Toward Automatic Verification of Quantum Programs

Xiaodi Wu

QuICS, University of Maryland

Outline

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Issues with Verifications

- The object of verification?

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Issues with Verifications

- The object of verification?
- Traditional, lightweight, and full verification?

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Issues with Verifications

- The object of verification?
- Traditional, lightweight, and full verification?

Verification of Quantum Programs

Motivation

- quantum programs: *less intuitive* and *error-prone*.
- comparing to classical: *harder* task with *less* study.
- QPL practice: Quipper, QWIRE, ScaffCC, Q#, qiskit, Forrest, ProjectQ, ...

Issues with Verifications

- The object of verification?
- Traditional, lightweight, and full verification?

Possible Long-term Target

- Scalable and Principled Verification of Quantum Programs!
- a library of verified quantum programs; automated tools to assist programmer; ...

Outline

Quantum While-Language

Syntax

A ***core*** language for imperative quantum programming

$$\begin{aligned} S ::= \mathbf{skip} & \mid q := |0\rangle \\ & \mid S_1; S_2 \\ & \mid \overline{q} := U[\overline{q}] \\ & \mid \mathbf{if}\ \left(\square m \cdot M[\overline{q}] = m \rightarrow S_m\right)\ \mathbf{fi} \\ & \mid \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od} \end{aligned}$$

Operational Semantics

A *configuration*: $\langle S, \rho \rangle$

- S is a quantum program or E (the empty program)
- ρ is a partial density operator in

$$\mathcal{H}_{\text{all}} = \bigotimes_{\text{all } q} \mathcal{H}_q$$

Operational Semantics

$$(Sk) \qquad \frac{}{\langle \mathbf{skip}, \rho \rangle \to \langle E, \rho \rangle}$$

$$(Ini) \qquad \frac{}{\langle q := |0\rangle, \rho \rangle \to \langle E, \rho_0^q \rangle}$$

- $type(q) = \mathbf{Boolean}$:

$$\rho_0^q = |0\rangle_q\langle 0|\rho|0\rangle_q\langle 0| + |0\rangle_q\langle 1|\rho|1\rangle_q\langle 0|$$

- $type(q) = \mathbf{integer}$:

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

Operational Semantics

$$(Uni) \qquad \frac{}{\langle \overline{q} := U[\overline{q}], \rho\rangle \rightarrow \langle E, U\rho U^\dagger\rangle}$$

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

$$\text{Convention : } E; S_2 = S_2.$$

$$(IF) \qquad \frac{}{\langle \mathbf{if}\ (\square m \cdot M[\overline{q}] = m \rightarrow S_m)\ \mathbf{fi}, \rho\rangle \rightarrow \langle S_m, M_m\rho M_m^\dagger\rangle}$$

for each outcome m

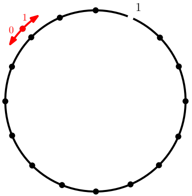
Operational Semantics

$$(L0)\qquad \frac{}{\langle \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od}, \rho\rangle \rightarrow \langle E, M_0\rho M_0^{\dagger}\rangle}$$

$$(L1)\qquad \frac{}{\langle \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S, \rho\rangle \rightarrow \langle S; \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S, M_1\rho M_1^{\dagger}}$$

Quantum 1-D Loop Walk

$$
\begin{aligned}
QW \equiv\, & c := |L\rangle; \\
& p := |0\rangle; \\
& \textbf{while } M[p] = no \textbf{ do} \\
& \quad c := H[c]; \\
& \quad c, p := S[c, p] \\
& \textbf{od}
\end{aligned}
$$



Operator Definition

$$S = \sum_{i=0}^{n-1} |L\rangle\langle L| \otimes |i \ominus 1\rangle\langle i| + \sum_{i=0}^{n-1} |R\rangle\langle R| \otimes |i \oplus 1\rangle\langle i|.$$

Denotational Semantics

Semantic function of quantum program S:

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

$$[\![S]\!](\rho) = \sum \{|\rho' : \langle S, \rho\rangle \to^* \langle E, \rho'\rangle|\} \text{ for all } \rho \in \mathcal{D}(\mathcal{H}_{\text{all}})$$

Observation:

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

for any quantum program S and 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

Motivation

A Quantum Programming Language

Floyd-Hoare Logic for Quantum Programs

Invariant Generation

Summary

Definitions

- A *quantum predicate* is a Hermitian operator (obsevable) P such that $0 \sqsubseteq P \sqsubseteq I$.

  [1] E. D'Hondt and P. Panangaden, Quantum weakest preconditions, *Mathematical Structures in Computer Science* 2006.

- A *correctness formula* is a statement of the form:

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

  where:
  - S is a quantum program
  - P and Q are quantum predicates.
  - Operator P is called the *precondition* and Q the *postcondition*.

Definitions

1. $\{P\}S\{Q\}$ is true in the sense of *total correctness*:

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

   if

$$tr(P\rho) \leq tr(Q[\![S]\!](\rho)) \text{ for all } \rho.$$

2. $\{P\}S\{Q\}$ is true in the sense of *partial correctness*:

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

   if

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

   for all ρ.

Proof System for Partial Correctness

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

(*Axiom Ini*)

$type(q) = \mathbf{Boolean}$:

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

$type(q) = \mathbf{integer}$:

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

(*Axiom Uni*) $\{U^\dagger PU\}\overline{q} := U[\overline{q}]\{P\}$

Proof System for Partial Correctness

(*Rule Seq*) $$\frac{\{P\}S_1\{Q\} \qquad \{Q\}S_2\{R\}}{\{P\}S_1;S_2\{R\}}$$

(*Rule IF*) $$\frac{\{P_m\}S_m\{Q\} \text{ for all } m}{\{\sum_m M_m^\dagger P_m M_m\}\textbf{if } (\square m \cdot M[\overline{q}] = m \rightarrow S_m) \textbf{ fi}\{Q\}}$$

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

(*Rule Ord*) $$\frac{P \sqsubseteq P' \quad \{P'\}S\{Q'\} \quad Q' \sqsubseteq Q}{\{P\}S\{Q\}}$$

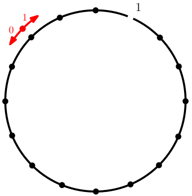
Theorem (Soundness and Completeness)

For any quantum program S and quantum predicates P, Q,

$$\models_{\text{par}} \{P\}S\{Q\} \text{ if and only if } \vdash_{PD} \{P\}S\{Q\}.$$

Quantum 1-D Loop Walk

$$
\begin{aligned}
QW \equiv\, & c := |L\rangle; \\
& p := |0\rangle; \\
& \textbf{while } M[p] = no \textbf{ do} \\
& \quad c := H[c]; \\
& \quad c, p := S[c, p] \\
& \textbf{od}
\end{aligned}
$$



Operator Definition

$$S = \sum_{i=0}^{n-1} |L\rangle\langle L| \otimes |i \ominus 1\rangle\langle i| + \sum_{i=0}^{n-1} |R\rangle\langle R| \otimes |i \oplus 1\rangle\langle i|.$$

Proof System for Total Correctness

Let P be a quantum predicate and $\epsilon > 0$. A function

$$t : \mathcal{D}(\mathcal{H}_{\mathrm{all}}) \text{ (density operators)} \rightarrow \mathbb{N}$$

is called a (P, ϵ)-*ranking function* of quantum loop:

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

if for all ρ:

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

Proof System for Total Correctness

$$(Rule\ LT)\quad \frac{\begin{array}{c}(1)\ \{Q\}S\{M_0^\dagger PM_0+M_1^\dagger QM_1\}\\ (2)\ \text{for any } \epsilon>0,\ t_\epsilon \text{ is a } (M_1^\dagger QM_1,\epsilon)-\text{ranking}\\ \text{function of loop}\end{array}}{\{M_0^\dagger PM_0+M_1^\dagger QM_1\}\mathbf{while}\ M[\overline{q}]=1\ \mathbf{do}\ S\ \mathbf{od}\{P\}}$$

Theorem (Soundness and Completeness)

For any quantum program S and quantum predicates P Q,

$$\models_{\text{tot}} \{P\}S\{Q\} \text{ if and only if } \vdash_{TD} \{P\}S\{Q\}.$$

[2] M. S. Ying, Floyd-Hoare logic for quantum programs, *ACM Transactions on Programming Languages and Systems* 2011

Outline

Super-Operator Labelled Graphs

A super-operator labelled graph is a 4-tuple $\mathcal{G} = \langle \mathcal{H}, L, l_0, \rightarrow \rangle$:

1. $\mathcal{H}$ is a Hilbert space;
2. L is a finite set of locations;
3. $l_0 \in L$ is the initial location
4. transition relation

$$l \stackrel{\mathcal{E}}{\rightarrow} l'$$

with $l, l' \in L$, $\mathcal{E}$ a super-operator: for every $l \in L$,

$$\sum \{ | \mathcal{E} : l \stackrel{\mathcal{E}}{\rightarrow} l' \text{ for some } l' | \} \approx \mathcal{I}.$$

Super-Operator Labelled Graphs

A super-operator labelled graph is a 4-tuple $\mathcal{G} = \langle \mathcal{H}, L, l_0, \rightarrow \rangle$:

1. $\mathcal{H}$ is a Hilbert space;
2. L is a finite set of locations;
3. $l_0 \in L$ is the initial location
4. transition relation

$$l \xrightarrow{\mathcal{E}} l'$$

with $l, l' \in L$, $\mathcal{E}$ a super-operator: for every $l \in L$,

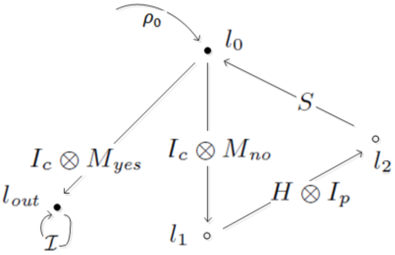
$$\sum \{ | \mathcal{E} : l \xrightarrow{\mathcal{E}} l' \text{ for some } l' | \} \approx \mathcal{I}.$$

Control-Flow Graph of Quantum Programs

A quantum program P can be represented by a graph $\mathcal{G}_P$.

Quantum 1-D Loop Walk

$$
\begin{aligned}
QW \equiv\, & c := |L\rangle; \\
& p := |0\rangle; \\
& \textbf{while } M[p] = no \textbf{ do} \\
& \quad c := H[c]; \\
& \quad c, p := S[c, p] \\
& \textbf{od}
\end{aligned}
$$



Operator Definition

$$S = \sum_{i=0}^{n-1} |L\rangle\langle L| \otimes |i \ominus 1\rangle\langle i| + \sum_{i=0}^{n-1} |R\rangle\langle R| \otimes |i \oplus 1\rangle\langle i|.$$

Invariants

- A set Π of paths is *prime* if for each

$$\pi = l_1 \stackrel{\mathcal{E}_1}{\rightarrow} ... \stackrel{\mathcal{E}_{n-1}}{\rightarrow} l_n \in \Pi$$

  its proper initial segments $l_1 \stackrel{\mathcal{E}_1}{\rightarrow} ... \stackrel{\mathcal{E}_{k-1}}{\rightarrow} l_k \notin \Pi$ for all $k < n$.

- Let $\mathcal{G} = \langle \mathcal{H}, L, l_0, \rightarrow \rangle$, Θ a quantum predicate (initial condition), $l \in L$. An *invariant* at l is a quantum predicate O such that for any density operator ρ, any prime set Π of paths from l_0 to l:

$$tr(\Theta\rho) \leq 1 - tr\left(\mathcal{E}_\Pi(\rho)\right) + tr\left(O\mathcal{E}_\Pi(\rho)\right)$$

  where $\mathcal{E}_\Pi = \sum \{|\mathcal{E}_\pi : \pi \in \Pi|\}$.

Theorem (Partial Correctness)

Let P be a quantum program. If O is an invariant at l_{out}^{P} in $\mathcal{S}_P$, then

$$\models_{par} \{\Theta\}P\{O\}$$

Inductive Assertion Maps

- Given $\mathcal{G} = \langle \mathcal{H}, L, l_0, \rightarrow \rangle$ with a cutset C and initial condition Θ.
- An *assertion map* is a mapping η from each cutpoint $l \in C$ to a quantum predicate $\eta(l)$.
- Π_l: the set of all basic paths from l to some cutpoint.
- l_π: the last location in a path π.
- An assertion map η is *inductive* if:
  - **Initiation**: for any density operator ρ:

$$tr(\Theta\rho) \leq 1 - tr\left(\mathcal{E}_{\Pi_{l_0}}(\rho)\right) + \sum_{\pi\in\Pi_{l_0}} tr\left(\eta(l_\pi)\mathcal{E}_\pi(\rho)\right);$$

  - **Consecution**: for any density operator ρ, each cutpoint $l \in C$:

$$tr(\eta(l)\rho) \leq 1 - tr\left(\mathcal{E}_{\Pi_l}(\rho)\right) + \sum_{\pi\in\Pi_l} tr\left(\eta(l_\pi)\mathcal{E}_\pi(\rho)\right).$$

Theorem (Invariance)

If η is an inductive assertion map, then for every cutpoint $l \in C$, $\eta(l)$ is an invariant at l.

Invariant Generation Problem

Given $\mathcal{G} = \langle \mathcal{H}, L, l_0, \Theta, \to \rangle$ with a cutset $C \subseteq L$. For each cutpoint $l \in C$, find a quantum predicate $\eta(l)$ such that $\eta : l \mapsto \eta(l)$ is an inductive map.

Reduce to a SDP (Semi-Definite Programming) Problem

- Assume $C = \{l_0, l_1, ..., l_m\}$.
- Write $O_i = \eta(l_i)$ for $i = 0, 1, ...m$.
- $\mathcal{E}^*_{ij} = \sum\{|\mathcal{E}^*_\pi : \text{basic path } l_i \overset{\pi}{\Rightarrow} l_j\ |\}$ for $i, j = 0, 1, ..., m$.

Theorem

Invariant Generation Problem is equivalent to find complex matrices $O_0, O_1, ..., O_m$ satisfying the constraints:

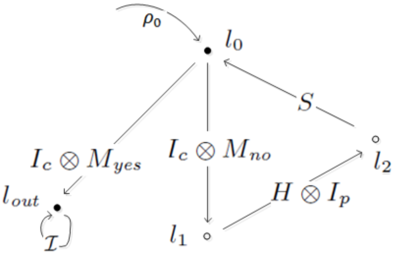
$$
\begin{aligned}
& 0 \sqsubseteq \sum_{j} \mathcal{E}_{0j}^{*}(O_j) + A, \\
& 0 \sqsubseteq \sum_{j \neq i} \mathcal{E}_{ij}^{*}(O_j) + (\mathcal{E}_{ii}^{*} - \mathcal{I})(O_i) + A_i \ (i = 0, 1, ..., m), \\
& 0 \sqsubseteq O_i \sqsubseteq I \ (i = 0, 1, ..., m),
\end{aligned}
$$

where:

$$
\begin{cases}
A = I - \sum_j \mathcal{E}_{0j}^{*}(I) - \Theta, \\
A_i = I - \sum_j \mathcal{E}_{ij}^{*}(I) \ (i = 0, 1, ..., m).
\end{cases}
$$

Quantum 1-D Loop Walk

$$
\begin{aligned}
QW \equiv\; & c := |L\rangle; \\
& p := |0\rangle; \\
& \textbf{while } M[p] = no \textbf{ do} \\
& \quad c := H[c]; \\
& \quad c, p := S[c, p] \\
& \textbf{od}
\end{aligned}
$$



Operator Definition

$$S = \sum_{i=0}^{n-1} |L\rangle\langle L| \otimes |i \ominus 1\rangle\langle i| + \sum_{i=0}^{n-1} |R\rangle\langle R| \otimes |i \oplus 1\rangle\langle i|.$$

Invariant SDPs for Quantum 1-D Loop Walk

Choose cut-set $C = \{l_0, l_3\}$ with $l_3 = l_{out}$. $\Theta = I$. Invariants O_0 and O_3 satisfy the following constraints:

$$
\begin{aligned}
0 &\sqsubseteq \mathcal{E}_{00}^*(O_0) + \mathcal{E}_{03}^*(O_3) - \Theta, && (1)\\
0 &\sqsubseteq (\mathcal{E}_{00}^* - \mathcal{I})(O_0) + \mathcal{E}_{03}^*(O_3), && (2)\\
0 &\sqsubseteq (\mathcal{E}_{33}^* - \mathcal{I})(O_3) - (I - \mathcal{E}_{33}^*(I)), && (3)\\
0 &\sqsubseteq O_0, O_3 \sqsubseteq I && (4)
\end{aligned}
$$

$\mathbb{E}_{00} = E_{00} \circ E_{00}^\dagger$, $\mathbb{E}_{03} = E_{03} \circ E_{03}^\dagger$, $\mathbb{E}_{33} = \mathcal{I}$,
$E_{00} = S(H \otimes I_p)(I_c \otimes M_{no})$, $E_{03} = I_c \otimes M_{yes}$, and I_c, I_p identities.

Invariant SDPs for Quantum 1-D Loop Walk

Choose cut-set $C = \{l_0, l_3\}$ with $l_3 = l_{out}$. $\Theta = I$. Invariants O_0 and O_3 satisfy the following constraints:

$$0 \sqsubseteq \mathcal{E}_{00}^*(O_0) + \mathcal{E}_{03}^*(O_3) - \Theta, \tag{1}$$
$$0 \sqsubseteq (\mathcal{E}_{00}^* - \mathcal{I})(O_0) + \mathcal{E}_{03}^*(O_3), \tag{2}$$
$$0 \sqsubseteq (\mathcal{E}_{33}^* - \mathcal{I})(O_3) - (I - \mathcal{E}_{33}^*(I)), \tag{3}$$
$$0 \sqsubseteq O_0, O_3 \sqsubseteq I \tag{4}$$

$\mathbb{E}_{00} = E_{00} \circ E_{00}^\dagger$, $\mathbb{E}_{03} = E_{03} \circ E_{03}^\dagger$, $\mathbb{E}_{33} = \mathcal{I}$,
$E_{00} = S(H \otimes I_p)(I_c \otimes M_{no})$, $E_{03} = I_c \otimes M_{yes}$, and I_c, I_p identities.

Solution

- $O_3 = I_c \otimes |1\rangle\langle 1| \to \mathrm{tr}(O_3\rho_{out}) \geq \mathrm{tr}(\Theta\rho_{in}) = 1$, i.e., always terminates at the position $|1\rangle$ regardless of the input state ρ_0. (O_0 omitted.)

Solving Constraints: ***Use SDP solvers***!

Applications

- Quantum walk on an *n*-circle. [3]
- Quantum Metropolis sampling on *n*-qubits. (1-qubit in [3])
- Repeat-Until-Success.
- Quantum Search.
- Quantum Bernoulli Factory.
- Recursively written Quantum Fourier Transformation.

[3] M. S. Ying, S. G. Ying and X. Wu, Invariants of quantum programs: characterisations and generation, *POPL* 2017.

Outline

Summary

Toward Automatic Verification of Quantum Programs

- scalable and principled verification!

Existing Techniques

- Quantum While-language (c. control, q. data).
- Quantum Hoare logic.
- Invariant Generation by SDPs.

Progress & Targets

- expressibility: quantum functionality, codespace, ...
- scalability: succinct or template representations, quantum verification, ...

Thank you!
Q & A

Quantum states

- The *state space* of a quantum system is a *Hilbert space* $\mathcal{H}$, i.e. a complex vector space with an inner product that is complete in the sense that every Cauchy sequence has a limit.
- For finite n, an n-dimensional Hilbert space is essentially the space $\mathbb{C}^n$ of complex vectors.
- A *pure quantum state* is represented by a *unit vector*, i.e. a vector with length 1.
- We use Dirac's notation $|\varphi\rangle, |\psi\rangle, \ldots$ to denote pure states.

Qubits

- A *Quantum bit* (qubit) is the quantum counterpart of *bit*.
- The state space of a qubit is the 2-dimensional Hilbert space.
- A pure state of qubit is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{with } |\alpha|^2 + |\beta|^2 = 1.$$

- A qubit can be in the basis states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- A qubit can also be in a superposition of $|0\rangle, |1\rangle$, e.g.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \end{pmatrix}$$

Mixed states

- A *mixed state* is represented by an *ensemble*

$$\{(p_1, |\psi_1\rangle), ..., (p_k, |\psi_k\rangle)\}$$

  meaning that the system is in state $|\psi_i\rangle$ with probability p_i.
- It is a quantum generalisation of a probability distribution over states.

Density matrices

- In the n-dimensional Hilbert space $\mathbb{C}^n$, an operator is represented by an $n \times n$ complex matrix A.
- The trace of an operator A is $tr(A) = \sum_i A_{ii}$ (the sum of the entries on the main diagonal).
- A positive semidefinite matrix ρ is called a *partial density matrix* if $tr(\rho) \leq 1$; in particular, a *density matrix* ρ is a partial density matrix with $tr(\rho) = 1$.

Mixed states = density matrices

- Matrix $|\psi\rangle\langle\psi|$ is the multiplication of column vector $|\psi\rangle$ and the row vector $\langle\psi|$ (the conjugate and transpose of $|\psi\rangle$).
- For any mixed state $\{(p_1, |\psi_1\rangle), ..., (p_k, |\psi_k\rangle)\}$,

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

  is a density operator
- For any density operator ρ, there is a mixed state $\{(p_1, |\psi_1\rangle), ..., (p_k, |\psi_k\rangle)\}$ such that

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

- In particular, a pure state $|\psi\rangle$ is identified with the density operator $\rho = |\psi\rangle\langle\psi|$.

Mixed states = density matrices

- Mixed state of a qubit:

$$\{(\frac{2}{3}, |0\rangle), (\frac{1}{3}, |-\rangle)\} \text{ with } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Density matrix:

$$\rho = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|-\rangle\langle -| = \frac{1}{6}\begin{pmatrix} 5 & -1 \\ -1 & 1 \end{pmatrix}$$

Unitary matrices

- *Dynamics* of a closed quantum system is described by a *unitary matrix*:
$$|\psi\rangle \mapsto U|\psi\rangle$$
- A matrix U is unitary if $U^\dagger U = I$, where $U^\dagger$ is the conjugate and transpose of U
- Hadamard matrix
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
is an unitary operator in the 2-dimensional Hilbert space
- $H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle$

Quantum gates – one-qubit gates

- Pauli gates:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Hadarmard gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Rotation about $x-$axis of the Bloch sphere:

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

Quantum gates – two-qubit gate

- The controlled-NOT (CNOT) gate:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- *CNOT generates entanglement*: separable state $|+0\rangle$ is transformed to EPR (Einstein-Podolsky-Rosen) pair:

$$CNOT(|+0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Super-operators

- *Dynamics* of an open quantum system is described by a *super-operator*:

$$\rho \mapsto \mathcal{E}(\rho)$$

- A super-operator is a mapping $\mathcal{E}$ from partial density operators to themselves:
  - completely positive;
  - $\mathrm{tr}(\mathcal{E}(\rho)) \leq \mathrm{tr}(\rho)$ for all ρ.
- A super-operator can be seen as a quantum counterpart of a transformation of probability distributions.

Kraus representation

- Löwner order: $A \sqsubseteq B$ if and only if $B - A$ is positive semidefinite.
- Each super-operator $\mathcal{E}$ has a Kraus representation:

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

  for all density matrices ρ, where the set $\{E_i\}$ of matrices satisfies the sub-normalisation condition: $\sum_i E_i^\dagger E_i \sqsubseteq I$
- We often write $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$.

Quantum measurements

- The way to extract information about a quantum system is quantum measurement.
- In quantum computation, measurement is used to read out a computational result.
- A *measurement* is modelled as a set of operators $M = \{M_m\}$ with $\sum_m M_m^\dagger M_m = I$.
- If a quantum system was in pure state $|\psi\rangle$ before the measurement, then:
  - the probability that measurement outcome is λ:

    $$p(m) = ||M_m|\psi\rangle||^2$$

    where $||\cdot||$ is the length of vector.
  - the state of the system after the measurement:

    $$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}$$

Quantum measurements

- If we perform a measurement M on a system in state ρ, then:
  - an outcome m is observed with probability $p(m) = \mathrm{tr}\big(M_m \rho M_m^\dagger\big)$;
  - after that, the system will be in state $M_m \rho M_m^\dagger / p(m)$.

- A major difference between classical and quantum systems:
  - *Measuring a classical system does not change its state.*
  - *The state of a quantum systems is changed after measuring it.*

Quantum measurements – example

- The measurement on a qubit in the computational basis $\{|0\rangle, |1\rangle\}$ is $M = \{M_0, M_1\}$:

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- If we perform M on a qubit in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:
  - the probability that we get outcome 0 is $|\alpha|^2$;
  - the probability that we get outcome 1 is $|\beta|^2$.
- If we perform M on a qubit in (mixed) state

$$\rho = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|+\rangle\langle +| = \frac{1}{6}\begin{pmatrix} 5 & 1 \\ 1 & 1 \end{pmatrix}$$

  - the probability that we get outcome 0 is $p(0) = tr\,(M_0 \rho M_0) = \frac{5}{6}$ and then the quibit is in state $|0\rangle$.
  - Outcome 1 is obtained with probability $p(1) = \frac{1}{6}$ and after that the qubit is in $|1\rangle$.