Notes on Introduction to Quantum Computing

Leon Windheuser

December 30, 2022

1 Basic Concepts

1.1 Quantum bits (qubits)

Classical bits: $0, 1$
Quantum bit *qubit*: Superposition of 0 and 1:
A quantum state $|\psi\rangle$ is described as

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

where

$$|\alpha|^2 + |\beta|^2 = 1 \quad (\textit{normalization}). \tag{2}$$

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

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

Different from classical bits, cannot (in general) directly observe / measure a qubit (the amplitudes α and β). Instead: "*standard*" measurement will result in

- 0 with probability $|\alpha|^2$
- 1 with probability $|\beta|^2$

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

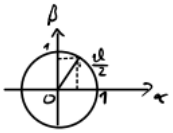
In practise: Can estimate the probabilities $|\alpha|^2$ and $|\beta|^2$ in experiments by repeating the same experiment many times (i.e via outcome statistics). These repetitions are called *trials* or *shots*.

Figure 1: Circuit notation

A useful graphical deputation of a qubit is the Bloch sphere representation: If α and β happen to be real-valued, then can find angle $\vartheta \in \mathbb{R}$ such that

$$\alpha = \cos\frac{\vartheta}{2}, \quad \beta = \sin\frac{\vartheta}{2} \tag{3}$$

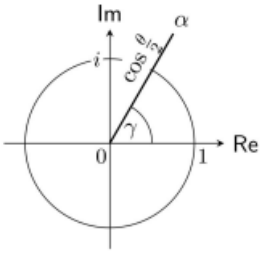
$$(\rightsquigarrow |\alpha|^2 + |\beta|^2 = \cos\frac{\vartheta}{2} + \sin\frac{\vartheta}{2}) = 1 \quad \checkmark$$



In general: represent

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

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



Then:

$$|\psi\rangle = e^{i\psi}\cos\frac{\vartheta}{2}\cdot|0\rangle + \underbrace{e^{i(\varphi+\gamma)}}_{=\,e^{i\varphi}\cdot e^{i\gamma}}\sin\frac{\vartheta}{2}\cdot|1\rangle \tag{4}$$

$$= \underbrace{e^{i\gamma}}_{\text{can be ignored here}}\left(\cos\frac{\vartheta}{2}\cdot|0\rangle + e^{i\varphi}\cdot\sin\frac{\vartheta}{2}\cdot|1\rangle\right) \tag{5}$$

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

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

on the surface of a sphere:

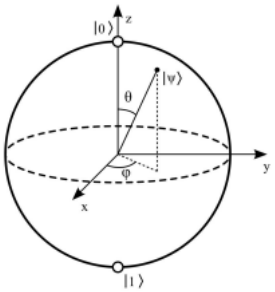


Figure 2: Bloch Sphere (Felix Bloch)

1.2 Single qubit gates

Principles 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 point $t' > t$.
Transition described by a complex unitary matrix U:

$$|\psi'\rangle = U \cdot |\psi\rangle \tag{6}$$

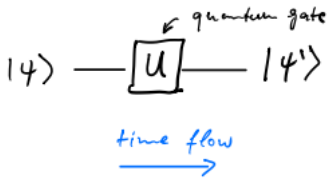


Figure 3: Circuit notation

Notes:

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

Examples:

- Quantum analogue of the classical NOT gate ($0 \leftrightarrow 1$) flip $|0\rangle \leftrightarrow |1\rangle$ leads to Pauli-X gate:

$$X \equiv \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{7}$$

Check: $X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$ and $X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$ ✓

- Pauli-Y gate:
$$Y \equiv \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{8}$$
- Pauli-Z gate:
$$Z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

  Z leaves $|0\rangle$ unchanged, but flips the sign of the coefficient of $|1\rangle$. Recall the Bloch Sphere representation:
$$|\psi\rangle = \cos\frac{\vartheta}{2} \cdot |0\rangle + e^{i\varphi} \sin\frac{\vartheta}{2} \cdot |1\rangle$$
  Then
$$\begin{aligned} Z|\psi\rangle &= \cos\frac{\vartheta}{2} \cdot |0\rangle \; - \; e^{i\varphi} \sin\frac{\vartheta}{2} \cdot |1\rangle \\ &\overset{e^{i\pi}=-1}{=} \cos\frac{\vartheta}{2} \cdot |0\rangle + \underbrace{e^{i\pi} e^{i\varphi}}_{e^{i(\varphi+\pi)}} \sin\frac{\vartheta}{2} \cdot |1\rangle \end{aligned}$$
  $\rightsquigarrow$ new Bloch Sphere angles: $\vartheta' = \vartheta, \varphi = \varphi + \pi$ (rotating by $\pi = 180°$ around z-axis)
  X, Y, Z gates are called Pauli matrices. The Pauli vector $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$ is a vector of 2×2 matrices.
- Hadamard Gate:
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

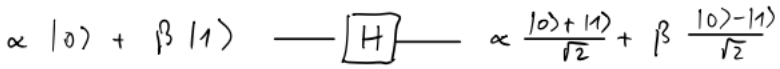


Figure 4: Hadamard Gate

- Phase Gate:
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$
- T Gate:
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$
  Note: $T^2 = S$ since $(e^{i\pi/4})^2 = e^{i\pi/2} = i$

Pauli matrices satisfy:

1. $\sigma_j^2 = I$ (identifity) for $j = 1, 2, 3$
2. $\sigma_j \cdot \sigma_k = -\sigma_k \sigma_j$ for all $j \neq k$
3. $[\sigma_j, \sigma_k] := \underbrace{\sigma_j \sigma_k - \sigma_k \sigma_j}_{\text{Commutator}} = 2i\sigma_l$ for (j, k, l) a cyclic permutation of (1,2,3).

General definition of matrix exponential

$$exp(A) \equiv e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k, \quad A \in \mathbb{C}^{n \times n} \tag{10}$$

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

$$\begin{aligned} e^{iAx} &= \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k)!} (ix)^{2k} \underbrace{A^{2k}}_{(A^2)^k = I^k = I}}_{\text{even}} + \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k+1)!} (ix)^{2k+1} \underbrace{A^{2k+1}}_{(A^2)^k \cdot A = I^k \cdot A = A}}_{\text{odd}} \\ &= \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k)!} (-1)^k x^{2k}}_{=\cos x} \cdot I + \underbrace{\sum_{k=0}^{\infty} \frac{1}{(2k+1)!} (-1)^k x^{2k+1}}_{=i \sin x} \cdot A \\ &= \cos x \cdot I + i \sin x A \end{aligned}$$

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

This can be used to define the following rotation operators via the Pali matrices. Let $\vartheta \in \mathbb{R}$:

$$R_x(\vartheta) := e^{-i\vartheta X/2} = \cos \frac{\vartheta}{2} I - i \sin \frac{\vartheta}{2} X = \begin{pmatrix} \cos \frac{\vartheta}{2} & -i \sin \frac{\vartheta}{2} \\ -i \sin \frac{\vartheta}{2} & \cos \frac{\vartheta}{2} \end{pmatrix} \tag{11}$$

$$R_y(\vartheta) := e^{-i\vartheta Y/2} = \cos \frac{\vartheta}{2} I - i \sin \frac{\vartheta}{2} Y = \begin{pmatrix} \cos \frac{\vartheta}{2} & -\sin \frac{\vartheta}{2} \\ \sin \frac{\vartheta}{2} & \cos \frac{\vartheta}{2} \end{pmatrix} \tag{12}$$

$$R_z(\vartheta) := e^{-i\vartheta Z/2} = \cos \frac{\vartheta}{2} I - i \sin \frac{\vartheta}{2} Z = \begin{pmatrix} e^{-i\vartheta/2} & 0 \\ 0 & e^{i\vartheta/2} \end{pmatrix} \tag{13}$$

General case: Rotation about an axis $\vec{v} \in \mathbb{R}^3$ (normalized such that $\|\vec{v}\|) = \sqrt{v_1^2 + v_2^2 + v_3^3} = 1$):
using the notation:

$$\langle \vec{v}|\vec{\sigma}\rangle = \vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 = \begin{pmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{pmatrix} \tag{14}$$

It holds that $(\vec{v}\cdot\vec{\sigma})^2 = I$.
We define the rotation operator around axis $\vec{v}$ as

$$R_v(\vartheta) := e^{-i\vartheta(\vec{v}\cdot\vec{\sigma})/2} = \cos\frac{\vartheta}{2}I - i\sin\frac{\vartheta}{2}(\vec{v}\cdot\vec{\sigma}) \tag{15}$$

Note: R_x, R_y, R_z are special cases corresponding to $\vec{v} = (1,0,0)$, $\vec{v} = (0,1,0)$, and $\vec{v} = (0,0,1)$.

Can derive that the Bloch Sphere representaiton of $R_{\vec{v}}(\vartheta)$ is a "conventional" rotation (in three dimensions) by angle ϑ about axis $\vec{v}$.

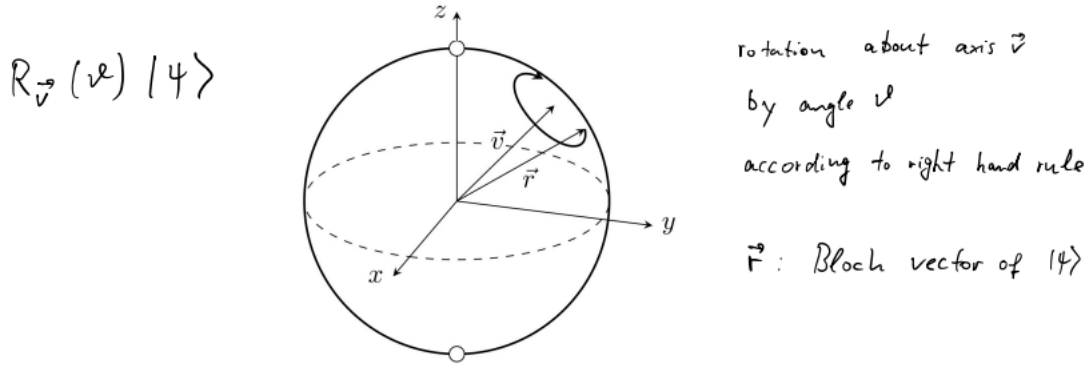


Figure 5: Circuit notation

Z-Y decomposition of an arbitrary 2×2 unitary matrix:
For any unitary matrix $U \in \mathbb{C}^{n\times n}$ there exist real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = e^{i\alpha} \underbrace{\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}}_{R_z(\beta)} \cdot \underbrace{\begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}}_{R_y(\gamma)} \cdot \underbrace{\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}}_{R_z(\delta)} \tag{16}$$

1.3 Multiple qubits

So far: Single qubits, superposition of basis states $|0\rangle$ and $|1\rangle$. For two qubits, this generalizes to $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{17}$$

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

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad \text{(normalization)}. \tag{18}$$

Can identify the basis states with unit vectors:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{19}$$

Thus:

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4 \tag{20}$$

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

$$\begin{array}{lll} 0 & \text{with probability} & |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ 1 & \text{with probability} & |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{array}$$

Wavefunction directly after measurement:

$$\begin{aligned} \text{if measured 0:} \quad |\psi'\rangle &= \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \\ \text{if measured 1:} \quad |\psi'\rangle &= \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} \end{aligned}$$

Mathematical formalism for constructing two qubit states: Tensor product of vector space.
Can combine two (arbitrary) vector spaces V and W to form the tensor product $V \otimes W$.

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

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

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

Let $\{|i\rangle_v : i = 1, ..., m\}$ be a basis of of V, and let $\{|j\rangle_w : j = 1, ..., n\}$ be a basis of of W, then

$$\{|i\rangle_v \otimes |j\rangle_w : i = 1, ..., m, j = 1, ..., n\}$$

is a basis of $V \otimes W$. In particular, $dim(V \otimes W) = dim(V) \cdot dim(W)$.
Note: $|i\rangle_v \otimes |j\rangle_w$ is also written as $|ij\rangle$.

Basic properties of tensor product:

- $\forall |v\rangle \in V, |w\rangle \in W \wedge \alpha \in \mathbb{C}$:

$$\alpha(|v\rangle \otimes |w\rangle) = (\alpha|0\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle) \tag{21}$$

- $\forall |v_1\rangle, |v_2\rangle \in V \wedge |w\rangle \in W$:

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \tag{22}$$

- $\forall |v\rangle \in V \wedge |w_1\rangle, |w_2\rangle \in W$:

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \tag{23}$$

Vector notation using standard basis, e.g.

$$\begin{aligned} |v\rangle &= v_1|0\rangle + v_2|1\rangle = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \\ |w\rangle &= w_1|0\rangle + w_2|1\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \\ |v\rangle \otimes |w\rangle &= (v_1|0\rangle + v_2|1\rangle) \otimes (w_1|0\rangle + w_2|1\rangle) \\ &= v_1w_1|00\rangle + v_1w_2|01\rangle + v_2w_1|10\rangle + v_2w_2|11\rangle \end{aligned}$$

Thus:

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

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

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

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

$$\langle \sum_j \alpha_j |v_j\rangle \otimes |w_j\rangle | \sum_k \beta_k |v_k\rangle \otimes |w_k\rangle \rangle := \sum_j \sum_k \alpha_j^* \beta_k \langle v_j | v_k \rangle \cdot \langle w_j | w_k \rangle \quad (24)$$

Generalization to n qubits: 2^n computational basis states

$$\{\underbrace{|0, ..., 0\rangle}_{\text{length } n}, |0, ..., 0, 1\rangle, ...|1, ..., 1\rangle\}$$

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

$$|\psi\rangle = \sum_{x_0=0}^{1} \sum_{x_1=0}^{2} \cdots \sum_{x_{n-1}}^{1} \alpha_{x_n - 1, ..., x_1, x_0} \cdot |x_{n-1}, ..., x_1 x_0\rangle \quad (25)$$

with $\alpha_x \in \mathbb{C}$ for all $x \in \{0, ..., 2^n - 1\}$, such that $\|\psi\|^2 = \sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$ (normalization).

$\rightsquigarrow$ In general *"hard"* to simulate on classical computer (for large n) due to "curse of dimensionality".
Vector space as tensor products: $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{(2^n)}$

1.4 Multiple qubit gates

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

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

Can be expressed as

$$|a, b\rangle \mapsto |a, a \oplus b\rangle \quad \forall a, b \in \{0, 1\} \tag{26}$$

, where $\oplus$ is the addition modulo 2.

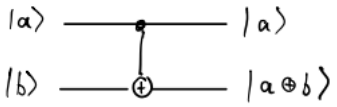


Figure 6: CNOT circuit notation

Matrix representation:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{27}$$

, with the Pauli-X matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Figure 7: Alternative CNOT circuit notation

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

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

Figure 8: Controlled-U gate

Figure 9: Example: Controlled-Z gate

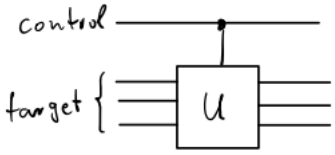


Figure 10: Controlled-U for multiple target qubits

Note: Single qubit and CNOT gates are universal: They can be used to implement an arbitraty unitray operation on n qubits (Quantum analogue of univerisity of classical NAND gate). Proof in Nielsen and Chuang section 4.5.

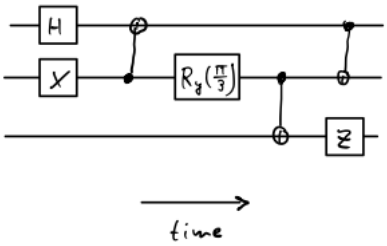
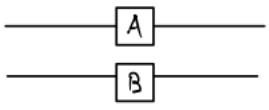


Figure 11: Example of a circuit lousisting only of single qubit gates and CNOTs

1.4.1 Matrix Kronecker Products

Matrix representation of single qubit gates acting in parallel:



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

$$|a, b\rangle \mapsto (A|a\rangle) \otimes (B|b\rangle) \tag{28}$$

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

$$
\begin{aligned}
|00\rangle &\mapsto |0\rangle \otimes (Y|0\rangle) = i|01\rangle \\
|01\rangle &\mapsto |0\rangle \otimes (Y|1\rangle) = -i|00\rangle \\
|10\rangle &\mapsto |1\rangle \otimes (Y|0\rangle) = i|11\rangle \\
|11\rangle &\mapsto |1\rangle \otimes (Y|1\rangle) = -i|10\rangle
\end{aligned}
$$

Matrix representation:

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

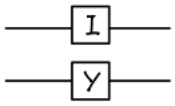
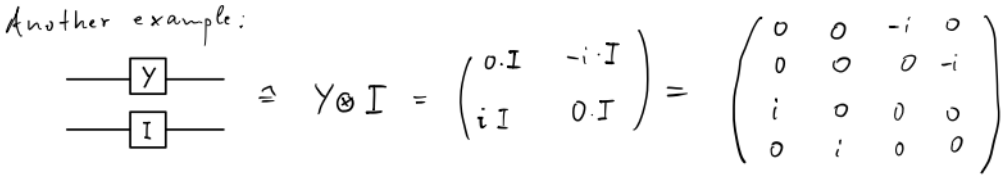


Figure 12: Circuit notation

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

$$
A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp \times nq} \tag{29}
$$

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



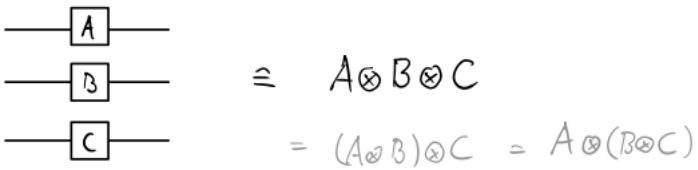
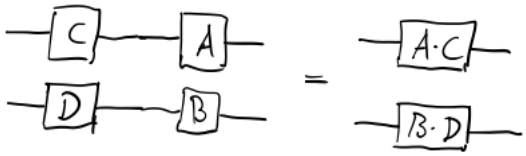


Figure 13: Generalization to arbitrary number of tensor factors possible

Basic properties:

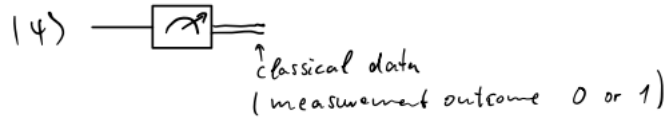
1. $(A \otimes B)^* = A^* \otimes B^*$ (elementwise complex conjugation)
2. $(A \otimes B)^T = A^T \otimes B^T$ (transposition)
3. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
4. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ (associative property)
5. $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$ (for matrix of compatible dimensions)



6. Kronecker product of Hermitian matrices is Hermitian.
7. Kronecker product of unitary matrices is unitary (follows from 3. and 5.)

1.5 Quantum measurement

Review: measurement of a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with resepct to the computational basis $\{|0\rangle, |1\rangle\}$.



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

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

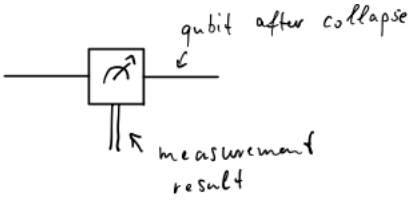
Representation of $|\psi\rangle$ w.r.t $\{|+\rangle, |-\rangle\}$ basis:

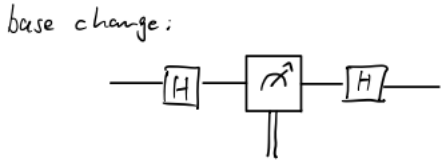
$$\alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

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

$$\begin{aligned} + \quad &\text{with probability} \quad \frac{|\alpha+\beta|^2}{2} \\ - \quad &\text{with probability} \quad \frac{|\alpha-\beta|^2}{2} \end{aligned}$$

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





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

1.5.1 Abstract general definition 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 measurement $|\psi\rangle$, result m occurs with probability

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \|M_m|\psi\rangle\|^2 \tag{30}$$

, state after measurement is:

$$\frac{M_m|\psi\rangle}{\|M_m|\psi\rangle\|} \tag{31}$$

The measurement operators satisfy the completeness relation

$$\sum_m M_m^\dagger M_m = I \tag{32}$$

such that probabilities sum to 1:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \left\langle\psi\middle|\sum_m M_m^\dagger M_m\middle|\psi\right\rangle \langle\psi|\psi\rangle = 1 \tag{33}$$

since $\sum_m M_m^\dagger M_m = I$.

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

$$\begin{aligned} M_0 &:= |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}(1,0) = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \\ M_1 &:= |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}(0,1) = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} \\ \rightsquigarrow p(0) &= \left\langle \psi \middle| M_0^\dagger M_0 \middle| \psi \right\rangle = \langle \psi | M_0 | \psi \rangle = |\alpha|^2 \\ p(1) &= \left\langle \psi \middle| M_1^\dagger M_1 \middle| \psi \right\rangle = \langle \psi | M_1 | \psi \rangle = |\beta|^2 \end{aligned}$$

1.5.2 Projective Measurements

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

$$P = \sum_{j=1}^{m} |u_j\rangle\langle u_j| \tag{34}$$

$$P|w\rangle = \sum_{j=1}^{m} \underbrace{\langle u_j | w\rangle}_{\text{inner product}} \tag{35}$$

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

$$A = U \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix} U^\dagger = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| \tag{36}$$

$$= \sum_{k=1}^{m} \widetilde{\lambda_k} P_k \quad \text{with } \{\widetilde{\lambda_1} ... \widetilde{\lambda_m}\} \text{ the distinct eigenvalues} \tag{37}$$

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

$$M = \sum_m \lambda_m P_m \tag{38}$$

with P_m: projection onto eigenspace with eigenvalue λ_m. The possible outcomes of the measurement correspond to the eigenvalues λ_m.
Probability of getting result λ_m when measuring a quantum state $|\psi\rangle$:

$$p(\lambda_m) = \langle\psi|P_m|\psi\rangle \tag{39}$$

State of the quantum system directly after the measurement:

$$\frac{P_m|\psi\rangle}{\|P_m|\psi\rangle\|} = \frac{P_m|\psi\rangle}{\sqrt{p(\lambda_m)}} \tag{40}$$

Remarks:

- Projective measurements are special cases of general measurement framework
- Projective measurements combined with unitary transformations are equivalent to general measurement framework, see pages 94, 95 in Nielsen and Chuang.

Average value of a projective measurement:

$$\mathbb{E}[M] = \sum_m \lambda_m p(\lambda_m) = \sum_m \lambda_m \langle\psi|P_m|\psi\rangle \tag{41}$$

$$= \left\langle \psi \middle| \sum_m \lambda_m P_m \middle| \psi \right\rangle = \langle\psi|M|\psi\rangle = \langle M\rangle \tag{42}$$

Corresponding standard deviation:

$$\Delta(M) := \sqrt{\langle M^2\rangle - \langle M\rangle^2} = \sqrt{\langle (M - \langle M\rangle)^2\rangle} \tag{43}$$

Examples:

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

  $$P_m = |u_m\rangle\langle u_m| \quad \text{for } m = 1, 2$$

  Define observable M by

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

- Measuring Pauli-Z

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

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

1.6 The Heisenberg uncertainty principle

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

$$\langle\psi|AB|\psi\rangle = x + iy, \quad x, y \in \mathbb{R} \tag{44}$$

$$\langle\psi|AB|\psi\rangle^* = \big\langle\psi\big|(AB)^\dagger\big|\psi\big\rangle = \big\langle\psi\big|B^\dagger A^\dagger\big|\psi\big\rangle = \langle\psi|BA|\psi\rangle \tag{45}$$

Thus

$$\langle\psi|[A,B]|\psi\rangle = 2iy \quad \text{and} \quad \langle\psi|\{A,B\}|\psi\rangle = 2x \tag{46}$$

where $\{A,B\} := AB + BA$ is the anti-Commutator.

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4 \cdot \underbrace{|\langle\psi|AB|\psi\rangle|^2}_{x^2+y^2} \tag{47}$$

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

$$|\langle\psi|[A,B]|\psi\rangle|^2 \overset{(47)}{\leq} 4 \cdot |\langle\psi|AB|\psi\rangle|^2 \leq 4 \cdot \big\langle\psi\big|A^2\big|\psi\big\rangle \cdot \big\langle\psi\big|B^2\big|\psi\big\rangle \tag{48}$$

Suppose C and D are two observables: substitute $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ leads to Heisenberg uncertainty principle:

$$\Delta(C) \cdot \Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2} \tag{49}$$

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

2 Entanglement and its applications

A n-qubit state $|\psi\rangle$ ($n \geq 2$) is called entangled if it cannnot be written as a tensor product of single-qubit states; i.e

$$|\psi\rangle \neq |\psi_{n-1}\rangle \otimes \cdots \otimes |\psi_0\rangle \tag{50}$$

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

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

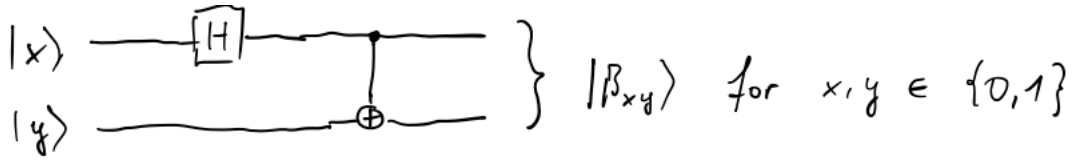


Figure 14: Quantum circuit to create Bell states

2.1 Quantum teleportation

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

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

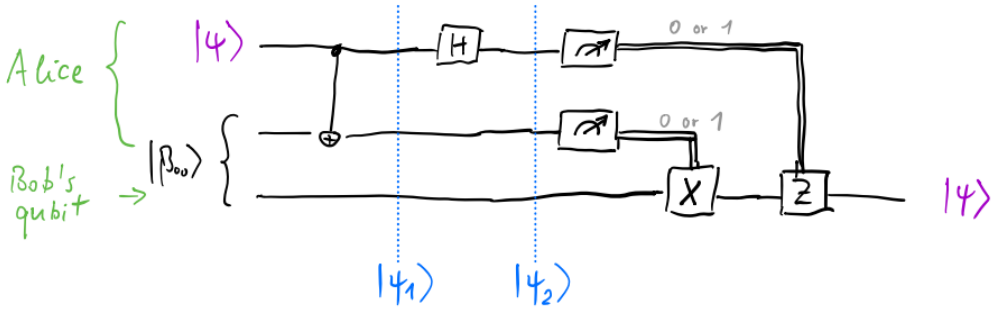


Figure 15: Quantum circuit for teleporting $|\psi\rangle$

Input:

$$|\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle+\beta|1\rangle)\otimes|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta\underbrace{|1\rangle(|00\rangle + |11\rangle)}_{\text{CNOT}}\right]$$

after CNOT:

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

after Hadamard:

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}[\alpha(|0\rangle + |1\rangle)\cdot(|00\rangle + |11\rangle)] + \beta(|0\rangle - |1\rangle)\cdot((|10\rangle + |01\rangle)) \\
&= \frac{1}{2}(\alpha|000\rangle + \alpha|011\rangle\alpha|100\rangle + \alpha|111\rangle) + \beta|010\rangle + \beta|001\rangle - \beta|110\rangle - \beta|101\rangle) \\
&= \frac{1}{2}(\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle) + \beta|010\rangle + \beta|001\rangle - \beta|110\rangle - \beta|101\rangle \\
&= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))
\end{aligned}$$

Now Alice measures her qubits w.r.t computational basis, e.g. projective measurement with

$$\begin{aligned}
P_1 &= |00\rangle\langle 00| \otimes I, \quad P_2 = |01\rangle\langle 10| \otimes I \\
P_3 &= |10\rangle\langle 10| \otimes I, \quad P_2 = |11\rangle\langle 11| \otimes I
\end{aligned}$$

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

$$|00\rangle(\alpha|0\rangle + \beta|1\rangle) = |00\rangle \underbrace{|\psi\rangle}_{\text{Qubit at Bob's place}}$$

similarly:

$$
\begin{aligned}
00 &\mapsto \alpha|0\rangle + \beta|1\rangle \\
01 &\mapsto \alpha|1\rangle + \beta|0\rangle \\
10 &\mapsto \alpha|0\rangle - \beta|1\rangle \\
11 &\mapsto \alpha|1\rangle - \beta|0\rangle
\end{aligned}
$$

Alice transmits her measurement result to Bob (classical information), Bob then applies Pauli-X and / or Pauli-Z to recover $|\psi\rangle$. Even though wavefunction collapse is instantaneous, no faster-than-light transfer possible due to required classical communication.

2.2 EPR and the Bell inequality

EPR: Einstein, Podolsky, Rosen EPR paper: *"Can quantum mechanical description of physical relatiy be considered complete?"* (1935)
The another argue that quantum mechanics is incomplete since it lacks certain "elements of reality" (property can be predicted with certainity).

Scenario: Alice and Bob are far from each other, but share the entangled two-qubit "spin-singlet" state

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

Alice and Bob measure the observable $\vec{v} \circ \vec{\sigma} = v_1 X + v_2 Y + v_3 Z$ (with $v \in \mathbb{R}^3, \|\vec{v}\| = 1$) on their respective qubit. (Recall $\vec{v} \circ \vec{\sigma}$ is Hermitian and unitary, and has eigenvalues ± 1)

Alice performs her measurement immediately before Bob. Example:

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

  $$
  \begin{aligned}
  1: &\quad \text{wavefunction collapses to } |01\rangle \\
  0: &\quad \text{wavefunction collapses to } |10\rangle
  \end{aligned}
  $$

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

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

  $$|\beta_{11}\rangle = \frac{-1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \tag{51}$$

namely:

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

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

- General observable $\vec{v} \circ \vec{\sigma}$, 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 $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

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

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

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

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

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

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = e^{i\vartheta}\frac{1}{\sqrt{2}}(|ab\rangle - |ba\rangle)$$

$\rightsquigarrow$ 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 result (after performing her measurement) since they are far apart (speed of light too slow).

EPR argument: "Property" $\vec{v} \circ \vec{\sigma}$ of a qubit is an "element of reality". However, quantum mechanics does not a priori specify this property for all possible $\vec{v}$ (but only probabilities), and is thus an incomplete description of reality.
Instead, "Hidden variable theory": There must be additional variables "hidden" in a qubit which determine Bob's measurement of $\vec{v} \circ \vec{\sigma}$ for all possible $\vec{v} \in \mathbb{R}^3$.

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

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

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

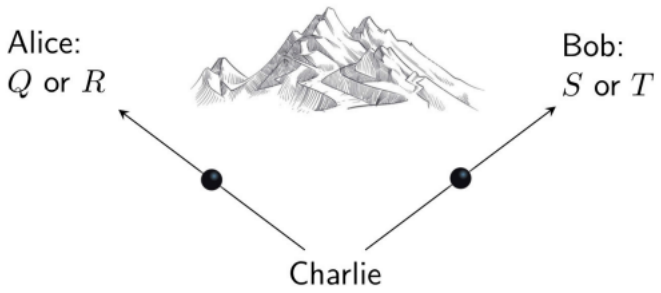


Figure 16: Charlie prepares two particles, sends one to Alice and one to Bob.

By convention binary property values: $Q, R, S, T \in \{\pm 1\}$. Alice decides randomly whether to measure property Q or R and Bob decides randomly to measure property S or T.
Alice and Bob perform their measurement (almost) simultaneously, such that no information about their result can be transmitted in between.
After completing this protocol, Alice and Bob need to analyse their measurement data.
Consider the quantity:

$$QS + RS + RT - QT = \underbrace{(Q+R)}_{\pm 2 \text{ or } 0} S + \underbrace{(R-Q)}_{0 \text{ or } \pm 2} T = \pm 2 \tag{52}$$

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

$$\mathbb{E}[QS + RS + RT - QT] = \sum_{q,r,s,t\in\{\pm 1\}} p(\underbrace{qs + rs + rt - qt}_{\pm 2}) \tag{53}$$

$$\leq \sum_{q,r,s,t\in\{\pm 1\}} p(q,r,s,t) \cdot 2 = 2 \tag{54}$$

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

$$\mathbb{E}[QS] + \mathbb{E}[RS] + \mathbb{E}[RT] - \mathbb{E}[QT] \leq 2 \tag{55}$$

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

Compare with "quantum" realization of the experiment: Charlie prepares two-qubit singlet state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and sends the first qubit to Alice and the second to Bob. Observables

$$Q = \underbrace{Z_1}_{\text{acts on first qubit}}, \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}}$$

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

Measurement averages (c.f. Exericse 8.1):

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

$$\langle RS\rangle = \frac{1}{\sqrt{2}}$$

$$\langle RT\rangle = \frac{1}{\sqrt{2}}$$

$$\langle QS\rangle = -\frac{1}{\sqrt{2}}$$

$\rightsquigarrow \langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \not\leq 2$ (Violates Bell's inequality!)

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

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

$\rightsquigarrow$ Nature is not "*locally realistic*". (Most common viewpoint: Realism does not hold)

Practical lesson: Use entanglement as a resource.

3 Quantum Search Algorithnms

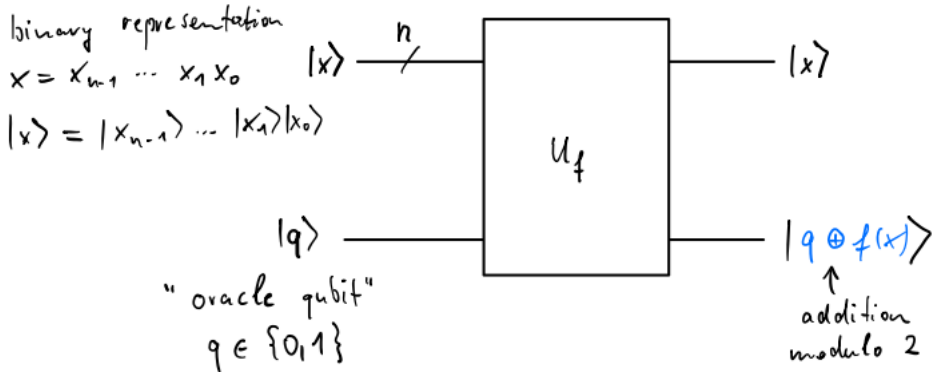
Classical search algorithm through N unordered elements $\mathcal{O}(N)$.
Quantum Grover's algorithm: $\mathcal{O}(\sqrt{N})$ (given certain predictions).

3.1 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 corresponding indictor function $f : \{0, ..., N-1\} \mapsto \{0, 1\}$ by

$$f(x) = \begin{cases} 0, & \text{if element } x \text{ is not a solution} \\ 1, & \text{if element } x \text{ is a solution} \end{cases} \tag{56}$$

Quantum version of f? $\rightsquigarrow$ Quantum "oracle" U_f defined for computational basis states as



Note: U_f maps basis states to basis states and satisfies

$$U_f^2 = I \quad (\text{since } q \oplus f(x) \oplus f(x) = q) \tag{57}$$

Thus U_f permutes basis states and is in particular unitary.
Initialize oracle qubit in superposition $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \overset{U_f}{\mapsto} \begin{cases} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(x) = 0 \\ |x\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(x) = 1 \end{cases} \tag{58}$$

In summary:

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \overset{U_f}{\mapsto} \underbrace{-1^{f(x)}}_{\text{only this part relevant for the following}} |x\rangle \otimes \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{\text{Oracle qubit unchanged}} \tag{59}$$

$\rightsquigarrow$ Effective action of oracle

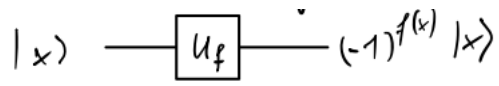


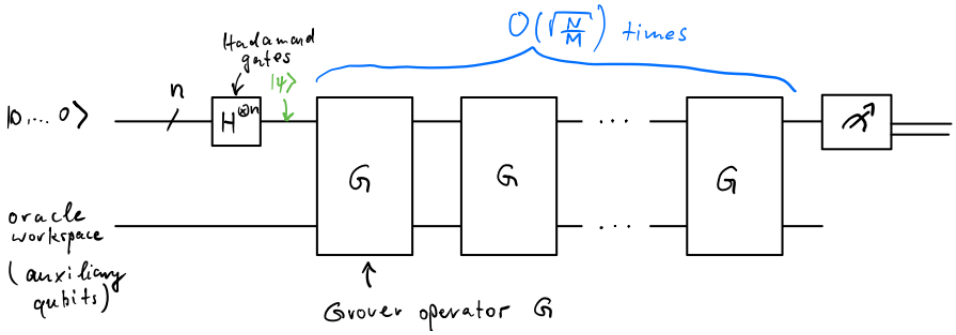
Figure 17: Oracle "marks" solution by a phase flip.

How could one construct such an oracle without knowing solution already?
Example: Factorization of a large integer $m \in \mathbb{N}$: Finding prime factor of m is "difficult" on a classical computer (no known algorithm with polynomial runtime in the bit length of m).
But testing whether a given $x \in \mathbb{N}$ divides m is simple.

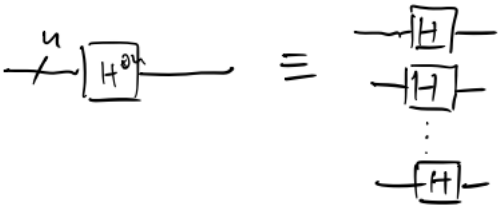
Can perform arithmeti operations for trial divisions on a digital quantum computer as well $\rightsquigarrow$ Oracle which recognizes a solution x.

3.2 Grover's Algorithm

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



Initial Hadamard transform:



Note: For $x \in \{0,1\}$:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{zx} |z\rangle \tag{60}$$

Applied to several qubits:

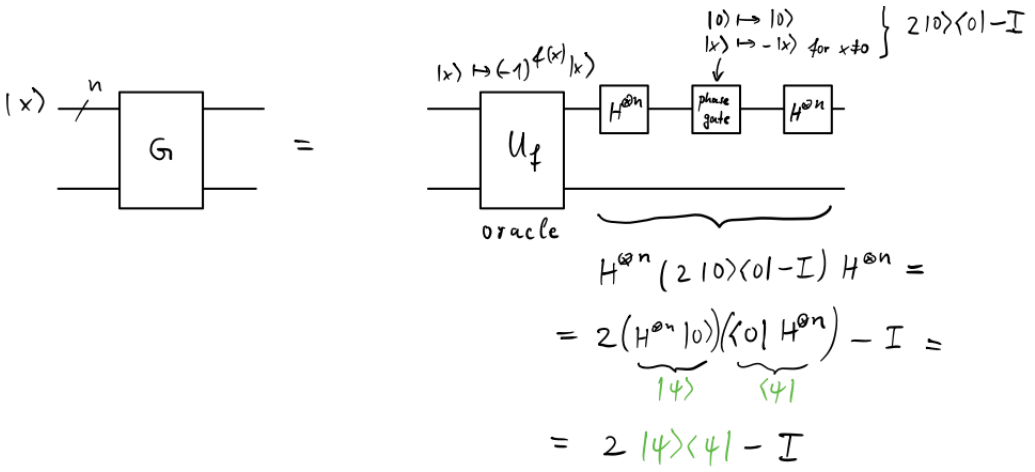
$$H^{\otimes n}|x_1, ..., x_n\rangle = \underbrace{(H|x_1\rangle)}_{\frac{1}{\sqrt{2}}\sum_{z_1=0}^{1}(-1)^{x_1 z_1}|z_1\rangle} \otimes \cdots \otimes (H|x_n\rangle) \tag{61}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} \underbrace{|z\rangle}_{\text{bit string}} \tag{62}$$

In particular:

$$H^{\otimes n}|0, ..., 0\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N} |z\rangle =: |\psi\rangle \text{ equal superposition state} \tag{63}$$

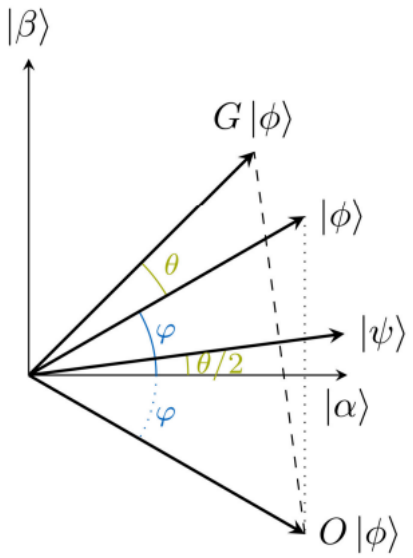
Definition of Grover operator G:



In summary

$$G := (2|\psi\rangle\langle\psi| - I)U_f \tag{64}$$

Geometric interpretation:



Define

$$|\alpha\rangle := \frac{1}{\sqrt{N-M}} \sum_{x=0, f(x)=0}^{N} |x\rangle \tag{65}$$

$$|\beta\rangle := \frac{1}{\sqrt{M}} \sum_{x=0, f(x)=1}^{N} |x\rangle \tag{66}$$

Angle ϑ defined by $\sin\frac{\vartheta}{2} = \sqrt{\frac{N}{M}}$ such that $|\psi\rangle = \cos\frac{\vartheta}{2}|\alpha\rangle + \sin\frac{\vartheta}{2}|\beta\rangle$

Note: By definition $U_f|a\rangle = \alpha$, $U_f|\beta\rangle = -|\beta\rangle \rightsquigarrow U_f$ is a reflection about $|\alpha\rangle$ within subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$

Likewise $2|\psi\rangle\langle\psi| - I$ is a reflection about $|\psi\rangle$:

Since $|\psi\rangle$ is part of subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$, G leaves subspace invariant!
Thus G is a product of two reflections $\rightsquigarrow G$ is a rotation by angle ϑ

$$|\phi\rangle = \cos\varphi|\alpha\rangle + \cos\varphi|\beta\rangle \tag{67}$$

$$\rightsquigarrow G|\phi\rangle = \cos(\varphi+\vartheta)|\alpha\rangle + \cos(\varphi+\vartheta)|\beta\rangle \tag{68}$$

For k applicants of G:

$$G^k|\phi\rangle = \cos(\phi + k \cdot \vartheta)|\alpha\rangle + \sin(\phi + k \cdot \vartheta)|\beta\rangle \tag{69}$$

For initial state $|\psi\rangle$: $\psi = \frac{\vartheta}{2}$

$$G^k|\phi\rangle = \cos((k + \frac{1}{2})\vartheta)|\alpha\rangle + \sin((k + \frac{1}{2})\vartheta)|\beta\rangle \tag{70}$$

Goal: Rotate to $|\beta\rangle$, i.e. $(k + \frac{1}{2})\vartheta \stackrel{!}{=} \frac{\pi}{2}$
since $\sin\frac{\vartheta}{2} = \sqrt{\frac{M}{N}}$ for $M \ll N \quad \vartheta \approx 2\sqrt{\frac{M}{N}}$
Thus need $\mathcal{O}(\sqrt{\frac{M}{N}})$ rotations ($k \cdot \vartheta$ should be $\mathcal{O}(1), k \approx \frac{1}{\vartheta}$).
Final step: standard measurement will collapse quantum state (with high probability) to a basis state forming $|\beta\rangle$, i.e. a solution!

3.3 Optimality of the search algorithm

Goal: Show that any quantum search algorithm needs $\Omega(\sqrt{N})$ oracle calls $\rightsquigarrow \mathcal{O}(\sqrt{N})$ is already optimal.
For simplicity: Single solution x Recall that oracle flips sign of solutions: $O_x = I - 2|x\rangle\langle x| \quad$ (denoted U_f in previous section)
Most general form of algorithm: Oracle calls interleaved with unitary $U_1, U_2, ...$

State after k steps:

$$|\psi_k^\star\rangle = U_k O_x U_{k-1} O_x \cdots U_1 O_x |\psi_0\rangle \tag{71}$$

We also define

$$|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi_0\rangle \tag{72}$$

Strategy of proof: Upper bound of

$$D_k := \sum_{x=0}^{N-1} || \underbrace{|\psi_k^\star\rangle}_{\text{Case that } x \text{ is a solution}} - |\psi_k\rangle||^2 \tag{73}$$

D_k grows as $\mathcal{O}(k^2)$, but must be $\Omega(N)$ to distinguish between N alternatives.
First show that $D_k \leq 4k^2$ by induction:
$k = 0 \rightsquigarrow D_0 = 0$ ✓
$k \mapsto k + 1$:

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

Rest of proof in the official script on Moodle.
In summary: $\underbrace{D_k \leq 4 \cdot k^2 \quad \text{and} \quad D_k \geq c \cdot N}_{k \geq \sqrt{\frac{cN}{4}} \rightsquigarrow \text{Number of oracle evaluations}}$