Introduction to Quantum Computing

Paolo Cremonesi

POLITECNICO
MILANO 1863

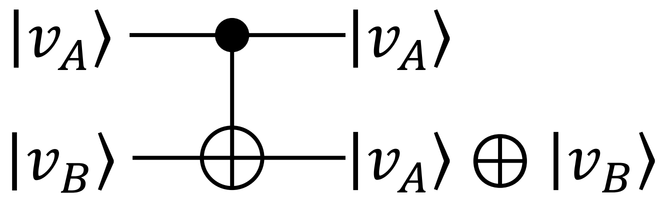
Multiple-Qubits Gates

Multiple-Qubits Gates

- There are quantum gates which apply **only to multiple qubits**

- In this course will see only few of them:
  - CNOT
  - SWAP
  - CCNOT (Toffoli gate)
  - …

Controlled NOT (CNOT)



($\oplus$ is the XOR operator)
NB: this notation is valid only for basis states $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$

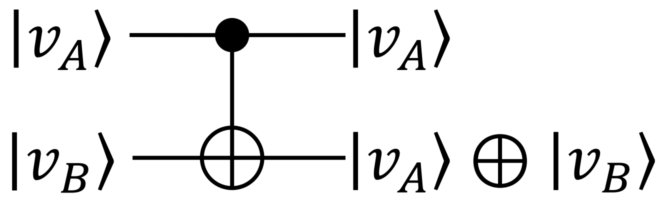
- CNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- If the control qubit $|v_A\rangle$ is $|\mathbf{1}\rangle$, then the target qubit $|v_B\rangle$ is flipped
  - as with gate X
- If we apply the CNOT gate to $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$

$$|v_A v_B\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|\mathbf{1}0\rangle + a_1 b_1|\mathbf{1}1\rangle$$

  we invert the last two amplitudes

- $\mathrm{CNOT}|v_A v_B\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 \mathbf{b_0} \\ a_1 \mathbf{b_1} \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 \mathbf{b_1} \\ a_1 \mathbf{b_0} \end{bmatrix}$

Controlled NOT (CNOT)



($\oplus$ is the XOR operator)
NB: this notation is valid only for basis states $|0\rangle$ or $|1\rangle$

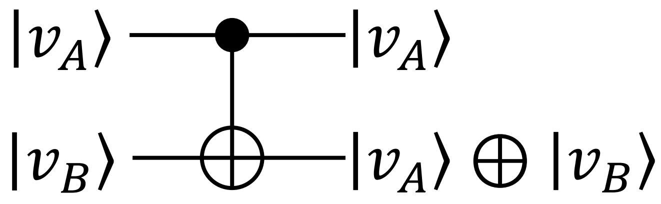
- CNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- If the control qubit $|v_A\rangle$ is $|1\rangle$, then the target qubit $|v_B\rangle$ is flipped
  - as with gate X
- **More in general**, if we apply the CNOT gate to

$$|v_C\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

  we invert the last two amplitudes c_2 and c_3

- $\mathrm{CNOT}|v_C\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{bmatrix}$

Controlled NOT (CNOT)



($\oplus$ is the XOR operator)

NB: this notation is valid only for basis states $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$

- CNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- If the control qubit $|v_A\rangle$ is $|\mathbf{1}\rangle$, then the target qubit $|v_B\rangle$ is flipped
  - as with gate X
- Example
  - $|v_0 v_1\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|10\rangle$
  - $\mathrm{CNOT}|v_A v_B\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{3}}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$

Generic Controlled Gate

- Controlled $C_U = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$
- If control qubit $|v_A\rangle$ is $|1\rangle$, then target gate U is applied to qubit $|v_B\rangle$
- Apply the generic controlled gate C_U to
  - $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$
  - $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$
- and obtain

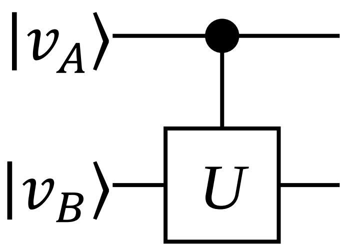
$$C_U|v_A v_B\rangle = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

- If $|v_A\rangle = |0\rangle$ ($a_0 = 1$ and $a_1 = 0$)

$$C_U|0 v_B\rangle = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ 0 \\ 0 \end{bmatrix}$$

- If $|v_A\rangle = |1\rangle$ ($a_0 = 0$ and $a_1 = 1$)

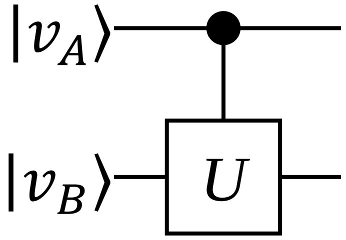
$$C_U|1 v_B\rangle = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ U|v_B\rangle \end{bmatrix}$$

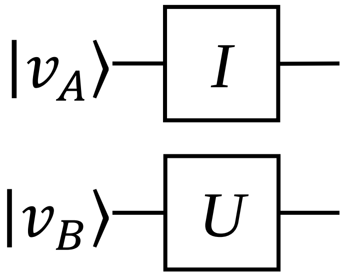


Generic Controlled Gate: important

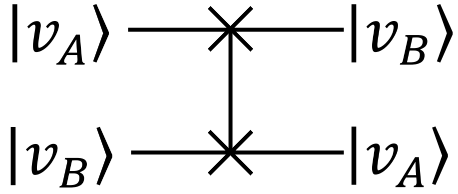
- Important:

$$\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \text{ is } \textbf{not equivalent} \text{ to } I \otimes U$$



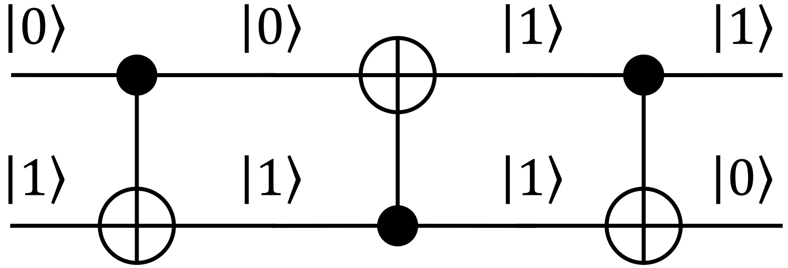


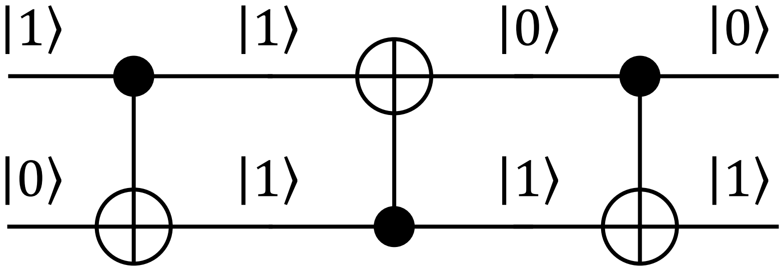
Multiple-Qubits Gates: SWAP

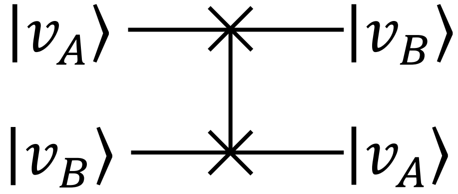


- $\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
- How it works? The state of $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$ is described with their tensor product
  - $|v_A v_B\rangle = a_0 b_0|00\rangle + \boldsymbol{a_0 b_1}|01\rangle + \boldsymbol{a_1 b_0}|10\rangle + a_1 b_1|11\rangle$
- If we apply the SWAP gate
  - $\mathrm{SWAP}|v_A v_B\rangle \; = a_0 b_0|00\rangle + \boldsymbol{a_1 b_0}|01\rangle + \boldsymbol{a_0 b_1}|10\rangle + a_1 b_1|11\rangle$
- which is identical to the tensor product $|v_B v_A\rangle$
  - $|v_B v_A\rangle = b_0 a_0|00\rangle + b_0 a_1|01\rangle + b_1 a_0|10\rangle + b_1 a_1|11\rangle$

Multiple-Qubits Gates: SWAP as CNOT^3

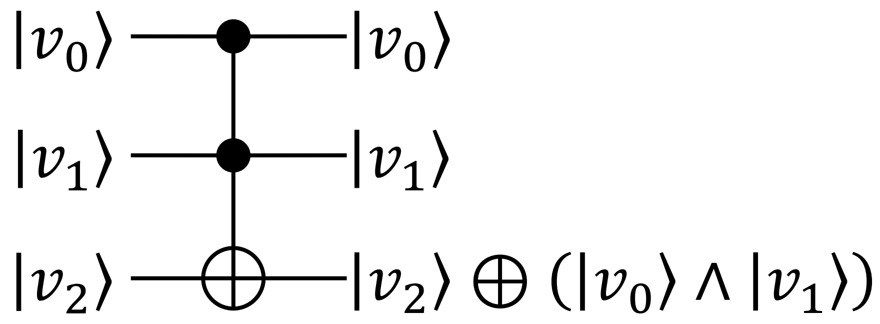






Multiple-Qubits Gates: CCNOT (or Toffoli)

- $\mathrm{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$



- CNOT gate with 2 control bits instead of 1
  - target qubit $|v_2\rangle$ is inverted when **both control qubits are 1**

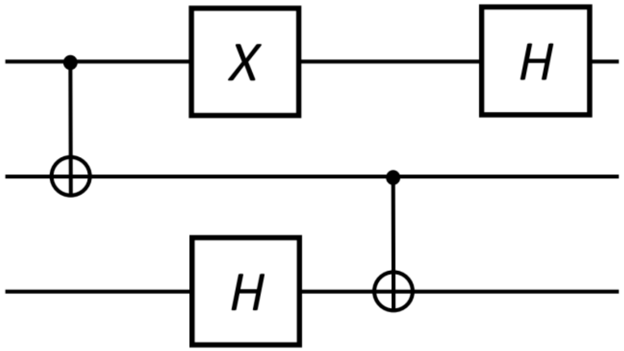
Universal quantum gates

- **Finite** set of gates that can **approximate** any quantum circuit
  - any other unitary operation
- Two-qubit gates are universal
  - any arbitrary *n*-qubit operation can be decomposed as a product of two-qubit gates
- Many possible choices
  - Toffoli + Hadamard
  - …

Quantum Circuit

- We can express a quantum circuit as one matrix
  - we must follow three rules:
  - composition across wires is achieved by **tensor product**
  - composition along (sets of) wires is achieved by matrix product, but **right to left**
  - composition across wires requires to use the identity matrix for qubits without gates

- Example



- $(H \otimes I \otimes I) \cdot (I \otimes CNOT) \cdot (X \otimes I \otimes H) \cdot (CNOT \otimes I)$

Entanglement

- It takes 2^n real numbers to describe the state of *n*-qubits
  - why?
    - the state of *n*-qubits are described by their tensor product
    - this leads to 2^n complex coefficients, equivalent to 2^{n+1} real coefficients
    - one real degree of freedom is removed by the normalization
    - one real degree of freedom is removed because the global phase is meaningless
- It takes $2n$ real numbers to describe n qubits (2 real numbers per qubit)
- $2^n \gg 2n \rightarrow$ most n-qubit states are not described in terms of n separate qubits
  - multiple-qubits states that cannot be written as the tensor product of *n* single-qubits are called **entangled states**
  - states that can be written as a tensor product from the constituent subsystems are called **separable states**

Entanglement example

- The elements of the **Bell states** are entangled
- For instance, the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be described in terms of the state of each of its component qubits separately
- If we have two qubits $v_A = a_0|0\rangle + a_1|1\rangle$ and $v_B = b_0|0\rangle + b_1|1\rangle$
- It is impossible to find a_0, b_0, a_1, b_1, such that

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

  - since

$$(a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle$$

  - and $a_0 b_1 = 0$ implies that either $a_0 b_0 = 0$ or $a_1 b_1 = 0$, none of which is true

Entanglement

- Entanglement is **not basis dependent**
  - the notion of superposition is basis-dependent

- Entanglement is not an absolute property of a quantum state
  - depends on the particular decomposition of the system into subsystems under consideration
  - states entangled with respect to one decomposition may be unentangled with respect to other decompositions
  - when we say that a state is **entangled,** we mean that it is entangled with respect to his decomposition **into individual qubits**

Entangling gates

- Not all two-qubit gates can be written as the tensor product of single-qubit gates
  - a generic 2-qubits gate has 16 complex values
  - two single-qubit gates have 4 + 4 = 8 total complex values

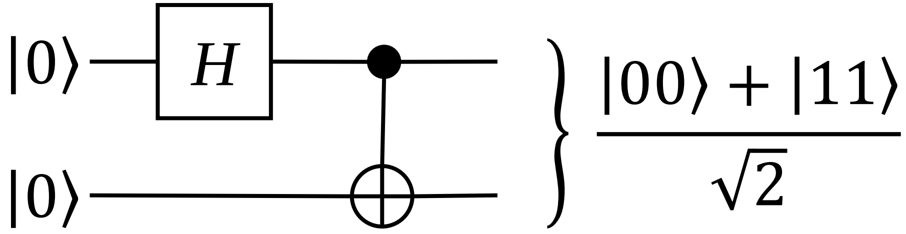
- Such a gate is called an **entangling gate**

- One example of an entangling gate is the CNOT gate

Bell states

- Four specific two-qubit states are designated as **Bell states**
  - maximally entangled two-qubit states
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

- Bell states can be created with the following circuit

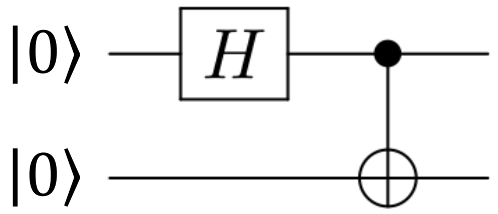


- For the four basic two-qubit inputs, $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, the circuit creates the four Bell states

Entanglement

- If we have a set of N qubits that are entangled and wish to apply a quantum gate on $M < N$ qubits in the set, we will have to extend the gate to take N qubits. This application can be done by combining the gate with an identity matrix such that their tensor product becomes a gate that act on N qubits
  - it is difficult to simulate large entangled quantum systems using classical computers
    - the state vector of a quantum register with *n* qubits is 2^n complex entries
- Bell states are of fundamental importance to quantum computing
  - Bell states are maximally entangled in the sense that, when looked at separately, the state of each qubit is as uncertain as possible
- Unentangled states are the least entangled states possible in the sense that, when looked at separately, the state of each qubit is as certain as possible

Bell states: how to create (example)



$$\Big(\mathrm{CNOT}\cdot(H\otimes I)\Big)\big|(|v_0\rangle\otimes|v_1\rangle)\big\rangle$$

- $H\otimes I = \frac{1}{\sqrt{2}}\begin{bmatrix}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} & \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\\ \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} & -\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{bmatrix}$
- $\mathrm{CNOT}(H\otimes I) = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\0 & 1 & 0 & -1\\1 & 0 & -1 & 0\end{bmatrix}$
- $\big(\mathrm{CNOT}(H\otimes I)\big)|00\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\0 & 1 & 0 & -1\\1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}$

this operator creates
a Bell state

Exercises: Bell states in Hadamard basis

- Show that the Bell state

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- has the same form when expresses in Hadamard basis

$$|\Phi^+\rangle = \frac{|+\,+\rangle + |-\,-\rangle}{\sqrt{2}}$$

- (and the same holds for the other Bell states)

Exercises: Bell states in Hadamard basis

- Hadamard basis are defined as

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

- We need invert the definitions, to express the computational basis in terms Hadamard basis

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

- Substitute these expressions into $|00\rangle$ and $|11\rangle$

$$|00\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle + |-\rangle}{\sqrt{2}} = \frac{|+\,+\rangle + |+\,-\rangle + |-\,+\rangle + |-\,-\rangle}{2}$$

$$|11\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{|+\,+\rangle - |+\,-\rangle - |-\,+\rangle + |-\,-\rangle}{2}$$

- Substitute these expressions into the definition of $|\Phi^+\rangle$ and obtain

$$|\Phi^+\rangle = \frac{|+\,+\rangle + |-\,-\rangle}{\sqrt{2}}$$

Multi qubits measurement

- What happens when measuring one qubit in a two-qubits system?

$$|v_C\rangle = |v_A v_B\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

- The state of the system can be always described as

$$|v\rangle = c_{01}|0\rangle \otimes \frac{c_0|0\rangle + c_1|1\rangle}{c_{01}} + c_{23}|1\rangle \otimes \frac{c_2|0\rangle + c_3|1\rangle}{c_{23}}$$

- with $c_{01} = \sqrt{c_0^2 + c_1^2}$ and $c_{23} = \sqrt{c_2^2 + c_3^2}$
- If qubit $|v_A\rangle$ is measured as $|0\rangle$ then $c_2 = 0$ and $c_3 = 0$
- The state of qubit $|v_B\rangle$ becomes

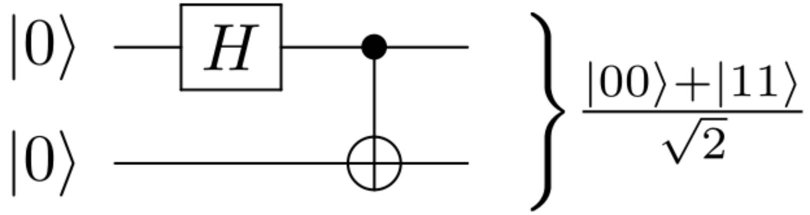
$$|v_B\rangle = \frac{c_0|0\rangle + c_1|1\rangle}{c_{01}}$$

this is a valid qubit
(normalized to 1)

Multi qubits measurement: example

- What happens when measuring one qubit in a two-qubits system?

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



- The state of the system can be described as

$$|v\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$$

- If qubit A is measured as $|0\rangle$ the state of qubit B becomes $|v_B\rangle = |0\rangle$
- If qubit A is measured as $|1\rangle$ the state of qubit B becomes $|v_B\rangle = |1\rangle$

The measurement of a bit determines the second qu-bit
This is weird, since the measurement affects only 1 qubit

Limits of Quantum Information

No-cloning principle: why it matters?

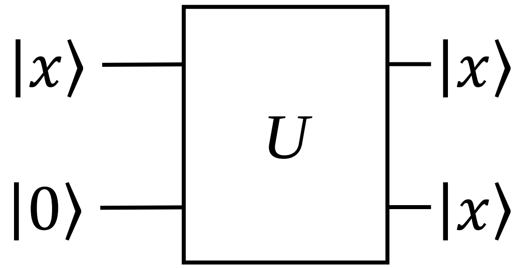
- Cloning violates quantum mechanic principles
  - no-signaling (instantaneous transfer of information)
  - put infinite amount of info inside a qubit
    - Map an arbitrarily long classical bit-string to a unique qubit state
    - Communicate the single qubit
    - Receive the qubit
    - Make an arbitrary number of copies by cloning
    - Perform **quantum state tomography** (which requires several copies of the qubit) to recover the original classical information.
- Makes quantum error correction harder

No-cloning principle: demonstration

- We have two qubits, one with state $|x\rangle$ the other with state $|0\rangle$
- We want to copy qubit $|x\rangle$ onto qubit $|0\rangle$
- We need to find a cloning gate U such that

$$U(|x\rangle|0\rangle) = |x\rangle|x\rangle$$

- If such gate exists, we can apply it to both qubits $|x\rangle$ and $|y\rangle$
  - $U(|x\rangle|0\rangle) = |x\rangle|x\rangle \qquad U(|y\rangle|0\rangle) = |y\rangle|y\rangle$
- Apply the inner product to both sides
  - left: $\langle 0|\langle x|U^H U|y\rangle|0\rangle = \langle 0|\langle x|y\rangle|0\rangle = \langle x|y\rangle\langle 0|0\rangle = \langle x|y\rangle$
  - right: $\langle x|\langle x|y\rangle|y\rangle = \langle x|y\rangle^2$
  - combined: $\langle x|y\rangle = \langle x|y\rangle^2$



- which is not true in general
  - only if $x = y$ (remember that for qubits $x^2 = y^2 = 1$) or if x and y are orthogonal ($\langle x|y\rangle = 0$)

No-cloning principle: CNOT apparent violation

- We apply CNOT gate to $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = |0\rangle$
- To compute the output, we use the notation

$$\mathrm{CNOT}|v_A\rangle|v_B\rangle = |v_A\rangle|v_A \oplus v_B\rangle$$

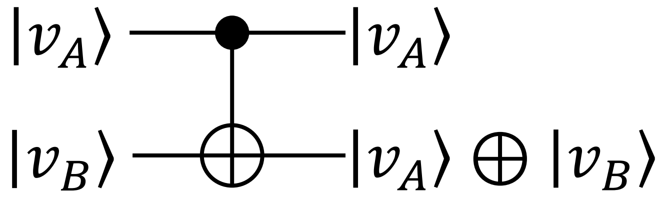
- Replacing $|v_B\rangle$ with $|0\rangle$ we obtain

$$\mathrm{CNOT}|v_A\rangle|0\rangle = |v_A\rangle|v_A \oplus 0\rangle = |v_A\rangle|v_A\rangle$$

- We have copied qubit $|v_A\rangle$ on qubit $|0\rangle$
- Where is the error?
- The **informal** notation

$$\mathrm{CNOT}|v_A\rangle|v_B\rangle = |v_A\rangle|v_A \oplus v_B\rangle$$

- can be used only when $|v_A\rangle$ and $|v_b\rangle$ are basis state
- It is **not valid** when $|v_A\rangle$ and $|v_b\rangle$ are in superposition



NB: this notation is valid only for basis states $|0\rangle$ or $|1\rangle$

No-cloning principle: CNOT apparent violation

- Different point of view …

- We apply CNOT gate to $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = |0\rangle$
- To compute the output, we first compute $|v_A\rangle|0\rangle$

$$|v_A\rangle|0\rangle = a_0|00\rangle + a_1|10\rangle$$

- Then, we apply the CNOT gate that flips $|10\rangle$ to $|11\rangle$

$$\mathrm{CNOT}|v_A\rangle|0\rangle = a_0|00\rangle + a_1|11\rangle$$

- If we wish to copy $|v_A\rangle$ onto $|0\rangle$, the output state would have been $|v_A\rangle|v_A\rangle$

$$a_0^2|00\rangle + a_0a_1|01\rangle + a_0a_1|10\rangle + a_1^2|11\rangle$$

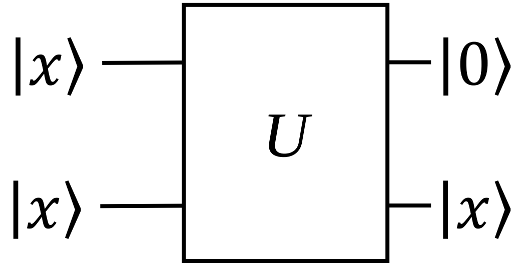
- The two output states are different
  - the first output is an entangled state (CNOT creates entanglement)
  - the second is a copy of two qubits

No-deleting principle

- **There does not exist a gate *U* that can delete one of two copies of a qubit**
- Demonstration similar to no-cloning
- We need to find a deleting gate *U* such that

$$U(|x\rangle|x\rangle) = |0\rangle|x\rangle$$

- If such gate exists, we can apply it to both qubits $|x\rangle$ and $|y\rangle$
  - $U(|x\rangle|x\rangle) = |0\rangle|x\rangle \qquad U(|y\rangle|y\rangle) = |0\rangle|y\rangle$
- Apply the inner product to both sides
  - left: $\langle x|\langle x|U^H U|y\rangle|y\rangle = \langle x|\langle x|y\rangle|x\rangle = \langle x|y\rangle\langle x|y\rangle = \langle x|y\rangle^2$
  - right: $\langle x|\langle 0|0\rangle|y\rangle = \langle x|y\rangle$
  - combined: $\langle x|y\rangle^2 = \langle x|y\rangle$
- which is not true in general (only if $x = y$ or if x and y are orthogonal)



No-signaling principle: the problem

- Alice and Bob are at different ends of the universe, but each have one qubit of a Bell pair $|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- Alice can measure her qubit $|a\rangle$ whenever she wants, and this will collapse Bob's qubit $|b\rangle$ to the same state
- **We are interested in whether Bob can infer whether Alice has measured her qubit or not**
- If he can, then Alice can transfer information to Bob instantaneously
- For example, Alice can measure her qubit $|a\rangle$ when some event occurs, thus signaling this information to Bob

Example of quantum correlation: Bell pair

- Suppose Alice and Bob each have one qubit of a Bell pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|+\,+\rangle + |-\,-\rangle}{\sqrt{2}}$$

- If Alice and Bob **both measure in the computational basis**
    - Alice measures first and obtains $|0\rangle$ or $|1\rangle$ with probability 50%
    - Bob's qubit instantaneously collapse to the same state measured by Alice, $|0\rangle$ or $|1\rangle$
    - Bob's measures second and obtains the same value measured by Alice with probability 100%
    - each observer's result is random individually, but if they compare results afterward, they will find perfect correlation in their measurements

Example of quantum correlation: Bell pair

- Suppose Alice and Bob each have one qubit of a Bell pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|+\,+\rangle + |-\,-\rangle}{\sqrt{2}}$$

- If Alice measure in the **Hadamard** basis and Bob in the **computational** basis
  - Alice measures first and obtains $|+\rangle$ or $|-\rangle$ with probability 50%

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

  - Bob’s qubit instantaneously collapse to the same state measured by Alice, $|+\rangle$ or $|-\rangle$
  - Bob’s measures second and obtains $|0\rangle$ or $|1\rangle$ with probability 50%
    - regardless of the outcome of Alice’s measurement
  - Bob and Alice discover the lack of correlation after the measurement

Thanks

Paolo Cremonesi

POLITECNICO
MILANO 1863