Introduction to Quantum Computing

Hamza Haddaoui, WS21

Summary

Quantum bits

Classical bits are 0 and 1.

Quantum bits are a superposition of $|0\rangle$ and $|1\rangle$.

Ket-notation: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad$ *where* $\alpha, \beta \in \mathbb{C},\ \alpha^2 + \beta^2 = 1$

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}$$

We cannot directly observe/measure qubits (the probabilities α and β).

When a measurement is performed, the qubit collapses into state $|0\rangle$ with probability $|\alpha|^2$, or collapses into state $|1\rangle$ with probability $|\beta|^2$.

Wavelength collapse: Upon measurement, the qubit collapses to either $|0\rangle$ or $|1\rangle$.

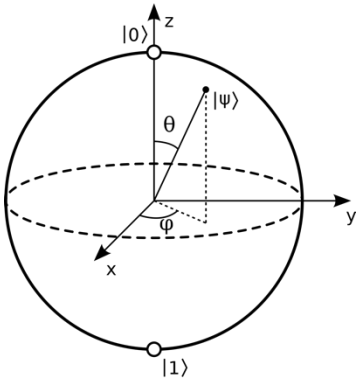
Estimation of these parameters is done by repeating the same experiment many times and measuring the number of outcomes for each state.

Bloch sphere

Representation of a qubit $|\psi\rangle$ in 3D space, with respect to angles θ and φ.

We can assume that: $\begin{cases}\alpha = e^{i\varphi_0}\cos\frac{\theta}{2}\\ \beta = e^{i\varphi_1}\sin\frac{\theta}{2}\end{cases}$ since it holds that $|\alpha|^2 + |\beta|^2 = (\cos\frac{\theta}{2})^2 + (\sin\frac{\theta}{2})^2 = 1$

$$\begin{aligned}|\psi\rangle &= \alpha|0\rangle + \beta|1\rangle\\ &= e^{i\varphi_0}\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi_1}\sin\left(\frac{\theta}{2}\right)|1\rangle\\ &= e^{i\varphi_0}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\varphi_1-\varphi_0)}\sin\left(\frac{\theta}{2}\right)|1\rangle\right]\\ &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad \text{(global phase is irrelevant)}\end{aligned}$$



The point of the surface of the Bloch sphere, is defined by:

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

Single qubit gates

Principle of time evolution: The quantum state $|\psi\rangle$ at current time point t transitions to a state $|\psi'\rangle$ at a later time point $t' > t$.

This transition is described by a complex unitary (norm preserving) matrix U: $(U^\dagger U = UU^\dagger = I)$

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

Pauli matrices

Pauli vector, composed of three 2x2 matrices: $\boldsymbol{\sigma} = (\sigma_X \quad \sigma_Y \quad \sigma_Z)$

- Pauli-X: $\sigma_X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ flips $|0\rangle$ into $|1\rangle$ and viceversa
- Pauli-Y: $\sigma_Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$
- Pauli-Z: $\sigma_Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ flips $|1\rangle$ by π

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

$[\sigma_j, \sigma_k] = \sigma_j \cdot \sigma_k - \sigma_k \cdot \sigma_j = 2i\sigma_l \quad$ where l is part of the cyclic-permutation (j, k, l)

Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ $\alpha|0\rangle + \beta|1\rangle \xrightarrow{H} \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

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

T-gate $\mathrm{T} = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}$ $T^2 = S$

Matrix exponential

Let $A \in \mathbb{C}^{n\times n}$ be a matrix, so that $A^2 = I$ and $x \in \mathbb{R}$.

$$e^A = \sum_{k=0}^{\infty}\frac{1}{k!}A^k$$

$$e^{iAx} = \sum_{k=0}^{\infty}\frac{1}{k!}(iAx)^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{(2k)!}(iAx)^{2k} + \sum_{k=0}^{\infty}\frac{1}{(2k+1)!}(iAx)^{2k+1}$$

Divide the sum into even/odds

$$= \sum_{k=0}^{\infty}\frac{1}{(2k)!}(-x^2)^k + \sum_{k=0}^{\infty}\frac{1}{(2k+1)!}(iAx)(iAx)^{2k}$$

$(iAx)^{2k} = ((iAx)^2)^k = (-x^2)^k$

$$= \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k}}{(2k)!}\cdot I + \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{(2k+1)!}\cdot A\cdot i$$

$\cos(x) = \sum_{n=0}^{\infty}(-1)^k\frac{x^{2n}}{(2n)!}$

$\sin(x) = \sum_{n=0}^{\infty}(-1)^k\frac{x^{2n+1}}{(2n+1)!}$

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

Rotation operators

Matrices perform a rotation of a qubit about an axis, which is x for R_x, y for R_y and z for R_z.

$$R_X(\theta) = e^{i\theta\frac{x}{2}} = \cos\left(\frac{\theta}{2}\right)\cdot I - i\sin\left(\frac{\theta}{2}\right)X = \begin{pmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$$

$$R_Y(\theta) = e^{i\theta\frac{y}{2}} = \cos\left(\frac{\theta}{2}\right)\cdot I - i\sin\left(\frac{\theta}{2}\right)Y = \begin{pmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$$

$$R_Z(\theta) = e^{i\theta\frac{z}{2}} = \cos\left(\frac{\theta}{2}\right)\cdot I - i\sin\left(\frac{\theta}{2}\right)Z = \begin{pmatrix}e^{-\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix}$$

For a general, normalized vector $\vec{v}$ it holds that:

$$\vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 = v_1\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + v_2\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} + v_3\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}v_3 & v_1 - iv_2\\ v_1 + iv_2 & v_3\end{pmatrix}$$

Therefore: $R_{\vec{v}}(\theta) = e^{-i\theta(\vec{v}\cdot\vec{\sigma})} = \cos(\theta)\,I - i\sin(\theta)\,(\vec{v}\cdot\vec{\sigma})$

Moreover, it holds that:

$$(\vec{v}\cdot\vec{\sigma})^2 = I \to \begin{pmatrix}v_3 & v_1 - iv_2\\ v_1 + iv_2 & v_3\end{pmatrix}\begin{pmatrix}v_3 & v_1 - iv_2\\ v_1 + iv_2 & v_3\end{pmatrix} = \begin{pmatrix}v_1^2 + v_2^2 + v_3^2 & 0\\ 0 & v_1^2 + v_2^2 + v_3^2\end{pmatrix} = I$$

Z-Y decomposition

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

$$U = e^{i\alpha}\begin{pmatrix}e^{-i\frac{\beta}{2}} & 1\\ 1 & e^{i\frac{\beta}{2}}\end{pmatrix}\begin{pmatrix}\cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2}\\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2}\end{pmatrix}\begin{pmatrix}e^{-i\frac{\delta}{2}} & 0\\ 0 & e^{i\frac{\delta}{2}}\end{pmatrix} = e^{i\alpha}\cdot R_Z(\beta)\cdot R_Y(\gamma)\cdot R_Z(\delta)$$

Multiple qubits

Computation basis states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

General 2-qubit state $\rightarrow |\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

$$\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in \mathbb{C}, |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{1} \end{pmatrix} = \alpha_{00} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_{01} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_{10} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_{11} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

If we measure only the first qubit of a two-qubit state, the wavefunction collapses in:

$$\begin{cases} 0\text{: } p(0) = |\alpha_{00}|^2 + |\alpha_{01}|^2 \ \rightarrow \quad |\psi'\rangle = \dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \\ 1\text{: } p(1) = |\alpha_{10}|^2 + |\alpha_{11}|^2 \ \rightarrow \quad |\psi'\rangle = \dfrac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} \end{cases}$$

Generalization to n bits $\rightarrow |\psi\rangle = \sum_{x_0=0}^{1} \sum_{x_1=0}^{1} \cdots \sum_{x_{n-1}=0}^{1} \alpha_{x_{n-1}} \ldots \alpha_{x_1} \alpha_{x_0} |x_{n-1}, \ldots, x_1, x_0\rangle = \sum_{x=0}^{2^{n-1}} \alpha_x |x\rangle$

$\alpha_x \in \mathbb{C}\ \forall x \in \{0,1,\ldots,2^{n-1}\}$ such that $\sum_{x=0}^{2^{n-1}} |\alpha_x|^2 = 1$

Multiple qubits are constructed as tensor product of vector spaces.

Tensor product of vector spaces

Let V, W be two vector spaces. The elements in the tensor product $V \otimes W$ are linear combination of "tensor products" $|v\rangle \otimes |w\rangle$ consisting of elements $|v\rangle \in V, |w\rangle \in W$.

Properties:

- $\dim(V \otimes W) = \dim(V) \cdot \dim(W)$
- $\forall\ |v\rangle \in V, |w\rangle \in W$ and $\alpha \in \mathbb{C}$: $\alpha(|v\rangle \otimes |w\rangle) = (\alpha|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle)$
- $\forall\ |v_1\rangle, |v_2\rangle \in V$ *and* $|w\rangle \in W$: $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
- $\forall\ |v\rangle \in V$ *and* $|w_1\rangle, |w_2\rangle \in W$: $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

Inner product on $V \otimes W$

$\left\langle \sum_j \alpha_j |v_j\rangle \otimes |w_j\rangle \middle| \sum_k \beta_k |\tilde{v}_j\rangle \otimes |\tilde{w}_j\rangle \right\rangle := \sum_j \sum_k \alpha_j^* \beta_k \langle v_j|\tilde{v}_k\rangle \langle w_j|\tilde{w}_k\rangle$

N.B. Not every element of $V \otimes W$ can be written in the form $|v\rangle \otimes |w\rangle$;
e.g., Bell state: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

example:

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

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

$|v\rangle \otimes |w\rangle = (v_1|0\rangle + v_2|1\rangle) \otimes (w_1|0\rangle + w_2|1\rangle) = v_1w_1|00\rangle + v_1w_2|01\rangle + v_2w_1|10\rangle + v_2w_2|11\rangle$

Thus: $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} v_1w_1 \\ v_1w_2 \\ v_2w_1 \\ v_2w_2 \end{pmatrix}$

Multiple qubit gates

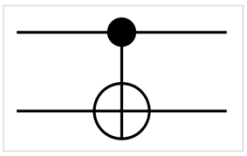
Operation on multiple qubits (n) are described by unitary matrices $U \in \mathbb{C}^{2^n \times 2^n}$

CNOT gate

The first qubit in the control bit, while the remaining are the target.
Target qubit(s) are flipped if control qubit is 1: $|1b\rangle \to |1\rangle \otimes (X|b\rangle)$

$$|a, b\rangle \to |a, a \oplus b\rangle$$

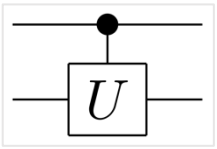
$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$



Controlled gate

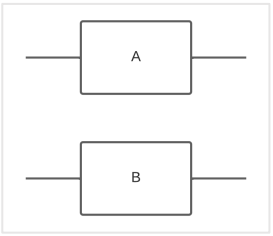
Generalization of CNOT gate, where the target operator is different from the Pauli-X gate.

$$|10\rangle \to |1\rangle \otimes (X|0\rangle), |11\rangle \to |1\rangle \otimes (X|1\rangle)$$
$$U_{CU} = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$



Unitary gates in parallel

$$|ab\rangle \to (A|a\rangle) \otimes (B|b\rangle) \to (A \otimes B)|ab\rangle$$



Kronecker Product

Given the matrices $A \in \mathbb{C}^{m \times n}$ *and* $A \in \mathbb{C}^{p \times q}$:

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

Properties:

- $(A \otimes B)^{\$} = A^{\$} \otimes B^{\$}$ (*where* \$ *can be* $*, T, \dagger$)
- $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- $(A \otimes B) \cdot (C \otimes D) = AC \otimes BD$ (*where* $\cdot$ *is the matrix multiplication*)
- Kronecker product of two unitary matrices, is unitary
- Kronecker product of two Hermitian matrices, is Hermitian.

Quantum measurements

Given an orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$ (made of orthogonal and normalized vectors), any qubit can be represented with respect to it: $|\psi\rangle = \alpha_1|u_1\rangle + \alpha_2|u_2\rangle$.
Measurement outcome will be $|u_1\rangle$ with probability $|\alpha_1|^2$ and $|u_1\rangle$ with probability $|\alpha_2|^2$.

example:

$$\{|0\rangle,|1\rangle\} \to \{|+\rangle,|-\rangle\}: \quad \begin{cases} |+\rangle = \dfrac{|1\rangle+|0\rangle}{\sqrt{2}} = \dfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \\ |-\rangle = \dfrac{|1\rangle-|0\rangle}{\sqrt{2}} = \dfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \end{cases}$$

$$\{|+\rangle,|-\rangle\} \to \{|0\rangle,|1\rangle\}: \quad \begin{cases} |0\rangle = \dfrac{|+\rangle+|-\rangle}{\sqrt{2}} = \begin{pmatrix}1\\0\end{pmatrix} \\ |1\rangle = \dfrac{|+\rangle-|-\rangle}{\sqrt{2}} = \begin{pmatrix}0\\1\end{pmatrix} \end{cases}$$

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.
Result m will occur with probability:

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

The state after measurement will be:

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

The measurement operators satisfy the completeness relation $\sum_m M_m^\dagger M_m = I$, such that probabilities sum up to 1:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1$$

example:
Measurement with respect to computational basis $\{|0\rangle,|1\rangle\}$:

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}(1 \quad 0) = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \to \; p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = (\alpha^* \quad \beta^*)\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = |\alpha|^2$$

$$M_1 = |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}(0 \quad 1) = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} \to \; p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = (\alpha^* \quad \beta^*)\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = |\beta|^2$$

Projective measurements

A square matrix $P \in \mathbb{C}^{n\times n}$ is called <u>*orthogonal projection matrix*</u> if it is Hermitian ($H^\dagger = H$) and satisfies $P^2 = P$.
Let V be a k-dimensional subspace of $\mathbb{C}^n$, and $\{|u_1\rangle,\dots,|u_k\rangle\}$ an orthonormal basis of V.
Then:

$$P = \sum_{j=1}^{m} |u_j\rangle\langle u_j|$$

is the **projector** onto V.
<u>Relation to spectral decomposition:</u>
Every normal matrix $A \in \mathbb{C}^{n\times n} (i.e.\ [A, A^\dagger] = AA^\dagger - A^\dagger A = 0)$ is diagonalizable by an orthonormal basis, that is, there exist a unitary $U \in \mathbb{C}^{n\times n}$ and eigenvalues $\lambda_1,\dots\lambda_n \in \mathbb{C}$ such that:

$$A = U\begin{pmatrix}\lambda_1 & 0 & 0\\0 & \ddots & 0\\0 & 0 & \lambda_n\end{pmatrix}U^\dagger = \sum_{j=1}^{n}\lambda_j|u_j\rangle\langle u_j| = \sum_{k=1}^{m}\tilde{\lambda}_k P_k$$

Where the $|u_j\rangle$ are the column vectors of U, and $\tilde{\lambda}_k$ are the distinct eigenvalues of A.
P_m are the associated projectors onto the corresponding eigenspaces.

A projective measurement is described by an observable M, a Hermitian operator acting on the quantum system.

$$M = \sum_m \lambda_m P_m$$

Where P_m is the projector onto the eigenspace of M with eigenvalue λ_m.
The possible outcomes of the measurement correspond to the eigenvalues λ_m:

$$p(\lambda_m) = \langle\psi|P_m|\psi\rangle = \|P_m|\psi\rangle\|^2$$

The state of the quantum system after measurement is:

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

Projective measurements are special cases of general measurements framework when the measurement operators are Hermitian and orthogonal projectors.
In general, measurement w.r.t. orthonormal basis is a projective measurement.
Projective measurements combined with unitary transformations are equivalent to general measurement framework.

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

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

Heisenberg Uncertainty principle

Suppose A, B Hermitian operators ($A = A^\dagger, B = B^\dagger$), $|\psi\rangle$ a quantum state.
$\langle\psi|AB|\psi\rangle = x + iy \qquad x, y \in \mathbb{R}$

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

Thus:

$\langle\psi|[A,B]|\psi\rangle = x + iy - (x - iy) = 2iy$

$\langle\psi|[\{A,B\}]|\psi\rangle = x + iy + (x - iy) = 2x$

Therefore:

$$\begin{cases} |\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = (|2iy|^2 + |2x|^2) = 4(x^2+y^2) \\ |\langle\psi|AB|\psi\rangle|^2 = |x+iy|^2 = \left|\sqrt{x^2+y^2}\right|^2 = x^2 + y^2 \end{cases} \rightarrow |\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2$$

Applying Cauchy-Schwarz inequality ($|\langle v|w\rangle|^2 \leq \|v\|^2\|w\|^2$)to $v = A|\psi\rangle$, $w = B|\psi\rangle$

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

$|\langle\psi|[A,B]|\psi\rangle|^2 \leq 4|\langle\psi|AB|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$

Suppose C, D are observables. We substitute $A = C - \langle C\rangle$, $B = D - \langle D\rangle$

Heisenberg uncertainty principle: $\Delta C \cdot \Delta D \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}$

Interpretation for experiments → repeated preparation of state $|\psi\rangle$ measure C in some cases, D in other cases, to obtain standard deviations ΔC and ΔD.

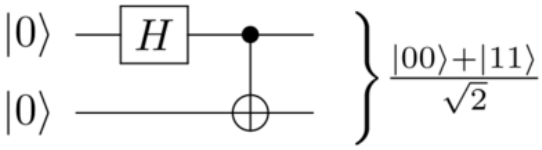
Entanglement

A n-qubit state $|\psi\rangle$ $(n \geq 2)$ is called entangled if it cannot be written as tensor product of single-qubit states:

$$|\psi\rangle \neq |\varphi_{n-1}\rangle \otimes ... \otimes |\varphi_0\rangle, \quad \forall |\varphi_0\rangle, ... |\varphi_{n-1}\rangle \in \mathbb{C}^2$$

For example, ***Bell states*** *(EPR states – Einstein, Podolsky, Rosen):*

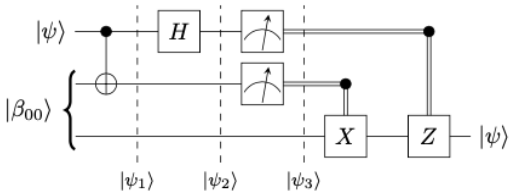
- $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$



Quantum teleportation

Scenario: *Alice and Bob want to communicate (from distance).*
When visiting each other long ago, they generated an EPR pair $|\beta_{00}\rangle$*, and each keeps one qubit of the pair.*
Now Alice's task is to send another (unknown) qubit $|\psi\rangle$ to Bob.
N.B. Alice cannot just measure the qubit and send the classical information to Bob: the classical measurement, does not reveal the unknown amplitudes α and β.

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



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

After CNOT: $|\psi_1\rangle = \frac{1}{\sqrt{2}}\big(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\big)$

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

Subsequently, Alice measures her qubits w.r.t. **computational basis**, corresponding to projective measurement with:

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

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

If Alice measures…	Bob obtains
$00 \to \alpha\|0\rangle + \beta\|1\rangle$	$Z^0X^0(\alpha\|0\rangle + \beta\|1\rangle) = \|\psi\rangle$
$01 \to \alpha\|1\rangle + \beta\|0\rangle$	$Z^0X^1(\alpha\|1\rangle + \beta\|0\rangle) = \|\psi\rangle$
$10 \to \alpha\|0\rangle - \beta\|1\rangle$	$Z^1X^0(\alpha\|0\rangle - \beta\|1\rangle) = \|\psi\rangle$
$11 \to \alpha\|1\rangle - \beta\|0\rangle$	$Z^1X^1(\alpha\|1\rangle - \beta\|0\rangle) = \|\psi\rangle$

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

EPR and Bell inequality

Authors of the EPR paper 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 but share the entangled two-qubit state $|\beta_{11}\rangle$.
The first qubit belongs to Alice and the second to Bob.
Alice and Bob measure the observable $\vec{v}\cdot\vec{\sigma} = v_1X + v_2Y + v_3Z$, with $\vec{v}\in\mathbb{R}^3, \|\vec{v}\| = 1$
$\vec{v}\cdot\vec{\sigma}$ is Hermitian and unitary and has eigenvalues ± 1.

Alice performs her measurement immediately before Bob.

- $\vec{v} = (0,0,1)$ → observable is $Z = 1\cdot|0\rangle\langle 0| + (-1)\cdot|1\rangle\langle 1|$, i.e., standard measurement w.r.t. computational basis.
  If Alice measures eigenvalue $+1$, the wavefunction collapses to $|01\rangle$,
  If Alice measures eigenvalue -1, the wavefunction collapses to $|10\rangle$.
  Bob will always obtain the opposite measurement result.

- $\vec{v} = (1,0,0)$ →observable is $X = 1\cdot|+\rangle\langle +| + (-1)\cdot|-\rangle\langle -|$, i.e., standard measurement w.r.t. basis $\{|+\rangle, |-\rangle\}$. Given that:
  $$\begin{cases} |0\rangle = \dfrac{|+\rangle + |-\rangle}{\sqrt{2}} \\ |1\rangle = \dfrac{|+\rangle - |-\rangle}{\sqrt{2}} \end{cases} \quad \rightarrow \quad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = -\frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$$
  If Alice measures eigenvalue $+1$, the wavefunction collapses to $|+-\rangle$.,
  If Alice measures eigenvalue -1, the wavefunction collapses to $|-+\rangle$.
  Bob will always obtain the opposite measurement result.

- General $\vec{v}$: We denote eigenstates of the observable $\vec{\boldsymbol{v}}\cdot\vec{\boldsymbol{\sigma}}$ as $|a\rangle$, $|b\rangle$. Then, there exist complex numbers $\alpha, \beta, \gamma, \delta$ such that:
  $$\begin{cases} |0\rangle = \alpha|a\rangle + \beta|b\rangle \\ |1\rangle = \gamma|a\rangle + \delta|b\rangle \end{cases} \quad \rightarrow \quad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = (\alpha\delta - \beta\gamma)\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$$
  $$|\beta_{11}\rangle = e^{i\theta}\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$$
  The term $(\alpha\delta - \beta\gamma)$ is the determinant of the **unitary** base change matrix U (between the orthonormal $\{|0\rangle, |1\rangle\}$ and $\{|a\rangle, |b\rangle\}$): $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$
  It holds that $|\det(U)| = 1$, and we can represent $\det(U) = e^{i\theta}$ for some angle $\theta\in\mathbb{R}$.

  Bob will obtain opposite measurement result of Alice (the global phase factor $e^{i\theta}$ is not relevant for measurements).
  Therefore Alice can predict Bob's measurement result. On the other hand, there is no possibility that Alice could somehow influence Bob's measurement after performing her measurement since they are far apart (speed of light too slow to travel from Alice to Bob).

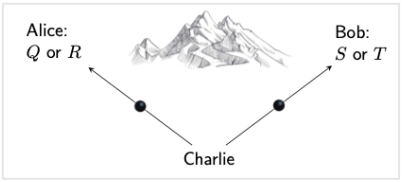
EPR argument → "property" $\vec{v}\cdot\vec{\sigma}$ of a qubit is thus an "element of reality"; however, quantum mechanics does not a priori specify this property for all possible $\vec{v}$ (but only probabilities) and is thus an incomplete description of reality.

"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 $\vec{v}$ (this idea turned out to be **wrong**).

Bell's inequality: experimental test which can invalidate local hidden variable theories
Here local means that no faster-than-light communication is possible (which is almost universally accepted, otherwise one could send information back- wards in time according to special relativity).

Experimental setup for Bell's inequality

<u>*Many repetitions of the following setup:*</u> *Charlie experimentally prepares two particles and sends one to Alice and one to Bob, who perform measurements on the received particle.*
We assume that the particles have some (abstract) properties, each of which can assume two possible values ± 1.



Alice measures a property denoted $\boldsymbol{Q}$ *of her particle, or (another) property* $\boldsymbol{R}$*, randomly deciding which one to measure; corresponding measurement values* $\boldsymbol{Q}, \boldsymbol{R} \in \{\pm 1\}$.
Analogously for Bob with $\boldsymbol{S}, \boldsymbol{T} \in \{\pm 1\}$.
Alice and Bob perform their measurements (almost) simultaneously, such that no information about the result can be transmitted in between (assuming no faster-than-light communication).
After completing the experiment, Alice and Bob meet to analyze their measurement data.

Considering the quantity:

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

$(Q + R)$ can assume value ± 2, when $(R - Q)$ assume value 0,
or it can assume value 0 when $(R - Q)$ assume value ± 2.
Denoting by $p(q, r, s, t)$ the probability that the two-particle system before measurement is in state $Q = q, R = r, S = s, T = t$, then the expected value of the above equation is:

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

The last equality follows from the fact that probabilities sum to 1.
Since $\mathbb{E}$ is linear, one arrives at the following **Bell's inequality**:

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

<u>Quantum realization of the experiment</u>
Charlie sends the state $|\beta_{11}\rangle$ to Alice (1^{st} qubit) and Bob (2^{nd} qubit). The observables are:

$$Q = Z_1, \quad R = X_1, \quad S = \frac{-Z_2 - X_2}{\sqrt{2}}, \quad T = \frac{Z_2 - X_2}{\sqrt{2}}$$

The expected values of the measurements are:

$$\langle QS \rangle = \frac{1}{\sqrt{2}}, \quad \langle RT \rangle = \frac{1}{\sqrt{2}}, \quad \langle RS \rangle = \frac{1}{\sqrt{2}}, \quad \langle QT \rangle = -\frac{1}{\sqrt{2}}$$

Inserted into the Bell's inequality:

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

<u>This violates Bell's inequality.</u>
Actual laboratory experiments (using photons) agree with prediction by quantum mechanics, thus not all (implicit) assumptions leading to the Bell inequality can be satisfied. **realism**: physical properties PQ, PR, PS, PT have definite values independent of observation. **locality**: Alice performing her measurement cannot influence Bob's measurement and vice versa. In summary, nature is not "locally realistic". (Most common point of view: realism does not hold.) Practical lesson: use entanglement as resource.

Quantum search algorithms

Speed up in comparison to classic computers.

Classical search through N elements $\rightarrow O(N)$

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

Quantum oracles

We consider a search space of $N = 2^n$ elements, labelled from 0 to $N-1$.

We assume that there exist M solutions (naturally, $1 \leq M \leq N$).

Solutions are defined by a function:

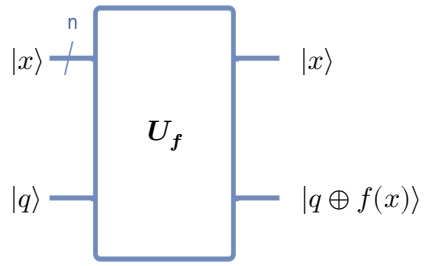
$$f: \{0, \dots, N-1\} \rightarrow \{0,1\}: \qquad f(x) \begin{cases} 0 \text{ if element x is not a solution} \\ 1 \text{ if element x is a solution} \end{cases}$$

In quantum computer this function is implemented by a quantum "oracle".

The operator is unitary ($U_f^2 = I$) and maps basis states to basis states.

The inputs are the binary representation of the element $|x\rangle$ and the "oracle qubit" $|q\rangle$. Outputs are the input vector $|x\rangle$ and the outcome of the operator.

The oracle "marks" the solution by a phase flip of the "oracle qubit".



Initializing oracle qubit, e.g. in superposition $|-\rangle$:

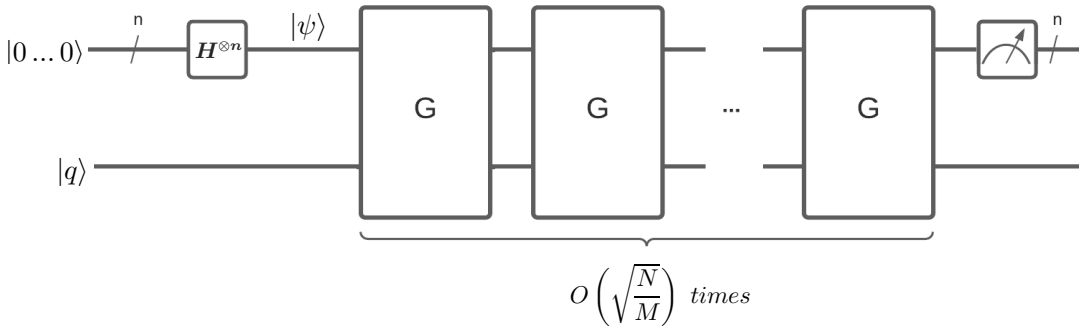
$$|x\rangle \otimes |-\rangle \overset{U_f}{\rightarrow} \begin{cases} |x\rangle \otimes |-\rangle & if\ f(x) = 0 \\ -|x\rangle \otimes |-\rangle & if\ f(x) = 1 \end{cases}$$

In summary: $|x\rangle \otimes |q\rangle \overset{U_f}{\rightarrow} (-1)^{f(x)} |x\rangle \otimes |q\rangle$

Grover's algorithm

Search algorithm, for $N = 2^n$ elements with M possible solutions.

We initialize the input to 0 ($|x_{N-1} \dots x_0\rangle = |0 \dots 0\rangle$) and the auxiliary qubit for the oracle to 0.



Hadamard transform

Definition of Hadamard per single qubit: *For* $x \in \{0,1\}$ $\quad H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{x \cdot z} \ |z\rangle$

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

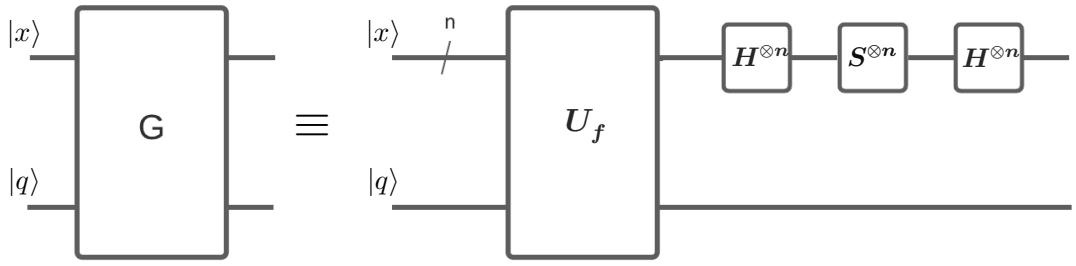
$$= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n - 1} (-1)^{\boldsymbol{x} \cdot \boldsymbol{z}} \ |z\rangle$$

In particular, for the above circuit, we obtain the **equal superposition state**:

$$\boldsymbol{H^{\otimes n}} |0, \dots 0\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} \ |z\rangle = |\psi\rangle$$

Grover operator G

The Grover operator is composed of the Oracle, two Hadamard gates with a Phase gate in between.



Phase gate:

Flips the sign of all computational basis states, except for $|0\rangle$:

$$\begin{cases} |0\rangle \to |0\rangle \\ |x\rangle \to -|x\rangle \ \textit{for}\ x > 0 \end{cases} \quad \to (2|0\rangle\langle 0| - I)|x\rangle$$

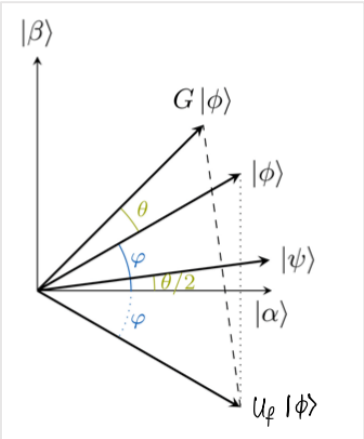
Hadamard + phase gates:

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

Full Grover operator: $G = H^{\otimes n}\ S^{\otimes n}\ H^{\otimes n}\ U_f = (2|\psi\rangle\langle\psi| - I)U_f$

Geometric interpretation of Grover's algorithm

Objective of the Grover's algorithm is to apply several rotations of the quantum state towards the $|\beta\rangle$ state.



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

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

The rotation angle θ is defined by $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$, such that:

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

By definition, U_f is a reflection across $|\alpha\rangle$ within subspace spanned by $\{|\alpha\rangle, |\beta\rangle\}$:

$$\begin{cases} U_f|\alpha\rangle = |\alpha\rangle \\ U_f|\beta\rangle = -|\beta\rangle \end{cases}$$

Likewise, $(2|\psi\rangle\langle\psi| - I)$ is a reflection across $|\psi\rangle$.

Since $|\psi\rangle$ is part of the subspace spanned by $|\alpha\rangle, |\beta\rangle$, Grover operator leaves subspace invariant.

Thus, G is product of two reflections → G is a rotation by angle θ:

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

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

Algebraic derivation

$G|\phi\rangle = (2|\psi\rangle\langle\psi| - I)\ U_f|\phi\rangle$

$= 2|\psi\rangle[\langle\psi|U_f|\phi\rangle] - U_f|\phi\rangle$

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

II. $\begin{cases} U_f|\alpha\rangle = |\alpha\rangle \\ U_f|\beta\rangle = -|\beta\rangle \end{cases}$

III. $U_f|\phi\rangle = cos(\varphi)\,U_f|\alpha\rangle + sin(\varphi)\,U_f|\beta\rangle = cos(\varphi)\,|\alpha\rangle - sin(\varphi)\,|\beta\rangle$

IV. $\langle\psi|U_f|\phi\rangle = (cos(\frac{\theta}{2})\,\langle\alpha| + sin(\frac{\theta}{2})\,\langle\beta|)(cos(\varphi)\,|\alpha\rangle - sin(\varphi)\,|\beta\rangle)$
$= cos(\frac{\theta}{2})\,cos(\varphi) - sin(\frac{\theta}{2})\,sin(\varphi)$
$= cos(\frac{\theta}{2} + \varphi)$

$$= 2\left(\cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle\right)\cos\left(\frac{\theta}{2}+\varphi\right) - (\cos(\varphi)\,|\alpha\rangle - \sin(\varphi)\,|\beta\rangle)$$

$$= \left(2\cos\left(\frac{\theta}{2}\right)\boldsymbol{\cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}+\boldsymbol{\varphi}\right) - \cos(\varphi)\right)|\alpha\rangle + \left(\sin\left(\frac{\theta}{2}\right)\boldsymbol{\cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}+\boldsymbol{\varphi}\right) + \sin(\varphi)\right)|\beta\rangle$$

$$= \left(2\cos\left(\frac{\theta}{2}\right)\left(\left[\cos\left(\frac{\theta}{2}\right)\cos(\varphi) - \sin\left(\frac{\theta}{2}\right)\sin(\varphi)\right]^{(1)} - \cos(\varphi)\right)\right)|\alpha\rangle$$
$$+ \left(2\sin\left(\frac{\theta}{2}\right)\left(\left[\cos\left(\frac{\theta}{2}\right)\cos(\varphi) - \sin\left(\frac{\theta}{2}\right)\sin(\varphi)\right]^{(1)} + \sin(\varphi)\right)\right)|\beta\rangle$$

$$= \left(\mathbf{2}\boldsymbol{\cos}^{\mathbf{2}}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\cos(\varphi) - \mathbf{2}\boldsymbol{\cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\boldsymbol{\sin}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\sin(\varphi) - \cos(\varphi)\right)|\alpha\rangle$$
$$+ \left(\mathbf{2}\boldsymbol{\sin}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\boldsymbol{\cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\cos(\varphi) - \mathbf{2}\boldsymbol{\sin}^{\mathbf{2}}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)\sin(\varphi) + \sin(\varphi)\right)|\beta\rangle$$

$$= ([\cos(\theta)+1]^{(2)}\cos(\varphi) - [\sin(\theta)]^{(3)}\sin(\varphi) - \cos(\varphi))|\alpha\rangle$$
$$+ ([\sin(\theta)]^{(3)}\cos(\varphi) - [1-\cos(\theta)]^{(4)}\sin(\varphi) + \sin(\varphi))|\beta\rangle$$

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

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

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

(1) – $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$
(2) – $2\cos^2(\alpha) = \cos 2\alpha + 1$
(3) – $2\cos(\alpha)\sin(\alpha) = \sin(2\alpha)$
(4) – $2\sin^2(\alpha) = 1 - \cos 2\alpha$

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

Starting from state $|\psi\rangle$ (**equal superposition state**) with initial angle $\varphi = \frac{\theta}{2}$

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

We want to rotate $|\psi\rangle$ to $|\beta\rangle$ $\rightarrow \begin{cases} (k+\frac{1}{2})\ \theta = \frac{\pi}{2} \\ \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}} \end{cases} \xrightarrow{M \ll N} \theta \approx 2\sqrt{\frac{M}{N}}$

In the last step we used the Taylor approximation: $\sin(x) \approx x$ for $x \ll 1$

In the final step, we measure the quantum bits. These will collapse (with high probability) to a basis state forming $|\beta\rangle$ (thus, a solution).

Optimality of the search algorithm

Goal is to show that any quantum search algorithm has lower bound complexity of $\Omega(\sqrt{N})$.
In fact, $O(\sqrt{N})$ is the optimal complexity.
Without loss of generality, we consider a problem with a single solution x.
Recall, that Oracle flips the sign of the (unique) solution: $\mathcal{O}_x = I - 2|x\rangle\langle x|$
The algorithm initializes a state (the equal superposition state) $|\psi\rangle$ and performs unitary operations U_k interleaved with oracle calls $\mathcal{O}_x$.
After K steps the algorithm finds a solution x: the state of the system will be:

$$|\psi_K^x\rangle = U_K \mathcal{O}_x U_{K-1} \mathcal{O}_x \dots U_1 \mathcal{O}_x |\psi_0\rangle$$

We also define another state, for which Oracle calls are omitted:

$$|\psi_K\rangle = U_K U_{K-1} \dots U_1 |\psi_0\rangle$$

We want to prove … by finding the upper bound of:

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

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

1st step: we prove that $D_k \le 4k^2$ (D_k must grow no faster than $O(k^2)$) by induction:
$k = 0$: $D_0 = 0$
$k \to k+1$

$$D_{k+1} = \sum_{x=0}^{N-1} \| \mathcal{O}_x |\psi_K^x\rangle - |\psi_K\rangle \|^2$$

$$= \sum_{x=0}^{N-1} \| \mathcal{O}_x (|\psi_K^x\rangle - |\psi_K\rangle) + (\mathcal{O}_x - I)|\psi_K\rangle \|^2 \qquad \mathcal{O}_x - I = -2|x\rangle\langle x| \quad \text{since} \quad \mathcal{O}_x = I - 2|x\rangle\langle x|$$

$$= \sum_{x=0}^{N-1} \| \mathcal{O}_x (|\psi_K^x\rangle - |\psi_K\rangle) - 2|x\rangle\langle x|\psi_K\rangle \|^2 \qquad \boldsymbol{b} = \mathcal{O}_x(|\psi_K^x\rangle - |\psi_K\rangle)\,,\ \boldsymbol{c} = -2|x\rangle\langle x|\psi_K\rangle$$

$$= \sum_{x=0}^{N-1} \| b + c \|^2$$

$$\le \sum_{x=0}^{N-1} (\|b\|^2 + 2\|b\| \cdot \|c\| + \|c\|^2) \qquad \mathcal{O}_x \text{ is unitary} - \text{norm is } 1$$

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

$$\le D_k + 4 \left(\sum_{x=0}^{N-1} \| |\psi_K^x\rangle - |\psi_K\rangle \|^2 \right)^{\frac{1}{2}} \left(\sum_{x=0}^{N-1} |\langle x|\psi_K\rangle|^2 \right)^{\frac{1}{2}} + 4 \sum_{x=0}^{N-1} |\langle x|\psi_K\rangle|^2$$

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

$$\le 4k^2 + 8k + 4 = 4(k+1)^2 \quad (\text{induction step})$$

$\| |\psi_K^x\rangle - |\psi_K\rangle \| \cdot |\langle x|\psi_K\rangle| \le \| |\psi_K^x\rangle - |\psi_K\rangle \|^2$ (Cauchy-Schwarz)

$$\sum_{x=0}^{N-1} (|\langle x|\psi_K\rangle|^2) = 1$$

2nd step: D_k must be $\Omega(N)$

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

Suppose that $|\langle x||\psi_K^x\rangle|^2 \geq \frac{1}{2} \quad \forall x$ (probability of success, at least 50%).

Without loss of generality: $\langle x||\psi_K^x\rangle = |\langle x||\psi_K^x\rangle|$ (can multiply $|x\rangle$ by an arbitrary phase vector)

$\||\psi_K^x\rangle - |x\rangle\|^2 = \||\psi_K^x\rangle\|^2 - 2\langle x||\psi_K^x\rangle + \||x\rangle\|^2$ (norm of vectors $|\psi_K^x\rangle$ and $|x\rangle$ is 1)

$= 2 - 2\big|\langle x|\big|\psi_K^x\rangle\big| \leq 2 - \sqrt{2}$ $\qquad$ $\big(|\langle x||\psi_K^x\rangle|^2 \geq \frac{1}{2} \rightarrow |\langle x||\psi_K^x\rangle| \geq \frac{1}{\sqrt{2}}$, not considering negative values$\big)$

Therefore:

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

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

$$= \sum_{x=0}^{N-1} \||x\rangle\|^2 - \mathcal{R}e\{\langle x||\psi_K\rangle\} + \||\psi_K\rangle\|^2$$

$$\geq 2N - 2\sum_{x=0}^{N-1} |\langle x||\psi_K^x\rangle| \cdot 1 \geq 2N - 2\sqrt{N}$$

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

$$\geq \sum_{x=0}^{N-1} \||\psi_K^x\rangle - |x\rangle\|^2 - 2\sum_{x=0}^{N-1} \||\psi_K^x\rangle - |x\rangle\| \cdot \||x\rangle - |\psi_K\rangle\| + \sum_{x=0}^{N-1} \||x\rangle - |\psi_K\rangle\|^2$$

$$= E_k + F_k - 2\sum_{x=0}^{N-1} \|a_x\| \cdot \|b_x\| \qquad (\|a\| \cdot \|b\| \geq |\langle a||b\rangle|)$$

$$\geq E_k + F_k - 2\sqrt{E_k}\sqrt{F_k}$$

$$= (\sqrt{F_k} - \sqrt{E_k})^2$$

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

$$= N\left(\sqrt{2 - \frac{2}{\sqrt{N}}} - \sqrt{2-\sqrt{2}}\right)$$

$$\cong N(\sqrt{2} - \sqrt{2-\sqrt{2}} \quad = c \cdot N \qquad (asyntotically\ equivalent)$$

In summary: $D_k \leq 4k^2$ and $D_k \geq c \cdot N \quad \rightarrow \quad k \geq \sqrt{c\frac{N}{4}}$ (#oracle evaluations for result)

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.

Density operator

So far, we used the state vector $|\psi\rangle$ to describe a quantum system.
An alternative (and convenient) formulation for quantum system about which we only have partial knowledge is the **density operator** (or density matrix).

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:

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

Unitary operations
A unitary transformation U maps $|\psi_i\rangle \to U|\psi_i\rangle$ (equivalently, $\{p_i, |\psi_i\rangle\} \to \{p_i, U|\psi_i\rangle\}$).
Thus, the density operator is transformed as:

$$\rho \xrightarrow{U} \sum_i p_i U \, |\psi_i\rangle\langle\psi_i| \, U^\dagger = U\rho U^\dagger$$

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

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \mathrm{tr}[M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|]$$

Thus, the overall probability for measurement result m equals:

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

After measurement, the state i collapses to:

$$|\psi_i\rangle \to \frac{M_m|\psi_i\rangle}{\|M_m|\psi_i\rangle\|} =: |\psi_i^m\rangle$$

Thus:

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle|\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\|M_m|\psi_i\rangle\|^2} = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{p(m)} = \frac{M_m\rho M_m^\dagger}{\mathrm{tr}\left[M_m^\dagger M_m \rho\right]}$$

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

$$\frac{p(i|m)}{p(m|i)} = \frac{p_i}{p(m)}$$

Note that ρ_m is now expressed solely in terms of ρ and the measurement operators, without explicit reference to the ensemble.

General properties of the density operator

Characterization of density operators - n operator ρ is the density operator associated to some ensemble if and only if:

I. $\mathrm{tr}[\rho] = 1$ *(trace condition)*
II. ρ is a positive operator *(positive condition)*

N.B., ρ is called a positive operator 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 *(each arrow shows a direction of the proof)*

I$\Longrightarrow$II

Suppose $\rho = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|$, then:

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

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

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

I$\Longleftarrow$II

Since ρ is an operator (i.e. a Hermitian matrix), and thus, according to the spectral theorem, there exist real eigenvalues λ_j and corresponding orthonormal eigenvectors $|\varphi_j\rangle$, such that:

$$\rho = \sum_j \lambda_j \left|\varphi_j\right\rangle\left\langle\varphi_j\right|$$

Since ρ satisfies the trace condition:

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

Due to positivity condition, $\lambda_j \geq 0 \;\forall j$.

Thus, we can interpret the eigenvalues λ_j as probabilities $\rightarrow \left\{\lambda_j, \left|\varphi_j\right\rangle\right\}$ is an ensemble and gives rise to ρ.

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

- "**pure state**": quantum system in a state $|\psi\rangle$, with corresponding density operator $\rho = |\psi\rangle\langle\psi|$ such that $\mathrm{tr}[\rho^2] = \mathrm{tr}[|\psi\rangle\langle\psi||\psi\rangle\langle\psi|] = \mathrm{tr}[|\psi\rangle\langle\psi|] = \langle\psi|\psi\rangle = 1$
- "**mixed state**": ρ describing a quantum state that cannot be written as $\rho = |\psi\rangle\langle\psi|$. Intuitively, in the ensemble representation of ρ, all the probabilities are < 1. Therefore, $\mathrm{tr}[\rho^2] = \sum_i p_i^2 < 1$

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 described 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 $1{=}\mathrm{tr}[\rho^2] = \sum_i \lambda_i$.

Moreover, $\mathrm{tr}[\rho^2] = \sum_i \lambda_i^2 \leq 1$,

with " $= 1$" precisely if one eigenvalue is 1 and the others are 0.

example:

ensemble representation is not unique!

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

$$With \begin{cases} |a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle \\ |b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle \end{cases}$$

For the following: given an ensemble $\{p_i, |\psi_i\rangle\}$., set $\left|\widetilde{\psi}_i\right\rangle = \sqrt{p_i}|\psi_i\rangle$ such that $\rho = \sum_j \left|\widetilde{\psi}_i\right\rangle\left\langle\widetilde{\psi}_i\right|$. We say that the ensemble $\left\{\left|\widetilde{\psi}_i\right\rangle\right\}$ generates the density operator. (N.B., the vectors are not normalized in general).
To relate an ensemble $\left\{\left|\widetilde{\psi}_i\right\rangle\right\}_{i=1,\dots m}$ to another $\left\{|\widetilde{\varphi}_i\rangle\right\}_{i=1,\dots n}$ 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 $\left\{\left|\widetilde{\psi}_i\right\rangle\right\}$ and $\left\{\left|\widetilde{\varphi}_j\right\rangle\right\}$ generate the same density matrix if and only if, for some unitary matrix (u_{ij}) holds that:

$$\left|\widetilde{\psi}_i\right\rangle = \sum_j u_{ij}|\widetilde{\varphi}_j\rangle$$

Proof

$\Longrightarrow$

Insert definitions

$\Longleftarrow$

Use the spectral decomposition of the density matrix $\rho = \sum_k \lambda_k |\mathcal{X}_k\rangle\langle\mathcal{X}_k|$ with $\langle\mathcal{X}_k|\mathcal{X}_l\rangle = \delta_{kl}$, set $|\mathcal{X}_k\rangle = \sqrt{\lambda_k}|\mathcal{X}_k\rangle$, express $\left|\widetilde{\psi}_i\right\rangle = \sum_k v_{ik}|\mathcal{X}_k\rangle$ for some complex coefficients v_{ik}. Then:

$$\sum_k \left|\widetilde{\mathcal{X}}_k\right\rangle\left\langle\widetilde{\mathcal{X}}_k\right| = \rho = \sum_i \left|\widetilde{\psi}_i\right\rangle\left\langle\widetilde{\psi}_i\right| = \sum_{k,l}\left(\sum_i v_{ik}v_{il}^*\right)\left|\widetilde{\mathcal{X}}_k\right\rangle\left\langle\widetilde{\mathcal{X}}_k\right|$$

In other words, if (v_{ik}) is a unitary matrix. By the same arguments, $|\varphi_j\rangle = \sum_k w_{jk}\left|\widetilde{\mathcal{X}}_k\right\rangle$ for a unitary matrix (w_{jk}). Thus:

$$\left|\widetilde{\psi}_i\right\rangle = \sum_k v_{ik}\left|\widetilde{\mathcal{X}}_k\right\rangle = \sum_k v_{ik}\, w_{jk}^*|\widetilde{\varphi}_j\rangle = \sum_j (vw^\dagger)_{ij}|\widetilde{\varphi}_j\rangle$$

And $(vw^\dagger)$ is (as product of two unitary matrices) again unitary.

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

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}$$

The reduced density operator

Partial trace
Let $n_1, n_2 \in \mathbb{N}$
The partial trace operations, are defined in terms of the conventional matrix trace by:

$\mathrm{tr}_1 \colon \mathbb{C}^{n_1 n_2 \times n_1 n_2} \to \mathbb{C}^{n_2 \times n_2}$, $\mathrm{tr}_1[M_1 \otimes M_2] = \mathrm{tr}[M_1]\cdot M_2$

$\mathrm{tr}_2 \colon \mathbb{C}^{n_1 n_2 \times n_1 n_2} \to \mathbb{C}^{n_1 \times n_1}$, $\mathrm{tr}_2[M_1 \otimes M_2] = \mathrm{tr}[M_2]\cdot M_1$

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 extension:

$\mathrm{tr}_1[\alpha M_1 \otimes M_2 + \beta N_1 \otimes N_2] = \alpha \cdot \mathrm{tr}[M_1 \otimes M_2] + \beta \cdot \mathrm{tr}_1[N_1 \otimes N_2]$

Consider a composite quantum system, consisting of subsystems A and B.
Let the quantum system be described by operator ρ_{AB}.
The reduced density operator for system A is defined by

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

Analogously, for system B: $\rho^B = \mathrm{tr}_A[\rho^{AB}]$
For any quantum states $|a_1\rangle, a_2\rangle \in A$ and $|b_1\rangle, b_2\rangle \in B$:

$$\mathrm{tr}_B[|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|] \;=\; |a_1\rangle\langle a_2| \cdot \mathrm{tr}[|b_1\rangle\langle b_2|] \;=\; |a_1\rangle\langle a_2| \cdot \langle b_2|b_1\rangle$$

which can be used as definition of partial trace, together with the requiring linearity.
Note that $|a_1\rangle\langle a_2|$ is a matrix, and $\langle b_2|b_1\rangle$ a complex number.
Moreover, $|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|$ can be written as $|a_1 b_1\rangle\langle a_2 b_2|$.

Given a density matrix ρ for subsystem A and a density matrix σ for subsystem B, suppose that the overall density matrix is the Kronecker product of ρ and σ:

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

Then:

$$\mathrm{tr_B}[\rho \otimes \sigma] = \rho\,\mathrm{tr}[\sigma] = \rho \qquad\qquad \mathrm{tr_A}[\rho \otimes \sigma] = \sigma\,\mathrm{tr}[\rho] = \sigma$$

$\rho^{AB} = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle$ and A: first qubit, B: second qubit.
Explicitly, expanding ρ^{AB} leads to:

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

The partial trace over subsystem B is:

$$\begin{aligned}\rho^A = \mathrm{tr_B}[\rho^{AB}] &= \frac{1}{2}(\mathrm{tr_B}[|00\rangle\langle 00|] + \mathrm{tr_B}[|00\rangle\langle 11|] + \mathrm{tr_B}[|11\rangle\langle 00|] + \mathrm{tr_B}[|11\rangle\langle 11|]) \\ &= \frac{1}{2}(|0\rangle\langle 0|\langle 0|0\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |1\rangle\langle 1|\langle 1|1\rangle) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}\end{aligned}$$

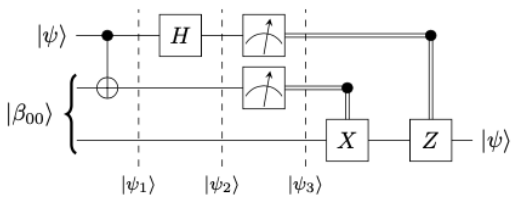
note, that the composite system is in the "pure state" $|\psi\rangle$, whereas the subsystem is described by the "mixed state" $\frac{I}{2}$ ($\mathrm{tr}[\rho^A] = \mathrm{tr}[\frac{I}{2}] = \frac{1}{2}\mathrm{tr}[I] = \frac{1}{2} < 1$)

<u>Motivation/justification for partial trace</u>: 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 $M \otimes I$, where I here denotes the identity matrix on subsystem B. In particular:

$$\langle M\rangle = \mathrm{tr}[M\rho^A] = \mathrm{tr}[(M \otimes I)\rho^{AB}] = \langle M \otimes I\rangle$$

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

<u>Application to quantum teleportation:</u>
At $|\psi_3\rangle$ Alice has completed her measurements (her qubits have "collapsed"), but Bob does not know her measurement results yet.



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

Thus, directly after Alice's measurements, system (from Bob's perspective) is in state:

$$|\varphi_1\rangle = |00\rangle(\alpha|0\rangle + \beta|1\rangle) \quad \text{with probability} \frac{1}{4}$$
$$|\varphi_2\rangle = |01\rangle(\alpha|1\rangle + \beta|0\rangle) \quad \text{with probability} \frac{1}{4}$$
$$|\varphi_3\rangle = |10\rangle(\alpha|0\rangle - \beta|1\rangle) \quad \text{with probability} \frac{1}{4}$$
$$|\varphi_4\rangle = |11\rangle(\alpha|1\rangle - \beta|0\rangle) \quad \text{with probability} \frac{1}{4}$$

The corresponding density matrix of ensemble $\left\{\frac{1}{4}, \left|\varphi_j\right\rangle\right\}_{j=1,\ldots,4}$:

$$\rho^{AB} = \frac{1}{4}\sum_{j=1}^{4}\left|\varphi_j\right\rangle\left\langle\varphi_j\right| = \frac{1}{4}\begin{pmatrix} |\mathbf{00}\rangle\langle\mathbf{00}| \otimes (\alpha|0\rangle + \beta|1\rangle)\ (\alpha^*\langle 0| + \beta^*\langle 1|) + \\ |\mathbf{01}\rangle\langle\mathbf{01}| \otimes (\alpha|1\rangle + \beta|0\rangle)\ (\alpha^*\langle 1| + \beta^*\langle 0|) + \\ |\mathbf{10}\rangle\langle\mathbf{10}| \otimes (\alpha|0\rangle - \beta|1\rangle)\ (\alpha^*\langle 0| - \beta^*\langle 1|) + \\ |\mathbf{11}\rangle\langle\mathbf{11}| \otimes (\alpha|1\rangle - \beta|0\rangle)\ (\alpha^*\langle 1| - \beta^*\langle 0|) \end{pmatrix}$$

In the above expression, the terms corresponding to the first two (Alice's) qubits are of the form $|a_1a_2\rangle\langle a_1a_2|$. Tracing them out, gives $\mathrm{tr}_\mathrm{A}[|a_1a_2\rangle\langle a_1a_2|] = \langle a_1a_2|a_1a_2\rangle = \langle a_1|a_1\rangle\langle a_2|a_2\rangle = 1$.

Thus, the reduced density operator describing Bob's qubit is:

$$\rho^B = \mathrm{tr}_\mathrm{A}[\rho^{AB}] = \frac{1}{4}\begin{pmatrix} (\alpha|0\rangle + \beta|1\rangle)\ (\alpha^*\langle 0| + \beta^*\langle 1|) + \\ (\alpha|1\rangle + \beta|0\rangle)\ (\alpha^*\langle 1| + \beta^*\langle 0|) + \\ (\alpha|0\rangle - \beta|1\rangle)\ (\alpha^*\langle 0| - \beta^*\langle 1|) + \\ (\alpha|1\rangle - \beta|0\rangle)\ (\alpha^*\langle 1| - \beta^*\langle 0|) \end{pmatrix} = \frac{1}{4}(2(|\alpha|^2 + |\beta|^2)|0\rangle\langle 0| + 2(|\alpha|^2 + |\beta|^2)|1\rangle\langle 1|)$$
$$= \frac{1}{4}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}$$

ρ^B is thus independent of $|\psi\rangle$.

Since $\rho^B = \frac{I}{2}$, any measurement by Bob cannot reveal any information about $|\psi\rangle$ *(Alice cannot transmit information via the instantaneous wavefunction collapse to Bob).*

Quantum operators

In general, changes of quantum states affected by unitary time evolution or wave function collapse during measurement.
Quantum operations are a mathematical generalization and unification of these concepts (also called "quantum channels").
Abstractly: $\rho' = \varepsilon(\rho)$

- Unitary time evolution: $\varepsilon(\rho) = U\rho U^\dagger$
- Measurements (M_m): $\varepsilon(\rho) = M_m \rho M_m^\dagger$

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

  Consider the scenario of performing a measurement, without recording the outcome; the density matrix after the measurement, is a weighted sum over all possible outcomes:

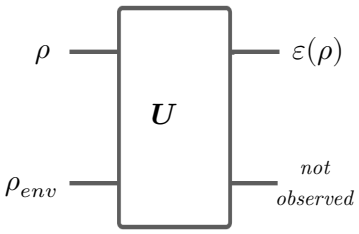
$$\varepsilon(\rho) = \sum_m p(m)\rho_m = \sum_m \varepsilon_m(\rho) = \sum_m M_m \rho\, M_m^\dagger$$

Different (but equivalent) perspective on quantum operations:

- System coupled with the environment (Stinespring dilation)
- Operator-sum (Kraus) representation
- Physically motivated axioms
- Choi matrix representation

Environments and quantum operations

"Open" quantum system can be regarded as interaction between a principal quantum system (initially in state ρ) and the environment (initially in state ρ_{env}).
The principal system interacts with the environment, meaning a time evolution of the overall system described by some unitary U.



$U(\rho \otimes \rho_{env})U^\dagger$
Output is the reduced density matrix of principal system:
$\varepsilon(\rho) = \mathrm{tr}_{\mathrm{env}}[U(\rho \otimes \rho_{env})U^\dagger]$

example: CNOT gate
We consider $\rho_{env} = |0\rangle\langle 0|$.
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:

$$U_{CNOT}(\rho \otimes |0\rangle\langle 0|)U_{CNOT}^\dagger = U_{CNOT}\left(\rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 10| + \rho_{10}|10\rangle\langle 00| + \rho_{11}|10\rangle\langle 10|\right)U_{CNOT}^\dagger$$
$$= \rho_{00}|00\rangle\langle 00| + \rho_{01}|00\rangle\langle 1\mathbf{1}| + \rho_{10}|1\mathbf{1}\rangle\langle 00| + \rho_{11}|1\mathbf{1}\rangle\langle 1\mathbf{1}|$$

$$\mathrm{tr}_{\mathrm{env}}\left[U_{CNOT}(\rho \otimes |0\rangle\langle 0|)U_{CNOT}^\dagger\right] = \rho_{00}|0\rangle\langle 0|\langle 0|0\rangle + \rho_{01}|0\rangle\langle 1|\langle 1|0\rangle + \rho_{10}|1\rangle\langle 0|\langle 0|1\rangle + \rho_{11}|1\rangle\langle 1|\langle 1|1\rangle$$
$$= \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| = \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix}$$

Equivalently, $\rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| = P_0\rho P_0^\dagger + P_1\rho P_1^\dagger$, with $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$.
(off-diagonal entries of ρ are set to 0).

Operator-sum representation

Let $\{|e_k\rangle\}$ be an orthonormal basis of the environment quantum system, assume without loss of generality $\rho_{env} = |e_0\rangle\langle e_0|$
(if environment is a mixed state, then we can equivalently work with a pure state in a larger environment).

$$\begin{aligned}\varepsilon(\rho) &= \mathrm{tr}_{\mathrm{env}}[U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger] \\ &= \sum_k \mathrm{tr}_{\mathrm{env}}[U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger\ (I \otimes |e_k\rangle\langle e_k|)] \\ &= \sum_k \langle e_k|U\ (\rho \otimes |e_0\rangle\langle e_0|)\ U^\dagger|e_k\rangle \\ &= \textstyle\sum_k E_k \rho E_k^\dagger \quad \textit{with } E_k \textit{ a complex matrix with entries } (E_k)_{lm} = \langle l, e_k|U|m, e_0\rangle\end{aligned}$$

The E_k's are called operation elements or Kraus operators of ε:

$$\varepsilon(\rho) = \sum_k E_k \rho E_k^\dagger$$

---

example: CNOT (see above)

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

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

Completeness relation of Kraus operators

If ε is trace-preserving, then for any density matrix ρ:

$$\begin{aligned}1 = \mathrm{tr}[\varepsilon(\rho)] = \mathrm{tr}\left[\sum_k E_k \rho E_k^\dagger\right] &= \sum_k \mathrm{tr}\left[E_k \rho E_k^\dagger\right] \\ &= \sum_k \mathrm{tr}\left[E_k^\dagger E_k \rho\right] \qquad (\textit{cyclic invariance} \rightarrow tr[AB] = tr[BA]) \\ &= \mathrm{tr}\left[\left(\sum_k E_k^\dagger E_k\right)\rho\right]\end{aligned}$$

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

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

PSD (Positive semidefinite) matrix
$A \in \mathbb{C}^{n\times n}$ is called positive semidefinite if A is Hermitian and $\langle v|Av\rangle \geq 0$ for all $v \in \mathbb{C}^n$
(the last condition holds if and only if all eigenvalues are ≥ 0).
"$A \leq B$" if $B - A$ is positive semidefinite

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

Remark: physical interpretation as measurement performed on environment with respect to $\{|e_k\rangle\}$ basis, i.e. measurement operators $|e_k\rangle\langle e_k|$:
For outcome k, state of principal system is:

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

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

System-environment model of a Kraus representation

Given trace-preserving $\varepsilon(\rho) = \sum_{k=0}^{n-1} E_k \rho E_k^\dagger$, is there a corresponding system-environment representation? Yes!

We define model environment as vector space of dimension n, with orthonormal basis $\{|e_k\rangle\}_{k=0,\dots,n-1}$. Assuming environment starts in state $|e_0\rangle$:

Define unitary U via $U|\psi\rangle|e_0\rangle = \sum_k E_k|\psi\rangle|e_k\rangle$ and extension to a unitary operator on combined system.

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

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

preserves orthogonality.

Remember that $\sum_k E_k^\dagger E_k = I$ due to completeness relation.

U has the desired property since:

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

Axiomatic approach to quantum operations

Alternative viewpoint: physically motivated axioms which a quantum operation ε must obey.

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

A2: ε is convex-linear: $\varepsilon\left(\sum_i p_i \rho_i\right) = \sum_i p_i \varepsilon(\rho_i)$ for any probabilistic vector ρ and density matrices $\{\rho_i\}$

A3: ε is a completely positive map: $\varepsilon(A)$ 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 $(I \otimes \varepsilon)(A)$ must be p.s.d. for any p.s.d. matrix A on combined system RQ.

Theorem: the map ε satisfies $A1, A2, A3$ if and only if $\varepsilon(\rho) = \sum_k E_k \rho E_k^\dagger$ for some set of complex matrices $\{E_k\}$ with $\sum_k E_k^\dagger E_k \le I$.

Proof:

$\Longleftarrow$

To verify A3: let A be a p.s.d. matrix on enlarged system RQ, then, for any vector $|\psi\rangle$ on RQ:

$$\langle\psi|(I \otimes \varepsilon)(A)|\psi\rangle = \sum_k \langle\psi|(I \otimes E_k)(A)(I \otimes E_k^\dagger)|\psi\rangle = \sum_k \langle\varphi_k|A|\varphi_k\rangle \ge 0$$

$\Longrightarrow$

Principal system (which ε acts on) denoted Q, dimension n.

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

Let $\left\{\left|j_Q\right\rangle : j = 1, \dots n\right\}$ an orthonormal basis of Q

Let $\left\{\left|j_R\right\rangle : j = 1, \dots n\right\}$ an orthonormal basis of R

Define the "maximally entangled state"

$$|\alpha\rangle := \sum_{j=1}^{n} \left|j_R\right\rangle\left|j_Q\right\rangle \in RQ$$

and "Choi matrix" which is p.s.d. by A3 (density matrix on combined system):

$$\sigma := (I \otimes \varepsilon)(|\alpha\rangle\langle a|)$$

Turns out to completely specific ε

For any state $|\psi\rangle = \sum_j \psi_j \left|j_Q\right\rangle$ on Q, set $\left|\tilde{\psi}\right\rangle = \sum_j \psi_j^* \left|j_R\right\rangle \in R$.

$$\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \left\langle\tilde{\psi}\right| \sum_{i,j} |i_R\rangle\langle j_R| \otimes \varepsilon\left(|i_Q\rangle\left\langle j_Q\right|\right) \left|\tilde{\psi}\right\rangle \qquad (\textit{inner product on } R)$$
$$= \sum_{i,j} \psi_i \psi_j^* \varepsilon(|i_Q\rangle\langle j_Q|) = \varepsilon(|\psi\rangle\langle\psi|)$$

Spectral decomposition $\rightarrow \sigma = \sum_k |s_k\rangle\langle s_k|$ for some states $|s_k\rangle$ on combined system (eigenvalues absorbed into $|s_k\rangle$).
Can represent $|s_k\rangle = \sum_{j,j'=1}^{n} s_{k,j,j'} |j_R\rangle\left|j'_Q\right\rangle$
For each k, define linear map $E_k : Q \rightarrow Q$ by $E_k\left|j_Q\right\rangle = \sum_{j'=1}^{n} s_{k,j,j'}\left|j'_Q\right\rangle$ and linear extension.
Then, $E_k|\psi\rangle = E_k \sum_j \psi_j \left|j_Q\right\rangle$

$$= \sum_{j,j'=1}^{n} \psi_j s_{k,j,j'} \left|j'_Q\right\rangle$$
$$= \sum_{j''=1}^{n} \sum_{j,j'=1}^{n} \psi_{j''} s_{k,j,j'} \langle j''_R|j_R\rangle \left|j'_Q\right\rangle$$
$$= \sum_{j''=1}^{n} \psi_{j''} \langle j''_R|s_k\rangle$$
$$= \left\langle\tilde{\psi}\right|\left.s_k\right\rangle \quad (\textit{inner product on } R)$$

$$\sum_k E_k |\psi\rangle\langle\psi| E_k^\dagger = \sum_k \left\langle\tilde{\psi}\right|\left.s_k\right\rangle\left\langle s_k\right|\left.\tilde{\psi}\right\rangle = \left\langle\tilde{\psi}\right| \sum_k |s_k\rangle\langle s_k| \left|\tilde{\psi}\right\rangle = \left\langle\tilde{\psi}\right|\left.\sigma\right|\tilde{\psi}\rangle = \varepsilon(|\psi\rangle\langle\psi|)$$
Holds for arbitrary $|\psi\rangle \in Q \overset{A2}{\rightarrow} \varepsilon(\rho) = \sum_k E_k \rho E_k^\dagger$ for any density matrix ρ.

Examples of quantum operations

- **Bit flip channel** - flips $|0\rangle \longleftrightarrow |1\rangle$ with probability $1-p$, $p \in [0,1]$
$$\begin{cases} E_0 = \sqrt{p} \cdot I \\ E_1 = \sqrt{1-p} \cdot X \end{cases}$$

- **Phase flip** – flips phase with probability $1-p$
$$\begin{cases} E_0 = \sqrt{p} \cdot I \\ E_1 = \sqrt{1-p} \cdot Z \end{cases}$$

- **Depolarizing channel** – Replace ρ by completely mixed state $\frac{I}{2}$ with probability p:
$$\varepsilon(\rho) = p \cdot \frac{I}{2} + (1-p) \cdot \rho$$
In the Bloch sphere representation, this corresponds to uniform contraction.

- **Amplitude damping** - $|1\rangle \rightarrow |0\rangle$ flip happens with probability γ
$$\begin{cases} E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \\ E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix} \end{cases}$$