - If $\text{type}(q) = \text{integer}$, then
     \begin{equation}
     \text{wp}.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
     \end{equation}

3. $\text{wp.\overline{q}} := U[\overline{q}].P = U^\dagger P U$.

4. $\text{wp}.S_1;S_2.P = \text{wp}.S_1.(\text{wp}.S_2.P)$. 
Structural Representation of Weakest Preconditions

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

2. 
   - If \(\text{type}(q) = \text{Boolean}\), then
     \[
     wp.q := |0\rangle.P = |0\rangle_q|0\rangle_P|0\rangle_q + |1\rangle_q|0\rangle_P|0\rangle_q|1\rangle.
     \]
   - If \(\text{type}(q) = \text{integer}\), then
     \[
     wp.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q|0\rangle_P|0\rangle_q|n\rangle.
     \]

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

4. \(wp.S_1;S_2.P = wp.S_1.(wp.S_2.P)\).

5. \(wp.\text{if } (\square m \cdot M[\bar{q}] = m \rightarrow S_m) \text{ fi}.P = \sum_m M_m^\dagger (wp.S_m.P)M_m\).
Structural Representation of Weakest Preconditions

1. \( \text{wp.skip}.P = P \).
2. 
   - If \( \text{type}(q) = \text{Boolean} \), then
     \[
     \text{wp}.q := |0\rangle.P = |0\rangle_q\langle 0|P|0\rangle_q\langle 0| + |1\rangle_q\langle 0|P|0\rangle_q\langle 1|.
     \]
   - If \( \text{type}(q) = \text{integer} \), then
     \[
     \text{wp}.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0|P|0\rangle_q\langle n|.
     \]
3. \( \text{wp.\overline{q}} := U[\overline{q}].P = U^\dagger PU \).
4. \( \text{wp.S}_1;S_2.P = \text{wp.S}_1.(\text{wp.S}_2.P) \).
5. \( \text{wp.if (□m} \cdot M[q] = m \rightarrow S_m) \text{ fi}.P = \sum_m M^\dagger_m (\text{wp.S}_m.P)M_m \).
6. \( \text{wp.while } M[q] = 1 \text{ do S od}.P = \bigsqcup_{n=0}^{\infty} P_n, \text{ where} \)
   \[
   \begin{cases}
   P_0 = 0_{\mathcal{H}_{\text{all}}}, \\
   P_{n+1} = M_0^\dagger PM_0 + M_1^\dagger (\text{wp.S}.P_n)M_1 \text{ for all } n \geq 0.
   \end{cases}
   \]
Structural Representation of Weakest Liberal Preconditions

1. \texttt{wlp.skip.P = P}.
Structural Representation of Weakest Liberal Preconditions

1. \( wlp.\text{skip}.P = P \).
2. 

3. \( wlp.\text{skip}.q = |0\rangle_P = |0\rangle_q \langle 0 | + |1\rangle_q \langle 1 | \). 

4. \( wlp.\text{skip}.q = U[q].P = U[q]^\dagger PU[q]. \)

5. \( wlp.\text{skip}.S_1; S_2.P = wlp.\text{skip}.S_1.(wlp.\text{skip}.S_2.P) \).

6. \( wlp.\text{skip}.\text{if} (\Box m \cdot M[q] : S_m) \text{fi}.P = \sum_m M[m]^\dagger (wlp.\text{skip}.S_m.P) M[m]. \)

7. \( wlp.\text{while} M[q] = 1 \text{do} S \text{od}.P = \sum_{n=0}^{\infty} P_n, \) where 

\[ 
\begin{align*}
P_0 &= I \text{Hall}, \\
P_{n+1} &= M[q]^\dagger_0 PM[q]_0 + M[q]^\dagger_1 (wlp.\text{skip}.S_1.P) M[q]_1
\end{align*} \] 

for all \( n \geq 0. \)
Structural Representation of Weakest Liberal Preconditions

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

2.
   - If \texttt{type(q)} = \texttt{Boolean}, then
     \[
     wlp.q := \ket{0}.P = \ket{0}_q\bra{0}|P\rangle\langle 0| + \ket{1}_q\bra{0}|P\rangle\langle 1|.
     \]
Structural Representation of Weakest Liberal Preconditions

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

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

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

▶ If \textit{type}(q) = \texttt{integer}, then

\[
\text{wlp}.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} |n\rangle_q\langle 0\mid P\mid 0\rangle_q\langle n \rangle.
\]
Structural Representation of Weakest Liberal Preconditions

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

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

3. $\texttt{wlp.\overline{q}} := \texttt{U[\overline{q}].P} = \texttt{U}^\dagger PU$. 
Structural Representation of Weakest Liberal Preconditions

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

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

\[
\texttt{wlp}.q := \ket{0}.P = \ket{0}_q \bra{0}_q \bra{0}_q \bra{0} + \ket{1}_q \bra{0}_q \bra{0}_q \bra{1}_q.
\]

▶ If \texttt{type}(q) = integer, then

\[
\texttt{wlp}.q := \ket{0}.P = \sum_{n=-\infty}^{\infty} \ket{n}_q \bra{0}_q \bra{0}_q \bra{n}_q.
\]

3. \texttt{wlp.q} := \texttt{U[q]}.P = \texttt{U}^\dagger P \texttt{U}.

4. \texttt{wlp.S_1;S_2}.P = \texttt{wlp.S_1.(wlp.S_2.P)}. 
Structural Representation of Weakest Liberal Preconditions

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

2. 
   - If \( \text{type}(q) = \text{Boolean} \), then
     \[
     wlp\cdot q := |0\rangle\cdot P = |0\rangle_q\langle 0|P\rangle_0\langle 0| + |1\rangle_q\langle 0|P\rangle_0\langle 1|.
     \]
   - If \( \text{type}(q) = \text{integer} \), then
     \[
     wlp\cdot q := |0\rangle\cdot P = \sum_{n=\infty}^{n=-\infty} |n\rangle_q\langle 0|P\rangle_0\langle n|.
     \]

3. \( wlp\cdot \bar{q} := U[\bar{q}]\cdot P = U^\dagger PU \).

4. \( wlp\cdot S_1; S_2\cdot P = wlp\cdot S_1\cdot (wlp\cdot S_2\cdot P) \).

5. \( wlp\cdot \texttt{if} (\square m \cdot M[\bar{q}] := m \rightarrow S_m) \texttt{fi} \cdot P = \sum_m M^+_m(wlp\cdot S_m\cdot P)M_m \).
Structural Representation of Weakest Liberal Preconditions

1. \( \text{wlp.skip}.P = P \).
2.  
   - If \( \text{type}(q) = \text{Boolean} \), then
     \[
     \text{wlp}.q := |0\rangle.P = |0\rangle_q\langle0|P|0\rangle_q\langle0| + |1\rangle_q\langle0|P|0\rangle_q\langle1|.
     \]
   - If \( \text{type}(q) = \text{integer} \), then
     \[
     \text{wlp}.q := |0\rangle.P = \sum_{n=-\infty}^{\infty} n\langle n|q\langle0|P|0\rangle_q\langle n|.
     \]
3. \( \text{wlp.}\bar{q} := U[\bar{q}].P = U^\dagger PU \).
4. \( \text{wlp.S}_1;S_2.P = \text{wlp.S}_1.(\text{wlp.S}_2.P) \).
5. \( \text{wlp.if} (\square m \cdot M[\bar{q}] := m \rightarrow S_m) \text{fi}.P = \sum_m M^\dagger_m (\text{wlp.S}_m.P)M_m \).
6. \( \text{wlp.while} \ M[\bar{q}] = 1 \text{ do } S \text{ od}.P = \bigcap_{n=0}^{\infty} P_n \), where
   \[
   \left\{ 
   \begin{array}{l}
   P_0 = I_{\text{H}_\text{all}}, \\
   P_{n+1} = M^\dagger_0 PM_0 + M^\dagger_1 (\text{wlp.S}.P_n)M_1 \text{ for all } n \geq 0.
   \end{array}
   \right.
   \]
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 $\rho \in \mathcal{D}(\mathcal{H}_{all})$:

$$\text{tr}((wp.S.P)\rho) = \text{tr}(P[S](\rho)).$$

$$\text{tr}((wlp.S.P)\rho) = \text{tr}(P[S](\rho)) + [\text{tr}(\rho) - \text{tr}(S(\rho))].$$

Fixed Point Characterisation

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

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

2. $wlp.\text{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\text{while}.P)) M_1.$
Proof System for Partial Correctness

\[(Ax - Sk) \quad \{P\} \textbf{Skip}\{P\}\]

\[(Ax - In) \text{ If } \text{type}(q) = \text{Boolean}, \text{ then}\]

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

\[\text{If } \text{type}(q) = \text{integer}, \text{ then}\]

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

\[(Ax - UT) \quad \{U^*P\bar{U}\}q := U\bar{q}\{P\}\]
Proof System for Partial Correctness (Continued)

(R - SC) \[
\begin{array}{c}
\{P\} S_1 \{Q\} \hspace{1cm} \{Q\} S_2 \{R\} \\
\{P\} S_1 ; S_2 \{R\}
\end{array}
\]

(R - IF) \[
\begin{array}{c}
\{P_m\} S_m \{Q\} \text{ for all } m \\
\{\sum_m M_m^\dagger P_m M_m\} \text{ if } (\square m \cdot M[\bar{q}] = m \to S_m) \text{ fi} \{Q\}
\end{array}
\]

(R - LP) \[
\begin{array}{c}
\{Q\} S \{M_0^\dagger P M_0 + M_1^\dagger Q M_1\} \\
\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\} \text{ while } M[\bar{q}] = 1 \text{ do } S \text{ od} \{P\}
\end{array}
\]

(R - Or) \[
\begin{array}{c}
P \sqsubseteq P' \hspace{1cm} \{P'\} S \{Q'\} \hspace{1cm} Q' \sqsubseteq Q \\
\{P\} S \{Q\}
\end{array}
\]
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

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

is a $(P, \epsilon)$-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
  
  $$t : \mathcal{D}(\mathcal{H}_{all}) \to \omega$$

  is a $(P, \epsilon)$-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. $t(\|S\| (M_1 \rho M_1^*)) \leq t(\rho)$;
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 $(P, \epsilon)$-bound function of quantum loop

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

  if for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$:
  1. $t \left( \left\lfloor S \right\rfloor \left( M_1 \rho M_1^\dagger \right) \right) \leq t(\rho)$;
  2. $\text{tr}(P\rho) \geq \epsilon$ implies

  $$t \left( \left\lfloor S \right\rfloor \left( M_1 \rho M_1^\dagger \right) \right) < t(\rho)$$
Characterisation of Bound Functions

The following two statements are equivalent:

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

2. $\lim_{n \to \infty} t_\epsilon(P(\llbracket S \rrbracket \circ E_1)n(\rho)) = 0$ for all $\rho \in D(Hall)$. 
Characterisation of Bound Functions

The following two statements are equivalent:

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

2. $\lim_{n \to \infty} tr (P([S] \circ E_1)^n(\rho)) = 0$ for all $\rho \in D(\mathcal{H}_{\text{all}})$. 
Proof System for Total Correctness

\[
\begin{align*}
\text{(R – LT)} & \quad \{Q\} S\{M_0^\dagger PM_0 + M_1^\dagger QM_1\} \\
& \quad \text{for any } \epsilon > 0, \ t_\epsilon \text{ is a } (M_1^\dagger QM_1, \epsilon) - \text{bound function of loop} \text{ while } M[\bar{q}] = 1 \text{ do } S \text{ od} \\
& \quad \frac{M_0^\dagger PM_0 + M_1^\dagger QM_1}{\{M_0^\dagger PM_0 + M_1^\dagger QM_1\}\text{while } M[\bar{q}] = 1 \text{ do } S \text{ od}\{P\}}
\end{align*}
\]
**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 $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

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