winter term 2022/2023

Introduction to Quantum Computing (IN2381)

Christian B. Mendl

1. Introduction

(see corresponding slides)

2. Basic concepts

2.1 Quantum bits (qubits)

(Nielsen and Chuang section 1.2)

Classical bits: $0, 1$

Quantum bit "qubit": superposition of 0 and 1:

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

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

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

ket-notation: $|\psi\rangle$ (motivation from inner product $\langle\varphi|\psi\rangle$)

Mathematical description: $|\psi\rangle \in \mathbb{C}^2$, with

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

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

Different from classical bits, cannot (in general) directly observe / measure a qubit (the amplitudes α and β)

Instead: "standard" measurement will result in

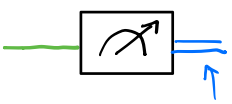
0 with probability $|\alpha|^2$

1 " $|\beta|^2$

The measurement also <u>changes</u> the qubit ("wavefunction collapse"):

If measuring 0, the qubit will be $|\psi\rangle = |0\rangle$ directly after the measurement, and likewise if measuring 1: qubit will be $|\psi\rangle = |1\rangle$.

In practice: can estimate the probabilities $|\alpha|^2$ and $|\beta|^2$ in experiments by repeating the same experiment many times (i.e. via outcome statistics).
These repetitions are called "trials" or "shots".

Circuit notation: 

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

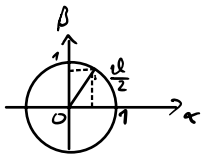
- two different polarizations of a photon, e.g. left/right circular
- alignment of a nuclear or electronic spin: $\uparrow$, $\downarrow$
- ground state or excited state of an atom (electronic state)
- clockwise or counterclockwise loop current states in a Josephson junction "superconducting qubit"

A useful graphical depiction of a qubit is the

Bloch sphere representation:

If α and β happen to be real-valued, then can find angle $\vartheta \in \mathbb{R}$ such that

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

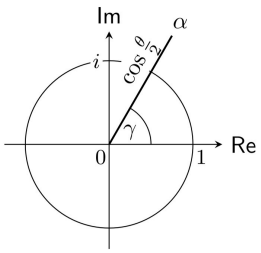


$$\left(\rightsquigarrow |\alpha|^2 + |\beta|^2 = \cos\left(\frac{\vartheta}{2}\right)^2 + \sin\left(\frac{\vartheta}{2}\right)^2 = 1 \ \checkmark\right)$$

in general: represent

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

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



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

Then:

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

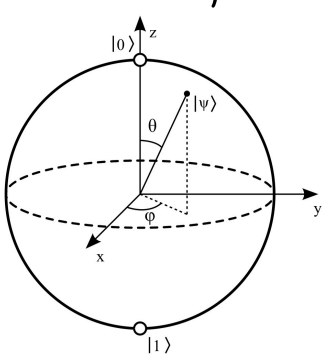
$$= \underbrace{e^{i\gamma}}_{\text{can be ignored here}} \left(\cos\left(\frac{\vartheta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\vartheta}{2}\right) |1\rangle \right)$$

Thus $|\psi\rangle$ is characterized by two angles ϑ and φ; these specify the point defined as

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

on the surface of a sphere:

Bloch sphere (Felix Bloch)



Source: https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg

Exercise: why are $|0\rangle$ and $|1\rangle$ at the poles?

2.2 Single qubit gates

(Nielsen and Chuang sections 1.3.1, 2.1.8, 4.2)

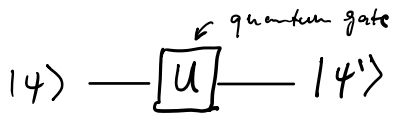
Principle of <u>time evolution</u>: the quantum state $|\psi\rangle$ at current time point t transitions to a new quantum state $|\psi'\rangle$ at a later time point $t' > t$.

Transition described by a complex unitary matrix U:

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

↑ matrix-vector multiplication

Circuit notation:



time flow →

Notes:
- circuit is read from left to right, but matrix times vector ($U|\psi\rangle$) from right to left
- U preserves normalization

Examples:
- quantum analogue of the classical NOT gate ($0 \leftrightarrow 1$)

  flip $|0\rangle \leftrightarrow |1\rangle$: leads to Pauli-X gate:

  $|0\rangle$ " $\begin{pmatrix}1\\0\end{pmatrix}$ $\quad$ $|1\rangle$ " $\begin{pmatrix}0\\1\end{pmatrix}$

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

(check: $X|0\rangle = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$,

$X|1\rangle = \cdots = |0\rangle$)

- 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 Bloch sphere representation:

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

Then:

$$Z|\psi\rangle = \cos\left(\frac{\vartheta}{2}\right)|0\rangle - e^{i\varphi}\sin\left(\frac{\vartheta}{2}\right)|1\rangle =$$

$$= \cos\left(\frac{\vartheta}{2}\right)|0\rangle + \underbrace{e^{i\pi}e^{i\varphi}}_{e^{i(\varphi+\pi)}}\sin\left(\frac{\vartheta}{2}\right)|1\rangle$$

($e^{i\pi} = -1$)

$\rightsquigarrow$ new Bloch sphere angles: $\vartheta' = \vartheta$, $\varphi' = \varphi + \pi$

(rotation by $\pi \hat{=} 180°$ around z-axis)

X, Y, Z gates are called <u>Pauli matrices</u>

The <u>Pauli vector</u> $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$

is a vector of 2×2 matrices

- Hadamard gate :

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

$$\alpha |0\rangle + \beta |1\rangle \quad \text{—} \boxed{H} \text{—} \quad \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

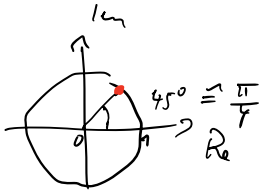
2.11.2022

- Phase gate :

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

- T gate :

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



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

Pauli matrices satisfy :

$\sigma_j^2 = I$ (identity) for $j = 1, 2, 3$ ($X \cdot X = I$, $Y \cdot Y = I$, $Z \cdot Z = I$)

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

$[\sigma_j, \sigma_k] := \sigma_j \sigma_k - \sigma_k \sigma_j = 2i\sigma_\ell$ for (j, k, ℓ) a cyclic permutation of $(1, 2, 3)$

↑ commutator

$[A, B] = A \cdot B - B \cdot A$

e.g. $j = 2$, $k = 3$, $\ell = 1$

$(1, 2, 3)$, $(2, 3, 1)$, $(3, 1, 2)$

General definition of <u>matrix exponential</u>:

$$\exp(A) \equiv e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k, \qquad A \in \mathbb{C}^{n\times n}$$

$A^k = A \cdot A \cdots A$ (k times)

Special case: $A^2 = I$, $x \in \mathbb{R}$ a real number

$$e^{iAx} = \sum_{\substack{k=0 \\ k \text{ even}}}^{\infty} \frac{1}{k!} (iAx)^k + \sum_{\substack{k=1 \\ k \text{ odd}}}^{\infty} \frac{1}{k!} (iAx)^k =$$

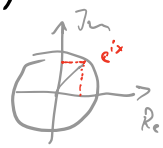
$$= \sum_{\tilde{k}=0}^{\infty} \frac{1}{(2\tilde{k})!} (ix)^{2\tilde{k}} \underbrace{A^{2\tilde{k}}}_{(A^2)^{\tilde{k}} = I} + \sum_{\tilde{k}=0}^{\infty} \frac{1}{(2\tilde{k}+1)!} (ix)^{2\tilde{k}+1} \underbrace{A^{2\tilde{k}+1}}_{(A^2)^{\tilde{k}} \cdot A = A}$$

($k = 2\tilde{k}$ in the first sum; $k = 2\tilde{k}+1$ in the second sum)

$$= \underbrace{\sum_{\tilde{k}=0}^{\infty} \frac{1}{(2\tilde{k})!} (-1)^{\tilde{k}} x^{2\tilde{k}}}_{\cos(x)} \cdot I + \underbrace{\sum_{\tilde{k}=0}^{\infty} \frac{1}{(2\tilde{k}+1)!} i\,(-1)^{\tilde{k}} x^{2\tilde{k}+1}}_{i \cdot \sin(x)} \cdot A$$

$$= \cos(x) \cdot I + i \sin(x)\, A \qquad (*)$$

(generalizes Euler's formula $e^{ix} = \cos(x) + i\sin(x)$)



This can be used to define the following <u>rotation operators</u> via the Pauli matrices: for $\vartheta \in \mathbb{R}$:

$$R_x(\vartheta) := e^{-i\vartheta X/2} = \cos\left(\tfrac{\vartheta}{2}\right) I - i \sin\left(\tfrac{\vartheta}{2}\right) X = \begin{pmatrix} \cos\left(\frac{\vartheta}{2}\right) & -i\sin\left(\frac{\vartheta}{2}\right) \\ -i\sin\left(\frac{\vartheta}{2}\right) & \cos\left(\frac{\vartheta}{2}\right) \end{pmatrix}$$

$$R_y(\vartheta) := e^{-i\vartheta Y/2} = \cos\left(\tfrac{\vartheta}{2}\right) I - i \sin\left(\tfrac{\vartheta}{2}\right) Y = \begin{pmatrix} \cos\left(\frac{\vartheta}{2}\right) & -\sin\left(\frac{\vartheta}{2}\right) \\ \sin\left(\frac{\vartheta}{2}\right) & \cos\left(\frac{\vartheta}{2}\right) \end{pmatrix}$$

$$R_z(\vartheta) := e^{-i\vartheta Z/2} = \cos\left(\tfrac{\vartheta}{2}\right) I - i \sin\left(\tfrac{\vartheta}{2}\right) Z = \begin{pmatrix} e^{-i\vartheta/2} & 0 \\ 0 & e^{i\vartheta/2} \end{pmatrix}$$

General case: rotation about an axis $\vec{v} \in \mathbb{R}^3$

(normalized such that $\|\vec{v}\| = \sqrt{v_1^2 + v_2^2 + v_3^2} \overset{!}{=} 1$):

using the notation:

$$\underbrace{\vec{v} \circ \vec{\sigma}}_{\langle \vec{v} | \vec{\sigma} \rangle} = v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3 = \begin{pmatrix} v_3 & v_1 - i v_2 \\ v_1 + i v_2 & -v_3 \end{pmatrix}$$

($\sigma_1 = X$, $\sigma_2 = Y$, $\sigma_3 = Z$)

It holds that $(\vec{v} \circ \vec{\sigma})^2 = I$:

$$(\vec{v} \circ \vec{\sigma})^2 = \begin{pmatrix} v_3^2 + (v_1 - i v_2)(v_1 + i v_2) & v_3 (v_1 - i v_2) + (v_1 - i v_2)(-v_3) \\ (v_1 + i v_2) v_3 - v_3 (v_1 + i v_2) & (v_1 + i v_2)(v_1 - i v_2) + (-v_3)^2 \end{pmatrix}$$

$$= \begin{pmatrix} v_1^2 + v_2^2 + v_3^2 & 0 \\ 0 & v_1^2 + v_2^2 + v_3^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We define the rotation operator around axis $\vec{v}$ as:

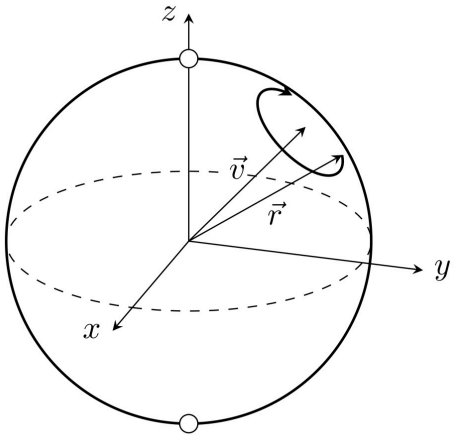
$$R_{\vec{v}}(\ell) := e^{-i \ell (\vec{v} \cdot \vec{\sigma})/2} = \cos\left(\tfrac{\ell}{2}\right) I - i \sin\left(\tfrac{\ell}{2}\right) (\vec{v} \circ \vec{\sigma})$$

Note: R_x, R_y, R_z are special cases, corresponding to

$\vec{v} = (1,0,0)$, $\vec{v} = (0,1,0)$, $\vec{v} = (0,0,1)$

Can derive that the Bloch sphere representation of $R_{\vec{v}}(\ell)$ is a "conventional" rotation (in three dimensions) by angle ℓ about axis $\vec{v}$!

$R_{\vec{v}}(\nu)\,|\psi\rangle$



rotation about axis $\vec{v}$
by angle ν
according to right hand rule

$\vec{r}$: Bloch vector of $|\psi\rangle$

<u>Z-Y decomposition</u> of an arbitrary 2×2 unitary matrix:

For any unitary matrix $U \in \mathbb{C}^{2\times 2}$ there exist
real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

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

2.3 Multiple qubits

(Nielsen and Chuang sections 1.2.1 , 2.1.7)

So far : single qubits , superposition of basis states $|0\rangle$ and $|1\rangle$

For two qubits, this generalizes to :

$$\{\, |00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle \,\}$$

as computational basis states : all combinations (bitstrings)
of 0s and 1s

General two-qubit state:

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

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:

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

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 result

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

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

Wavefunction directly after measurement:

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

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

normalization

Mathematical formalism for constructing two qubit states:

tensor product of vector spaces

Can combine two (arbitrary) vector spaces V and W to form the <u>tensor product</u> $V \otimes W$.

9.11.2022

The elements of $V \otimes W$ are linear combinations of "tensor products" $|v\rangle \otimes |w\rangle$ consisting of elements $|v\rangle \in V$, $|w\rangle \in W$.

Example: let $V = \mathbb{C}^2$, $W = \mathbb{C}^2$ be the single qubit spaces with basis $\{|0\rangle, |1\rangle\}$, then

$$\frac{1}{2} \underbrace{|0\rangle \otimes |0\rangle}_{= |00\rangle} + \frac{5i}{7} \underbrace{|1\rangle \otimes |0\rangle}_{= |10\rangle}$$

is an element of $V \otimes W$.

Let $\{|i\rangle_V : i = 1, \dots m\}$ be a basis of V, and $\{|j\rangle_W : j = 1, \dots n\}$ be a basis of W,

then $$\{|i\rangle_V \otimes |j\rangle_W : i = 1, \dots m, \ j = 1, \dots n\}$$

is a basis of $V \otimes W$.

In particular, $\dim(V \otimes W) = \dim(V) \cdot \dim(W)$

Note: $|i\rangle_V \otimes |j\rangle_W$ is also written as $|ij\rangle$.

Basic properties of tensor products:

- for all $|v\rangle \in V$, $|w\rangle \in W$ and $\alpha \in \mathbb{C}$:
$$\alpha \left(|v\rangle \otimes |w\rangle \right) = \left(\alpha |v\rangle \right) \otimes |w\rangle = |v\rangle \otimes \left(\alpha |w\rangle \right)$$
- for all $|v_1\rangle, |v_2\rangle \in V$ and $|w\rangle \in W$:
$$\left(|v_1\rangle + |v_2\rangle \right) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

- for all $|v\rangle \in V$ and $|w_1\rangle, |w_2\rangle \in W$:

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

Vector notation (using standard basis), e.g.

$$|v\rangle = v_1|0\rangle + v_2|1\rangle = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix},$$

$$|w\rangle = w_1|0\rangle + w_2|1\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}:$$

$$|v\rangle \otimes |w\rangle = (v_1|0\rangle + v_2|1\rangle) \otimes (w_1|0\rangle + w_2|1\rangle) =$$

$$= \underset{0}{v_1 w_1}|00\rangle + \underset{1}{v_1 w_2}|01\rangle + \underset{2}{v_2 w_1}|10\rangle + \underset{3}{v_2 w_2}|11\rangle$$

Thus: $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ v_2 w_1 \\ v_2 w_2 \end{pmatrix}$

Example: $\begin{pmatrix} 2 \\ 3 \end{pmatrix} \otimes \begin{pmatrix} 5 \\ 7 \end{pmatrix} = \begin{pmatrix} 10 \\ 14 \\ 15 \\ 21 \end{pmatrix}$

Note: not every element of $V \otimes W$ can be written in the form $|v\rangle \otimes |w\rangle$ with $|v\rangle \in V$ and $|w\rangle \in W$, for example the Bell state

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

$\langle v|w\rangle = \sum_j \overline{v_j} w_j$

Assuming that V and W have an inner product $\langle \cdot | \cdot \rangle$, define inner product on $V \otimes W$ by:

$$\left\langle \sum_j \alpha_j \underset{\in V}{|v_j\rangle} \otimes \underset{\in W}{|w_j\rangle} \;\middle|\; \sum_k \beta_k \underset{\in V}{|\tilde{v}_k\rangle} \otimes \underset{\in W}{|\tilde{w}_k\rangle} \right\rangle := \sum_j \sum_k \overline{\alpha_j}\, \beta_k \langle v_j|\tilde{v}_k\rangle \cdot \langle w_j|\tilde{w}_k\rangle$$

Generalization to n qubits: 2^n computational basis states

$$\{ |\underbrace{0,\dots 0}_{\text{length } n}\rangle, |0,\dots 0,1\rangle, |0\dots 10\rangle, \dots |11\dots 1\rangle \}$$

(all bit strings of length n)

Thus: general n-qubit quantum state, also denoted as "quantum register", given by:

$$|\psi\rangle = \sum_{x_0=0}^{1} \sum_{x_1=0}^{1} \cdots \sum_{x_{n-1}=0}^{1} \alpha_{x_{n-1}\dots x_1 x_0} \cdot |x_{n-1}\dots x_1 x_0\rangle =$$

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

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

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

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

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

2.4 Multiple qubit gates

(Nielsen and Chuang sections 1.3.2, 1.3.4, 2.1.7)

As for single qubits, an operation on multiple qubits is described by a unitary matrix U.

For n qubits: $U \in \mathbb{C}^{2^n \times 2^n}$

Example: <u>controlled-NOT</u> gate (also denoted CNOT):

two qubits: control and target,
target qubit gets flipped if control is 1:

$|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |10\rangle$

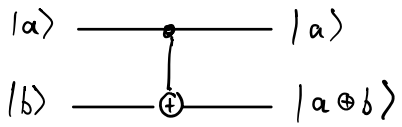
(control, target)

Can be expressed as:

$$|a, b\rangle \mapsto |a, a \oplus b\rangle \quad \text{for all} \quad a, b \in \{0,1\}$$

($\oplus$: addition modulo 2)

Circuit notation:



Matrix representation:

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

(Pauli-X)

unitary ✓

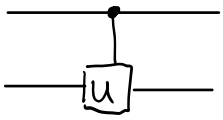
Alternative circuit notation:

Can generalize Pauli-X to any unitary operator U acting on target qubit $\rightsquigarrow$ controlled-U gate:

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

(control, target)

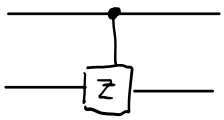
16. 11. 2022



$\hat{=}$

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \boxed{U} & \end{pmatrix}$$

Example: controlled - Z:

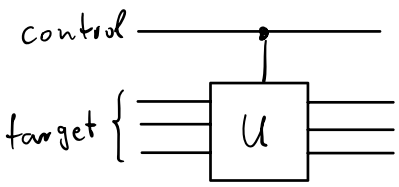


$\hat{=}$

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \boxed{\begin{matrix} 1 & \\ & -1 \end{matrix}} & \\ & & & Z \end{pmatrix}$$

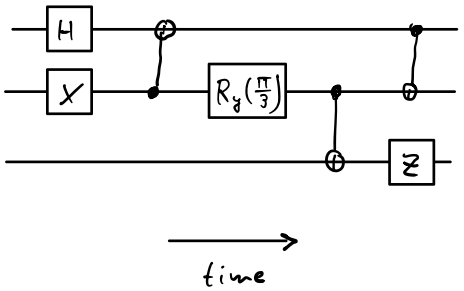
Exercise: show that controlled-Z gate is invariant when flipping control and target qubits.

Controlled-U for multiple target qubits:

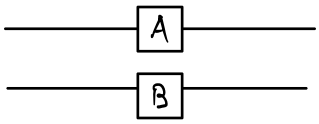


Note: single qubit and CNOT gates are <u>universal</u>: they can be used to implement an arbitrary unitary operation on n qubits (Quantum analogue of universality of classical NAND gate), proof in Nielsen and Chuang section 4.5

Example of a circuit consisting only of single qubit gates and CNOTs:



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



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), $B = Y$:

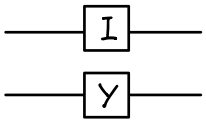
$$|00\rangle \mapsto |0\rangle \otimes \underbrace{(Y|0\rangle)}_{i|1\rangle} = i|01\rangle$$

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

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

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

Matrix representation:



$$\hat{=} \begin{pmatrix} \overbrace{\begin{matrix} 0 & -i \\ i & 0 \end{matrix}}^{Y} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \underbrace{\begin{matrix} 0 & -i \\ i & 0 \end{matrix}}_{Y} \end{pmatrix} = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} = I \otimes Y$$

(2×2)

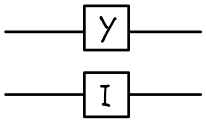
General formula: <u>Kronecker product</u> (matrix representation of tensor products of operators)

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

for $A \in \mathbb{C}^{m \times n}$, $B \in \mathbb{C}^{p \times q}$

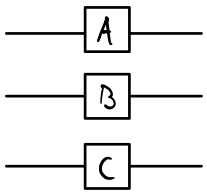
NumPy: `np.kron(A,B)`

Another example:



$$\widehat{=}\quad Y \otimes I = \begin{pmatrix} 0\cdot I & -i\cdot I \\ i\,I & 0\cdot I \end{pmatrix} = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -i \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}$$

Generalization to arbitrary number of tensor factors possible, e.g.



$$\widehat{=}\quad A \otimes B \otimes C$$

$$= (A \otimes B) \otimes C = A \otimes (B \otimes C)$$

Basic properties:

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

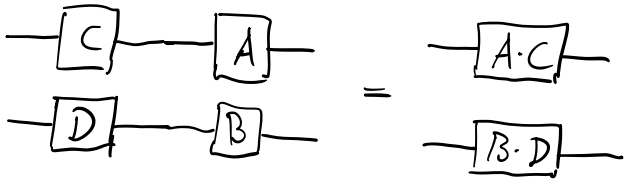
(b) $(A \otimes B)^T = A^T \otimes B^T$ (transposition)

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

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

(e) $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$ for matrices of compatible dimensions

↑ matrix-matrix multiplication



(f) Kronecker product of Hermitian matrices is Hermitian

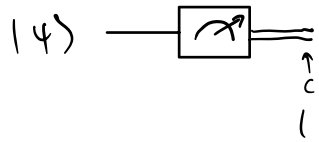
(g) Kronecker product of unitary matrices is unitary

(follows from (c) and (e))

2.5 Quantum measurement

(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 the computational basis $\{|0\rangle, |1\rangle\}$:



Linear algebra: can switch to a different (orthonormal) basis to represent a qubit, e.g.

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

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

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

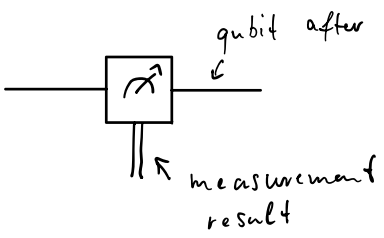
Representation of $|\psi\rangle$ w.r.t. $\{|+\rangle, |-\rangle\}$ basis:

$$\alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

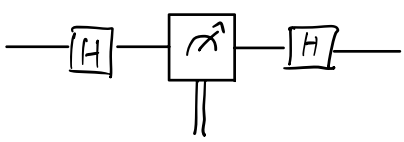
Can perform measurement with respect to orthonormal basis $\{|+\rangle, |-\rangle\}$, will obtain result

- $+$ with probability $\frac{|\alpha+\beta|^2}{2}$,
- $-$ with probability $\frac{|\alpha-\beta|^2}{2}$

Wavefunction collapse: immediately after the measurement, qubit will be in the state $|+\rangle$ if measured "+", likewise $|-\rangle$ " "−"



base change:



In general, given an orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$, one can represent a qubit as $|\psi\rangle = \alpha_1 |u_1\rangle + \alpha_2 |u_2\rangle$ and measure with respect to this orthonormal basis; will obtain measurement result "u_1" or "u_2" with respective probabilities $|\alpha_1|^2$ and $|\alpha_2|^2$.

23.11.2022

Abstract, general definition of quantum measurements:
Quantum measurements are described by a collection $\{M_m\}$ of <u>measurement operators</u> acting on the quantum system, with the index m labelleling possible measurement outcomes.
Denoting the quantum state before 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 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 probabilities sum to 1:

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

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

$$M_0 := |0\rangle\langle 0| = \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{2\times 1} \underbrace{\begin{pmatrix} 1 & 0 \end{pmatrix}}_{1\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

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

$$\rightsquigarrow p(0) = \langle \psi | M_0^\dagger M_0 |\psi\rangle = \langle \psi | M_0 |\psi\rangle = |\alpha|^2$$

$$p(1) = \cdots = |\beta|^2$$

Projective measurements

c.f. cheat sheet:

Projector onto subspace V with orthonormal basis $\{|u_1\rangle, \dots |u_m\rangle\}$:

$$P = \sum_{j=1}^{m} |u_j\rangle\langle u_j| \qquad P^\dagger = P, \quad P^2 = P$$

$$P|w\rangle = \sum_{j=1}^{m} |u_j\rangle \underbrace{\langle u_j | w\rangle}_{\text{inner product}}$$

Relation to spectral decomposition of a normal matrix $A \in \mathbb{C}^{n\times n}$:

$$A = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} U^\dagger = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| =$$

(λ_j: not necessarily all different)

$$= \sum_{k=1}^{m} \tilde{\lambda}_k P_k \quad \text{with } \{\tilde{\lambda}_1 .. \tilde{\lambda}_m\} \text{ the distinct eigenvalues}$$

(P_k: projection onto eigenspace of eigenvalue $\tilde{\lambda}_k$)

Definition: A <u>projective measurement</u> is described by an <u>observable</u> M, a Hermitian operator acting on the quantum system.

Spectral decomposition:

$$M = \sum_m \lambda_m P_m$$

with P_m: projection onto eigenspace with eigenvalue λ_m.

The possible outcomes of the measurement correspond to the eigenvalues λ_m.

Probability of getting result λ_m when measuring a quantum state $|\psi\rangle$:

$$p(\lambda_m) = \langle\psi| \underbrace{P_m}_{= P_m^2 = P_m^\dagger P_m \text{ since } P_m \text{ is projection}} |\psi\rangle.$$

State of the quantum system directly 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 general measurement framework
- Projective measurements combined with unitary transformations are equivalent to general measurement framework, see pages 94, 95 in Nielsen and Chuang

Average value of a projective measurement:

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

$$= \langle \psi | M | \psi \rangle = \langle M \rangle$$

(if $|\psi\rangle$ is clear from context)

Corresponding standard deviation

$$\Delta(M) := \sqrt{\langle M^2 \rangle - \langle M \rangle^2} = \sqrt{\langle (M - \langle M \rangle)^2 \rangle}$$

Examples:

- Measuring a qubit w.r.t. computational basis $\{|0\rangle, |1\rangle\}$ is actually a projective measurement
- In general: measurement w.r.t. orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$ is a projective measurement: set

  $P_m = |u_m\rangle\langle u_m|$ for $m = 1, 2$

  define observable M by

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

- Measuring Pauli-Z:

$$Z = 1 \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{P_1} + (-1) \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{P_2}$$

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

2.6 The Heisenberg uncertainty principle

Box 2.4 in Nielsen and Chuang

Suppose A and B are Hermitian operators, and $|\psi\rangle$ a quantum state

Write $\langle\psi|AB|\psi\rangle = x + iy$, $x, y \in \mathbb{R}$

$\langle\psi|AB|\psi\rangle^* = \langle\psi|(AB)^\dagger|\psi\rangle = \langle\psi|B^\dagger A^\dagger|\psi\rangle = \langle\psi|BA|\psi\rangle$

thus

$\langle\psi|\underbrace{[A,B]}_{AB-BA \text{ commutator}}|\psi\rangle = 2iy$ and $\langle\psi|\underbrace{\{A,B\}}_{AB+BA \text{ anti-commutator}}|\psi\rangle = 2x$

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4\underbrace{|\langle\psi|AB|\psi\rangle|^2}_{x^2+y^2} \quad (*)$$

Cauchy-Schwarz inequality applied to $|v\rangle = A|\psi\rangle$, $|w\rangle = B|\psi\rangle$:

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle \cdot \langle\psi|B^2|\psi\rangle$$

$$|\langle v|w\rangle|^2 \leq \|v\|^2 \cdot \|w\|^2$$

$$|\langle\psi|[A,B]|\psi\rangle|^2 \overset{(*)}{\leq} 4\cdot|\langle\psi|AB|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\cdot\langle\psi|B^2|\psi\rangle$$

Suppose C and D are two observables: substitute $A = C - \langle C\rangle$, $B = D - \langle D\rangle$

leads to Heisenberg uncertainty principle:

$$\Delta(C)\cdot\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}.$$

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

3. Entanglement and its applications

30.11.2022

A n-qubit state $|\psi\rangle$ $(n \geq 2)$ is called <u>entangled</u> if it cannot be written as tensor product of single-qubit states, i.e.

$$|\psi\rangle \neq |\varphi_{n-1}\rangle \otimes \dots \otimes |\varphi_0\rangle \quad \text{for any } |\varphi_0\rangle, \dots |\varphi_{n-1}\rangle \in \mathbb{C}^2$$

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

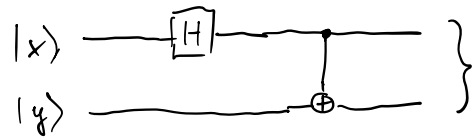
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad \neq |a\rangle|b\rangle$$

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

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

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

Quantum circuit to create Bell states:



$\} |\beta_{xy}\rangle$ for $x, y \in \{0,1\}$

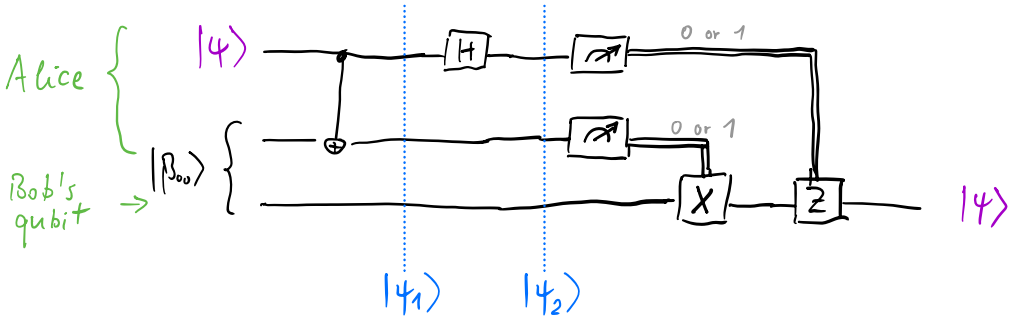
3.1 Quantum teleportation

(Nielsen and Chuang section 1.3.7)

Scenario: two (experimental physicists) Alice and Bob, are far away from each other

When visiting each other a long time ago, they generated the EPR pair $|\beta_{00}\rangle$ each keeping one qubit of the pair.
Alice's task is to send another (unknown) qubit $|\psi\rangle$ to Bob.
Note: measurement is not an option.

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



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

($|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$; CNOT)

after CNOT:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\right)$$

after Hadamard:

$$|\psi_2\rangle = \frac{1}{2}\left(\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\right) =$$

$$= \frac{1}{2}\left(\alpha|000\rangle+\alpha|011\rangle+\alpha|100\rangle+\alpha|111\rangle+\beta|010\rangle+\beta|001\rangle-\beta|110\rangle-\beta|101\rangle\right)$$

$$= \frac{1}{2}\left(|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\right)$$

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

$$|00\rangle(\alpha|0\rangle+\beta|1\rangle) = |00\rangle|\psi\rangle$$

($|\psi\rangle$: qubit at Bob's place)

Similarly:

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

Alice transmits her measurement result to Bob (classical information), Bob then applies Pauli-X and/or Pauli-Z to recover $|\psi\rangle$.

Even though wave function collapse is instantaneous,
no faster-than-light information transfer possible
due to required classical communication.

3.2 EPR and the Bell inequality

(Nielsen and Chuang section 2.6)

EPR: Einstein, Podolsky, Rosen

EPR paper: "Can quantum mechanical description of physical reality
be considered complete?" (1935)

The author argue that quantum mechanics is incomplete
since it lacks certain "elements of reality".
↑
property can be predicted with certainty

Scenario: Alice and Bob are far from each other,
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 $\vec{v}\cdot\vec{\sigma} = v_1 X + v_2 Y + v_3 Z$
(with $v \in \mathbb{R}^3$, $\|\vec{v}\| = 1$) on their respective qubit

(Recall $\vec{v}\cdot\vec{\sigma}$ is Hermitian and unitary, and has eigenvalues ± 1)

Alice performs her measurement immediately before Bob.

Example:

- $\vec{v} = (0,0,1)$, observable $Z = 1 \cdot |0\rangle\langle 0| + (-1)\,|1\rangle\langle 1|$
(standard measurement)

if Alice measures eigenvalue

1: wave function collapses to $|01\rangle$

-1: " $|10\rangle$

⇝ Bob will always obtain the opposite measurement result.

7.12.2022

- $\vec{v} = (1,0,0)$, observable : X, eigenstates $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$,
  corresponding eigenvalues ∓ 1
  (measurement w.r.t. $\{|+\rangle, |-\rangle\}$ basis)

  Can represent the wavefunction as

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

namely:

$$-\frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right) = -\frac{1}{\sqrt{2}}\left(\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) - \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)\right)$$

$$= \dots = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = |\beta_{11}\rangle$$

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

- general observable $\vec{v}\cdot\vec{\sigma}$, general unit vector $\vec{v} \in \mathbb{R}^3$:
  denote the orthogonal eigenstates of $\vec{v}\cdot\vec{\sigma}$ by $|a\rangle$, $|b\rangle$,
  then there exist complex numbers $\alpha, \beta, \gamma, \delta$ such that

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

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

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

  U is base change matrix between orthonormal $\{|0\rangle, |1\rangle\}$ and $\{|a\rangle, |b\rangle\}$ basis $\rightsquigarrow$ U unitary $\rightsquigarrow$ $|\det(U)| = 1$ (↑ Exercise 1.2(e))

  Can represent $\det(U) = e^{i\vartheta}$, $\vartheta \in \mathbb{R}$

  In summary: $\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = e^{i\vartheta}\frac{1}{\sqrt{2}}\left(|ab\rangle - |ba\rangle\right)$
  (opposite, opposite)

→ 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 too slow)

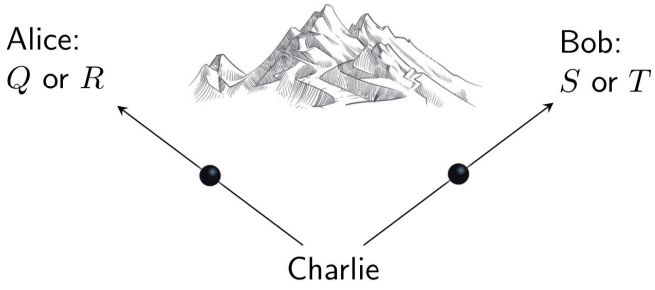
EPR argument: "property" $\vec{v} \cdot \vec{\sigma}$ of a qubit is an "element of reality", however, quantum mechanics does not a priori specify this property for all possible $\vec{v}$ (but only probabilities), and is thus an incomplete description of reality.

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

Bell's inequality: experimental test which can invalidate local hidden variable theories (Bell 1964)

"local" no faster-than-light communication possible
(otherwise one could send information backwards in time according to special relativity)

Experimental schematic: many repetitions (to collect statistics) of the following setup:



binary property values : $Q \in \{\pm 1\}$, $R \in \{\pm 1\}$, $S \in \{\pm 1\}$, $T \in \{\pm 1\}$

Alice decides randomly whether to measure property Q or R

Bob " S or T

Alice and Bob perform their measurement (almost) simultaneously, such that no information about the result can be transmitted in between.

After completing this protocol, Alice and Bob meet to analyze their measurement data.

Consider the quantity:

$$QS + RS + RT - QT = (Q+R)S + (R-Q)T = \pm 2$$

$$\underbrace{\pm 2}_{0} \quad \longleftrightarrow \quad \underbrace{0}_{\pm 2}$$

Denote by $p(q,r,s,t)$ the probability that the system before measurements is in state $Q=q$, $R=r$, $S=s$, $T=t$, then

$$\mathbb{E}[QS+RS+RT-QT] = \sum_{q,r,s,t \in \{\pm 1\}} p(q,r,s,t) \underbrace{(qs+rs+rt-qt)}_{\pm 2} \leq$$

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

By linearity of $\mathbb{E}$, arrive at the following

Bell inequality:

$$\mathbb{E}[QS] + \mathbb{E}[RS] + \mathbb{E}[RT] - \mathbb{E}[QT] \leq 2$$

Each term can be experimentally evaluated,

e.g. for $\mathbb{E}[QS]$: Alice and Bob average over cases where Alice measured Q and Bob measured S.

Compare with "quantum" realization of the experiment:

Charlie prepare the two-qubit singlet state

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

and sends the first qubit to Alice and the second to Bob.

Observables:

$$Q = Z_1 \quad \text{(first qubit)}, \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}} \quad \text{(second qubit)}$$

$$R = X_1, \qquad T = \frac{Z_2 - X_2}{\sqrt{2}}$$

Measurement averages (c.f. Exercise 8.1):

$$\langle QS \rangle \equiv \langle \psi | Q \otimes S | \psi \rangle = \frac{1}{\sqrt{2}}, \qquad \langle RS \rangle = \frac{1}{\sqrt{2}}$$

$$\langle RT \rangle = \frac{1}{\sqrt{2}}, \qquad \langle QT \rangle = -\frac{1}{\sqrt{2}}$$

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2} \not\leq 2$$

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, R, S, T have definite values independent of observation (measurement)
- locality: Alice performing her measurement cannot influence Bob's measurement and vice versa

$\rightsquigarrow$ Nature is not "locally realistic"
(most common viewpoint: realism does not hold)

Practical lesson: use entanglement as resource.

4. Quantum search algorithms

14. 12. 2022

(Nielsen and Chuang : section 6)

Classical search through N unordered elements $O(N)$

Quantum Grover's algorithm : $O(\sqrt{N})$ (given certain preconditions)

4.1 Quantum oracles

Search space of $N = 2^n$ elements, labelled $0, 1, \dots N-1$

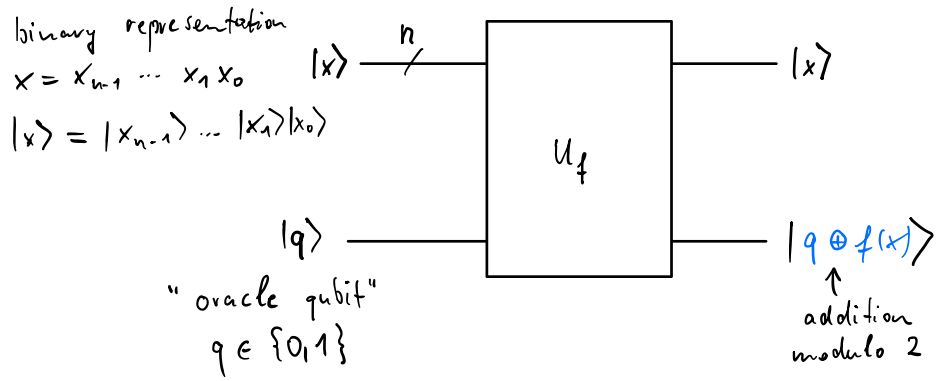
Assume there are M solutions (with $1 \leq M \leq N$)

Define corresponding indicator function $f : \{0 \dots N-1\} \to \{0,1\}$ by

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

Quantum version of f ?

$\rightsquigarrow$ quantum "oracle" U_f defined for computational basis states as



Note: 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 permutes basis states and is in particular unitary.

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

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xmapsto{U_f} \begin{cases} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(x) = 0 \\ |x\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(x) = 1 \end{cases}$$

In summary: $|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xmapsto{U_f} \underbrace{(-1)^{f(x)}|x\rangle}_{\text{only this part relevant for the following}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ ← oracle qubit unchanged

⇝ effective action of oracle: $|x\rangle$ — U_f — $(-1)^{f(x)}|x\rangle$

Oracle "marks" solution by a phase flip,

How could one construct such an oracle without knowing solution already?

Example: factorization of a large integer $m \in \mathbb{N}$:

Finding prime factor of m is "difficult" on a classical computer:
(no known algorithm with polynomial runtime in the bit length of m)

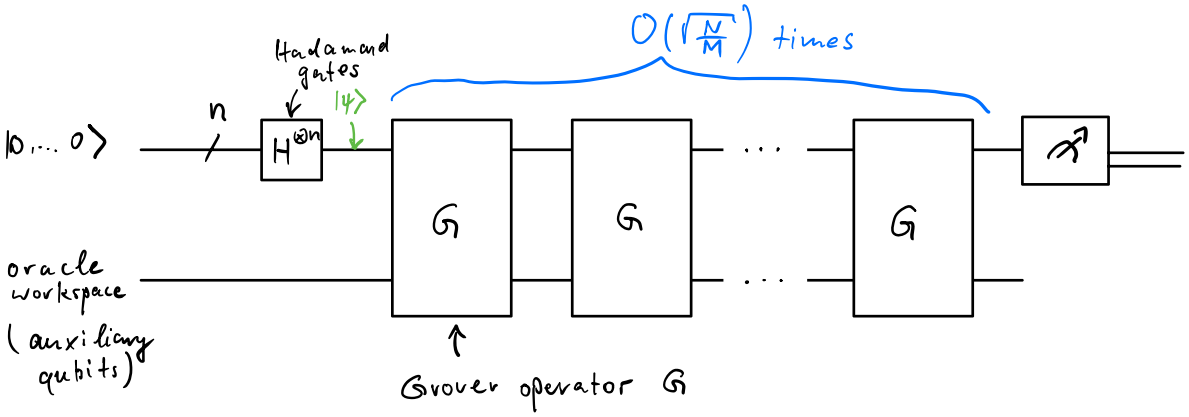
but testing whether a given $x \in \mathbb{N}$ divides m is simple.

Can perform arithmetic operations for trial division on a digital quantum computer as well ⇝ oracle which recognizes a solution x.

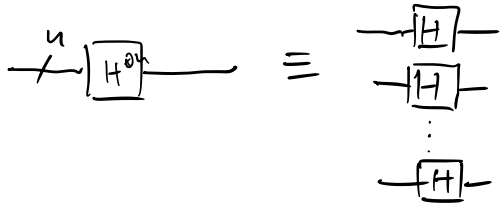
4.2 Grover's algorithm

Search space with $N = 2^n$ elements, M solutions

Overall circuit diagram for Grover's algorithm:



Initial Hadamard transform:



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

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:

$$\underbrace{H^{\otimes n}}_{H \otimes H \otimes \dots \otimes H} |x_1 \dots x_n\rangle = \underbrace{(H|x_1\rangle)}_{\frac{1}{\sqrt{2}} \sum_{z_1=0}^{1} (-1)^{x_1 z_1} |z_1\rangle} \otimes \dots \otimes (H|x_n\rangle) = \frac{1}{\sqrt{2^n}} \sum_{z_1 \dots z_n = 0}^{1} (-1)^{x_1 z_1 + \dots + x_n z_n} \overbrace{|z_1\rangle \dots |z_n\rangle}^{|z_1 \dots z_n\rangle}$$

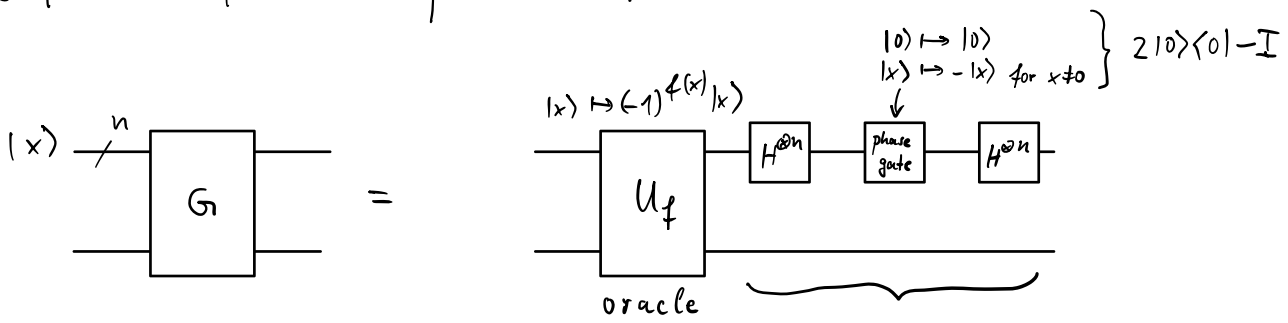
dot product

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

z: bit string

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

Definition of Grover operator G:



$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} =$$

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

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

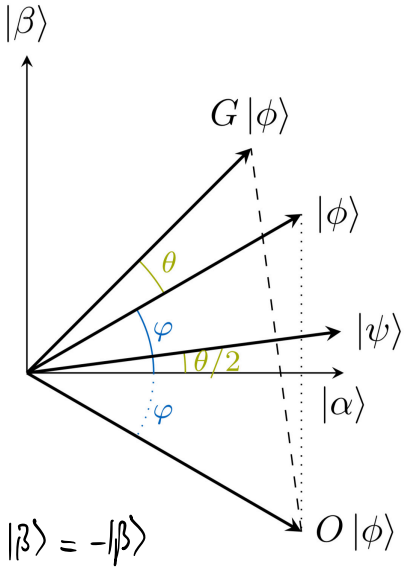
In summary $G = (2|\psi\rangle\langle\psi| - I)\,U_f$

Geometric interpretation

Define

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

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



angle ℓ defined by $\sin\left(\frac{\ell}{2}\right) = \sqrt{\frac{M}{N}}$,

such that $|\psi\rangle = \cos\left(\frac{\ell}{2}\right)|\alpha\rangle + \sin\left(\frac{\ell}{2}\right)|\beta\rangle$

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 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 subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$,

G leaves subspace invariant!

Thus G is a product of two reflections $\rightsquigarrow$

G is a rotation by angle ℓ

$$|\phi\rangle = \cos(\varphi)|\alpha\rangle + \sin(\varphi)|\beta\rangle$$

$$\rightsquigarrow G|\phi\rangle = \cos(\varphi+\ell)|\alpha\rangle + \sin(\varphi+\ell)|\beta\rangle$$

21.12.2022

[Algebraic derivation: see notes on Moodle]

For k applications of G:

$$G^k|\phi\rangle = \cos(\varphi + k\cdot\ell)|\alpha\rangle + \sin(\varphi + k\cdot\ell)|\beta\rangle$$

for initial state $|\psi\rangle$: $\varphi = \frac{\ell}{2}$

$$G^k|\psi\rangle = \cos\left((k+\tfrac{1}{2})\ell\right)|\alpha\rangle + \sin\left((k+\tfrac{1}{2})\ell\right)|\beta\rangle$$

Goal: rotate to $|\beta\rangle$, i.e. $(k+\frac{1}{2})\ell \overset{!}{=} \frac{\pi}{2}$

since $\sin\left(\frac{\ell}{2}\right) = \sqrt{\frac{M}{N}}$, for $M \ll N$ ($\sin(x) \approx x$ for $x \ll 1$) $\ell \approx 2\sqrt{\frac{M}{N}}$

Thus need $O\left(\sqrt{\frac{N}{M}}\right)$ rotations

$k \cdot \vartheta$ should be $O(1)$, $k \approx \frac{1}{\vartheta}$

$\left(k + \frac{1}{2} = \frac{\pi}{2\vartheta},\ k = \frac{\pi}{2\vartheta} - \frac{1}{2}\right)$

Final step: standard measurement,
will collapse quantum state (with high probability)
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: single solution x

Recall that oracle flips sign of solutions:

$$O_x = I - 2|x\rangle\langle x| \qquad \text{(denoted } U_f \text{ in previous section)}$$

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

State after k steps:

$$|\psi_k^x\rangle = U_k O_x U_{k-1} O_x \cdots U_1 O_x |\psi_0\rangle$$

($|\psi_0\rangle$: initial state)

We also define

$$|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi_0\rangle \qquad \text{(omit oracle calls)}$$

Strategy of proof: upper bound of

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

(x: case that x is solution)

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

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

$k = 0$: $D_0 = 0$ ✓

$k \to k+1$: $\| U_{k+1} (O_x |\psi_k^x\rangle - |\psi_k\rangle) \|^2$ (can be omitted inside norm)

$$D_{k+1} = \sum_x \| O_x |\psi_k^x\rangle - |\psi_k\rangle \|^2 =$$

$$= \sum_x \| \underbrace{O_x (|\psi_k^x\rangle - |\psi_k\rangle)}_{b} + \underbrace{(O_x - I)|\psi_k\rangle}_{-2|x\rangle\langle x|\psi_k\rangle = c} \|^2$$

$\| b+c \|^2 = \langle b+c | b+c \rangle \leq \|b\|^2 + 2\|b\| \cdot \|c\| + \|c\|^2$

$$\leq \sum_x \left(\|b\|^2 + 2\|b\| \cdot \|c\| + \|c\|^2 \right)$$

O_x is unitary $=$

$$\sum_x \Big(\underbrace{\| |\psi_k^x\rangle - |\psi_k\rangle \|^2}_{\text{Cauchy–Schwarz}} + 4 \underbrace{\| |\psi_k^x\rangle - |\psi_k\rangle \|}_{\text{Cauchy–Schwarz}} |\langle x|\psi_k\rangle| + 4 \underbrace{|\langle x|\psi_k\rangle|^2}_{\sum_x \cdots = 1} \Big)$$

$$\leq D_k + 4 \Big(\underbrace{\sum_x \| |\psi_k^x\rangle - |\psi_k\rangle \|^2}_{D_k} \Big)^{\frac{1}{2}} \Big(\underbrace{\sum_x |\langle x|\psi_k\rangle|^2}_{1} \Big)^{\frac{1}{2}} + 4$$

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

induction $\leq 4k^2 + 8k + 4 = 4(k+1)^2$ ✓

Second part of proof: D_k must be $\Omega(N)$:

To find solution x, want that $|\psi_k^x\rangle \approx |x\rangle$

Suppose $|\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$ for all x

(probability of success 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)

$$\rightsquigarrow \| |\psi_k^x\rangle - |x\rangle \|^2 = \underbrace{\| |\psi_k^x\rangle \|^2}_{1} - 2\langle x|\psi_k^x\rangle + \underbrace{\| |x\rangle \|^2}_{1}$$

$$= 2 - 2\underbrace{\langle x|\psi_k^x\rangle}_{\geq \frac{1}{\sqrt{2}}} \leq 2 - \sqrt{2}$$

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

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

$$F_k = \sum_x \left(\underbrace{\| |x\rangle \|^2}_{1} - 2\,\mathrm{Re}\,\langle x|\psi_k\rangle + \underbrace{\| |\psi_k\rangle \|^2}_{1} \right)$$

$$\geq 2N - 2 \underbrace{\sum_x |\langle x|\psi_k\rangle| \cdot 1}_{\leq \sqrt{\underbrace{\sum_x |\langle x|\psi_k\rangle|^2}_{=1}} \cdot \sqrt{\underbrace{\sum_x 1}_{=N}}} \geq 2N - 2\sqrt{N}$$

$$D_k = \sum_x \| \left(|\psi_k^x\rangle - |x\rangle \right) + \left(|x\rangle - |\psi_k\rangle \right) \|^2$$

$$\geq \sum_x \left(\| |\psi_k^x\rangle - |x\rangle \|^2 - 2 \| |\psi_k^x\rangle - |x\rangle \| \cdot \| |x\rangle - |\psi_k\rangle \| + \| |x\rangle - |\psi_k\rangle \|^2 \right)$$

$$= E_k + F_k - 2 \sum_x \overbrace{\| |\psi_k^x\rangle - |x\rangle \|}^{a_x} \cdot \overbrace{\| |x\rangle - |\psi_k\rangle \|}^{b_x}$$

$$\left| \sum_x a_x \cdot b_x \right| \leq |\langle a|b\rangle| \leq \|a\| \cdot \|b\|$$

$$\geq E_k + F_k - 2\sqrt{E_k}\sqrt{F_k} = \left(\sqrt{F_k} - \sqrt{E_k} \right)^2 \geq$$

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

$$= N \left(\sqrt{2 - \underbrace{\tfrac{2}{\sqrt{N}}}_{\to 0 \text{ as } N\to\infty}} - \sqrt{2-\sqrt{2}} \right)^2$$

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

↑ asymptotically equal to

In summary: $\underbrace{D_k \leq 4 \cdot k^2 \quad \text{and} \quad D_k \geq c \cdot N}$

$$k \geq \sqrt{\frac{cN}{4}}$$

↑ number of oracle evaluations

11.1.2023

Thought experiment: If it was possible to search using $O(\log(N))$ oracle calls, then a QC could solve NP-complete problems efficiently: just search through $2^{w(n)}$ witnesses using $w(n)$ oracle calls.

$w(n)$: bit length of a witness

5. The density operator

So far: state vector $|\psi\rangle$ describing a quantum state

Convenient alternative formulation for quantum systems about which we only have partial information:

density operator (also called density matrix)

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: ensemble of quantum states $\{p_i, |\psi_i\rangle\}$

The density operator ρ of the ensemble $\{p_i, |\psi_i\rangle\}$ is defined as

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

($\langle\psi_i|$: outer product)

Quantum mechanics in terms of density operators:

- unitary operations: a unitary transformation U maps $|\psi_i\rangle \mapsto U|\psi_i\rangle$, and the ensemble to $\{p_i, U|\psi_i\rangle\}$

  Thus the density operator is transformed as

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

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

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle \overset{tr[ABC]=tr[BCA]}{=} tr\left[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right]$$

$tr[|\psi\rangle\langle\varphi|] = \langle\varphi|\psi\rangle$

Thus overall probability for result m is:

$$p(m) = \sum_i p(m|i)\, p_i = \sum_i tr\left[M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right] p_i =$$

$$= tr\left[M_m^\dagger M_m \underbrace{\sum_i p_i |\psi_i\rangle\langle\psi_i|}_{\rho}\right] = tr\left[M_m^\dagger M_m \rho\right]$$

Density operator ρ_m after obtaining result m?

State i collapses to $|\psi_i\rangle \longmapsto \frac{M_m|\psi_i\rangle}{\|M_m|\psi_i\rangle\|} =: |\psi_i^m\rangle$

Thus:

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

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

$\uparrow$

$$\frac{p(i|m)}{p(m|i)} = \frac{p_i}{p(m)} \quad \text{(Bayes' theorem)}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(B|A)\cdot P(A)}{P(B)}$$

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 (positivity condition).

Remark: ρ is called a <u>positive operator</u> if it is Hermitian and all its eigenvalues are ≥ 0, equivalently if $\langle\varphi|\rho|\varphi\rangle \geq 0$ for all vectors $|\varphi\rangle$

Proof.

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

$$\mathrm{tr}[\rho] = \sum_i p_i \,\mathrm{tr}\left[|\psi_i\rangle\langle\psi_i|\right] = \sum_i p_i \underbrace{\langle\psi_i|\psi_i\rangle}_{1} = 1,$$

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

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle = \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \geq 0.$$

"$\Leftarrow$" ρ is an operator (i.e. a Hermitian matrix) $\rightsquigarrow$ by spectral theorem: there exist eigenvalues λ_j and corresponding orthonormal eigenvectors $|\varphi_j\rangle$ such that

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

Since ρ satisfies the trace condition:

$$1 = \mathrm{tr}[\rho] = \sum_j \lambda_j \,\mathrm{tr}\left[|\varphi_j\rangle\langle\varphi_j|\right] = \sum_j \lambda_j \underbrace{\langle\varphi_j|\varphi_j\rangle}_{1} = \sum_j \lambda_j,$$

due to positivity of ρ: $\lambda_j \geq 0$ for all j.

Thus can interpret eigenvalues λ_j as probabilities $\rightsquigarrow$ $\{\lambda_j, |\varphi_j\rangle\}$ is an ensemble which gives rise to ρ. □

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

Language regarding density operators:

"pure state"

Quantum system in a state $|\psi\rangle$, corresponding density operator

$$\rho = |\psi\rangle\langle\psi|$$

such that

$$\mathrm{tr}[\rho^2] = \mathrm{tr}[|\psi\rangle\langle\psi|\psi\rangle\langle\psi|] = \mathrm{tr}[|\psi\rangle\langle\psi|] \quad (\langle\psi|\psi\rangle = 1)$$
$$= \langle\psi|\psi\rangle = 1$$

"mixed state"

ρ describing quantum setup cannot be written as $\rho = |\psi\rangle\langle\psi|$;

intuition: in the ensemble representation $\{p_i, |\psi_i\rangle\}$ of ρ, all the probabilities are strictly smaller than 1.

Then $\mathrm{tr}[\rho^2] = \sum_i p_i^2 < 1$.

In general: Let ρ be a density operator. Then $\mathrm{tr}[\rho^2] \leq 1$, and $\mathrm{tr}[\rho^2] = 1$ 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 $1 = \mathrm{tr}[\rho] = \sum_i \lambda_i$.

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

Ensemble representation is not unique!

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

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 $\langle a|b\rangle \neq 0$)

18.1.2023

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

Ensemble $\{|\tilde{\psi}_i\rangle\}$ <u>generates</u> the density operator ρ.

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

Unitary freedom in the ensemble for density matrices:
The sets $\{|\tilde{\psi}_i\rangle\}$ and $\{|\tilde{\varphi}_j\rangle\}$ generate the same density matrix if and only if

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij}\,|\tilde{\varphi}_j\rangle$$

for some unitary matrix (u_{ij}).

Sketch of proof:
"$\Leftarrow$" Insert definitions.
"$\Rightarrow$" Use the spectral decomposition of the density matrix:

$$\rho = \sum_k \lambda_k\,|\chi_k\rangle\langle\chi_k| \quad \text{with} \quad \langle\chi_k|\chi_\ell\rangle = \delta_{k\ell},$$

set $|\tilde{\chi}_k\rangle = \sqrt{\lambda_k}\,|\chi_k\rangle$, express $|\tilde{\psi}_i\rangle = \sum_k v_{ik}\,|\tilde{\chi}_k\rangle$ for some complex coefficients v_{ik}.

Then

$$\sum_k |\tilde{\chi}_k\rangle\langle\tilde{\chi}_k| = \rho = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{k,\ell} \left(\sum_i v_{ik}\, v_{i\ell}^*\right) |\tilde{\chi}_k\rangle\langle\tilde{\chi}_\ell|$$

$$\sum_{k,\ell} \delta_{k,\ell}\,|\tilde{\chi}_k\rangle\langle\tilde{\chi}_\ell|$$

This equation can only be satisfied (since the $|\tilde{\chi}_k\rangle$ are orthogonal and thus $|\tilde{\chi}_k\rangle\langle\tilde{\chi}_\ell|$ linearly independent) if

$$\delta_{k,\ell} = \sum_i v_{ik}\, v_{i\ell}^* = (V^T V^*)_{k\ell} = (V^\dagger \cdot V)^*_{k\ell}$$

in other words, if (v_{ik}) is a unitary matrix.

By the same arguments, $|\tilde{\varphi}_j\rangle = \sum_k w_{jk} |\tilde{x}_k\rangle$

for a unitary matrix (w_{jk}). Thus

$$|\tilde{\varphi}_i\rangle = \sum_k v_{ik} |\tilde{x}_k\rangle = \sum_{k,j} v_{ik}\, w_{jk}^* |\tilde{\varphi}_j\rangle = \sum_j (v \cdot w^\dagger)_{ij} |\tilde{\varphi}_j\rangle,$$

and $v \cdot w^\dagger$ is (as product of unitary matrices) again unitary. □

The Bloch sphere picture for qubits can be generalized to mixed states by the representation

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2} \qquad \vec{r}\cdot\vec{\sigma} = r_1 X + r_2 Y + r_3 Z$$

with $\vec{r} \in \mathbb{R}^3$, $\|\vec{r}\| \le 1$, the Bloch vector of ρ (see sheet 11)

(Coincides with hitherto definition 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 by

$$tr_1 : \mathbb{C}^{n_1 n_2 \times n_1 n_2} \to \mathbb{C}^{n_2 \times n_2}, \quad tr_1[M_1 \otimes M_2] = tr[M_1]\cdot M_2,$$

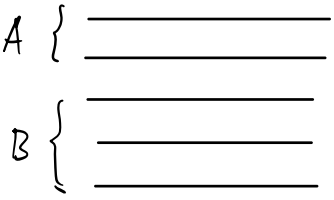
$$tr_2 : \mathbb{C}^{n_1 n_2 \times n_1 n_2} \to \mathbb{C}^{n_1 \times n_1}, \quad tr_2[M_1 \otimes M_2] = tr[M_2]\cdot M_1$$

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 extension.

$$tr_1[\alpha M_1 \otimes M_2 + \beta N_1 \otimes N_2] = \alpha\, tr_1[M_1 \otimes M_2] + \beta\, tr_1[N_1 \otimes N_2]$$

Consider a composite quantum system consisting of subsystem A and B,

for example: A: m qubits, B: n qubits



Let the quantum system be described by a density operator ρ^{AB}.

Define the <u>reduced density operator</u> for system A by

$$\rho^A = tr_B[\rho^{AB}]$$

↑ partial trace over system B

and analogously

$$\rho^B = tr_A[\rho^{AB}].$$

Examples:

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

$$tr_B[|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|] = |a_1\rangle\langle a_2| \cdot \underbrace{tr[|b_1\rangle\langle b_2|]}_{\langle b_2|b_1\rangle} = |a_1\rangle\langle a_2| \cdot \underbrace{\langle b_2|b_1\rangle}_{\in \mathbb{C}}$$

- Given a density matrix ρ for subsystem A and
  σ " B
  suppose that the overall density matrix is

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

Then $tr_B[\rho \otimes \sigma] = \rho \cdot \underbrace{tr[\sigma]}_{1} = \rho$

$$tr_A[\rho \otimes \sigma] = \underbrace{tr[\rho]}_{1} \cdot \sigma = \sigma$$

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

  Expanding ρ^{AB} leads to

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

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

$$\rho^A = \mathrm{tr}_B[\rho^{AB}] = \frac{1}{2}\left(|0\rangle\langle 0| \cdot \underbrace{\langle 0|0\rangle}_{1} + |0\rangle\langle 1| \cdot \underbrace{\langle 0|1\rangle}_{0} + |1\rangle\langle 0| \cdot \underbrace{\langle 1|0\rangle}_{0} + |1\rangle\langle 1| \cdot \underbrace{\langle 1|1\rangle}_{1}\right)$$

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

Note: composite system is in the "pure state" $|4\rangle$, whereas the subsystem is described by the "mixed state" $\frac{I}{2}$

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

Motivation / justification for partial trace:

Let M be any observable on subsystem A, then we want that ρ^A yields the same statistics for measuring M as ρ^{AB} for measuring $M \otimes I$ (on B)

In particular

$$\langle M \rangle = \mathrm{tr}_{\text{on } A}[M \cdot \rho^A] \overset{!}{=} \mathrm{tr}_{\text{on } AB}[(M \otimes I)\rho^{AB}] = \langle M \otimes I \rangle$$

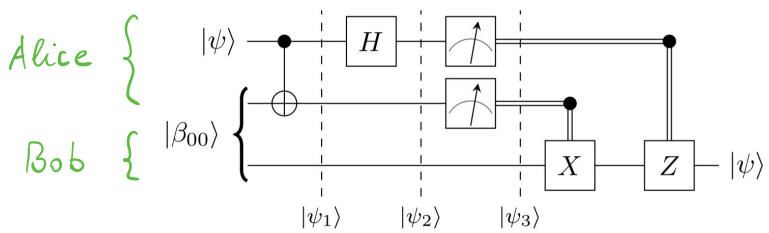
for all density operators ρ^{AB}. The partial trace operation for computing ρ^A from ρ^{AB} is the unique operation with this property.

(Nielsen and Chuang Box 2.6)

25.1.2023

Application to quantum teleportation: Why does quantum teleportation not allow for faster-than-light communication via the instantaneous 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 her measurement results yet.

Intermediate state $|\psi_2\rangle$: (see above)

$$|\psi_2\rangle = \frac{1}{2}\Big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big)$$

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

$$|\psi_1\rangle = |00\rangle(\alpha|0\rangle + \beta|1\rangle) \quad \text{with probability } \frac{1}{4}$$
$$|\psi_2\rangle = |01\rangle(\alpha|1\rangle + \beta|0\rangle) \quad "$$
$$|\psi_3\rangle = |10\rangle(\alpha|0\rangle - \beta|1\rangle) \quad "$$
$$|\psi_4\rangle = |11\rangle(\alpha|1\rangle - \beta|0\rangle) \quad "$$

Corresponding density matrix of ensemble $\{\frac{1}{4}, |\psi_j\rangle\}_{j=1..4}$:

$$\rho^{AB} = \frac{1}{4}\sum_{j=1}^{4} |\psi_j\rangle\langle\psi_j|$$
$$= \frac{1}{4}\Big(|00\rangle\langle 00| \otimes (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) +$$
$$+ |01\rangle\langle 01| \otimes (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) +$$
$$+ |10\rangle\langle 10| \otimes (\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) +$$
$$+ |11\rangle\langle 11| \otimes (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big)$$

Alice's qubits — Bob's qubit

Reduced density operator describing Bob's qubit:

$$\rho^B = \mathrm{tr}_A[\rho^{AB}] \overset{\mathrm{tr}[|a_1 a_2\rangle\langle a_1 a_2|] = \langle a_1 a_2 | a_1 a_2\rangle = 1,\ a_1, a_2 \in \{0,1\}}{=} \frac{1}{4}\Big((\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) +$$
$$(\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) +$$
$$(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) +$$
$$(\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big) =$$

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

coefficients of $|0\rangle\langle 1|$ and of $|1\rangle\langle 0|$ are 0

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

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

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

6. Quantum operations

(Nielsen and Chuang, section 8.2)

6.1 Motivation and overview

In general: changes of quantum states effected by unitary time evolution or wavefunction collapse during measurements.

Quantum operations (also called "quantum channels") are a (mathematical) generalization and unification of these concepts.

Abstractly: $\rho' = \mathcal{E}(\rho)$ — ρ: density matrix; $\mathcal{E}$: quantum operation

Special cases:

- unitary time evolution: $\mathcal{E}(\rho) = U \rho U^\dagger$
- measurement, with measurement operators $\{M_m\}$:

  recall that $p(m) = \mathrm{tr}[M_m^\dagger M_m \rho]$ — $p(m)$: probability for outcome m

  State after obtaining result m:

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

  Corresponding quantum channel (without renormalization):

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

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

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

→ density matrix after this process is weighted sum over all possible outcomes:

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

Different (but equivalent) perspectives on quantum operations:

- system coupled to environment (Stinespring dilation)
- operator-sum (Kraus) representation
- physically motivated axioms
- Choi matrix representation

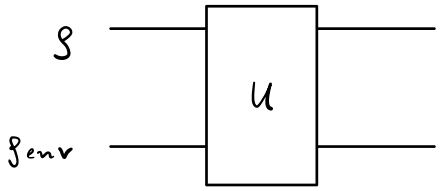
6.2 Environments and quantum operations

"Open" quantum system can be regarded as interaction 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:



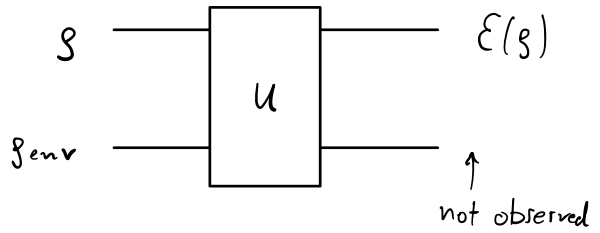
mathematical representation:

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

Output is the reduced density matrix of principal system:

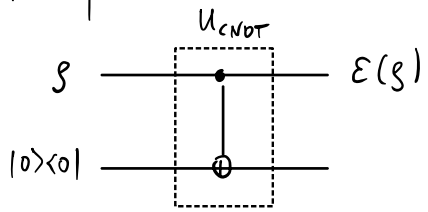
$$\mathcal{E}(\rho) = \mathrm{tr}_{env}\left[U(\rho \otimes \rho_{env}) U^\dagger \right]$$

↖ "trace out environment"



1.2.2023

Example:



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

then

$$U_{CNOT}(\rho \otimes |0\rangle\langle 0|) U_{CNOT}^\dagger = U_{CNOT}\left(\rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 10| + \rho_{10}|10\rangle\langle 00| + \rho_{11}|10\rangle\langle 10|\right) \cdot U_{CNOT}^\dagger$$

$$= \rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 11| + \rho_{10}|11\rangle\langle 00| + \rho_{11}|11\rangle\langle 11|$$

$$\mathrm{tr}_{env}[\dots] = \rho_{00}|0\rangle\langle 0|\underbrace{\langle 0|0\rangle}_{1} + \rho_{01}|0\rangle\langle 1|\underbrace{\langle 0|1\rangle}_{0} + \rho_{10}|1\rangle\langle 0|\underbrace{\langle 1|0\rangle}_{0} + \rho_{11}|1\rangle\langle 1|\underbrace{\langle 1|1\rangle}_{1}$$

$$= \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| = \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix} =$$

$$= P_0 \rho P_0 + P_1 \rho P_1 \quad \text{with} \quad P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1|$$

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

6.3 Operator-sum 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 in a mixed state, then can equivalently work with a pure state in a larger environment)

$\sum_k |e_k\rangle\langle e_k| = I$ (on env.)

$$\rightsquigarrow \mathcal{E}(\rho) = tr_{env}\left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right] =$$

$$= \sum_k tr_{env}\left[U\cdot(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \cdot (I \otimes |e_k\rangle\langle e_k|)\right]$$

$$= \sum_k \langle e_k| U\cdot(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger |e_k\rangle$$

$tr[A] = \sum_j \langle j|A|j\rangle$

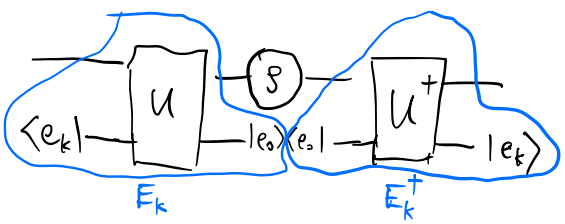
↑ inner product w.r.t. environment

$$= \sum_k E_k \rho E_k^\dagger \quad \text{with}$$

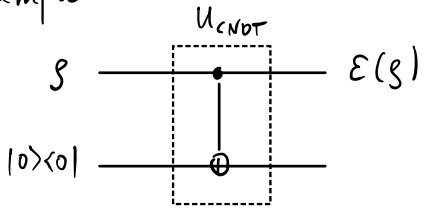
E_k a complex matrix with entries $(E_k)_{\ell m} = \langle \ell, e_k|U|m, e_0\rangle \equiv \langle \ell|\langle e_k|U|m\rangle|e_0\rangle \equiv (\langle \ell|\otimes\langle e_k|)U(|m\rangle\otimes|e_0\rangle)$

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:



$(E_0)_{\ell m} = \langle \ell, 0|U_{CNOT}|m, 0\rangle \rightsquigarrow E_0 = \begin{matrix} & m=0 & m=1 \\ \ell=0 & 1 & 0 \\ \ell=1 & 0 & 0 \end{matrix} = P_0$

↑ must not flip → $m=0$

$(E_1)_{\ell m} = \langle \ell, 1|U_{CNOT}|m, 0\rangle \rightsquigarrow E_1 = \begin{matrix} & m=0 & m=1 \\ \ell=0 & 0 & 0 \\ \ell=1 & 0 & 1 \end{matrix} = P_1$

↑ must flip → $m=1$

} agrees with previous derivation

Completeness relation of Kraus operators:

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

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

$$= \mathrm{tr}\Big[\Big(\sum_k E_k^\dagger E_k\Big)\cdot \rho\Big]$$

should hold for arbitrary ρ with $\mathrm{tr}[\rho]=1 \rightsquigarrow$

$$\sum_k E_k^\dagger E_k = I$$

We allow for quantum operations with $\sum_k E_k^\dagger E_k \leq I$ (see $\mathcal{E}_m$ from measurement example)

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

$A \in \mathbb{C}^{n\times n}$ is called positive semidefinite

if A is Hermitian and $\underbrace{\langle v|A|v\rangle \geq 0}$ for all $v \in \mathbb{C}^n$

$\Leftrightarrow$ all eigenvalues of A are ≥ 0

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

Remark: Physical interpretation as measurement performed on environment with respect to $\{|e_k\rangle\}$ basis; ie. measurement operators $|e_k\rangle\langle e_k|$:

For outcome k, state of principal system is

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

i.e. E_k's play the role of the measurement operators on principal system.

System – environment model of a Kraus representation

Given trace-preserving $\mathcal{E}(\rho) = \sum_{k=0}^{n-1} E_k \rho E_k^\dagger$,

is there a corresponding system–environment representation?

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

Define unitary U via $U|\psi\rangle|e_0\rangle = \sum_k E_k|\psi\rangle|e_k\rangle$

and matrix extension to a unitary operator on combined system

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

$$\langle\psi|\langle e_0|U^\dagger U|\varphi\rangle|e_0\rangle = \sum_{k,k'} \langle\psi|E_k^\dagger E_{k'}|\varphi\rangle \underbrace{\langle e_k|e_{k'}\rangle}_{\delta_{k,k'}} =$$

$$= \langle\psi| \underbrace{\sum_k E_k^\dagger E_k}_{=\mathbb{I}\ \text{(completeness relation)}} |\varphi\rangle = \langle\psi|\varphi\rangle$$

$\rightsquigarrow$ U preserves orthogonality

U has the desired property since

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

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

8.2.2023

6.4 Axiomatic approach to quantum operations

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

A1: $\mathrm{tr}[\mathcal{E}(\rho)]$ is 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:

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

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 quantum system Q by another quantum system R, then

$(I_R \otimes \mathcal{E}_Q)(A)$ must be p.s.d. for any p.s.d. matrix A on combined system RQ

Theorem: 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 set of complex matrices $\{E_k\}$ with $\sum_k E_k^\dagger E_k \leq I$.

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:

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

(I: identity map on R: maps density on R to itself; E_k: $n \times n$ matrix)

$$= \sum_k \underbrace{\langle\varphi_k|A|\varphi_k\rangle}_{\geq 0 \text{ since } A \text{ is p.s.d.}} \geq 0 \quad \checkmark$$

"$\Rightarrow$" Principal system (which $\mathcal{E}$ acts on) denoted Q, dimension n

Introduce another quantum system, labelled R, with same dimension as Q

Let $\{ |j_Q\rangle : j = 1 \dots n \}$ an orthonormal basis of Q — R { ——— ——— ———

$\{ |j_R\rangle : j = 1 \dots n \}$ " " R — Q { ——— ——— ———

Define the "maximally entangled state" (cf. exercise 12.1)

$$|\alpha\rangle := \sum_{j=1}^{n} |j_R\rangle |j_Q\rangle \in RQ \quad \text{and}$$

$$\sigma := (\mathcal{I} \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|) \quad \text{p.s.d. by A3, ie.}$$

↑ Choi matrix — density matrix on combined system

turns out to completely specify $\mathcal{E}$

For any state $|\psi\rangle = \sum_j \psi_j |j_Q\rangle$ on Q, set

$$|\tilde{\psi}\rangle := \sum_j \psi_j^* |j_R\rangle \text{ on } R \rightsquigarrow$$

$$\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \langle\tilde{\psi}| \sum_{ij} |i_R\rangle\langle j_R| \otimes \mathcal{E}(|i_Q\rangle\langle j_Q|) |\tilde{\psi}\rangle$$

↑ inner product on R

$$= \sum_{ij} \psi_i \psi_j^* \mathcal{E}(|i_Q\rangle\langle j_Q|) = \mathcal{E}(|\psi\rangle\langle\psi|) \quad (*)$$

Spectral decomposition $\rightsquigarrow$ $\sigma = \sum_k |s_k\rangle\langle s_k|$ for some states $|s_k\rangle$ on combined system (eigenvalues absorbed into $|s_k\rangle$)

↘ $\sigma = \sum_k \lambda_k |\varphi_k\rangle\langle\varphi_k|$, $|s_k\rangle = \sqrt{\lambda_k}\,|\varphi_k\rangle$

Can represent $|s_k\rangle = \sum_{j,j'=1}^{n} s_{k,j,j'} |j_R\rangle |j'_Q\rangle$

↑ coefficients

For each k, define a linear map $E_k : Q \to Q$ by

$$E_k |j_Q\rangle = \sum_{j'=1}^{n} s_{k,j,j'} |j'_Q\rangle \quad \text{and linear extension}$$

Then, $E_k |\psi\rangle = \sum_{j,j'=1}^{n} \psi_j s_{k,j,j'} |j'_Q\rangle =$

$= \sum_{j''=1}^{n} \sum_{j,j'=1}^{n} \psi_{j''} s_{k,j,j'} \underbrace{\langle j''_R | j_R \rangle}_{\delta_{j'',j}} |j'_Q\rangle$

$= \sum_{j''=1}^{n} \psi_{j''} \langle j''_R | s_k \rangle = \langle \tilde{\psi} | s_k \rangle$

↑ inner product on R

$$\sum_k E_k |\psi\rangle\langle\psi| E_k^+ = \sum_k \langle \tilde{\psi} | s_k \rangle \langle s_k | \tilde{\psi} \rangle =$$

$$= \langle \tilde{\psi} | \underbrace{\left(\sum_k |s_k\rangle\langle s_k| \right)}_{\sigma} | \tilde{\psi} \rangle = \langle \tilde{\psi} | \sigma | \tilde{\psi} \rangle \overset{(*)}{=} \mathcal{E}(|\psi\rangle\langle\psi|)$$

Holds for arbitrary $|\psi\rangle \in Q \overset{A2}{\rightsquigarrow}$

$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^+$ for any density matrix ρ. □

6.5 Examples of quantum operations

(Nielsen and Chuang, section 8.3)

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

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

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

- Phase flip (analogously):

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

- Depolarizing channel:

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

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

Bloch sphere representation: uniform contraction

- Amplitude damping (cf. exercise 13.1)

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

$$E_1 |1\rangle = \sqrt{\gamma}\, |0\rangle$$

Interpretation: $|1\rangle \to |0\rangle$ with probability γ.