Introduction to Quantum Computing

Gabriel Ribeiro Fernandes

October 2025

1 Introduction

(see Introduction slides)

2 Section 2

2.1 Section 2.1

(Nielsen and Chuang section 1.2)

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

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

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

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

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

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

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

Instead "standard measurement" will result in:

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

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

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

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

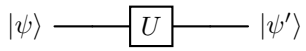
Circuit notation: 

2.2 Single qubit gates

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

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

Circuit notation:



Notes:

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

Examples:

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

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

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

- Pauli-Y gate:

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

- Pauli-Z gate:

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

  Z leaves $|0\rangle$ unchanged, but flips the sign of the coefficient of $|1\rangle$.
  Recall the block sphere representation of a general quantum state:

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

  Then:

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

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

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

- Hadamard gate:

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

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

- Phase gate:

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

- T gate:

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

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

Pauli matrices satisfy:

$\sigma_j^2 = identity.$

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

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

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

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

2.3 Multiple qubit

(Nielsen and Chang sections 1.2.1, 2.1.7)

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

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

Thus:

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

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

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

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

Wavefunction directly after measurement:

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

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

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

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

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

$$= \sum_{x=0}^{2^n-1} \alpha_x |x\rangle \qquad \text{binary representation} \tag{4}$$

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

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

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

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

2.4 Multiple qubit gates

(Nielsen and Chuang sections 1.3.2, 1.3.4, 2.17)

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

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

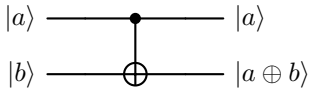
$$\underbrace{|0\rangle}_{control}\underbrace{|0\rangle}_{target} \mapsto |00\rangle,$$

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

Can be expressed as:

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

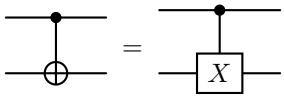
Circuit notation:



Matrix Representation:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} Pauli - X$$

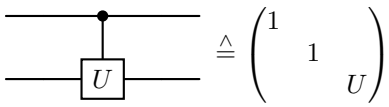
This matrix is unitary.
Alternative notation:



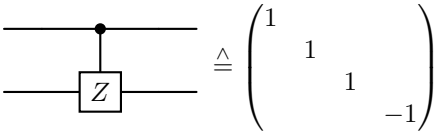
We can generalise Pauli-X to any unitary single-qubit gate U acting on the target qubit $\rightsquigarrow$ controlled U-gate:

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

Generalisation:

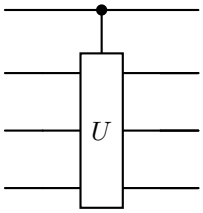


Example: controlled-z:

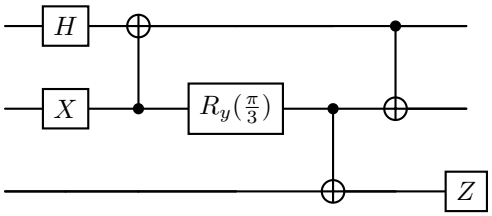


Exercice: show that controlled-z gate is invariant when flipping control and target qubits.

Controlled-U gate for multiple target qubits:

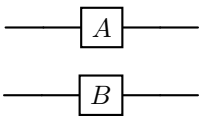


Note: single qubit and CNOT gates are universal: they can be used to implement an arbitrary unitary operation on n qubits.
(Quantum analogue of universality of classical NAND gate)
proof in Nielsen and Chang section 4.5
Example of a circuit consisting only of single qubit gates and CNOTs:



(time left to right)

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



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

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

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

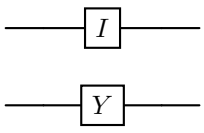
$$|00\rangle \mapsto |0\rangle \otimes \underbrace{(Y\,|0\rangle)}_{i|1\rangle} = i\,|01\rangle$$

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

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

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

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

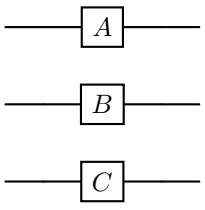


$$\triangleq \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \quad Pauli - Y = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} = I \otimes Y$$

General formula: Kronecker product (matrix representation of tensor products of operators)

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

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



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

Basic properties:

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

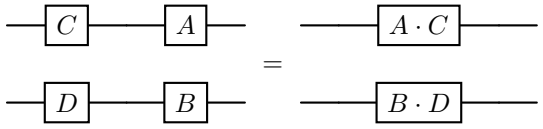
(b) $(A \otimes B)^T = A^T \otimes B^T$ (transposition)

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

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

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

for matrices of compatible dimensions.



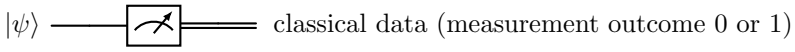
(side exchange because its read from left to right)

(f) Kronecker product of Hermitian matrices is Hermitian

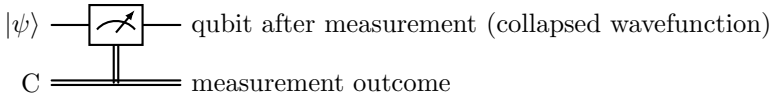
(g) Kronecker product of unitary matrices is unitary (follows from (c) & (e))

2.5 Quantum measurements

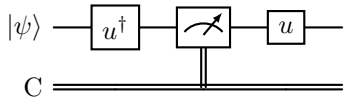
(Nielsen and Chuang sections 1.3.3, 2.2.3, 2.2.5)
Review: measurement of a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$with respect to computational basis$|0\rangle$, $|1\rangle$:



alternative notation:

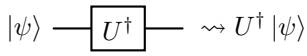


Unitary freedom of choice of measurement basis.
Given an orthonormal basis (ONB) $\{|u_1\rangle, |u_2\rangle\}$, we can measure with respect to this orthonormal basis by performing a base change before and after the measurement:
$U = (|u_1\rangle\, |u_2\rangle) \in \mathbb{C}^{2\times 2}$ unitary



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

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



$\rightsquigarrow U^\dagger |\psi\rangle = \alpha_2 |0\rangle\, \alpha_1 \beta |1\rangle$ $(U^\dagger |u_1\rangle = |0\rangle, U^\dagger |u_2\rangle = |1\rangle)$
We will obtain measurement result 0 or 1 with the respective probabilities $|\alpha_1|^2$ and $|\alpha_2|^2$
After measuring and applying U: $|\psi\rangle$will be in the state $|u_1\rangle$ or $|u_2\rangle$.

Abstract, general defenition of quantum measurements
Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the quantum system, with the index m labelling possible measurement outcomes.
Denoting the quantum state before the measurement by $|\psi\rangle$, result m occurs with probability:

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

state after the measurement is:

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

The measurement operators satisfy the completeness relation:

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

such that the probabilities sum to 1:

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

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

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

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

$$\rightsquigarrow p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}$$
$$= |\alpha|^2$$
$$p(1) = \langle\psi| M_1^\dagger M_1 |\psi\rangle = \ldots = |\beta|^2$$

Projective measurements

$\rightsquigarrow$ see projection-operators (moodle)

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

$$M = \sum_m \lambda_m P_m$$

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

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

State of the quantum system after the measurement:

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

Remarks:

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

Average value of a projective measurement

$$\mathbb{E}[M] = \sum_m \lambda_m p(\lambda_m) = \sum_m \lambda_m \langle\psi| P_m |\psi\rangle$$
$$= \langle\psi| \sum_m \lambda_m P_m |\psi\rangle = \langle\psi| M |\psi\rangle =: \langle M\rangle \quad |\text{if } |\psi\rangle \text{is clear from context.}$$

Corresponding standard deviation:

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

Examples:

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

- In general: measurement w.r.t. orthogonal basis $|u_1\rangle, |u_2\rangle$ is a projective measurement:
  $$\text{set } P_m = |u_m\rangle\langle u_m| \text{ for } m = 1, 2$$
  Define observable M by
  $$M \coloneqq \sum_{m=1}^{2} \lambda_m P_m \text{ with arbitrary } \lambda_1, \lambda_2 \in \mathbb{R}, \lambda_1 \neq \lambda_2$$

- Measuring Pauli-Z (as observable):
  $$z = 1 \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{P_0 = |0\rangle\langle 0|} + (-1) \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{P_1 = |1\rangle\langle 1|}$$
  Agrees with standard measurement w.r.t. the computational basis $\{|0\rangle, |1\rangle\}$.

2.6 The Heisenberg uncertainty principle

Supose C and D are two observables and $|\psi\rangle$a quantum state.
Then:

$$\Delta(C) \cdot \Delta(D) \geq \frac{|\langle\psi| [C, D] |\psi\rangle|}{2} \qquad [A, B] \coloneqq AB - BA$$

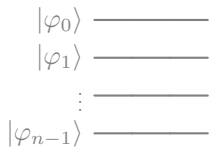
Interpretation for experiment: repeated preparation of $|\psi\rangle$, measure C in some cases and D in the other cases to obtain the standard deviations $\Delta(C)$ and $\Delta(D)$.

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

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

3 Entanglement and and its applications

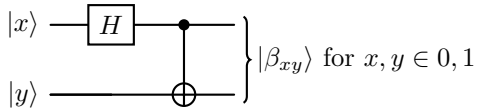
(Albert Einstein (1947): "spooky action at a distance")
A n-qubit state $|\psi\rangle (n \geq 2)$ is called entangled if it cannot be written as tensor product of single qubit states, i.e. $|\psi\rangle = |\varphi_{n-1}\rangle \otimes \ldots \otimes |\varphi_0\rangle$ for any $|\varphi_0\rangle, \ldots, |\varphi_{n-1}\rangle \in \mathbb{C}^2$



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

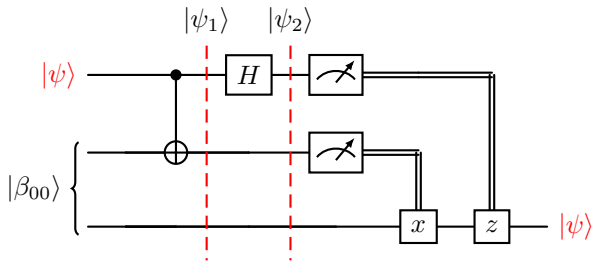
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |a\rangle\,|b\rangle$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Quantum circuit to create Bell states:



3.1 Quantum teleportation

(Nielsen and Chuang section 1.3.7)
Scenario: two (experimental physicists) Alice and Bob are far away from each other. When visiting eachoter in the past, they generated the EPR pair $|\beta_{00}\rangle$, each keeping one qubit of the pair.
Alice's task is to send another (unknown) qubit state $|\psi\rangle$ to Bob.
Note: measurement is not an option.
Quantum circuit for teleporting $|\psi\rangle$:



(wire 1 & 2 represent Alice's 2 qubits, wire 3 represents Bob's Qubit.)

Input:

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

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

after Hadamard:

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

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

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

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

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

similary:

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

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

3.2 EPR and the Bell inequality

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

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

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

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

Example:

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

  1: wavefunction collapses to $|01\rangle$

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

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

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

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

  namely:

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

If Alice measures eigenvalue 1, the wavefunction will collapse t $|+-\rangle \rightsquigarrow$ Bob'squbit is in state $|-\rangle$.
So he will certainly measure eigenvalue (-1). (conversly if Alice measures -1)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bell inequality:

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

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

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

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

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

Observables:

$$Q = Z_1 \ (_1\!\rightarrow \ \textit{first qubit (Alice)}) \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}} \ (_2\!\rightarrow \ \textit{second qubit (Bob)})$$

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

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

$\langle Q \cdot S \rangle + \langle R \cdot S \rangle + \langle R \cdot T \rangle - \langle Q \cdot T \rangle = 2\sqrt{2} \not\leq 2$ (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, S, R, T have definit values independent of observation (measurement)
- "locality": Alice performing her measurement cannot influence Bob's measurementand vice versa.

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

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

4 Quantum search algorithms

(Nielsen and Chuang: section 6)

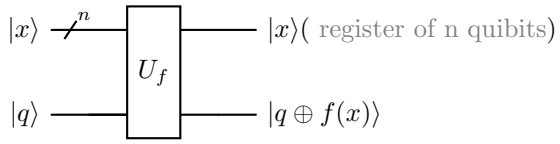
Classical search through N unordered elements: O(N)
Quantum Groover's algorithm: O($\sqrt{N}$) (under certain preconditions)

4.1 Quantum oracles

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

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

Quantum version of f?
$\rightsquigarrow$ quantum "oracle" U_f defined for computational basic states



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

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

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

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

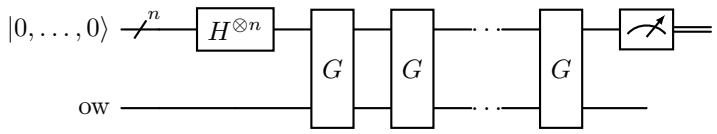
Effective action of oracle: $|x\rangle$ — U_f — $(-1)^{f(x)} |x\rangle$

$\rightsquigarrow$ oracle "marks" solutions by a phase flip.

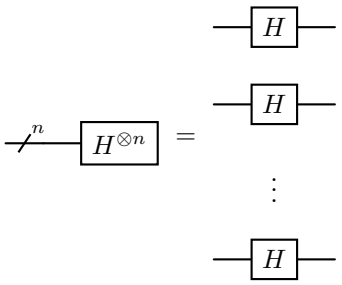
How could one construct such an oracle without knowing the solution already?
Example: factorisation of a large integer $m \in N$:
Finding prime factors of m is "difficult" on a classical computer:
(no known algorithm with polynomial runtime in the bitlength of m)
But testing whether a given $x \in \mathbb{N}$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

4.2 Grover's Algorithm

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



ow: oracle workspace (auxiliary qubit)
G: Groover operator



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

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

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

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

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

Applied to several qubits:

$$\underbrace{H^{\otimes n}}_{H\otimes H\otimes\ldots H}|x_1,\ldots,x_n\rangle = (H|x_1\rangle)\otimes\ldots\otimes(H|x_n\rangle) \overset{(1)}{=} \frac{1}{\sqrt{2^n}}\sum_{z_{1i}-z_n}^{1}(-1)^{z_1x_1+\ldots+z_nx_n}|z_1\ldots z_n\rangle$$

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

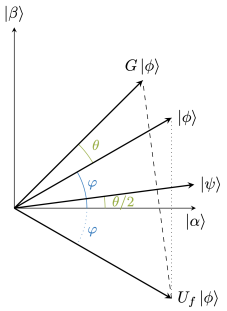
With:

(1): $H|x_1\rangle = \frac{1}{\sqrt{2}}\sum_{z_1=0}^{1}(-1)^{z_1x_1}|z_1\rangle$

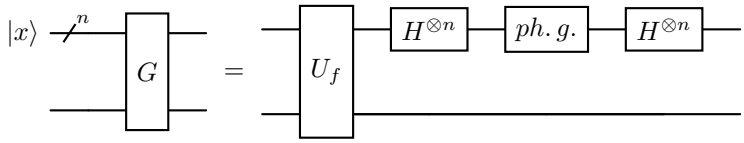
In particular: $H^{\otimes n}|0,\ldots,0\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}|z\rangle =: |\psi\rangle$equal superposition state

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

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



Definition of Grover operator G:



Captions:

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

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

All single qubit gates together:

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

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

Geometric interpretation

Define:

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

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

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

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

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

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

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

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

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

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

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

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

4.3 Optimality of the search algorithm

(Nielsen and Chuang section 6.6)

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

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

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

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

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

Strategy of proof: upper bound of

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

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

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

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

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

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

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

$k = 0:$ $\quad D_0 = 0$

$k \mapsto k+1:$

$$\begin{aligned}
D_{k+1} &= \sum_{x=0}^{N-1} \Big\| \underbrace{U_{k+1}O_x\,|\psi_k^x\rangle - U_{k+1}\,|\psi_k\rangle}_{U_{k+1}(O_x|\psi_k^x\rangle - |\psi_k\rangle)} \Big\|^2 \\
&\overset{(1)}{=} \sum_{x=0}^{N-1} \|O_x\,|\psi_k^x\rangle - |\psi_k\rangle\|^2 \\
&= \sum_{x=0}^{N-1} \Big\| \underbrace{O_x(|\psi_k^x\rangle - |\psi_k\rangle)}_{=:b} + \underbrace{(O_x - I)\,|\psi_k\rangle}_{-2|x\rangle\langle x\,|\,\psi_k\rangle =:c} \Big\|^2 \\
&\overset{(2)}{\leq} \sum_{x=0}^{N-1} (\|b\|^2 + 2\,\|b\|\cdot\|c\| + \|c\|^2) \qquad | \; O_x \text{ is unitary} \\
&= \sum_{x=0}^{N-1} (\||\psi_k^x\rangle - |\psi_k\rangle\|^2 + 4\,\||\psi_k^x\rangle - |\psi_k\rangle\|\cdot|\langle x\,|\,\psi_k\rangle| + 4\,|\langle x\,|\,\psi_k\rangle|) \\
&\overset{(3)}{\leq} D_k + 4\,\underbrace{(\sum_{x=0}^{N-1} \||\psi_k^x\rangle - |\psi_k\rangle\|^2)^{\frac{1}{2}}}_{\|u\|} \cdot \underbrace{(\sum_{x=0}^{N-1} |\langle x|\psi_k\rangle|^2)^{\frac{1}{2}}}_{\|v\|=1} + 4 \\
&= D_k + 4\sqrt{D_k} + 4 \\
&\overset{I.H.}{\leq} 4k^2 + 4\sqrt{4k^2} + 4 \\
&= 4(k+1)^2
\end{aligned}$$

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

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

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

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

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

$$\begin{aligned}
\rightsquigarrow \||\psi_k^x\rangle - |x\rangle\|^2 &= \||\psi_k^x\rangle\|^2 - 2\langle x|\psi_k^x\rangle + \||x\rangle\|^2 \\
&= 2 - 2\underbrace{\langle x|\psi_k^x\rangle}_{\leq \frac{1}{\sqrt{2}}} \\
&\leq 2 - \sqrt{2}
\end{aligned}$$

Therefore:

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

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

$$\begin{aligned}
F_k &= \sum_{x=0}^{N-1} (\||x\rangle\| - 2Re\langle x|\psi_k\rangle + \||psi_k\rangle\|^2) \\
&\overset{(4)}{\geq} 2 \cdot N - 2\sum_{x=0}^{N-1} \underbrace{|\langle x|\psi_k\rangle|}_{u_x} \cdot \underbrace{1}_{v_x} \\
&\overset{(3)}{\geq} 2 \cdot N - 2[(\underbrace{\sum_x |\langle x|\psi_k\rangle|^{\frac{1}{2}})^2}_{1} \cdot \underbrace{(\sum_x 1)^{\frac{1}{2}}}_{N}] \\
&= 2 \cdot N - 2\sqrt{N}
\end{aligned}$$

$$
\begin{aligned}
D_k &= \sum_{x=0}^{N-1} \|(|\psi_k^x\rangle - |x\rangle) + (|x\rangle - |\psi_k\rangle)\|^2 \\
&\geq \sum_{x=0}^{N-1} (\||\psi_k^x\rangle - |x\rangle\| - 2\,\||\psi_k^x\rangle - |x\rangle\| \cdot \||x\rangle - |\psi_k\rangle\|^2 + \||x\rangle - |\psi_k\rangle\|^2) \\
&= E_k + F_k - 2 \sum_{x=0}^{N-1} \underbrace{\||\psi_k^x\rangle - |x\rangle\|}_{=:a_x} \cdot \underbrace{\||x\rangle - |\psi_k\rangle\|}_{=:b_x} \\
&\geq E_k + F_k - 2 \underbrace{\sqrt{E_k}}_{\|a\|} \cdot \underbrace{\sqrt{F_k}}_{\|a\|} = (\sqrt{F_k} - \sqrt{E_k})^2 \\
&\geq (\sqrt{2N - 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N}\,)^2 \\
&= N \cdot (\sqrt{2} - \sqrt{2-\sqrt{2}})^2 \\
&= N(\sqrt{2 - \frac{2}{\sqrt{N}}} - \sqrt{2-\sqrt{2}}\,)^2 \qquad | \text{ with } \lim_{N\to\infty} \frac{2}{\sqrt{N}} \to 0 \\
&\cong N \cdot \underbrace{(\sqrt{2} - \sqrt{2-\sqrt{2}})^2}_{=:c \approx 0.42} \\
&= c \cdot N
\end{aligned}
$$

In summary:

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

with k being the number of oracle evaluations.

5 The density operator

So far the state vector $|\psi\rangle$ described a quantum state. A convenient alternative formulation for quantum systems about which we have only partial information is the 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, this defines an ensemble of quantum states $\{p_i, |\psi_i\rangle\}$.
The density operator ρ of the ensemble $\{p_i, |\psi_i\rangle\}$ is defined as:

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

Properties

Bra-Ket (Dirac) notation

- **Ket:**
  - $|\psi\rangle + |\varphi\rangle = |\psi + \varphi\rangle$
  - $a\,|\psi\rangle = |a\psi\rangle$
  - $|\psi\rangle = \langle\psi|^\dagger$

  Righthand-side rules:

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

  Complex conjugate:

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

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

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

Matrices

- **Normal matrix:**

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

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

- **Unitary matrix:**

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

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

- **Hermitian matrix:**

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

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

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

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

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

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