# Fundamentals of Quantum Computing

## Geilo Winter School

Franz G. Fuchs

19. - 24. January 2020

# Dirac/”Bra-ket” notation

- common notation for quantum states i.e. vectors in a complex Hilbert spaces $V$
- $|\rangle$ denotes a vector in a vector space $V$
- $\langle|$ denotes a linear functional on $V$, i.e. is an element of $V^*$
- we can identify a vector with a linear functional, i.e. a ”ket” with a ”bra”, and vice versa
- $\langle|\rangle : V \times V \to \mathbb{C}$ denotes the inner product
- $|\rangle\langle| : V \times V \to V \otimes V$ denotes the outer product

# A quantum bit

**Postulate 1 [Nielsen and Chuang(2000), page 80]**

Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the **state space** of the system. The system is completely described by its state vector, which is a **unit vector** in the system's state space.

# A quantum bit

A quantum bit (qubit) is a quantum mechanical system with a two-dimensional state space. A state $|\Phi\rangle$ is a unit vector in $\mathbb{C}^2$. Given an orthonormal basis $|\varphi_0\rangle, |\varphi_1\rangle$, a qubit can be written as

$$|\Phi\rangle = a_0 |\varphi_0\rangle + a_1 |\varphi_1\rangle \text{, with } a_0, a_1 \in \mathbb{C} \text{ and } \langle\Phi|\Phi\rangle = |a_0|^2 + |a_1|^2 = 1. \quad (1)$$

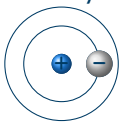
# A quantum bit

A quantum bit (qubit) is a quantum mechanical system with a two-dimensional state space. A state $|\Phi\rangle$ is a unit vector in $\mathbb{C}^2$. Given an orthonormal basis $|\varphi_0\rangle, |\varphi_1\rangle$, a qubit can be written as

$$|\Phi\rangle = a_0 |\varphi_0\rangle + a_1 |\varphi_1\rangle, \text{ with } a_0, a_1 \in \mathbb{C} \text{ and } \langle\Phi|\Phi\rangle = |a_0|^2 + |a_1|^2 = 1. \quad (1)$$

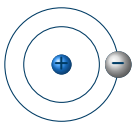
An example using states of hydrogen atoms

ground state



$$|\varphi_0\rangle = |0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

first excited state



$$|\varphi_1\rangle = |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

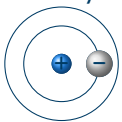
# A quantum bit

A quantum bit (qubit) is a quantum mechanical system with a two-dimensional state space. A state $|\Phi\rangle$ is a unit vector in $\mathbb{C}^2$. Given an orthonormal basis $|\varphi_0\rangle, |\varphi_1\rangle$, a qubit can be written as

$$|\Phi\rangle = a_0 |\varphi_0\rangle + a_1 |\varphi_1\rangle, \text{ with } a_0, a_1 \in \mathbb{C} \text{ and } \langle\Phi|\Phi\rangle = |a_0|^2 + |a_1|^2 = 1. \quad (1)$$

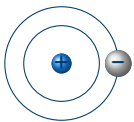
An example using states of hydrogen atoms

ground state



$$|\varphi_0\rangle = |0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

first excited state



$$|\varphi_1\rangle = |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Another example is photon polarization.

# A quantum bit

A quantum bit (qubit) is a quantum mechanical system with a two-dimensional state space. A state $|\Phi\rangle$ is a unit vector in $\mathbb{C}^2$. Given an orthonormal basis $|\varphi_0\rangle, |\varphi_1\rangle$, a qubit can be written as

$$|\Phi\rangle = a_0 |\varphi_0\rangle + a_1 |\varphi_1\rangle, \text{ with } a_0, a_1 \in \mathbb{C} \text{ and } \langle\Phi|\Phi\rangle = |a_0|^2 + |a_1|^2 = 1. \quad (1)$$

In contrast to classical mechanics, a **superposition** of basis states is possible. An example is the state $|\Phi\rangle = -\frac{1}{\sqrt{2}} |0\rangle + i\frac{1}{\sqrt{2}} |1\rangle$.

# Bloch sphere and superposition

The general state of a qubit can be written using polar representation

$$|\Phi\rangle = r_0 e^{i\theta_0} |0\rangle + r_1 e^{i\theta_1} |1\rangle . \tag{2}$$

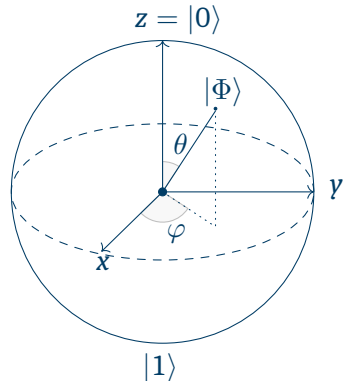
The global phase is irrelevant (for reasons explained later), we can multiply the state with $e^{-i\theta_0}$ and our (equivalent) state is

$$|\Phi\rangle = r_0 |0\rangle + r_1 e^{i\theta} |1\rangle , \quad \theta = \theta_1 - \theta_0. \tag{3}$$

Using that we have a unit vector, we can write

$$|\phi\rangle = \cos(\theta/2) |0\rangle + \sin(\theta/2) e^{i\phi} |1\rangle , \tag{4}$$

where $0 \leq \theta \leq \pi$, and $0 \leq \phi < 2\pi$.






SINTEF

# Multiple qubits

**Postulate 4 [Nielsen and Chuang(2000), page 94]**

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through $n$, and system number $i$ is prepared in the state $|\Phi_i\rangle$, then the joint state of the total system is $|\Phi_1\rangle \otimes |\Phi_2\rangle \otimes \cdots \otimes |\Phi_n\rangle$.

# Reminder: Tensor product

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix} \tag{5}$$

$$\begin{aligned} \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \otimes \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} &= \begin{pmatrix} a_{1,1} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} & a_{1,2} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} \\ a_{2,1} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} & a_{2,2} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} \\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} \end{pmatrix}. \end{aligned} \tag{6}$$

# Multiple qubits

The general state $|\Phi\rangle$ of $n$ qubits is a unit vector in $(\mathbb{C}^2)^{\otimes n} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{\text{n times}}$.

# Multiple qubits

The general state $|\Phi\rangle$ of $n$ qubits is a unit vector in $(\mathbb{C}^2)^{\otimes n} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{\text{n times}}$.

Using the standard basis for $\mathbb{C}^2$, a basis for $(\mathbb{C}^2)^{\otimes n}$ is given by the following $2^n$ vectors

$$
\begin{aligned}
|0\rangle_n &:= |\underbrace{00\ldots00}_{\text{n digits}}\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle = \begin{pmatrix}1,0 & \ldots & 0,0\end{pmatrix}^\mathsf{T} \\
|1\rangle_n &:= |\underbrace{00\ldots01}_{\text{n digits}}\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix}0,1 & \ldots & 0,0\end{pmatrix}^\mathsf{T} \\
&\vdots \\
|2^n-1\rangle_n &:= |\underbrace{11\ldots11}_{\text{n digits}}\rangle = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle = \begin{pmatrix}0,0 & \ldots & 0,1\end{pmatrix}^\mathsf{T}
\end{aligned}
\tag{7}
$$

# Multiple qubits

A general state can therefore be expressed as

$$|\Phi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2^n-2} \\ c_{2^n-1} \end{pmatrix}, \quad \sum_{i=0}^{2^n-1} |c_i|^2 = 1, \quad c_i \in \mathbb{C}. \tag{8}$$

# Multiple qubits

A general state can therefore be expressed as

$$|\Phi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2^n-2} \\ c_{2^n-1} \end{pmatrix}, \quad \sum_{i=0}^{2^n-1} |c_i|^2 = 1, \quad c_i \in \mathbb{C}. \tag{8}$$

Remark.

- The space $(\mathbb{C}^2)^{\otimes n}$ is a $2^n$-dimensional space. The dimension grows exponentially with the number of qubits.
- The state space of n classical bits, i.e., a binary string $\{0,1\}^n$ is an n-dimensional space. The dimension grows linearly with the number of bits.

# Product states and entanglement

A quantum state $|\Phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a **product state** if it can be expressed as a tensor product of $n$ single qubits $|\Phi_i\rangle$, i.e.,

$$|\Phi\rangle = \underbrace{\Phi_1 \otimes \cdots \otimes \Phi_n}_{\text{n times}} \tag{9}$$

Otherwise, it is **entangled**.

# Product states and entanglement

A quantum state $|\Phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a **product state** if it can be expressed as a tensor product of $n$ single qubits $|\Phi_i\rangle$, i.e.,

$$|\Phi\rangle = \underbrace{\Phi_1 \otimes \cdots \otimes \Phi_n}_{\text{n times}} \tag{9}$$

Otherwise, it is **entangled**.

Examples.

- Product state: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Entangled state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

# Important states and conventions

- Two-qubit Bell states

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

  (They form a maximally entangled basis, known as the Bell basis, of the four-dimensional Hilbert space for two qubits.)
- Superposition states

  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Sometimes one writes $|\Phi_1\rangle\,|\Phi_2\rangle$, which is short hand for $|\Phi_1\rangle \otimes |\Phi_2\rangle$.

# Quantum evolution

**Postulate 2 [Nielsen and Chuang(2000), page 81]**

The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\Phi\rangle$ of the system at time $t1$ is related to the state $|\Phi'\rangle$ of the system at time $t2$ by a **unitary operator** $U$ which depends only on the times $t1$ and $t2$,

$$|\Phi'\rangle = U|\Phi\rangle \tag{10}$$

# Operations on qubits

An operation applied by a quantum computer, which is also called a **gate**, to $n$ qubits is a **unitary matrix** $\mathbb{C}^{2^n \times 2^n}$.

- A matrix is U unitary, if $U^\dagger U = UU^\dagger = I$.
- Unitary matrices are norm-preserving, i.e., $\| U |\Phi\rangle \| = \| |\Phi\rangle \|$. This means that we get back a quantum state, which is a unit vector.
- Quantum operations are linear.
- Quantum operations are reversible.

# Operations on qubits

An operation applied by a quantum computer, which is also called a **gate**, to $n$ qubits is a **unitary matrix** $\mathbb{C}^{2^n \times 2^n}$.

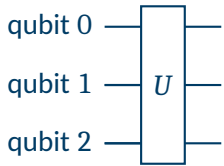
- A matrix is U unitary, if $U^\dagger U = UU^\dagger = I$.
- Unitary matrices are norm-preserving, i.e., $\| U \left|\Phi\right\rangle \| = \| \left|\Phi\right\rangle \|$. This means that we get back a quantum state, which is a unit vector.
- Quantum operations are linear.
- Quantum operations are reversible.

This seems restrictive at first, but:

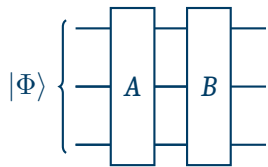
- A universal quantum computer is Turing-complete [Deutsch(1985)].
- All computations (including classical computations) can be madereversible [Bennett(1973)].

# Notation for quantum circuits

**Wires** represent qubits and **gates** are operations:

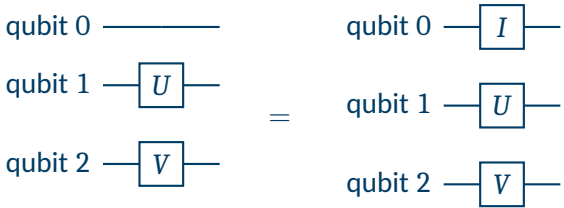



**Serially wired gates**. The state $BA\,|\Phi\rangle$ is represented as:



# Notation for quantum circuits

**Parallel gates**:

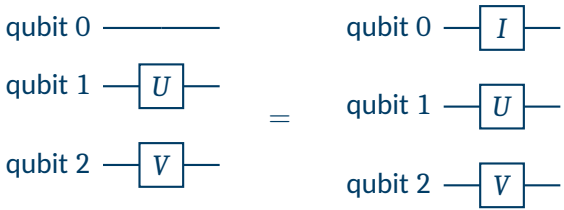





SINTEF

# Notation for quantum circuits

**Parallel gates**:

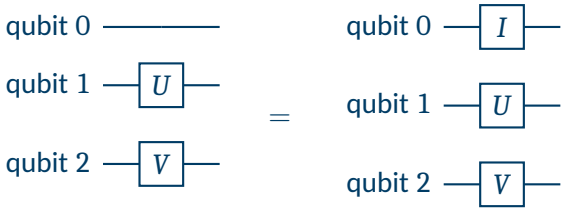



- If we have a product state $|\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle$ then we have

$$(I \otimes U \otimes V)\,|\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_0\rangle \otimes U\,|\psi_1\rangle \otimes V\,|\psi_2\rangle \tag{11}$$

# Notation for quantum circuits

**Parallel gates**:




- If we have a product state $|\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle$ then we have

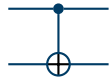
$$(I \otimes U \otimes V)\,|\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_0\rangle \otimes U\,|\psi_1\rangle \otimes V\,|\psi_2\rangle \tag{11}$$

- But for a general (entangled) state $|\Psi\rangle$ the action of $I \otimes U \otimes V$ cannot be determined in such a simple way. We need to explicitly calculate the effect of the $2^n \times 2^n$ matrix on the state $|\Psi\rangle$. This is essentially the reason why we in general need exponential amounts of memory (or time) to keep track of the full state in $2^n$-dimensional complex space.

# Examples of 1 qubit gates

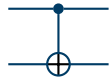
- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. We have that
  $H^2 = I, H|0\rangle = |+\rangle, H|1\rangle = |-\rangle, H|+\rangle = |0\rangle, H|-\rangle = |1\rangle.$
- Pauli gates $X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. We have that
  $X^2 = I, X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, X|+\rangle = |+\rangle, X|-\rangle = -|-\rangle.$
- Pauli gates $Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. We have that $Y^2 = I, Y|0\rangle = i|1\rangle, Y|1\rangle = -i|0\rangle.$
- Pauli gates $Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We have that $Z^2 = I, Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle.$
- Phase shift gates $R_\Phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix}$.
- Square root of NOT gate $\sqrt{X} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+1 \end{pmatrix}$. We have that $\sqrt{X}\sqrt{X} = X$.
- ...

# Examples of 2 qubit gates

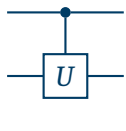
- controlled not gate $CNOT = CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$ 

  It has the effect
  $CNOT\,|00\rangle = |00\rangle\,, CNOT\,|01\rangle = |01\rangle\,, CNOT\,|10\rangle = |11\rangle\,, CNOT\,|11\rangle = |10\rangle.$

# Examples of 2 qubit gates

- controlled not gate $CNOT = CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$ 

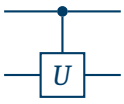
  It has the effect
  $CNOT\,|00\rangle = |00\rangle\,, CNOT\,|01\rangle = |01\rangle\,, CNOT\,|10\rangle = |11\rangle\,, CNOT\,|11\rangle = |10\rangle.$

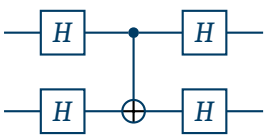
- controlled $U$ gate $CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix} =$ 

# Examples of 2 qubit gates

- controlled not gate $CNOT = CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$ 

  It has the effect
  $CNOT\,|00\rangle = |00\rangle\,, CNOT\,|01\rangle = |01\rangle\,, CNOT\,|10\rangle = |11\rangle\,, CNOT\,|11\rangle = |10\rangle.$

- controlled $U$ gate $CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix} =$ 


- Note that  $=$ 

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

# Universal quantum gate sets

A set $G$ of quantum gates universal if one can approximate any unitary transformation on any number of qubits with gates from $G$ to any desired precision $\varepsilon$, i.e. there is a sequence of gates $g_1, \ldots g_k \in G$, such that

$$\|U - U_k \ldots U_2 U_1\| \leq \varepsilon. \tag{12}$$

- The operator norm is defined by $\|U - U'\| = \max_{|v\rangle, with \||v\rangle\|=1} \| (U - U') |v\rangle \|$.
- $U_i$ is the unitary matrix for which gate $g_i$ is acting on $m$ qubits.

# Universal quantum gate sets

A set $G$ of quantum gates universal if one can approximate any unitary transformation on any number of qubits with gates from $G$ to any desired precision $\varepsilon$, i.e. there is a sequence of gates $g_1, \ldots g_k \in G$, such that

$$\|U - U_k \ldots U_2 U_1\| \leq \varepsilon. \tag{12}$$

- The operator norm is defined by $\|U - U'\| = \max_{|v\rangle, with \||v\rangle\|=1} \| (U - U') |v\rangle \|$.
- $U_i$ is the unitary matrix for which gate $g_i$ is acting on $m$ qubits.

Examples of universal gate sets:

- $G = \{CNOT, H, S = R_{\pi/2}, T = R_{\pi/4}\}$
- $G = \{CNOT, U(\theta, \phi, \lambda)\}$, where $U(\theta, \phi, \lambda) = \begin{pmatrix} e^{-i(\phi+\lambda)/2}\cos(\theta/2) & -e^{-i(\phi-\lambda)/2}\sin(\theta/2) \\ e^{i(\phi-\lambda)/2}\sin(\theta/2) & e^{i(\phi+\lambda)/2}\sin(\theta/2) \end{pmatrix}$

# Solovay-Kitaev theorem

Let $G$ be a universal gate set that is closed under inverses (i.e. if $g \in G$ then $g^{-1} \in G$) for $SU(n)$ and $\varepsilon > 0$ a desired accuracy. Then there is a constant $c$ such that for any $U \in SU(n)$ there exits a finite sequence $S$ of gates from $G$ of length $\mathcal{O}(log^c(1/\varepsilon))$ such that $d(U, S) < \varepsilon$.

This SK algorithm provides a proof of the theorem and an algorithm to find the sequence $S$ efficiently on a classical computer with running time $\mathcal{O}(log^{2.71}(1/\varepsilon))$.

# Computational complexity

For an efficient algorithm we require that the circuit contains polynomially many gates in the number of qubits $n$ and each gate has a compact representation in the universal gate set provided by the quantum computer.

# Gottesman-Knill theorem

**Beware!** A quantum circuit using only the following elements can be simulated efficiently on a classical computer:

- Preparation of qubits in computational basis states,
- Quantum gates from the Clifford group (Hadamard gates, controlled NOT gates, Phase Gate), and
- Measurements in the computational basis.

# How do we obtain information?

# How do we obtain information?

**Postulate 3 [Nielsen and Chuang(2000), page 84]**

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. [..]If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result $m$ occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{13}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{|M_m|\psi\rangle|} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{14}$$

The measurement operators satisfy the completeness equation $\sum_m M_m^\dagger M_m = I$.

# Measurement

- The completeness equation expresses the fact that probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1 \tag{15}$$

# Measurement

- The completeness equation expresses the fact that probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1 \tag{15}$$

- An important example is "measurement of a qubit in the **computational basis**": $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Notice $M_i^\dagger = M_i$, and $M_i M_i = M_i$ for $i \in \{0, 1\}$. Given a state $|\psi\rangle = a|0\rangle + b|1\rangle$, we have that
  - $p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \overline{a}\langle 0|0\rangle\langle 0|0\rangle a = |a|^2$, and the state after measurement is $M_0|\psi\rangle/|a| = a/|a||0\rangle = e^{i\theta_a}|0\rangle$.
  - $p(1) = |b|^2$ and the resulting state is $b/|b||1\rangle = e^{i\theta_b}|1\rangle$
- Measurement w.r.t. to the $|\pm\rangle$ basis.

  $\widetilde{M}_0 = 1/\sqrt{2}\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}, \widetilde{M}_1 = 1/\sqrt{2}\begin{pmatrix}0 & 0\\ 1 & -1\end{pmatrix}$
  - $p(0) = 1/2(\overline{a}+\overline{b})(a+b)$, and the state after measurement is $\frac{a+b}{\sqrt{2p(0)}}|0\rangle$.
  - $p(1) = 1/2(\overline{a}-\overline{b})(a-b)$ and the resulting state is $\frac{a-b}{\sqrt{2p(1)}}|1\rangle$

# Measurement

- Let's say we want to measure a state $|\psi\rangle$ in the basis given by a set of orthonormal vectors $u_i$.
- However, we can only "physically" measure in the computational basis $P_i = |i\rangle \langle i|$.

# Measurement

- Let's say we want to measure a state $|\psi\rangle$ in the basis given by a set of orthonormal vectors $u_i$.
- However, we can only "physically" measure in the computational basis $P_i = |i\rangle\langle i|$.

Idea: Apply basis change to computational basis before measurement.
The way to achieve this is to construct the unitary matrix $U$, where the columns consist of the vectors $u_i$ and apply the inverse of $U$ before measurement.

$$p_U(m) = \langle\psi|UP_m^\dagger P_m U^\dagger|\psi\rangle = \left\langle\psi'\middle|P_m^\dagger P_m\middle|\psi'\right\rangle, \quad \text{with } \left|\psi'\right\rangle = U^\dagger\left|\psi\right\rangle. \tag{16}$$

# Measurement

- Let's say we want to measure a state $|\psi\rangle$ in the basis given by a set of orthonormal vectors $u_i$.
- However, we can only "physically" measure in the computational basis $P_i = |i\rangle\langle i|$.

Idea: Apply basis change to computational basis before measurement.
The way to achieve this is to construct the unitary matrix $U$, where the columns consist of the vectors $u_i$ and apply the inverse of $U$ before measurement.

$$p_U(m) = \langle\psi|UP_m^\dagger P_m U^\dagger|\psi\rangle = \left\langle\psi'\middle|P_m^\dagger P_m\middle|\psi'\right\rangle, \quad \text{with } \left|\psi'\right\rangle = U^\dagger|\psi\rangle. \tag{16}$$

This is how we ended up with the matrices $\widetilde{M_0}, \widetilde{M_1}$ on the previous slide.

# Measurement

- A word of caution: It is wrong to think of a quantum state as a probability distribution.
- Coefficients are complex numbers unrestricted in sign, but probabilities are real, positive numbers.
- A quantum state **induces** a probability distribution through measurement.

# Measurement

- A word of caution: It is wrong to think of a quantum state as a probability distribution.
- Coefficients are complex numbers unrestricted in sign, but probabilities are real, positive numbers.
- A quantum state **induces** a probability distribution through measurement.
- Measurement is **irreversible**.

# Measurement

- A word of caution: It is wrong to think of a quantum state as a probability distribution.
- Coefficients are complex numbers unrestricted in sign, but probabilities are real, positive numbers.
- A quantum state **induces** a probability distribution through measurement.
- Measurement is **irreversible**.
- Global phase: Consider $|\phi\rangle = e^{-i\theta}|\psi\rangle$. Then we have

$$p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle = e^{i\theta}\langle\psi|M_m^\dagger M_m e^{-i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{17}$$

# Expectation value of an observable

Given a state $|\phi\rangle$ and an observable $A$, the expectation value of $A$ in the state $\phi$ is given by

$$\langle A \rangle_\phi := \langle \phi | A | \phi \rangle = \sum_i \lambda_i |\langle \phi | \psi_i \rangle|^2 . \tag{18}$$

Here, A is a self-adjoint operator on the Hilbert space $\mathbb{C}^{\otimes n}$, and $\{\lambda_i, |\psi_i\rangle\}$ is the set of eigenvalues and eigenvectors of $A$.

# No-cloning principle

Let $|\phi\rangle$ be an arbitrary quantum state on $n$ qubits.
$\nexists$ a unitary matrix that maps $|\phi\rangle \otimes |0\rangle$ to $|\phi\rangle \otimes |\phi\rangle$.

# No-cloning principle

Let $|\phi\rangle$ be an arbitrary quantum state on $n$ qubits.
$\nexists$ a unitary matrix that maps $|\phi\rangle \otimes |0\rangle$ to $|\phi\rangle \otimes |\phi\rangle$.

Proof.
Suppose there exists such a $U$. Then we have

$$\begin{aligned} U|\phi_1\rangle \otimes |0\rangle &= |\phi_1\rangle \otimes |\phi_1\rangle \\ U|\phi_2\rangle \otimes |0\rangle &= |\phi_2\rangle \otimes |\phi_2\rangle \end{aligned} \tag{19}$$

It follows that

$$\begin{aligned} \langle\phi_1|\phi_2\rangle &= \langle\phi_1|\phi_2\rangle \langle 0|0\rangle = (\langle\phi_1| \otimes \langle 0|)(|\phi_2\rangle \otimes |0\rangle) \\ &= (\langle\phi_1| \otimes \langle 0|)U^\dagger U(|\phi_2\rangle \otimes |0\rangle) = (\langle\phi_1| \otimes \langle\phi_1|)(|\phi_2\rangle \otimes |\phi_2\rangle) = \langle\phi_1|\phi_2\rangle^2 \end{aligned} \tag{20}$$

This is only true if $\langle\phi_1|\phi_2\rangle$ is 0 or 1. So $|\phi_1\rangle$, $|\phi_2\rangle$ are not general states.


Technology for a better society

Charles H Bennett.
Logical reversibility of computation.
*IBM journal of Research and Development*, 17(6):525–532, 1973.

David Deutsch.
Quantum theory, the church–turing principle and the universal quantum computer.
*Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

M.A. Nielsen and I.L. Chuang.
*Quantum Computation and Quantum Information*.
Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.