Introduction to Quantum Computing

Gabriel Ribeiro Fernandes

October 2025

1   Introduction

(see Introduction slides)

2 Section 2

2.1 Section 2.1

(Nielsen and Chuang section 1.2)

Classical bits: 0, 1
Quantum bits "qubits": superposition of 0 and 1

A quantum state $|\psi\rangle$ is described as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \alpha, \beta \in \mathbb{C}$$

with $|\alpha|^2 + |\beta|^2 = 1$ (normalisation)

ket-notation: $|\psi\rangle$ (motivation from inner product)
Mathematical description: $|\psi\rangle \in \mathbb{C}^2$, with

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Different from a classical bit, one cannot (in general) directly ovserve/measure a qubit (the amplitudes α and β).

Instead "standard measurement" will result in:

0 with probability $|\alpha|^2$.

1 with probability $|\beta|^2$.

The measurement also changes the qubit ("wavefunction collapse"):
If meausuring 0, the qubit will be $|\psi\rangle = |0\rangle$ directly after the measurement, and likewise if measuring 1, the qubit will be $|\psi\rangle = |1\rangle$.

In practice: One can estimate the probabilities $|\alpha|^2$ and $|\beta|^2$ in experiments by replicating the same experiment many times (i.e. via outcomes satistics).
The repetitions are called "trials" or "shots".

Circuit notation:
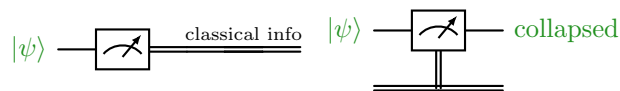
What is a qubit physicaly?
Many possible realizations, e.g. $|0\rangle$ and $|1\rangle$ are:

- two different polarizations of a photon, e.g. left/right circular.
- alignment of a nuclear or eletronic spin: $\uparrow, \downarrow$.

- ground state or excited state of an atom (electronic state).
- clockwise or counter-clockwise loop current states in a Josephson junction "superconducting qubit".

A useful graphical depiction of a qubit is the <u>Bloch sphere</u> representation:
If α and β happen to be real-valued, then we can find an angle $\theta \in \mathbb{R}$ such that:
(TODO: make figure and split math and added Bloch sphere)

$$\alpha = \cos\left(\frac{\theta}{2}\right), \beta = \sin\left(\frac{\theta}{2}\right)$$

$$(\rightsquigarrow |\alpha|^2 + |\beta|^2 = \cos\left(\frac{\theta}{2}\right)^2 + \sin\left(\frac{\theta}{2}\right)^2 = 1 \checkmark)$$

In general we represent α, β, (TODO: Add figure with Im Re sphere)

$$\alpha = e^{i\gamma} \cos\left(\frac{\theta}{2}\right)$$

$$\beta = e^{i(\gamma+\varphi)} \sin\left(\frac{\theta}{2}\right)$$

using so-called phase angles γ for α and $\gamma + \varphi$ for β.

Then:

$$|\psi\rangle = e^{i\gamma} \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\gamma+\varphi)} \sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$= e^{i\gamma}(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right)|1\rangle) \qquad | \; e^{i\gamma} \text{ can be ignored here}$$

Thus $|\psi\rangle$ is characterized by two angles θ and φ.
(TODO: start figure split here with Boch sphere)
They specify the point defined as:

$$\vec{r} \begin{pmatrix} cos(\varphi)sin(\theta) \\ sin(\varphi)sin(\theta) \\ cos(\theta) \end{pmatrix}$$

on the surface of a sphere specifically a <u>Bloch sphere</u> (Felix Bloch).
Exercice: why are $|0\rangle$ and $|1\rangle$ at the poles?
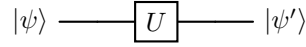
2.2 Single qubit gates

(Nielsen and Chang sections 1.3.1, 2.1.8, 4.2)
Principle of <u>time evolution</u>: the quantum state $|\psi\rangle$ at current time point t transitions to a new quantum state $|\psi'\rangle$ at a later time t' $\geq$ t.
The transition will always be described by a complex unitary matrix U.

$$|\psi'\rangle = U \cdot |\psi\rangle$$

Circuit notation:

$$|\psi\rangle \;\rule{1cm}{0.4pt}\; \boxed{U} \;\rule{1cm}{0.4pt}\; |\psi'\rangle$$

Notes:

- The circuit is read from left to right, but the matrix time vector ($U\,|\psi\rangle$) from right to left.

- U preserves normalisation.

Examples:

- quantum analogue of classical NOT-gate ($0 \leftrightarrow 1$) flip $|0\rangle \leftrightarrow |1\rangle$
  $\rightsquigarrow$ Pauli-X gate:

$$X \equiv \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(check: $x\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$)
analogue for 1 to 0.

- Pauli-Y gate:

$$Y \equiv \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- Pauli-Z gate:

$$Z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Z leaves $|0\rangle$ unchanged, but flips the sign of the coefficient of $|1\rangle$.

Recall the block sphere representation of a general quantum state:

$$|\psi\rangle = cos(\frac{\theta}{2})\,|0\rangle + e^{i\varphi}sin(\frac{\theta}{2})\,|1\rangle$$

Then:

$$Z\,|\psi\rangle = cos(\frac{\theta}{2})\,|0\rangle - e^{i\varphi}sin(\frac{\theta}{2})\,|1\rangle \tag{1}$$

$$= cos(\frac{\theta}{2})\,|0\rangle + e^{i(\varphi+\pi)}sin(\frac{\theta}{2})\,|1\rangle \qquad \text{(with } e^{i\pi} = -1\text{)} \tag{2}$$

$\rightsquigarrow$ new Block sphere angles: $\theta' = \theta$, $\varphi' = \varphi + \pi$
(rotation by $\pi = 180\deg$ around z-axis)
x, y and z gates are called Pauli matrices.
The <u>Pauli vector</u> $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (x, y, z)$ is a vector of 2x2 matrices.

- Hadamard gate:

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

$$\alpha \left| 0 \right\rangle + \beta \left| 1 \right\rangle \longrightarrow \boxed{H} \longrightarrow \alpha \frac{\left| 0 \right\rangle + \left| 1 \right\rangle}{\sqrt{2}} + \beta \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}}$$

- Phase gate:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- T gate:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i \frac{\pi}{4}} \end{pmatrix}$$

Note: $T^2 = S$ (since $(e^{i\frac{\pi}{4}})^2 = e^{i\frac{\pi}{2}} = i$); $T^4 = S^2 = Z$

Pauli matrices satisfy:

$\sigma_j^2 = identity.$

$\sigma_j \cdot \sigma_k = -\sigma_k \cdot \sigma_j$ for all $j \neq k$

Commutator: $[\sigma_j, \sigma_k] := \sigma_j \sigma_k - \sigma_k \sigma_j = 2i \, \sigma_l$ for (j, k, l) — which is a cyclic permutation of (1,2,3)

Matrix exponential and rotation gates $R_x(\theta) \, R_y(\theta), R_z(\theta)$ (pdf in Moodle) Z-Y decomposition of an arbitrary 2x2 matrix:
For any unitary matrix $U \in \mathbb{C}^{2x2}$ there exists real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that:

$$U = e^{i\alpha} \cdot R_z(\beta) \cdot R_y(\gamma) \cdot R_z(\delta) = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\gamma}{2}\right) & -\sin\left(\frac{\gamma}{2}\right) \\ \sin\left(\frac{\gamma}{2}\right) & \cos\left(\frac{\gamma}{2}\right) \end{pmatrix} \cdot \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}$$

2.3 Multiple qubit

(Nielsen and Chang sections 1.2.1, 2.1.7)

So far: single qubits, superposition of basis states $\left| 0 \right\rangle$ and $\left| 1 \right\rangle$.
For two qubits, this generalises to:

     $\left| 00 \right\rangle, \left| 01 \right\rangle, \left| 10 \right\rangle, \left| 11 \right\rangle$

as computational basis states: all combinations (bitstrings) of 0s and 1s.
General two-qubit state:

$$\left| \psi \right\rangle = \alpha_{00} \left| 00 \right\rangle + \alpha_{01} \left| 01 \right\rangle + \alpha_{10} \left| 10 \right\rangle + \alpha_{11} \left| 11 \right\rangle$$

with amplitudes $\alpha_{ij} \in \mathbb{C}$ such that:

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad \text{(normalization)}$$

Can identify the basis states with unit vectors:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Thus:

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4$$

What happens if we measure only one qubit of a two-qubit state?
Say we measure the first qubit: obtain the result.

0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$

Wavefunction directly after measurement:

if we measured 0: $|\psi'\rangle = \dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

if we measured 1: $|\psi'\rangle = \dfrac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$

Mathematical formalism for constructing two-qubit states:
Tensor product of vector spaces can combine two (arbitrary) vector spaces V and W to form the tensor product $V \otimes W$.
(Look into the "Tensor products of vector spaces" — Moodle)

Generalisation to n qubits: 2^n computational basis states
$\{|0,\ldots,0\rangle, |0,\ldots,0,1\rangle, |0,\ldots,1,0\rangle, \ldots, |1,\ldots,1\rangle\}$ (all bit strings of length n)
Thus, a general n-qubit quantum state, also denoted as "quantum register", is given by:

$$|\psi\rangle = \sum_{x_0=0}^{1} \sum_{x_1=0}^{1} \cdots \sum_{x_{n-1}=0}^{1} \alpha_{x_{n-1},\ldots,x_1,x_0} |x_{n-1}\ldots x_1 x_0\rangle \tag{3}$$

$$= \sum_{x=0}^{2^n-1} \alpha_x |x\rangle \qquad \text{binary representation}$$

$$\tag{4}$$

with $\alpha_x \in \mathbb{C}$ for all $x \in \{0,\ldots,2^n-1\}$ such that:

$$\||\psi\rangle\|^2 = \sum_{x=0}^{2^n-1} |\alpha_x|^2 \overset{!}{=} 1 \quad \text{(normalisation)}$$

7

$\rightsquigarrow$ in general "hard" to simulate on a classical computer (for large n) due to this "curse of dimensionality".

Vector space as tensor products: $\underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{\text{n times}} = (\mathbb{C}^2)^{\otimes n} \approx \mathbb{C}^{(2^n)}$

2.4   Multiple qubit gates

(Nielsen and Chuang sections 1.3.2, 1.3.4, 2.17)

As for single qubits, an operation on multiple qubits is described by an unitary matrix U.
For n qubits: $U \in \mathbb{C}^{2^n \times 2^n}$

Example: Controlled-NOT gate (also denoted CNOT)
two qubits: control and target
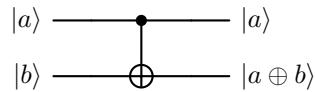target qubit gets flipped if control is 1:

$$\underbrace{|00\rangle}_{control|target} \mapsto \quad |00\rangle,$$

$$|01\rangle \mapsto |01\rangle, \; |10\rangle \mapsto |11\rangle, \; |11\rangle \mapsto |10\rangle$$

Can be expressed as:

$$|ab\rangle \mapsto |a, a \oplus b\rangle, \forall a, b \in \{0, 1\} \qquad |a \oplus b \text{ defined as "addition modulo 2"}$$
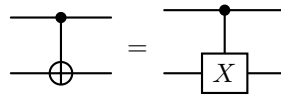
Circuit notation:

$$|a\rangle \quad\longrightarrow\bullet\longrightarrow\quad |a\rangle$$
$$|b\rangle \quad\longrightarrow\oplus\longrightarrow\quad |a \oplus b\rangle$$

Matrix Representation:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \boxed{0 & 1} \\ 0 & 0 & \boxed{1 & 0} \end{pmatrix} Pauli - X$$
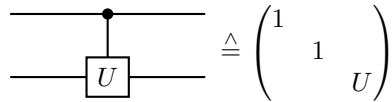
This matrix is unitary.
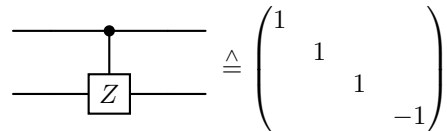Alternative notation:

(circuit) $=$ (circuit with X)

We can generalise Pauli-X to any unitary single-qubit gate U acting on the target qubit $\leadsto$ controlled U-gate:

$$|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |1\rangle \otimes (U |0\rangle), |11\rangle \mapsto (|1\rangle \otimes (U |1\rangle)$$
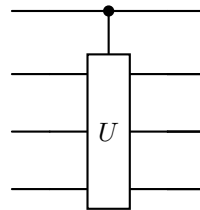
9

Generalisation:

$$
\begin{array}{c}\text{(controlled-U circuit)}\end{array} \quad \triangleq \begin{pmatrix} 1 & & \\ & 1 & \\ & & U \end{pmatrix}
$$

Example: controlled-z:

$$
\begin{array}{c}\text{(controlled-Z circuit)}\end{array} \quad \triangleq \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}
$$

Exercice: show that controlled-z gate is invariant when flipping control and target qubits.
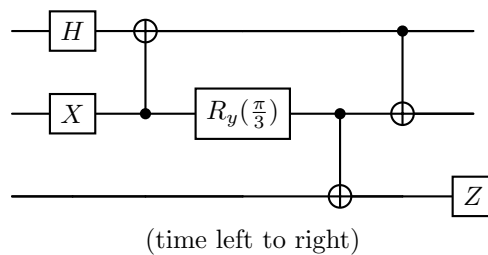
Controlled-U gate for multiple target qubits:

Note: single qubit and CNOT gates are universal: they can be used to implement an arbitrary unitary operation on n qubits.
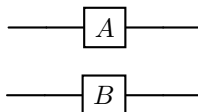(Quantum analogue of universality of classical NAND gate)
proof in Nielsen and Chang section 4.5
Example of a circuit consisting only of single qubit gates and CNOTs:

(time left to right)

Matrix Kronecker products: matrix representation of single qubit gates acting in parallel:

10

Operation on basis states: $a, b \in \{0, 1\}$

$$\underbrace{|a, b\rangle}_{|a\rangle \otimes |b\rangle} \mapsto (A\,|a\rangle) \otimes (B\,|b\rangle) = (A \otimes B)\,|a, b\rangle$$

Example: A = I (identity), B = Y:

$$|00\rangle \mapsto |0\rangle \otimes \underbrace{(Y\,|0\rangle)}_{i|1\rangle} = i\,|01\rangle$$

$$|01\rangle \mapsto |0\rangle \otimes \underbrace{(Y\,|1\rangle)}_{-i|0\rangle} = -i\,|00\rangle$$

$$|10\rangle \mapsto |1\rangle \otimes (Y\,|0\rangle) = i\,|11\rangle$$

$$|11\rangle \mapsto |1\rangle \otimes (Y\,|1\rangle) = -i\,|10\rangle$$

Matrix Representation:
(ket on the left of mapto represents column and resulting one on the row)

$$\hat{=} \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} Pauli - Y = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} = I \otimes Y$$

General formula: <u>Kronecker product</u> (matrix representation of tensor products of operators)

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp \times nq}$$

$\forall A \in \mathbb{C}^{m \times n}, B \in \mathbb{C}^{p \times q}$ (NumPy np.kron(A, B))
Generalise to arbitrary number of tensor factors, e.g.

$$\hat{=} A \otimes B \otimes C = (A \otimes B) \otimes C = A \otimes (B \otimes C)$$

Basic properties:

(a) $(A \otimes B)^* = A^* \otimes B^*$ (elementwise complex conjugation)

(b) $(A \otimes B)^T = A^T \otimes B^T$ (transposition)

(c) $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

(d) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ (associative property)

(e) $\underbrace{(A \otimes B) \cdot (C \otimes D)}_{\text{matrix-matrix multiplication}} = (A \cdot C) \otimes (B \cdot D)$

for matrices of compatible dimensions.

(side exchange because its read from left to right)

(f) Kronecker product of Hermitian matrices is Hermitian

(g) Kronecker product of unitary matrices is unitary (follows from (c) & (e))

2.5 Quantum measurements

(Nielsen and Chuang sections 1.3.3, 2.2.3, 2.2.5)
Review: measurement of a single qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ with respect to computational basis $|0\rangle$, $|1\rangle$:

classical data (measurement outcome 0 or 1)
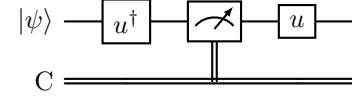
alternative notation:

qubit after measurement (collapsed wavefunction)

measurement outcome

Unitary freedom of choice of measurement basis.

Given an orthonormal basis (ONB) $\{|u_1\rangle, |u_2\rangle\}$, we can measure with respect to this orthonormal basis by performing a base change before and after the measurement:

$U = (|u_1\rangle |u_2\rangle) \in \mathbb{C}^{2\times2}$ unitary

$|\psi\rangle$ ── $u^\dagger$ ── 📐 ── u ──

C ════════════════════

(measurement with respect to $\{|u_1, |u_2\rangle\rangle\}$, using a standard basis measurement)

Representing the qubit $|\psi\rangle = \alpha_1 |u_1\rangle + \alpha_2 |u_2\rangle$, $\alpha_1, \alpha_2 \in \mathbb{C}$

$|\psi\rangle$ ── $U^\dagger$ ── $\leadsto U^\dagger |\psi\rangle = \alpha_2 |0\rangle \alpha_1 \beta |1\rangle$ $(U^\dagger |u_1\rangle = |0\rangle, U^\dagger |u_2\rangle = |1\rangle)$

We will obtain measurement result 0 or 1 with the respective probabilities $|\alpha_1|^2$ and $|\alpha_2|^2$

After measuring and applying U: $|\psi\rangle$ will be in the state $|u_1\rangle$ or $|u_2\rangle$.

Abstract, general defenition of quantum measurements

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the quantum system, with the index m labelling possible measurement outcomes.

Denoting the quantum state before the measurement by $|\psi\rangle$, result m occurs with probability:

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

state after the measurement is:

$$\frac{M_m |\psi\rangle}{\|M_m |\psi\rangle\|}$$

The measurement operators satisfy the completeness relation:

$$\sum_m M_m^\dagger M_m = I,$$

such that the probabilities sum to 1:

$$\sum_m p(m) = \sum_m \langle\psi| \underbrace{\sum_m M_m^\dagger M_m}_{I} |\psi\rangle = \langle\psi|\psi\rangle = 1$$

Example: measurement of a qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ with respect to computational basis $\{|0\rangle, |1\rangle\}$:

$$M_0 := \underbrace{|0\rangle \langle 0|}_{\text{outer product}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$M_1 := |1\rangle \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rightsquigarrow p(0) = \langle \psi | M_0^\dagger M_0 |\psi\rangle = \langle \psi | M_0 |\psi\rangle \qquad = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= |\alpha|^2$$

$$p(1) = \langle \psi | M_1^\dagger M_1 |\psi\rangle = \dots \qquad = |\beta|^2$$

Projective measurements
$\rightsquigarrow$ see projection-operators (moodle)

Definition: a projective measurement is described by an observable M, a Hermitian operator acting on the quantum system spectral decomposition $\rightsquigarrow$

$$M = \sum_m \lambda_m P_m$$

with P_m: projection onto the eigenspace with eigenvalue λ_m.
The possible outcomes of the measurement correspond to the eigenvalues λ_m.
Probability of obtaining measurement result λ_m :

$$p(\lambda_m) = \langle \psi | P_m |\psi\rangle \quad | P_m^\dagger P_m = P_m \text{ since } P_m \text{ is a projection}$$

State of the quantum system after the measurement:

$$\frac{P_m |\psi\rangle}{\| P_m |\psi\rangle \|} = \frac{P_m |\psi\rangle}{\sqrt{p(\lambda_m)}}.$$

Remarks:

- Projective measurements are special cases of a general measurement framework

- Projective measurement combined with transformations (and auxiliary qubit) are equivalent to the general measurement formalism/framework. (Proof: see pages 94, 95 in Nielsen and Chuang)

Average value of a projective measurement

$$\mathbb{E}[M] = \sum_m \lambda_m p(\lambda_m) = \sum_m \lambda_m \langle \psi | P_m |\psi\rangle$$

$$= \langle \psi | \sum_m \lambda_m P_m |\psi\rangle = \langle \psi | M |\psi\rangle =: \langle M \rangle \quad |\text{if } |\psi\rangle \text{ is clear from context.}$$

Corresponding <u>standard deviation</u>:

$$\Delta(M) := \sqrt{\langle M^2 \rangle - \langle M \rangle^2} \qquad \text{|with } \langle M^2 \rangle = \langle \psi | M^2 | \psi \rangle$$
$$= \sqrt{\langle M - \langle M \rangle \rangle^2}$$

Examples:

- Measuring a qubit w.r.t. (with respect to) computational basis $\{|0\rangle, |1\rangle\}$ is actually a projective measurement: $P_0 = |0\rangle \langle 0|, P_1 = |1\rangle \langle 1|$
  $p(0) = \langle \psi | P_0 | \psi \rangle = \langle \psi | 0 \rangle \langle 0 | \psi \rangle = |\langle 0 | \psi \rangle|^2$
  $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \rightsquigarrow |\langle 0 | \psi \rangle|^2 = |\alpha|^2$

- In general: measurement w.r.t. orthogonal basis $|u_1\rangle, |u_2\rangle$ is a projective measurement:
  $$\text{set } P_m = |u_m\rangle \langle u_m| \text{ for } m = 1, 2$$

Define observable M by

$$M := \sum_{m=1}^{2} \lambda_m P_m \text{ with arbitrary } \lambda_1, \lambda_2 \in \mathbb{R}, \lambda_1 \neq \lambda_2$$

- Measuring Pauli-Z (as observable):

$$z = 1 \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{P_0 = |0\rangle \langle 0|} + (-1) \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{P_1 = |1\rangle \langle 1|}$$

Agrees with standard measurement w.r.t. the computational basis $\{|0\rangle, |1\rangle\}$.

2.6 The Heisenberg uncertainty principle

Supose C and D are two observables and $|\psi\rangle$ a quantum state.
Then:
$$\Delta(C) \cdot \Delta(D) \geq \frac{|\langle \psi | [C, D] | \psi \rangle|}{2} \qquad [A, B] := AB - BA$$

Interpretation for experiment: repeated preparation of $|\psi\rangle$, measure C in some cases and D in the other cases to obtain the standard deviations $\Delta(C)$ and $\Delta(D)$.

Remark: "popular statement: $C \hat{=} \hat{x}$ (position operator)
$D \hat{=} \hat{p}$ (momentum operator)

$\rightsquigarrow$ see handout Heisenberg-uncertainty-principle.pdf for derivation.

3 Entanglement and and its applications

(Albert Einstein (1947): "spooky action at a distance")

A n-qubit state $|\psi\rangle$ ($n \geq 2$) is called entangled if it cannot be written as tensor product of single qubit states, i.e. $|\psi\rangle = |\varphi_{n-1}\rangle \otimes \ldots \otimes |\varphi_0\rangle$ for any $|\varphi_0\rangle, \ldots, |\varphi_{n-1}\rangle \in \mathbb{C}^2$

$$|\varphi_0\rangle \;\text{———}$$
$$|\varphi_1\rangle \;\text{———}$$
$$\vdots \;\text{———}$$
$$|\varphi_{n-1}\rangle \;\text{———}$$

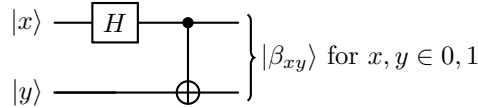Example: Bell states, also denoted EPR states (Einstein-Podolsky-Rosen)

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |a\rangle |b\rangle$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Quantum circuit to create Bell states:

$\left.\begin{array}{c} |x\rangle \;-\;\boxed{H}\; \\ |y\rangle \end{array}\right\} |\beta_{xy}\rangle$ for $x, y \in 0, 1$

3.1 Quantum teleportation

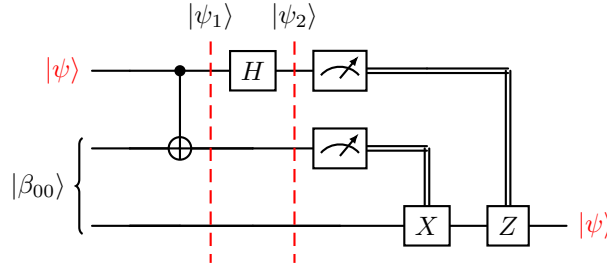(Nielsen and Chuang section 1.3.7)

Scenario: two (experimental physicists) Alice and Bob are far away from each other. When visiting eachoter in the past, they generated the EPR pair $|\beta_{00}\rangle$, each keeping one qubit of the pair.

Alice's task is to send another (unknown) qubit state $|\psi\rangle$ to Bob.

Note: measurement is not an option.

Quantum circuit for teleporting $|\psi\rangle$:

Input:

$$|\psi\rangle |\beta_{00}\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (|00\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle))$$

after CNOT:
$\frac{1}{\sqrt{2}}(\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle))$

after Hadamard:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$
$$= \frac{1}{2}(\alpha |000\rangle + \alpha |011\rangle + \alpha |100\rangle + \alpha |111\rangle + \beta |010\rangle + \beta |001\rangle - \beta |110\rangle - \beta |101\rangle)$$
$$= \frac{1}{2} |00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)$$

Now Alice measures her qubits w.r.t computational basis.
Projective measurement with

$$P_1 = |00\rangle \langle 00| \otimes I, \ P_2 = |01\rangle \langle 01| \otimes I,$$
$$P_3 = |10\rangle \langle 10| \otimes I, \ P_4 = |11\rangle \langle 11| \otimes I$$

If Alice measures 00, then $|\psi_2\rangle$ will collapse to:

$$|00\rangle (\alpha |0\rangle + \beta |1\rangle) = |00\rangle |\psi\rangle \text{ (qubit at bobs place)}$$

similary:

$$00 \longrightarrow \alpha |0\rangle + \beta |1\rangle$$
$$01 \longrightarrow \alpha |1\rangle + \beta |0\rangle$$
$$10 \longrightarrow \alpha |0\rangle - \beta |1\rangle$$
$$11 \longrightarrow \alpha |1\rangle - \beta |0\rangle$$

Alice transmits her measurement results to Bob (classical information).
Bob then applies Pauli-X and/or Pauli-Z if necessary to recover the original state $|\psi\rangle$.
Even though the wavefunction collapse is instantanious, it does not allow for "faster-than-light" information transfer due to the required classical communication and the randomness of the measurement outcome.

3.2 EPR and the Bell inequality

(Nielsen and Chuang section 2.6)
(Albert Einstein (1926): "god does not play dice")

EPR (Einstein-Podolsky-Rosen) paper:
"Can quantum mechanical description of physical reality be considered complete?"

The authors argue that quantum mechanics is incomplete, since it lacks certain "elements of reality" (properties that can be predicted with certainty).

Scenario: Alice and Bob are far away from eachother but share the entangled two-qubit "spin-singlet" state
$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
Alice and Bob measure the observable $\vec{v} \circ \vec{\sigma} = v_1 X + v_2 Y + v_3 Z$
(with $\vec{v} \in \mathbb{R}^3, \|\vec{v}\| = 1$) on their respective qubit.
Recall that $\vec{v} \circ \vec{\sigma}$ is Hermitian and unitary and has eigenvalues ± 1.
Alice performs her measurement immediatly before Bob.

Example:

- $\vec{v} = (0,0,1)$, observable $Z = 1 \cdot |0\rangle \langle 0| + (-1) \cdot |1\rangle \langle 1|$ | (standard measurement)
  if Alice measures the eigenvalue:

    1: wavefunction collapses to $|01\rangle$

    -1: wavefunction collapsed to $|10\rangle$

  $\rightsquigarrow$ Bob will always obtain the opposite measurement result.

- $\vec{v} = (1,0,0)$: observable X, eigenstates $|\pm\rangle = \frac{1}{\sqrt{2}}(\alpha |0\rangle \pm \beta |1\rangle)$
  (measurement w.r.t. $|+\rangle, |-\rangle$ basis)
  We can represent the wavefunction as:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$$

  namely:

$$-\frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) = -\frac{1}{\sqrt{2}}(\frac{1}{2}(\alpha |0\rangle + \beta |1\rangle)(\alpha |0\rangle - \beta |1\rangle) - \frac{1}{2}(\alpha |0\rangle - \beta |1\rangle)(\alpha |0\rangle + \beta |1\rangle))$$
$$= \dots$$
$$= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$= |\beta_{11}\rangle$$

18

If Alice measures eigenvalue 1, the wavefunction will collapse to $|+-\rangle \rightsquigarrow$ Bob's qubit is in state $|-\rangle$.
So he will certainly measure eigenvalue (-1). (conversly if Alice measures -1)

- general observable $\vec{v} \circ \vec{\sigma}$, general unit vector $\vec{v} \in \mathbb{R}^3$: denote the orthogonal eigenstates of $\vec{v} \circ \vec{\sigma}$ by $|a\rangle, |b\rangle$, then there exist complex numbers α, β, γ and δ such that:

$$|0\rangle = \alpha |\alpha\rangle + \beta |\beta\rangle$$
$$|1\rangle = \gamma |\alpha\rangle + \delta |\beta\rangle$$

Inserted into $|\beta_{11}\rangle$ (see also Exercice 8.1(a)):

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \underbrace{(\alpha\delta - \beta\gamma)}_{det(U) \text{ with } U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}} \frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$$

U is a base change matrix between the orthonormal $\{|0\rangle, |1\rangle\}$ and $\{|a\rangle, |b\rangle\}$ basis $\rightsquigarrow$ U unitary $\rightarrow |det(U)| = 1$ (Ex. 1.2(e)) Can represent det(U) = $e^{i\theta}, \theta \in \mathbb{R}$
In summary: $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = e^{i\theta}\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$
$\rightsquigarrow$ as before: Bob will obtain opposite measurement result as Alice.
Therefore Alice can predict Bob's measurement result.

However, there is no possibility that alice could influence Bob's measurement (after performing her measurement) since they are far apart (speed of light is too slow)
EPR argument: "property" $\vec{v} \circ \vec{\sigma}$ of a qubit is an "element of reality".
Quantum mechanics does not a priori specify this property for all possible $\vec{v}$ (but only probabilities), and is thus an incomplete description of reality.

Instead: "hidden variable theory": there must be additional variables "hidden" in a qubit which determines Bob's measurement of $\vec{v} \circ \vec{\sigma}$ for all possible $\vec{v} \in \mathbb{R}^3$.

(Niels Bohr (October 1927): "Stop telling God what to do.")
Bell's inequality: experimental test which can <u>invalidate</u> local hidden variable theories. (Bell 1964)

"<u>local</u>": no faster-than-light communication possible (otherwise one could send information backwards in time according to special relativity)
Experimental schematic: many repetitions (to collecect satistics of the following setup):
"TODO import image"

- Charlie: prepares two particles one for Alice and one for Bob.

- Alice: decides randomly whether to measure Q or R.

- Bob: decides randomly whether to measure S or T.

Binary property values: $Q \in \pm 1, R \in \pm 1, S \in \pm 1, T \in \pm 1$.
Alice and Bob perform their measurement (almost) simultaniously, such that no information about the result can be transmitted in between them.
After this protocol, Alice and Bob meet to analyze their measurement data.
Consider the quantity:

$$Q \cdot S + R \cdot S + R \cdot T - Q \cdot T = \underbrace{(Q + R)}_{\pm 2 \,\vee\, 0} \cdot S + \underbrace{(R - Q)}_{0 \,\vee\, \pm 2} \cdot T = \pm 2$$

Denote by p(q,r,s,t) the proability that the system is in the state $\{Q = q, R = r, S = s, T = t\}$ before this measurements , then we compute the average value:

$$\mathbb{E}[Q \cdot S + R \cdot S + R \cdot T - Q \cdot T] = \sum_{p,r,s,t \in \pm 1} p(q,r,s,t) \cdot \underbrace{(q \cdot s + r \cdot s + r \cdot t - q \cdot t)}_{\pm 2}$$

$$\leq \sum_{p,r,s,t \in \pm 1} p(q,r,s,t) \cdot 2 = 2$$

By linearity of $\mathbb{E}[]$, we arrive at the following:

Bell inequality:

$$\mathbb{E}[Q \cdot S] + \mathbb{E}[R \cdot S] + \mathbb{E}[R \cdot T] + \mathbb{E}[Q \cdot T] \leq 2$$

Each term can be experimentally evaluated, e.g. $\mathbb{E}[Q \cdot S]$: Alice and Bob average over cases where Alice measured Q and Bob measured S.

Compare with a "quantum" realization of the experiment:
    Charlie prepares the two-qubit singlet state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

and sends the first qubit to Alice and the 2nd to Bob.

Observables:

$Q = Z_1$ ($_1 \rightarrow$ *first qubit (Alice)*) $S = \dfrac{-Z_2 - X_2}{\sqrt{2}}$ ($_2 \rightarrow$ *second qubit (Bob)*)

$R = X_1$ $T = \dfrac{Z_2 - X_2}{\sqrt{2}}$

Measurement averages (c.f. Exercise 8.1)
$\langle Q \cdot S \rangle = \langle \psi | Q \otimes S | \psi \rangle = \frac{1}{\sqrt{2}}$, $\langle R \cdot S \rangle = \frac{1}{\sqrt{2}}$
$\langle R \cdot T \rangle = \frac{1}{\sqrt{2}}$, $\langle Q \cdot T \rangle = -\frac{1}{\sqrt{2}}$

$\langle Q \cdot S \rangle + \langle R \cdot S \rangle + \langle R \cdot T \rangle - \langle Q \cdot T \rangle = 2\sqrt{2} \nleq 2$ (violates Bell's inequality!)

Actual laboratory experiments using photons agree with predictions by quantum mechanics thus not all (implicit) assumptions leading to Bell's inequality can be satisfied.

- "realism": physical properties Q, S, R, T have definit values independent of observation (measurement)

- "locality": Alice performing her measurement cannot influence Bob's measurementand vice versa.

⤳ Nature is not "locally realistic" (most common viewpoint: realism does not hold)
Practical lesson: we can use entanglement as a ressource.

(John Wheeler: If you are not completely confused by quantum mechanics, you do not understand it.)

4 Quantum search algorithms

(Nielsen and Chuang: section 6)

Classical search through N unordered elements: O(N)
Quantum Groover's algorithm: $O(\sqrt{N})$ (under certain preconditions)

4.1 Quantum oracles

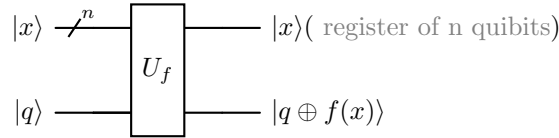Search space of $N = 2^n$ elements, labelled 0, 1, …, N-1.
Assume there are M solutions (with $1 \leq M \leq N$)
Define the corresponding <u>indicator function</u> $f : 0, \ldots, N-1 \to 0, 1$

$$f(x) = \begin{cases} 0, & \text{if element x is } \underline{\text{not}} \text{ a solution} \\ 1, & \text{if element x } \underline{\text{is}} \text{ a solition} \end{cases}$$

Quantum version of f?
⇝ quantum "oracle" U_f defined for computational basic states

Notes:
With $x = x_{n-1} \ldots x_1 x_0 \Rightarrow |x\rangle = |x_{n-1}\rangle \ldots |x_1\rangle |x_0\rangle$.
U_f maps basis states to basis states and satisfies $U_f^2 = I(q \oplus f(x) \oplus f(x) = q)$
Thus U_f permites basis states and is in particular unitary.

Initialize the oracle in superpositions $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \overset{U_f}{\longmapsto} \begin{cases} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ |x\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases}$$

In summary: $|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \overset{U_f}{\longmapsto} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ | (oracle qubit unchanged)

Effective action of oracle: $|x\rangle \longrightarrow \boxed{U_f} \longrightarrow (-1)^{f(x)} |x\rangle$

⇝ oracle "marks" solutions by a phase flip.

How could one construct such an oracle without knowing the solution already?
Example: factorisation of a large integer $m \in N$:
   Finding prime factors of m is "difficult" on a classical computer:
   (no known algorithm with polynomial runtime in the bitlength of m)
But testing whether a given $x \in \mathbb{N}$ divides m is simple.
One can perform arithmetic operations for trial division on a digital quantum
computer as well ⇝ oracle which recognizes a solution x. (Remark: "better"
quantum algorithm for integer factorisation: Shor's algorithm.)

4.2   Grover's Algorithm

Search space with $N = 2^n$ element and M solutions; overall circuit diagramm for Grover's algorithm: (Apply G $O(\sqrt{\frac{N}{M}})$ times.)
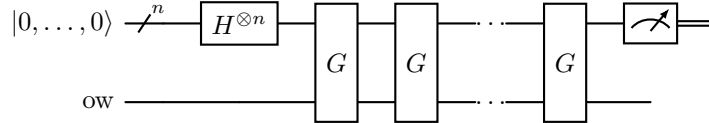
ow: oracle workspace (auxiliary qubit)
G: Groover operator

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

Note: $H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

for $x \in \{0, 1\}$

$$H |x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{z \cdot x} |z\rangle$$

Applied to several qubits:

$$\underbrace{H^{\otimes n}}_{H \otimes H \otimes \dots H} |x_1, \dots, x_n\rangle = (H |x_1\rangle) \otimes \dots \otimes (H |x_n\rangle) \overset{(1)}{=} \frac{1}{\sqrt{2^n}} \sum_{z_{1i} - z_n}^{1} (-1)^{z_1 x_1 + \dots + z_n x_n} |z_1 \dots z_n\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{z=0}^{2^n - 1} (-1)^{x \cdot z} |z\rangle \quad \text{| z is a bitstring}$$
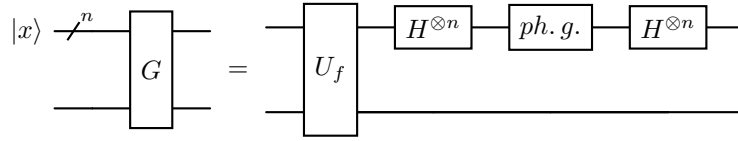
With:

(1): $H |x_1\rangle = \frac{1}{\sqrt{2}} \sum_{z_1=0}^{1} (-1)^{z_1 x_1} |z_1\rangle$

In particular: $H^{\otimes n} |0, \dots, 0\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle =: |\psi\rangle$ equal superposition state

$$|\alpha\rangle := \frac{1}{\sqrt{N-M}} \sum_{\substack{x=0 \\ f(x)=0}}^{N-1} |x\rangle$$

$$|\beta\rangle := \frac{1}{\sqrt{M}} \sum_{\substack{x=0 \\ f(x)=1}}^{N-1} |x\rangle$$

Definition of Grover operator G:

Captions:

U_f (oracle): $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$

$ph.\,g.$ (phase gate): $2|0\rangle\langle 0| - I = \begin{cases} |0\rangle \mapsto |0\rangle \\ |x\rangle \mapsto -|x\rangle \ for\, x \neq 0 \end{cases}$

All single qubit gates together:

$$H^{\otimes n} \cdot (2|1\rangle\langle 1| - I) \cdot H^{\otimes n} = 2 \underbrace{(H^{\otimes n} |0\rangle)}_{|\psi\rangle} \underbrace{(H^{\otimes n} \langle 0|)}_{\langle \psi|} - I$$

$$= 2|\psi\rangle\langle\psi| - I$$

In summary: $G = (2|\psi\rangle\langle\psi| - I) \cdot U_f$

Geometric interpretation

Define:

Angle θ is defined by $sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$ such that:

$$|\psi\rangle = cos(\frac{\theta}{2})|\alpha\rangle + sin(\frac{\theta}{2}|\beta\rangle)$$

Note: by definition $U_f |\alpha\rangle = |\alpha\rangle$, $U_f |\beta\rangle = -|\beta\rangle$

$\rightsquigarrow U_f$ is a reflection about $|\alpha\rangle$ within the subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$.

Likewise: $2|\psi\rangle\langle\psi| - I$ is a reflection about $|\psi\rangle$ since $|\psi\rangle$ is part of the subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$ G leaves this subspace invariant!

Thus G is a rotation by thed angle θ:
$|\phi\rangle \, cos(\varphi) \, |\alpha\rangle + sin(\varphi) \, |\beta\rangle$
$\rightsquigarrow G \, |\phi\rangle = cos(\varphi + \theta) \, |\alpha\rangle + sin(\varphi + \theta) \, |\beta\rangle$ (see handout for algebraic derivation)

For k applications of G:
$$G^k \, |\phi\rangle = cos(\varphi + k \cdot \theta) \, |\alpha\rangle + sin(\varphi + k \cdot \theta) \, |\beta\rangle$$

For initial state $|\phi\rangle = |\psi\rangle : \varphi = \frac{\theta}{2}$
$$G^k \, |\varphi\rangle = cos((k + \tfrac{1}{2})\theta) \, |\alpha\rangle + sin((k + \tfrac{1}{2})\theta) \, |\beta\rangle$$

Goal: rotate to $|\beta\rangle$, i.e. $(k + \tfrac{1}{2}\theta) \overset{!}{=} \frac{\pi}{2}$
since $sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}} \overset{\text{for M} \ll \text{N}}{\rightsquigarrow} \theta \approx 2\sqrt{\frac{M}{N}}$

Thus $O(\sqrt{\frac{N}{M}})$ rotations are needed $: k + \dfrac{1}{2} \overset{!}{=} \dfrac{\pi}{2\theta}, k \overset{!}{=} \dfrac{\pi}{2\theta} - \dfrac{1}{2}$

$$\rightsquigarrow k = O(\sqrt{\dfrac{N}{M}}) \text{for N} \mapsto \infty$$

Final step: standard measurement, will collapse quantum state (with high probabilitiy) to a basis state forming $|\beta\rangle$, i.e. a solution!

4.3 Optimality of the search algorithm

(Nielsen and Chuang section 6.6)

Goal: show that any quantum search algorithm needs $\Omega(\sqrt{N})$ oracle calls
$\rightsquigarrow O(\sqrt{N})$ is already optimal.

For simplicity we assume a single solution x:
Recall that oracle flips sign of solutions:
$\quad O_x = I - 2 \, |x\rangle \, \langle x|$ (denoted U_f in the previous section)

Most general form of algorithm: oracle calls interleaved with unitary operations
$U_1, U_2, \ldots$

State after k steps:
$\quad |\psi_k^x\rangle = U_k O_x U_{k-1} O_x \, \ldots \, U_1 \, |\psi_0\rangle$ — with $|\psi_0\rangle$ = initial state

We also define:
$\quad |\psi_k\rangle = U_k U_{k-1} \ldots U_0 \, |\psi_0\rangle$

Strategy of proof: upper bound of

$$D_k := \sum_{x=0}^{N-1} \| \, |\psi_k^x\rangle - |\psi_k\rangle \, \|^2$$

25

D_k grows as $O(k^2)$, but must be $\Omega(N)$ to distinguish between N alternatives.
(see below)

The following equations and inequalities are going to be used in the proof bellow:

$$\text{Unitary Norm: } \|U\| = 1 \Rightarrow \|U_{k+1}\,|x\rangle\| = \||x\rangle\| \tag{1}$$

$$\text{Spec. Cauchy-Sch.: } \|b+c\|^2 = \langle b+c, b+c\rangle \leq \|b\|^2 + 2\,\|b\| \cdot \|c\| + \|c\|^2 \tag{2}$$

$$\text{Cauchy-Schwarz: } \sum_x u_x \cdot v_x \leq \|u\| \cdot \|v\| \tag{3}$$

First show that $D_k \leq 4k^2$ by induction:

$$k = 0: \qquad D_0 = 0$$
$$k \mapsto k+1:$$

$$D_{k+1} = \sum_{x=0}^{N-1} \|\underbrace{U_{k+1}O_x\,|\psi_k^x\rangle - U_{k+1}\,|\psi_k\rangle}_{U_{k+1}(O_x|\psi_k^x\rangle - |\psi_k\rangle)}\|^2$$

$$\overset{(1)}{=} \sum_{x=0}^{N-1} \|O_x\,|\psi_k^x\rangle - |\psi_k\rangle\|^2$$

$$= \sum_{x=0}^{N-1} \|\underbrace{O_x(|\psi_k^x\rangle - |\psi_k\rangle)}_{=:b} + \underbrace{(O_x - I)\,|\psi_k\rangle}_{-2|x\rangle\langle x\,|\,\psi_k\rangle =:c}\|^2$$

$$\overset{(2)}{\leq} \sum_{x=0}^{N-1} (\|b\|^2 + 2\,\|b\| \cdot \|c\| + \|c\|^2) \qquad |\ O_x \text{ is unitary}$$

$$= \sum_{x=0}^{N-1} (\||\psi_k^x\rangle - |\psi_k\rangle\|^2 + 4\,\||\psi_k^x\rangle - |\psi_k\rangle\| \cdot |\langle x\,|\,\psi_k\rangle| + 4\,|\langle x\,|\,\psi_k\rangle|)$$

$$\overset{(3)}{\leq} D_k + 4\,\underbrace{(\sum_{x=0}^{N-1} \||\psi_k^x\rangle - |\psi_k\rangle\|^2)^{\frac{1}{2}}}_{\|u\|} \cdot \underbrace{(\sum_{x=0}^{N-1} |\langle x|\psi_k\rangle|^2)^{\frac{1}{2}}}_{\|v\|=1} + 4$$

$$= D_k + 4\sqrt{D_k} + 4$$

$$\overset{I.H.}{\leq} 4k^2 + 4\sqrt{4k^2} + 4$$

$$= 4(k+1)^2$$

Second part of the proof: D_x must be in $\Omega(N)$:

For the next proof step we will need the following equations and inequalities:

$$Re(z) \leq |z| \; \forall z \in \mathbb{C} \tag{4}$$

To find a solution x, we want that $|\psi_k^x\rangle \sim |x\rangle$ suppose that $|\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2} \; \forall x$. (probability of success is at least 50%)

w.l.o.g. $\langle x|\psi_k^x\rangle = |\langle x|\psi_k^x\rangle|$ (can multiply $|x\rangle$ by phase factor)

$$\leadsto \left\| |\psi_k^x\rangle - |x\rangle \right\|^2 = \left\| |\psi_k^x\rangle \right\|^2 - 2\langle x|\psi_k^x\rangle + \left\| |x\rangle \right\|^2$$
$$= 2 - 2\underbrace{\langle x|\psi_k^x\rangle}_{\leq \frac{1}{\sqrt{2}}}$$
$$\leq 2 - \sqrt{2}$$

Therefore:
$$E_k := \sum_{x=0}^{N-1} \left\| |\psi_k^x\rangle - |x\rangle \right\| \leq (2 - \sqrt{2}) \cdot N$$

Define $F_k := \sum_{x=0}^{N-1} \left\| |x\rangle - |\psi_k\rangle \right\|^2$, then

$$F_k = \sum_{x=0}^{N-1} \left(\left\| |x\rangle \right\| - 2Re\langle x|\psi_k\rangle + \left\| |psi_k\rangle \right\|^2 \right)$$

$$\overset{(4)}{\geq} 2 \cdot N - 2\sum_{x=0}^{N-1} \underbrace{|\langle x|\psi_k\rangle|}_{u_x} \cdot \underbrace{1}_{v_x}$$

$$\overset{(3)}{\geq} 2 \cdot N - 2[(\underbrace{\sum_x |\langle x|\psi_k\rangle|^{\frac{1}{2}})^2}_{1} \cdot (\underbrace{\sum_x 1)^{\frac{1}{2}}}_{N}]$$

$$= 2 \cdot N - 2\sqrt{N}$$

27

$$D_k = \sum_{x=0}^{N-1} \| (|\psi_k^x\rangle - |x\rangle) + (|x\rangle - |\psi_k\rangle) \|^2$$

$$\geq \sum_{x=0}^{N-1} \left(\| |\psi_k^x\rangle - |x\rangle \| - 2 \| |\psi_k^x\rangle - |x\rangle \| \cdot \| |x\rangle - |\psi_k\rangle \|^2 + \| |x\rangle - |\psi_k\rangle \|^2 \right)$$

$$= E_k + F_k - 2 \sum_{x=0}^{N-1} \underbrace{\| |\psi_k^x\rangle - |x\rangle \|}_{=:a_x} \cdot \underbrace{\| |x\rangle - |\psi_k\rangle \|}_{=:b_x}$$

$$\geq E_k + F_k - 2 \underbrace{\sqrt{E_k}}_{\|a\|} \cdot \underbrace{\sqrt{F_k}}_{\|a\|} = (\sqrt{F_k} - \sqrt{E_k})^2$$

$$\geq \left(\sqrt{2N - 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N} \right)^2$$

$$= N \cdot (\sqrt{2} - \sqrt{2 - \sqrt{2}})^2$$

$$= N \left(\sqrt{2 - \frac{2}{\sqrt{N}}} - \sqrt{2 - \sqrt{2}} \right)^2 \qquad | \text{ with } \lim_{N \to \infty} \frac{2}{\sqrt{N}} \to 0$$

$$\cong N \cdot \underbrace{(\sqrt{2} - \sqrt{2 - \sqrt{2}})^2}_{=:c \approx 0.42}$$

$$= c \cdot N$$

In summary:

$$\underbrace{D_k \leq 4k^2 \text{ and } D_k \geq cN}_{k \geq \sqrt{\frac{cN}{4}}}$$

with k being the number of oracle evaluations.

5 The density operator

So far the state vector $|\psi\rangle$ described a quantum state. A convenient alternative formulation for quantum systems about which we have only partial information is the <u>density operator</u> (also called <u>density matrix</u>).

5.1 Ensembles of quantum states

(Nielsen and Chuang section 2.4.1)

Consider a quantum system which is in one of several states $|\psi_i\rangle$ with probability p_i, this defines an <u>ensemble</u> of quantum states $\{p_i, |\psi_i\rangle\}$.
The <u>density operator</u> ρ of the ensemble $\{p_i, |\psi_i\rangle\}$ is defined as:

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

Quantum mechanichs in terms of the density operator:

- unitary operations: a unitary transformation U maps $|\psi_i\rangle \mapsto U \cdot |\psi_i\rangle$, and the ensemble to $\{p_i, U|\psi_i\rangle\}$.
  Thus the density operator is transformed as:

$$\rho \overset{U}{\mapsto} \sum_i p_i U |\psi_i\rangle \underbrace{\langle\psi_i| U^\dagger}_{=(U|\psi_i\rangle)^\dagger} = U(\sum_i p_i |\psi_i\rangle \langle\psi_i|)U^\dagger = U\rho U^\dagger$$

- measurement: measurement operators $\{M_m\}$, if the system is in the state $|\psi_i\rangle$, then the probability for the result m, given by i, is

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle$$

with: $\langle\psi| A |\psi\rangle = \mathrm{tr}[A |\psi\rangle \langle\psi|]$ and $\mathrm{tr}[A \cdot B \cdot C] = tr[B \cdot C \cdot A] = \mathrm{tr}[C \cdot A \cdot B]$

$$\Rightarrow \mathrm{tr}[M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|] = \|M_m |\psi_i\rangle\|^2$$

Thus the overall probability for the result m is:

$$p(m) = \sum_i p(m|i)\, p_i = \sum_i \mathrm{tr}[M - m^\dagger M_m |\psi_i\rangle \langle\psi_i|] \cdot p_i$$

$$= \mathrm{tr}[M_m^\dagger M_m \sum_i p_i |\psi_i\rangle \langle\psi_i|] = \mathrm{tr}[M_m^\dagger M_m \rho]$$

Density operator ρ_m after obtaining result m?
State i collapses as follows: $|\psi_i\rangle \mapsto \frac{M_m|\psi_i\rangle}{\|M_m|\psi_i\rangle\|} =:= |\psi_i^m\rangle$
Thus:

With:

(Baye's theorem): $P(A|B) = \dfrac{P(A \cap B)}{P(B)} = \dfrac{P(B|A)}{P(B)}$ \hfill (1)

$$\rho_m = \sum_i p(i|m) \cdot |\psi_i^m\rangle \langle \psi_i^m| = \sum_i p(i|m) \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\|M_m |\psi_i\rangle\|^2}$$

$$\overset{(1)}{=} \sum_i p_i \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{p(m)} = \boxed{\frac{M_m \rho M_m^\dagger}{\mathrm{tr}[M_m^\dagger M_m \rho]}}$$

Note that ρ_m is now expressed in terms of ρ and the measurement operators, without explicit reference to the ensemble $\{p_i, |\psi_i\rangle\}$

5.2 General properties of the density operator

(Nielsen and Chuang section 2.4.2)

Characterization of density operators: An operator ρ is the density matrix associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if:

1. $\mathrm{tr}[\rho] = 1$ (trace condition)

2. ρ is a positive operator (positive condition)

Remark: ρ is called a positve operator if it is Hermitian and all its eigenvalues are ≥ 0, equivalently if $\overline{\langle \varphi| \rho |\varphi\rangle \geq 0}$ for a vectors $|\varphi\rangle$.

Proof.

" $\Rightarrow$ "Suppose $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$, then

$$\mathrm{tr}[\rho] = \sum_i p_i \mathrm{tr}[|\psi_i\rangle \langle \psi_i|] = \sum_i p_i \langle \psi_i|\psi_i\rangle = 1 \quad | \sum_i p_i = 1 \text{ (prob. distr.)}$$

and for any state $|\varphi\rangle$:

$$\langle \varphi| \rho |\varphi\rangle = \sum_i p_i \langle \varphi|\psi_i\rangle \langle \psi_i|\varphi\rangle = \sum_i p_i \underbrace{|\langle \varphi|\psi_i\rangle|^2}_{\geq 0} \geq 0$$

" $\Leftarrow$ "ρ is an operator (i.e. a Hermition matrix) $\rightarrow$ by spectral theorem:

There exist eigenvalues λ_j and corresponding orthonormal eigen vectors $|\varphi_j\rangle$ such that:

$$\rho = \sum_j \lambda_j |\varphi_j\rangle \langle \varphi_j|.$$

Since ρ satisfies the trace condition:

$$1 = \mathrm{tr}[\rho] = \sum_j \lambda_j \mathrm{tr}[|\varphi_j\rangle \langle \varphi_j|] = \sum_j \lambda_j \langle \varphi_j|\varphi_j\rangle = \sum_j \lambda_j$$

Due to positivity of $\rho : \lambda_j \geq 0, \forall j$

Thus we can interpret eigenvalues λ_j as probabilities $\rightsquigarrow$

$\{\lambda_j, |\varphi_j\rangle\}$ is an ensemble which gives rise to ρ.

$\square$

From now on, we define a density operator as positive operator ρ with $\text{tr}[\rho] = 1$.

Language regarding density operators:

<table>
<tr><td>"pure state"</td><td>"mixed state"</td></tr>
<tr><td>Quantum system in a state $|\psi\rangle$, with the corresponding density operator:</td><td>ρ describing a quantum setup cannot be written as $\rho = |\psi\rangle\langle\psi|$; intuition: In the ensemble represen- tation:</td></tr>
<tr><td>$$\rho = |\psi\rangle\langle\psi|$$</td><td></td></tr>
<tr><td>such that:</td><td>$\{p_i, |\psi_i\rangle\}$ of ρ,</td></tr>
<tr><td>$\text{tr}[\rho^2] = \text{tr}[|\psi\rangle\langle\psi|\psi\rangle\langle\psi|] = \langle\psi|\psi\rangle = 1$</td><td>all the probabilities are strictly smaller than 1. Then, $\text{tr}[\rho^2] = \sum_i p_i^2 < 1$</td></tr>
</table>

In general: Let ρ be a density operator. Then $\text{tr}[\rho^2] \leq 1$, and $\text{tr}[\rho^2] = 1$ if and only if ρ describes a pure quantum state.

Proof: Denote the eigenvalues of ρ by $\{\lambda_i\}$, then $0 \leq \lambda_i \leq 1$ since ρ is positive and $1 = \text{tr}[\rho] = \sum_i \lambda_i$.

Moreover, $\text{tr}[\rho^2] = \sum_i \lambda_i^2 \leq 1$, with "$= 1$" precisely if one of the eigenvalues is 1 and the other are 0.

The ensemble representation is not unique!
Example:

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \qquad = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b|$$

$$= \begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{1}{4} \end{pmatrix} \qquad \text{with } |a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$$

$$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$$

(But note that $|0\rangle$, $|1\rangle$ are the (unique) eigenvectors of ρ, and $\langle a|b\rangle \neq 0$)

For the following: given an ensemble $\{p_i, |\psi_i\rangle\}$, set $|\widetilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$ such that $\rho = \sum_i |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|$.

Ensemble $\{|\widetilde{\psi}\rangle_i\}$ <u>generates</u> the density operator ρ.

To relate an $\{|\widetilde{\psi}_i\rangle\}_{i=1...m}$ to another $\{|\widetilde{\varphi}_j\rangle\}_{j=1...n}$ in case $m \neq n$, we "pad" one of the ensembles with zero vectors, such that without loss of generality $m = n$.

Unitary freedome in the ensemble of density marices:
The set $\{|\widetilde{\psi}_i\rangle\}$ and $\{|\widetilde{\varphi}_j\rangle\}$ generate the same density matrix if and only if:

$$|\widetilde{\psi}\rangle_i = \sum_j u_{ij} |\widetilde{\varphi}_j\rangle$$

for some unitary matrix (u_{ij}).

Sketch of proof:
"$\Leftarrow$" Insert definitions

$$\sum_i |\widetilde{\psi}_i\rangle \langle\widetilde{\psi}_i| = \sum_i (\sum_j u_{ij} |\widetilde{\varphi}_j\rangle)(\sum_{j'} u^*_{ij'} \langle\widetilde{\varphi}_j|)$$
$$= \sum_{jj'}$$

"$\Rightarrow$"
Use the spectral decomposition of the density matrix:

$$\rho = \sum_k \lambda |\widetilde{\chi}_k\rangle \langle\widetilde{\chi}_k| \text{ with } \langle\chi_k|\chi_l\rangle = \delta_{kl}$$
$$\text{set } |\widetilde{\chi}_k\rangle = \sqrt{\lambda_k} |\chi_k\rangle \ , \ |\widetilde{\psi}_i\rangle = \sum_k v_{ik} |\widetilde{\chi}_k\rangle \ (1)$$

for some complex coefficients v_{ik}

$$\text{Then } \sum_k |\widetilde{\chi}_k\rangle \langle\widetilde{\chi}_k| = \sum_{k,l} \delta_{k,l} |\widetilde{\chi}_k\rangle \langle\widetilde{\chi}_k| = \rho = \sum_i |\widetilde{\psi}_i\rangle \langle\widetilde{\psi}_i|$$
$$\overset{(1)}{=} \sum_{j,l} (\sum_i v_{ik} v^*_{il}) |\widetilde{\chi}_k\rangle \langle\widetilde{\chi}_l|$$

This equation can only be satisfied (since the $|\widetilde{\chi}_k\rangle$ are orthogonal and thus $|\widetilde{\chi}_k\rangle \langle\widetilde{\chi}_l|$ linearly independent) if
$$\forall k, l : \delta_{kl} = \sum_i v_{ik} v^*_{il} = (V^T V^*)_{kl} = (V^\dagger V)^*_{kl} \Leftrightarrow V^\dagger V = I \text{ (V is unitary)}$$

In other words, if V is a unitary matrix.
By the same arguments: $|\widetilde{\varphi}_j\rangle = \sum_k \omega_{jk} |\widetilde{\chi}_k\rangle$ for a unitary matrix (ω_{jk})

Thus: $|\widetilde{\psi}_i\rangle = \sum_k v_{ik} |\widetilde{\chi}_k\rangle = \sum_{k,j} v_{ik} \omega^*_{jk} |\widetilde{\varphi}_j\rangle = \sum_j (V \cdot \omega^\dagger)_{jk} |\widetilde{\varphi}_j\rangle$ and $V \cdot \omega^\dagger$ is
(as a product of unitary matrice) again unitary.

The <u>Block Sphere</u> picture of a qubits can be generalized to <u>mixed states</u> by the representation:
$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}$$

with $\vec{r} \in \mathbb{R}^3, \|\vec{r}\| \leq 1$, the <u>Bloch sphere</u> of ρ (see sheet 11)
(coincides with hitherto definition of Bloch vector in case $\rho = |\psi\rangle\langle\psi|$.)

5.3 The reduced density operator

(Nielsen and Chuang section 2.4.3)

Definition (partial trace): Let $n_1, n_2 \in \mathbb{N}$.
The <u>partial trace</u> operations are defined in terms of the conventional matrix trace (tr) by:

$$\mathrm{tr}_1 : \mathbb{C}^{n_1 n_2 \times n_1 n_2} \longmapsto \mathbb{C}^{n_2 \times n_2}, \mathrm{tr}_1[M_1 \otimes M_2] = \mathrm{tr}[M_1] \cdot M_2.$$
$$\mathrm{tr}_2 : \mathbb{C}^{n_1 n_2 \times n_1 n_2} \longmapsto \mathbb{C}^{n_1 \times n_1}, \mathrm{tr}_2[M_1 \otimes M_2] = \mathrm{tr}[M_2] \cdot M_1.$$
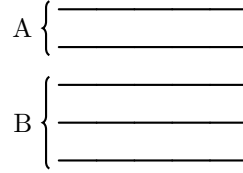
for all $M_1 \in \mathbb{C}^{n_1 \times n_1}$ and $M_2 \in \mathbb{C}^{n_2 \times n_2}$, together with linear expansion:

$$\mathrm{tr}_1[\alpha\, M_1 \otimes M_2 + \beta\, N_1 \otimes N_2] = \alpha\, \mathrm{tr}_1[M_1 \otimes M_2] + \beta\, \mathrm{tr}_1[M_1 \otimes M_2]$$
$$\mathrm{tr}_2\left[\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}\right] = \begin{pmatrix} \mathrm{tr}[B_{11}] & \mathrm{tr}[B_{12}] \\ \mathrm{tr}[B_{21}] & \mathrm{tr}[B_{22}] \end{pmatrix} \in \mathbb{C}^{2\times 2}$$

Consider a composite quantum system consisting of subsystems A and B for example:

$A : m$ qubits, $B : n$ qubits

$\Rightarrow n_1 = 2^m \wedge n_2 = 2^n$

Let the quantum system be described by a density operator ρ^{AB}.
Define the <u>reduced density operator for system A by:</u>

$$\rho^A = \mathrm{tr}_B[\rho^{AB}]$$

and analgously for system B by:

$$\rho^B = \mathrm{tr}_A[\rho^{AB}]$$

Examples:

- For any quantum states $|a_1\rangle, |a_2\rangle \in A \wedge |b_1\rangle, |b_2\rangle \in B :$

$$\text{tr}_B[\underbrace{|a_1\rangle \langle a_2|}_{M_1} \otimes \underbrace{|b_1\rangle \langle b_2|}_{M_2}] = |a_1\rangle \langle a_2| \cdot \underbrace{\text{tr}\,|b_1\rangle \langle b_2|}_{\langle b_2|b_1\rangle} = |a_1\rangle \langle a_2| \cdot \underbrace{\langle b_2|b_1\rangle}_{\in \mathbb{C}}$$

- Given a density matrix ρ for a subsystem A and σ for subsystem B. Suppose that the overall density matrix is:

$$\rho^{AB} = \rho \otimes \sigma$$

$$\text{Then:}\ \ \text{tr}_B[\rho^{AB}] = \rho \cdot \underbrace{\text{tr}[\sigma]}_{1} = \rho$$

$$\text{tr}_A[\rho^{AB}] = \sigma \cdot \underbrace{\text{tr}[\rho]}_{1} = \sigma$$

- $\rho^{AB} = |\psi\rangle \langle \psi|$ with $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (Bell state) Expanding ρ^{AB} leads to:

$$\rho^{AB} = \frac{1}{2}(|00\rangle + \langle 00|)(\langle 00| + \langle 11|)$$

$$= \frac{1}{2}(|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|)$$

$$\rho^A = \text{tr}[\rho^{AB}]$$

$$= \frac{1}{2}(|0\rangle \langle 0| \cdot \langle 0|0\rangle + |0\rangle + \langle 1| \cdot \langle 1|0\rangle + |1\rangle \langle 0| \cdot \langle 0|1\rangle + |1\rangle \langle 1| \cdot \langle 1|1\rangle)$$

$$= \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{\mathbb{I}}{2} \quad |\mathbb{I} \equiv \mathbb{1} \equiv I$$

Note: composite system is the "pure state" $|\psi\rangle$, whereas the subsystem is described by the "mixed state" $\frac{\mathbb{I}}{2}$.

$$\text{(Indeed a mixed state:}\ \ \text{tr}\left[\left(\frac{\mathbb{I}}{2}\right)^2\right] = \frac{1}{4}\text{tr}[\mathbb{I}] = \frac{1}{2} < 1.\text{)}$$

Motivation / justification for partial trace:
Let M be any observable or subsystem A, then we want that ρ^A yields the same statistics for measuring M as ρ^{AB} for measuring $M \otimes \mathbb{I}$.
In particular:

$$\langle M \rangle_A = \text{tr}[M \cdot \rho^A] \overset{!}{=} \text{tr}_{AB}[(M \otimes \mathbb{I}) \cdot \rho^{AB}] = \langle M \otimes \mathbb{I} \rangle_{AB}$$

for all observables M and all density operators ρ^{AB}.
The partial trace operator for computing ρ^A from ρ^{AB} is the unique operation with this property (Nielsen and Chuang Box 2.6).

Application to quantum teleportation: Why does quantum teleportation not allow for faster than light communication via the instantanious wavefunction-collapse?

Recall the corresponding quantum circuit:
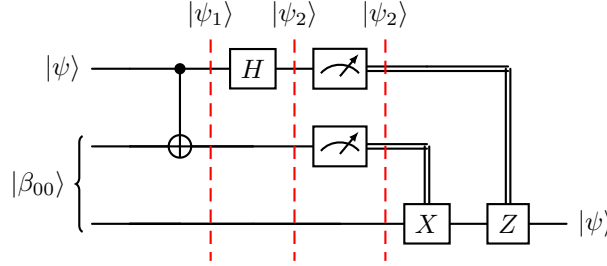
At $|\psi_3\rangle$, Alice has completed her measurements(her qubits have "collapsed"), but Bob does not know the measurement results yet.

Intermediate state $|\psi_2\rangle$: (see previous lecture)

$$|\psi_2\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+ |01\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

Thus, directly after Alice's measurement, the system is in the state (from Bob's perspective, who does not know the measurement results yet);

$$|\varphi_1\rangle = |00\rangle(\alpha|0\rangle + \beta|1\rangle); \text{ with probability } \frac{1}{4}$$

$$|\varphi_2\rangle = |01\rangle(\alpha|1\rangle + \beta|0\rangle); \qquad "$$
$$|\varphi_3\rangle = |01\rangle(\alpha|0\rangle - \beta|1\rangle); \qquad "$$
$$|\varphi_4\rangle = |11\rangle(\alpha|1\rangle - \beta|0\rangle); \qquad "$$

Corresponding density matrix of ensemble $\frac{1}{4}, |\varphi_j\rangle_{j=1\ldots4}$:

$$\rho^{AB} = \frac{1}{4}\sum_{j=1}^{4}|\varphi_j\rangle\langle\varphi_j|$$

$$= \frac{1}{4}(|00\rangle\langle00| \otimes (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle0| + \beta^*\langle1|)$$
$$+ \quad |01\rangle\langle01| \otimes (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle1| + \beta^*\langle0|)$$
$$+ \quad |10\rangle\langle10| \otimes (\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle0| - \beta^*\langle1|)$$
$$+ \quad |11\rangle\langle11| \otimes (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle1| - \beta^*\langle0|))$$

Alice's qubits | Bob's qubits

Reduced density operator describing Bob's qubit:

$$(1) : \text{tr}[|a_1 a_2\rangle \langle a_1 a_2|] = \langle a_1 a_2 | a_1 a_2 \rangle = 1 \quad \forall a_1, a_2 \in 0, 1$$

$$\rho^B = \text{tr}_A[\rho^{AB}] \overset{(1)}{=} \frac{1}{4}((\alpha |0\rangle + \beta |1\rangle)(\alpha^* \langle 0| + \beta^* \langle 1|)$$
$$+ \quad (\alpha |1\rangle + \beta |0\rangle)(\alpha^* \langle 1| + \beta^* \langle 0|)$$
$$+ \quad (\alpha |0\rangle - \beta |1\rangle)(\alpha^* \langle 0| - \beta^* \langle 1|)$$
$$+ \quad (\alpha |1\rangle - \beta |0\rangle)(\alpha^* \langle 1| - \beta^* \langle 0|))$$

$$= \frac{1}{4}\left(2\underbrace{(|\alpha|^2 + |\beta|^2)}_{=1} |0\rangle \langle 0| + 2(|\alpha|^2 + |\beta|^2) |1\rangle \langle 1| \right)$$

$$= \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{\mathbb{I}}{2}$$

$\rightsquigarrow$ independent of $|\psi\rangle$ (α and β coefficients)

Since $\rho^B = \frac{\mathbb{I}}{2}$, any measurements by Bob cannot reveal any information about $|\psi\rangle$, i.e. Alice cannot transmit information (encoded in α, β) via the instantanious wavefunction collapse to Bob.

6 Quantum operations

(Nielsen and Chuang section 8.2)

6.1 Motivation and overview

In general: changes of quantum states affected by unitary time evolution or wavefunction collapse during measurement. Quantum operations (also called "quantum channels") are a (mathematical) generalization and unification of these concepts.

Abstractly:

$$\rho' = \mathcal{E}(\rho)$$
$$\text{with } \mathcal{E} \coloneqq \text{quantum operation and } \rho \coloneqq \text{density matrix}$$

Special cases:

- unitary time evolution: $\mathcal{E}(\rho) = U \cdot \rho \cdot U^\dagger$

- measurements, with measurement operations M_m:

  recall that $p(m) = \text{tr}[M_m^\dagger M_m \rho]$ | $p(m) \coloneqq$ "probability of outcome m"
  State after obtaining result m:

  $$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{tr}[M_m^\dagger M_m \rho]} = \frac{M_m \rho M_m^\dagger}{p(m)}$$

  Corresponding quantum channel (without normalisation):

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

  $p(m) = \text{tr}[\mathcal{E}(\rho)]$ is the probability that outcome m occurs.

Consider the scenario of performing a measurement, but not recording the outcome:

$\rightsquigarrow$ density matrix after this process is the weighted sum over all possible outcomes:

$$\mathcal{E}(\rho) = \sum_m p(m) \cdot \rho_m = \sum_m M_m \rho M_m^\dagger \coloneqq \text{"operator-sum (Kraus) representation of } \mathcal{E}\text{"}$$

Different (but equivalent) perspectives on quantum operations:

- system coupled to environment (Stinespring dilation)

- operator-sum (Kraus) representation

- physically motivated axioms
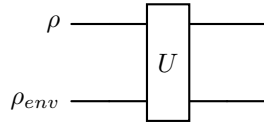
- Choi matrix representation

6.2 Environments and quantum operations

"Open" quantum systems can be regarded as interactions between a:

- principal quantum system (initially in state ρ)

- environment (initially in state ρ_{env})

The principal system interacts with the environment, i.e. a time evolution of the overall system described by some unitary U:
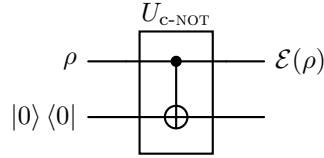
Circuit diagram:

ρ ──────┤ ├──────

┤ U ├

ρ_{env} ──────┤ ├──────

mathematical representation:

$$U \cdot (\rho \otimes \rho_{env}) \cdot U^{\dagger}$$

Example:

$U_{\text{c-NOT}}$

ρ ────────●──────── $\mathcal{E}(\rho)$

$|0\rangle\langle 0|$ ────────⊕────────

Represents $\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} = \rho_{00}\,|0\rangle\langle 0| + \rho_{01}\,|0\rangle\langle 1| + \rho_{10}\,|1\rangle\langle 0|\,\rho_{11}\,|1\rangle\langle 1|$, then:

$$U_{\text{c-NOT}} \cdot (\rho \otimes |0\rangle\langle 0|)U_{\text{c-NOT}}^{\dagger}$$
$$= U_{\text{c-NOT}} \cdot (\rho_{00}\,|00\rangle\langle 00| + \rho_{01}\,|00\rangle\langle 10| + \rho_{10}\,|10\rangle\langle 00|\,\rho_{11}\,|10\rangle\langle 10|)U_{\text{c-NOT}}^{\dagger}$$
$$= \qquad \rho_{00}\,|00\rangle\langle 00| + \rho_{01}\,|00\rangle\langle 11| + \rho_{10}\,|11\rangle\langle 00|\,\rho_{11}\,|11\rangle\langle 11|$$

$$\text{tr}_{env}[\ldots] = \qquad \rho_{00}\,|0\rangle\langle 0|\,\langle 0|0\rangle + \rho_{01}\,|0\rangle\langle 1|\,\langle 1|0\rangle + \rho_{10}\,|1\rangle\langle 0|\,\langle 0|1\rangle\,\rho_{11}\,|1\rangle\langle 1|\,\langle 1|1\rangle$$
$$= \qquad \rho_{00}\,|0\rangle\langle 0| + \rho_{11}\,|1\rangle\langle 1|$$
$$= \qquad \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix}$$
$$= \qquad P_0 \rho P_0 + P_1 \rho P_1 \text{ with } P_0 = |0\rangle\langle 0|,\ P_1 = |1\rangle\langle 1|$$

(off-diagonal entries of ρ are set to zero)

6.3 Operator-sum (Kraus) representation

Let $|e_k\rangle$ be an orthonormal basis of the environment quantum system, assume w.l.o.g. $\rho_{env} = |e_0\rangle\langle e_0|$ (see tutorial 12: if environment is a mixed state, then can equivalently work with a pure state in a larger environment)

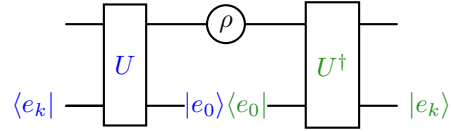$$(1): \sum_k |e_k\rangle\langle e_k| = I \text{ on environment}$$

$$(2): \text{tr}[A\,|j\rangle\langle j|] = \langle j|\,A\,|j\rangle$$

$$\rightsquigarrow \mathcal{E}(\rho) = \text{tr}_{env}[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger]$$

$$\overset{(1)}{=} \sum_k \text{tr}_{env}[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \cdot (I \otimes |e_k\rangle\langle e_k|)]$$

$$\overset{(2)}{=} \sum_k \langle e_k|\,U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\,|e_k\rangle$$

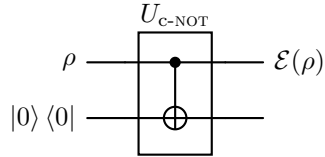$$= \sum_k E_k \rho E_k^\dagger$$

with E_k a complex matrix with entries $(E_k)_{lm} = \langle l, e_k|U|m, e_0\rangle$
The E_k's are called <u>operation elements</u> or <u>Kraus operators</u> of $\mathcal{E}$:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

Revisit example:

$(E_0)_{lm} = \langle l, 0|U_{CNOT}|m, 0\rangle \qquad \rightsquigarrow E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = P_0$

$(E_1)_{lm} = \langle l, 1|U_{CNOT}|m, 0\rangle \qquad \rightsquigarrow E_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = P_1$

Look at official lecture for extra notes P_0 and P_1 agree with previous derivation.

If $\mathcal{E}$ is trace-preserving, then for any density matrix of ρ:

$$1 \overset{!}{=} \mathrm{tr}[\mathcal{E}(\rho)] = \mathrm{tr}[\sum_k E_k \rho E_k^\dagger] = \sum_k \mathrm{tr}[E_k \rho E_k^\dagger] \overset{*}{=} \sum_k \mathrm{tr}[E_k^\dagger E_k \rho] = \mathrm{tr}[(\sum_k E_k^\dagger E_k)\rho]$$

*: cyclic invariance

should hold for arbitrary ρ with $\mathrm{tr}[\rho] = 1 \rightsquigarrow \sum_k E_k^\dagger E_k = I$

We allow for quantum channels with $\sum_k E_k^\dagger E_k \leq I$

"$A \leq B$" if B-A is positive semidefinite (p.s.d.)

> $A \in \mathbb{C}^{n \times n}$ is called $\underline{\text{positive semidefinite}}$ if A is Hermitian and $\langle V | A | V \rangle \geq$
> 0 for all $v \in \mathbb{C}^n \Leftrightarrow \overline{\text{all eigenvalue of A are}} \geq 0$

$\sum_k E_k^\dagger E_k \overset{!}{\leq} I$ stems from requiremet that $\mathrm{tr}[\mathcal{E}(\rho)] \overset{!}{\leq} 1$

Remark: $\underline{\text{Physical interpretation}}$ of a quantum channel as measurement performed on environment with respect to e_k basis, i.e. the measurement operators $|e_k\rangle \langle e_k|$:

For outcome k, state of principal system is:

$$\rho_k \propto \mathrm{tr}_{env}[\, |e_k\rangle \langle e_k| U(\rho \otimes |e_0\rangle \langle e_0|)U^\dagger |e_k\rangle \langle e_k| \,] = E_k \rho E_k^\dagger$$

, i.e. E_k's play the role of the measurement operators on the principal system.
$\underline{\text{System-environment model of Krans representation}}$

Given trace-preserving $\mathcal{E}(\rho) = \displaystyle\sum_{k=0}^{n-1} E_k \rho E_k^\dagger$, is there a corresponding system-

environment representation?
Yes: Define model environment as vector space of dimension n with orthonormal basis $|e_k\rangle_{k=0,\ldots,n-1}$, assume that environment starts in $|e_0\rangle$ state.

Define unitary U via $U \cdot |\psi\rangle |e_0\rangle \overset{(*)}{=} \sum_k E_k |\psi\rangle |e_k\rangle$ and use matrix extension to

a unitary operator on the combined system.

This is possible since for any principal quantum states $|\psi\rangle$,

$$\langle\psi| \langle e_0| U^\dagger U |\varphi\rangle |e_0\rangle \overset{(*)}{=} \sum_{k,k'} \langle\psi| E_k^\dagger E_{k'} |\varphi\rangle \langle e_k | e_{k'}\rangle$$

$$= \langle\psi| \sum_k E_k E_k^\dagger |\varphi\rangle = \langle\psi|\varphi\rangle = I$$

(completeness relation)

U has the desired property since:

$$\mathrm{tr}_{env}[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger] \stackrel{(*)}{=} \sum_{k,k'} \mathrm{tr}_{env}[\,(E_k\rho E_{k'}) \otimes |e_k\rangle\langle e_{k'}|\,]$$

$$= \sum_{k,k'} E_k\rho E_{k'}^\dagger \underbrace{\langle e_{k'}|e_k\rangle}_{\delta_{kk'}}$$

$$= \sum_k E_k\rho E_k^\dagger$$

6.4 6.4 Axiomatic approach to quantum operations

Alternative viewpoint: physically motivated axioms which a quantum operation $\mathcal{E}$ has to obey:

A1: $\mathrm{tr}[\mathcal{E}(\rho)]$ is the probability that the process $\mathcal{E}$ occurs, thus $0 \le \mathrm{tr}[\mathcal{E}(\rho)] \le 1$ for all density matrices ρ.

A2: $\mathcal{E}$ is convex-linear:

$\mathcal{E}(\sum_i p_i\rho_i) = \sum_i p_i\mathcal{E}(\rho_i)$ for any probability vector p and density matrices ρ

A3: $\mathcal{E}$ is a <u>completely positive</u> map:

$\mathcal{E}(A)$ must be positive semidefinite (p.s.d.) for any p.s.d. matrix A
Moreover, when enlarging the principal system Q by another quantum system R, then $(I \otimes \mathcal{E})(A)$ must be p.s.d. for any p.s.d. A on the conbined system RQ. I on R and $\mathcal{E}$ on Q

Theroem: The map $\mathcal{E}$ satisfies A1, A2, A3 if and only if

$$\mathcal{E}(\rho) = \sum_k E_k\rho E_k^\dagger$$

for some some set of complex matrices E_k with $\sum_k E_k^\dagger E_k \le I$

Sketch of proof:
" $\Leftarrow$ " to verify A3: Let A be a p.s.d. matrix on enlarged system RQ, then, for any vector $|\psi\rangle$ on RQ:

$$\langle\psi|\,(I \otimes \mathcal{E})(A)\,|\psi\rangle = \sum_k \langle\psi|\,(I \otimes E_k)A(I \otimes E_k^\dagger)\,|\psi\rangle$$

$$= \sum_k \langle\psi_k|\,A\,|\psi_k\rangle \ge 0$$

" $\Rightarrow$ " Principal syste (which $\mathcal{E}$ acts on) denoted Q, dimension n. Introduce another quantum system, labelled R, with some dimension as Q.

6.5 Currently in Work

6.6 Currently in Work

6.7 Examples of quantum channels

(Nielsen and Chuang section 8.3)

Bit flip channel: flip $|0\rangle \leftrightarrow |1\rangle$ with probability $1 - p, p \in [0, 1]$

$$E_0 = \sqrt{p} \cdot I, E_1 = \sqrt{1 - p} \cdot X$$

$$\mathcal{E}_{BF}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger = p \cdot \rho + (1 - p) X \rho X$$

Recall Block vector $\vec{r}$ of density matrix: $\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}$

$$\text{tr}[\rho^2] = \frac{1}{2}(1 + \|\vec{r}\|^2), \text{ see Exercise 11.2}$$

$$X \cdot X \cdot X = X$$
$$Y \cdot Y \cdot Y = -Y$$
$$Z \cdot Z \cdot Z = -Z$$

$$\mathcal{E}_{BF}(\rho) = \frac{I + \vec{r'} \cdot \vec{\sigma}}{2} \text{ with } \vec{r'} = \begin{pmatrix} p \ r_1 + (1 - p)r_1 \\ p \ r_2 + (1 - p)r_2 \\ p \ r_3 + (1 - p)r_3 \end{pmatrix} = \begin{pmatrix} r_1 \\ (2p - 1)r_2 \\ (2p - 1)r_3 \end{pmatrix}$$

- Phase flip (analgously)

$$E_0 = \sqrt{p}I, E_1 = \sqrt{1 - p}Z$$

$$\mathcal{E}_{PF}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger$$
$$= p \cdot \rho + (1 - p) Z \rho Z$$

$$\vec{r'} = \begin{pmatrix} (2p - 1)r_1 \\ (2p - 1)r_2 \\ r_3 \end{pmatrix}$$

For $p = \frac{1}{2}$: by unitary freedom of Kraus representation:

$$P_0 := \frac{1}{\sqrt{2}} E_0 + \frac{1}{\sqrt{2}} E_1 = \frac{1}{2}I + \frac{1}{2}Z = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle \langle 0|$$

$$P_1 := \frac{1}{\sqrt{2}} E_0 - \frac{1}{\sqrt{2}} E_1 = \frac{1}{2}I - \frac{1}{2}Z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle \langle 1|$$

$$\rightsquigarrow \mathcal{E}_{PF,\frac{1}{2}}(\rho) = P_0 \rho P_0 + P_1 \rho P_1$$

(equivalent to standard basis measurement)

- Deplolarizing channel:

  Replace ρ by the completely mixed state $\frac{I}{2}$ with probability p:

  $$\mathcal{E}_{DP}(\rho) = p \cdot \frac{I}{2} + (1-p)\rho$$

  Block sphere representation: uniform contraction: (images in official script)
  Circuit representation of deplolarizing channel:
  (Make circuit here)

  Kraus form of deplolarizing channel:
  trick: for a normalized density matrix ρ $\operatorname{tr}[\rho] = 1$

  $$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}$$

  $$\rightsquigarrow \mathcal{E}_{DP}(\rho) = (1 - p + p\frac{1}{4})\rho + \frac{\rho}{4}(X\rho X + Y\rho Y + Z\rho Z)$$

  $$\rightsquigarrow E_0 = \sqrt{1 - \frac{3}{4}p}I, E_1 = \frac{\sqrt{P}}{2}X, E_2 = \frac{\sqrt{P}}{2}Y, E_3 = \frac{\sqrt{P}}{2}Z$$
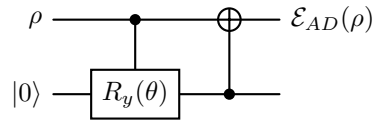
- Amplitude damping (see Nielsen and Chuang section 8.3.5, Exercice 13.1)
  e.g. photon in cavity

  $|0\rangle$: no photon
  $|1\rangle$: single photon

  $$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

  $E_1 |1\rangle = \sqrt{\gamma} |0\rangle$ Interpretation : $|1\rangle \rightarrow |0\rangle$ with probability γ

  Circuit representation:

  with $\gamma = \sin\left(\frac{\theta}{2}\right)^2$

- Phase damping (Nielsen and Chuang section 8.3.6)

"phase information" is lost

model: apply a "phase kick" $R_Z(\theta) = e^{-\frac{\theta}{2}Z} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$

with random angle $\theta \sim \frac{1}{\sqrt{4\pi\gamma}}e^{-\frac{\theta^2}{4\gamma}}$ (Gaussian distribution)

initial state $|\psi\rangle = a|0\rangle + b|1\rangle$
density matrix after random phase kick:

$$\rho = \frac{1}{\sqrt{4\pi\gamma}} \int_{-\infty}^{+\infty} R_Z(\theta) |\psi\rangle \langle\psi| R_Z(\theta)^\dagger e^{\frac{\theta^2}{4\gamma}} d\theta$$

$$= \begin{pmatrix} |a|^2 & ab^* e^{-\gamma} \\ a^*b\, e^{-\gamma} & |b|^2 \end{pmatrix}$$

off-diagonal entities are damped by $e^{-\gamma}$

Kraus form: $E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}$, $E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{pmatrix}$

unitary freedome $\rightsquigarrow$ can show that channel is equivalent to phase
channel is equivalent to phase flip channel:

$$\tilde{E}_0 = \sqrt{\alpha} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tilde{E}_1 \sqrt{1-\alpha}Z \text{ with } \alpha = \frac{1 + \sqrt{1-\lambda}}{2}$$

Application to Schrödinger's cat:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|dead\rangle |0\rangle + |alive\rangle |1\rangle)$$

$$\rho = |\psi\rangle \langle\psi| = \frac{1}{2} \begin{pmatrix} |dead\rangle |0\rangle \langle dead| \langle 0| + |dead\rangle |0\rangle \langle alive| \langle 1| \\ |alive\rangle |1\rangle \langle dead| \langle 0| + |alive\rangle |1\rangle \langle alive| \langle 1| \end{pmatrix}$$

off-diagonal entries $\rightarrow 0$ due to decoherence

$\rightarrow$ classical ensemble

$$\frac{1}{2}(|dead\rangle |0\rangle \langle dead| \langle 0| + |alive\rangle |1\rangle \langle alive| \langle 1|)$$

Properties

Bra-Ket (Dirac) notation

- **Ket:**

  - $|\psi\rangle + |\varphi\rangle = |\psi + \varphi\rangle$
  - $a\,|\psi\rangle = |a\psi\rangle$
  - $|\psi\rangle = \langle\psi|^{\dagger}$

  Righthand-side rules:

  - $\langle\psi \mid \varphi + \zeta\rangle = \langle\psi \mid \varphi\rangle + \langle\psi \mid \zeta\rangle$
  - $\langle\psi \mid a\varphi\rangle = a\,\langle\psi \mid \varphi\rangle$

  Complex conjugate:

  - $\langle\psi \mid \varphi\rangle^{*} = \langle\varphi \mid \psi\rangle$

  All left side rules can be build ontop of these (antilinearly)

- Riesz Representation Theorem results in: $\langle\psi|\,|\varphi\rangle = \langle\psi \mid \varphi\rangle = \psi \cdot \varphi$

Matrices

- **Normal matrix:**

  A is normal if it commutes with its conjugate transpose $A^{\dagger}$:

  $$A\ normal \Leftrightarrow A^{\dagger}A = AA^{\dagger}$$

- **Unitary matrix:**

  U is unitary if its matrix inverse $U^{-}1$ equals its conjugate transpose $U^{\dagger}$:

  $$U\ unitary \Leftrightarrow U^{\dagger}U = UU^{\dagger} = I$$

  Properties: For any unitary matrix U of finite size, the following hold:

  - $|\det(U)| = 1$
  - $\det(U)\ =: e^{i\theta}, \theta \in \mathbb{R}$

- **Hermitian matrix:**

  H is Hermitian if it's a square matrix that is equal to its conjugate transpose $H^{\dagger}$:

  $$H\ hermitian \Leftrightarrow H^{\dagger} = H$$

  For any hermitian matrix H of finite size, the following hold:

- All eigenvalues are real.
- Eigenvectors corresponding to distinct eigenvalues are orthogonal.
- In real-valued matrices, "Hermitian" just means symmetric ($A = A^T$)

- **Pauli matrices:**
  All Pauli matrices $M \in \{X, Y, Z\}$ also notated as $\sigma_i \mid i \in [3]$ satisfy these properties:

  $\sigma_j^2 = I$

  $\sigma_j \sigma_k = -\sigma_k \sigma_j \quad \forall j, k \in [3] \mid j \neq k$

  $[\sigma_j, \sigma_k] = \sigma_j \sigma_k - \sigma_k \sigma_j = 2i\sigma_l \quad \forall (j, k, l) \in \mathrm{Cyc}(1, 2, 3)$

  $\sigma_j \sigma_k = i\sigma_l \quad \forall (j, k, l) \in \mathrm{Cyc}(1, 2, 3)$

- **Diagonal matrices:**
  All Diagonal matrices $D \in R^{n \times n}$ satisfy these properties:

  $$e^{D \cdot x} = \begin{pmatrix} e^{d_{11} \cdot x} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{d_{nn} \cdot x} \end{pmatrix}$$

- **Density matrix/operator:**
  The density operator $\rho = \sum_i p_i \ket{\psi_i} \bra{\psi_i}$ has these properties:

  - ρ *hermitian* : $\rho^\dagger = (\ket{\psi}\bra{\psi})^\dagger = \ket{\psi}\bra{\psi} = \rho$
  - ρ *idempotent* : $\rho^2 = \ket{\psi}\braket{\psi|\psi}\bra{\psi} = \ket{\psi}\bra{\psi} = \rho \mid$ if **pure** state.
  - $\mathrm{tr}[\rho] = \sum_i p_i = \sum_i \lambda_i = 1$
  - May be rewritten as such: $\rho = \frac{I + (\vec{r} \cdot \vec{\sigma})}{2}$
  - ρ is positive semi-definite so all eigenvalues are positive: $\bra{\psi} P \ket{\psi} \geq 0$
  - The 2 eigenvalues of ρ can be calulcated as such: $\frac{1 \pm \|\vec{r}\|}{2}$