ADVANCED ARCHITECTURES
INTENSIVE COMPUTATION

Quantum Computing

Annalisa Massini

Lecture 18-19

2023-2024

References

- *Dancing with Qubits*
  Robert S. Sutor – Packt> – 2019

- *Quantum Computation and Quantum Information*
  Michael A. Nielsen & Isaac L. Chuang – Cambridge Press – 2010

- *Principles of quantum computation and Information*
  G. Benenti, G. Casati, G. Strini – World Scientific Pub – 2004
  - *Ch. 3* Quantum Computation

- *https://qiskit.org/textbook/what-is-quantum.html*

- *https://en.wikipedia.org/wiki/Quantum_logic_gate*

QUANTUM SYSTEMS

Quantum Computing

- **Quantum computing** exploits **quantum-mechanical effects** – in particular *superposition* and *entanglement* – to more efficiently execute a computation

- Theory of ***quantum mechanics*** originated from the crisis arisen in physics and ended in the early 1920s after a quarter century

- **Quantum mechanics** allows the calculation of properties and behaviour of physical systems

- **Quantum mechanics** has been an indispensable part of science ever since, and has been applied to everything including the *structure of the atom*, *nuclear fusion in stars*, *superconductors*, the *structure of DNA*, and the *elementary particles of nature*

Quantum Computing

- **Quantum mechanics** is a **mathematical framework** or *set of rules* for the construction of physical theories
- For example, *quantum electrodynamics* describes with fantastic accuracy the interaction of atoms and light, and is built up within the framework of quantum mechanics and contains *specific rules* not determined by quantum mechanics
- **Quantum computing** basically deals with the manipulation of **quantum systems**
- The ability to control *single quantum systems* is essential to exploit the power of quantum mechanics to quantum computing

Quantum Computing

- Compared to traditional digital computing, **quantum computing** offers the potential to **dramatically reduce** both **execution time** and **energy consumption**

- We will define the **common terms** and **concepts** used for quantum computing

- We will **not** discuss **how** the constructs are related to the foundations of quantum mechanics

Quantum Computing

- In the mathematical formulation of quantum mechanics, the **state** of a **quantum mechanical system** is:
  - a **vector ψ** belonging to a (separable) **complex Hilbert space $\mathcal{H}$**
  - **vector ψ** is postulated to be normalized under the **inner product** and it is well-defined up to a complex number of modulus 1 (the **global phase**)
  - Physical quantities of interest – position, momentum, energy, spin – are represented by observables, which are **Hermitian linear operators** acting on the Hilbert space

- A **complex Hilbert space** is a complex vector space with an inner product which is also complete with respect to the norm defined by the inner product (complete here means that every Cauchy sequence of vectors converges to a vector in the sense that the norm of differences approaches zero)
- The inner product between the vectors $v = [v_0 \quad \cdots \quad v_{N-1}]^T$ and $w = [w_0 \quad \cdots \quad w_{N-1}]^T$ (T denotes transpose so v and w are vectors column vectors) is given by $\sum_0^{N-1} v_i w_i^*$ where * denotes the complex conjugate

Quantum Computing

- The elementary unit of quantum information and the basic building block of quantum computation is the **qubit**, short for *quantum bit*
- The **qubit** can be seen as the quantum mechanical generalization of a bit used in classical computers
- More precisely, a **qubit** is a two-dimensional quantum system

- The **qubit** can be prepared, manipulated and measured in a controlled way

- A **quantum computer** can be seen as a ***collection of n qubits*** and its wave function (*mathematical description of the quantum state of an isolated quantum system, complex-valued*) resides in a 2^n-dimensional complex Hilbert space

Quantum Computing

- We said that the state of any quantum system is always represented by a **vector in a complex vector space**, the Hilbert space of wave functions

- **Quantum algorithms** are always expressible as **transformations** acting on the Hilbert vector space of wave functions

- For quantum computing we need only deal with **finite quantum systems**
- It suffices to consider finite dimensional complex vector spaces with an inner product

Quantum Computing

- **Quantum state spaces and the tranformations** acting on them can be described in terms of **vectors** and **matrices** respectively
- Qubit are represented using the **bra-ket** notation invented by Paul Dirac
  - **ket** is for column vectors: $|x\rangle = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$
  - **bra** is for row vectors: $\langle x| = \begin{bmatrix} x_0 & x_1 \end{bmatrix}$
- Any ket $|x\rangle$ has a corresponding bra $\langle x|$
- We can **convert** between them using the **conjugate transpose** (denoted by the $*$ or $\dagger$ operation) , that is the **vector is transposed** and the **elements are complex conjugated**

Quantum Computing

- A fundamental feature of the quantum theory is that it usually cannot predict with certainty what will happen, but only give **probabilities**

- Mathematically, a probability is found by taking the *square of the absolute value* of a complex number, known as a **probability amplitude**

QUBITS

Qubit

- Just as a classical bit has a state – either 0 or 1 – a qubit also has a state
- Two possible states for a qubit are the states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

  which correspond to the states 0 and 1 for a classical bit

- The vectors $\mathbf{|0\rangle}$ and $\mathbf{|1\rangle}$
  - encode the two basis states of a two-dimensional Hilbert vector space
  - are **normalized and mutually orthogonal quantum states** (representing the values 0 and 1 of a classical bit)
  - are known as computational basis states
  - together give the **computational basis**, and span the two-dimensional linear vector (Hilbert) space of the qubit

Qubit

- **Qubits** are described as **mathematical objects** with certain specific properties
- **Qubits**, like bits, can be realized as actual physical systems
- Treating qubits as abstract entities allows us to construct a general theory of quantum computation and information which does not depend upon a specific system for its realization

- The difference between bits and qubits is that a qubit can be in a state other than $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$

- Since the **states** $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ **form an orthonormal basis**, we can represent any 2D vector with a linear combination of these two states, that in quantum mechanics is denoted ***superposition***

Qubit

- The **state of a qubit** may be expressed, using the **superposition principle**, as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are *complex numbers* – called **probability amplitudes** – constrained by the normalization condition

$$|\alpha|^2 + |\beta|^2 = 1$$

- A **probability amplitude** is a quantity which when absolute-squared gives probability, hence $|\alpha|^2$ and $|\beta|^2$ are probabilities
- We can also write:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- In general, a **qubit is a vector** in a two-dimensional complex vector space

Qubit

- Differently from the classical case, we cannot examine a qubit to determine its quantum state, that is, the values of α and β, we can only acquire much more restricted information about the quantum state

- **Measurement** corresponds to transforming the quantum information (stored in a quantum system) into classical information

- A central principle of **quantum mechanics** is that **measurement outcomes are probabilistic**

Qubit

- Measuring a qubit typically corresponds to reading out a classical bit, i.e. whether the qubit is 0 or 1

- When we measure a qubit we get either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$

- Naturally, $|\alpha|^2 + |\beta|^2 = 1$ since the probabilities must sum to one

- The ability of a qubit to be in a superposition state runs counter to our *common sense* understanding of the physical world
- A classical bit is like a coin: either heads or tails up
- By contrast, a qubit can exist in a continuum of states between $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ – until *it is observed*

Qubit

- The ***inner product*** (generalization of the *dot product*) between a **bra** (row vector), given by $\langle a| = [a_0^* \quad a_1^*]$, and a **ket** (column vector), given by $|b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$
is: $$(\langle a|)(|b\rangle) = \langle a|b\rangle = a_0^*\, b_0 + a_1^*\, b_1$$

- The **inner product** is useful to understand the **measurements**

- To find the probability of measuring a state $|\psi\rangle$ in the state $|x\rangle$ we do:

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

Qubit

- Exploiting the orthonormal basis given by the states $|0\rangle$ and $|1\rangle$ and the ***superposition*** of these two states we can define the qubit's ***statevector*** q_0 and write the state in the form:

$$|q_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$$

- In fact:

$$|q_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{i}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \end{bmatrix} =$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{i}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$$

Qubit

- As we said, when we measure $|\psi\rangle$, the probability of measuring $|x\rangle$ is obtained by taking the **inner product** of $|x\rangle$ and the state we are measuring and then **squaring the magnitude**, i.e. $p(|\psi\rangle) = |\langle x|\psi\rangle|^2$

- For example, for the state $|q_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$, the probability of measuring $|0\rangle$ is 1/2

In fact: $$\langle 0|q_0\rangle = \frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{i}{\sqrt{2}}\langle 0|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} + \frac{i}{\sqrt{2}}\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}$$
$$= \frac{1}{\sqrt{2}}1 + \frac{i}{\sqrt{2}}0 = \frac{1}{\sqrt{2}}$$

and $$|\langle 0|q_0\rangle|^2 = \frac{1}{2}$$

Qubit

- On the other hand, if we want the probabilities to add up to 1 (which they should), we need to **ensure that the statevector is properly normalized**, that is **its magnitude to be 1**:

$$\langle\psi|\psi\rangle=1$$

- Thus, if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then the normalization condition is

$$|\alpha|^2 + |\beta|^2 = 1$$

- And we obtain the factors of $\sqrt{2}$ we saw before

- Notice that, nowhere does it tell us that $|x\rangle$ can only be either $|0\rangle$ or $|1\rangle$
- The measurements we have considered so far are in fact only one of an infinite number of possible ways to measure a qubit

Qubit

- Measuring the state $|0\rangle$ or the state $|1\rangle$ will give us the output 1 with certainty
- Notice that if we consider a state such as $\begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$ and apply the **measurement** rule we obtain:

$$|\langle x|(i|1\rangle)|^2 = |i\langle x|1\rangle|^2 = |i|^2|\langle x|1\rangle|^2 = |\langle x|1\rangle|^2$$

- The **factor *i* disappears** once we take the magnitude of the complex number

- This effect is completely independent of the measured state $|x\rangle$
- The probability for the state $i|1\rangle$ is identical to that for $|1\rangle$

Qubit

- Since measurements are the only way we can extract any information from a qubit, this implies that the two states $|1\rangle$ and $i|1\rangle$ are equivalent in all ways that are physically relevant

- More generally, we refer to any overall factor γ on a state for which $|\gamma|^2 = 1$ as ***global phase***

- States that differ only by a global phase (such as $|a\rangle$ and $\gamma\,|a\rangle$) are ***physically indistinguishable***, in fact:

$$|\langle x|(\gamma|a\rangle)|^2 = |\gamma\langle x|a\rangle|^2 = |\langle x|a\rangle|^2$$

Qubit

- We know that the amplitudes contain information about the probability of finding the qubit in a specific state
- Once we have measured the qubit, we know with certainty what the state of the qubit is
- **For example**
  - If we measure a qubit in the state $|q\rangle$ and find it in the state $|0\rangle$
  - Then, if we measure again, there is a 100% chance of finding the qubit in the state $|0\rangle$

- This means **the act of measuring changes the state of our qubits**

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \xrightarrow{measure|0\rangle} |\psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

- We refer to this as **collapsing the state of the qubit**

Qubit

- If we constantly measure each of our qubits to keep track of their value at each point in a computation, they would always simply be in a well-defined state of either $|0\rangle$ or $|1\rangle$ and they would be no different from classical bits
- To achieve truly **quantum computation** we must allow the qubits to explore more complex states
- **Measurements** are therefore only used when we need to extract an output, and are all **placed at the end of a quantum circuit**
- In general, a quantum computation is composed of **three steps**:
  - Preparation of the input state
  - Implementation of the **unitary** transformation acting on this state
  - Measurement of the output state

Qubit

- Since a global phase for a state never has any observable consequences, the states $|\psi\rangle$ and $e^{i\gamma}|\psi\rangle$ both produce the same observable consequences
- In fact, all complex number with absolute value 1 can be expressed according to Euler's formula as $e^{i\gamma} = \cos\gamma + i\sin\gamma$ and it holds that $\left|e^{i\gamma}\right| = 1$ since the absolute value of a complex number $z = a + ib$ is: $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$,
- It is useful to always choose the global phase such that the coefficient of the ket $|0\rangle$ is real and non-negative:
- We can express α and β in polar form: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = r_1 e^{i\varphi_1}|0\rangle + r_2 e^{i\varphi_2}|1\rangle = e^{i\varphi_1}(r_1|0\rangle + r_2 e^{i(\varphi_2-\varphi_1)}|1\rangle)$
- That is the same as: $r_1|0\rangle + r_2 e^{i(\varphi_2-\varphi_1)}|1\rangle$

Qubit

- Hence the state of a single qubit $|\psi\rangle$ can be represented by

$$|\psi\rangle = r_1|0\rangle + r_2 e^{i\varphi}|1\rangle$$

- with:
  - $r_1, r_2 \in \mathbb{R}$, ${r_1}^2 + {r_2}^2 = 1$ and $0 \le \varphi < 2\pi$

- Moreover, we can find $0 \le \theta < \pi$ with $r_1 = \cos\frac{\theta}{2}$ and $r_2 = \sin\frac{\theta}{2}$ so that:

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

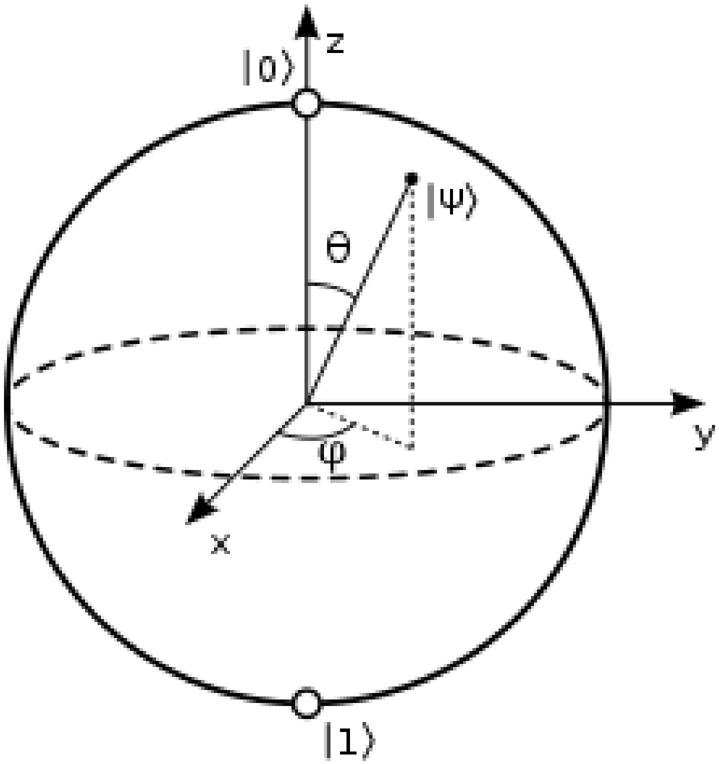
Qubit

- We can describe the **state of any qubit** using the two **variables $\boldsymbol{\varphi}$** and $\boldsymbol{\theta}$:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \quad \text{with } 0 \le \theta \le \pi, \;\; 0 \le \varphi < 2\pi$$

- If we interpret
  - θ and φ as spherical coordinates
  - with radius $r = 1$ (since the magnitude of the qubit state is 1)

  we can plot any single qubit state on the surface of a sphere, known as the ***Bloch sphere***

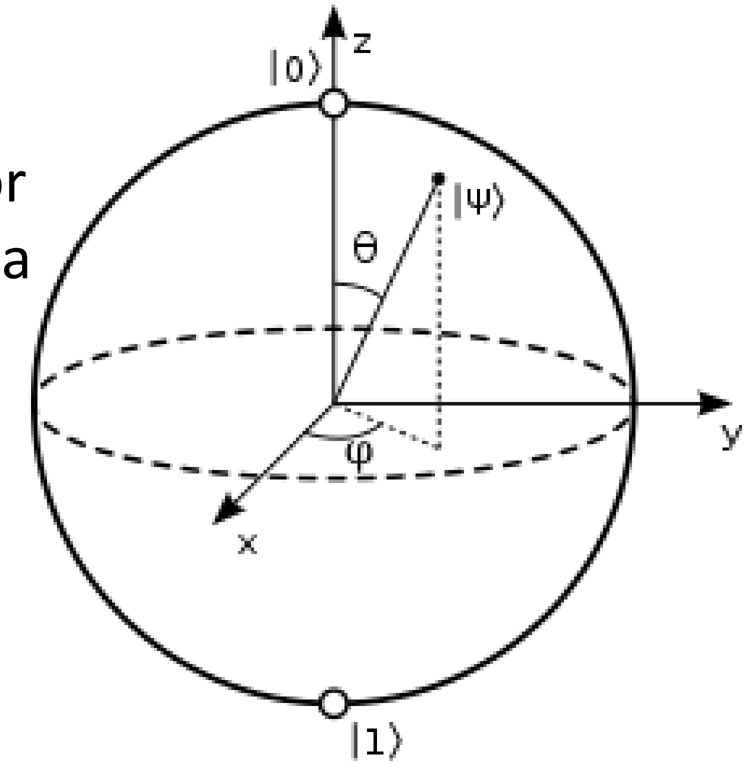


Qubit

- The **Bloch sphere** can be embedded in a **three-dimensional space of Cartesian coordinates**:

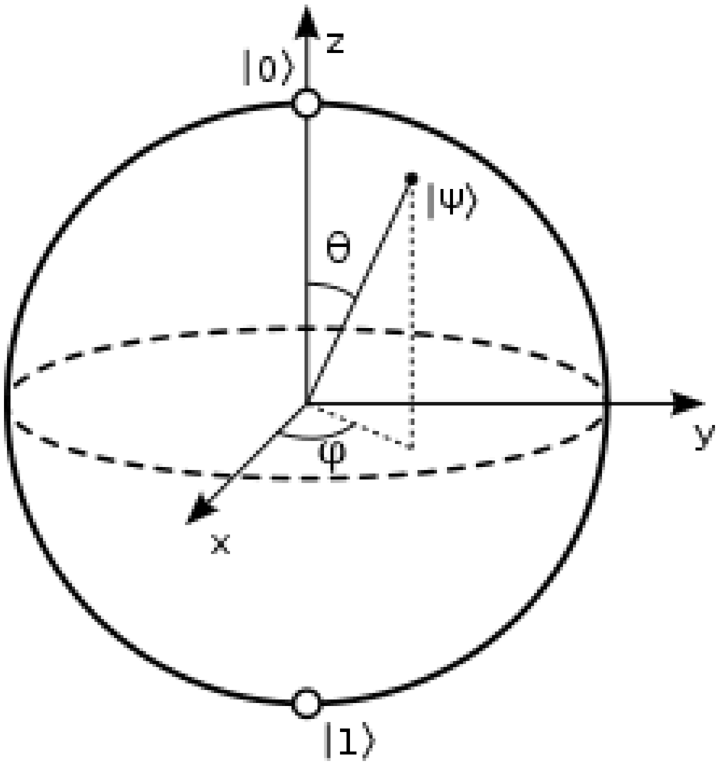
$$\begin{cases} x = \cos\phi \sin\theta \\ y = \sin\phi \sin\theta \\ z = \cos\theta \end{cases}$$

- By definition, a ***Bloch vector*** is a vector whose components *(x, y, z)* single out a point on the Bloch sphere
- Therefore, each Bloch vector must satisfy the normalization condition $x^2 + y^2 + z^2 = 1$

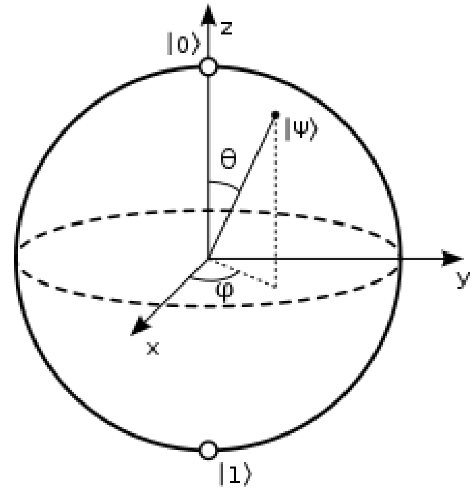


Qubit

- To avoid confusing the **qubit *statevector*** with its ***Bloch vector*** remember that:
  - The ***statevector*** is the vector that holds the amplitudes for the two states our qubit can be in
  - The ***Bloch vector*** is a visualisation method that maps the 2D, complex statevector onto real, 3D space



Qubit



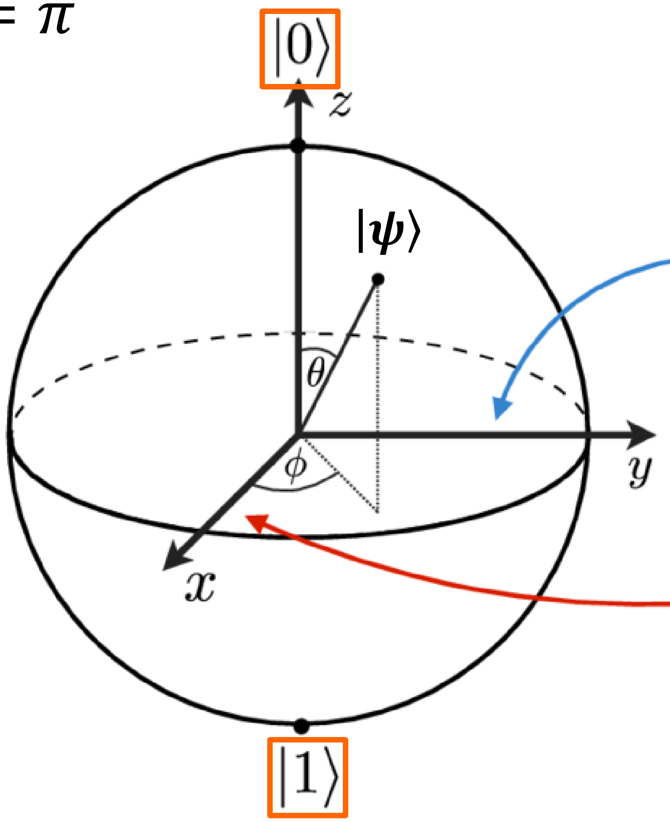
- For the generic state $|\psi\rangle$ we can write:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1+\cos\theta}{2}} \\ (\cos\phi + i\,\sin\phi)\sqrt{\frac{1-\cos\theta}{2}} \end{bmatrix}$$

$$= \begin{bmatrix} \sqrt{\frac{1+\cos\theta}{2}} \\ (\cos\phi + i\,\sin\phi)\sqrt{\frac{1-\cos^2\theta}{2(1+\cos\theta)}} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1+\cos\theta}{2}} \\ \frac{\cos\phi\sin\theta + i\,\sin\phi\sin\theta}{\sqrt{2(1+\cos\theta)}} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x+i\,y}{\sqrt{2(1+z)}} \end{bmatrix}$$

Qubit

- Note that single qubit states $|0\rangle$ and $|1\rangle$ (which are orthogonal) are not orthogonal vectors on the Bloch sphere, i.e. as points along the positive and the negative z axis represented as $\theta = 0$ and $\theta = \pi$



$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

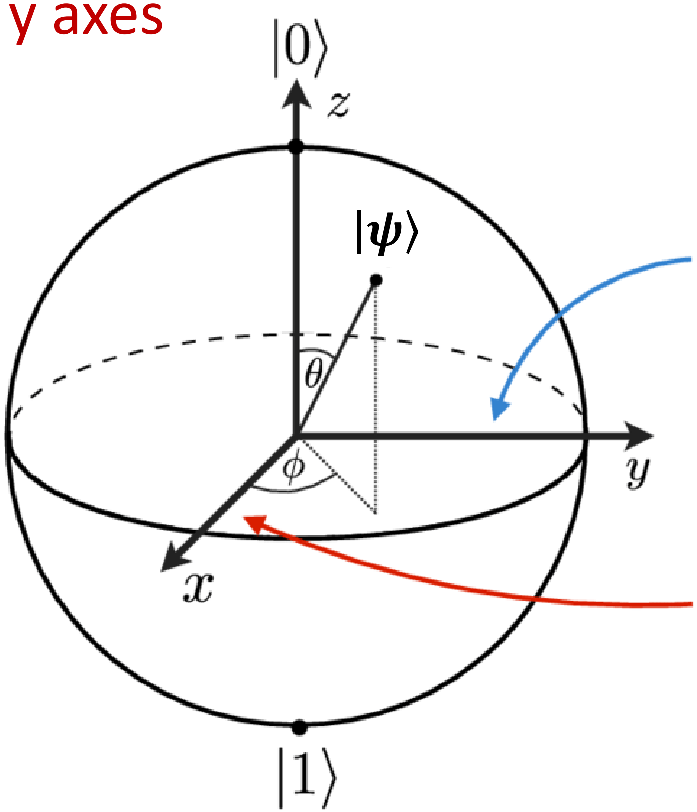
$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

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

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

Qubit

- Apart from canonical states $|0\rangle$ and $|1\rangle$ which permit to describe the qubit state with a linear combinations of two vectors lying on the z-axis, there are other four remarkable states that lie along the x and y axes



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

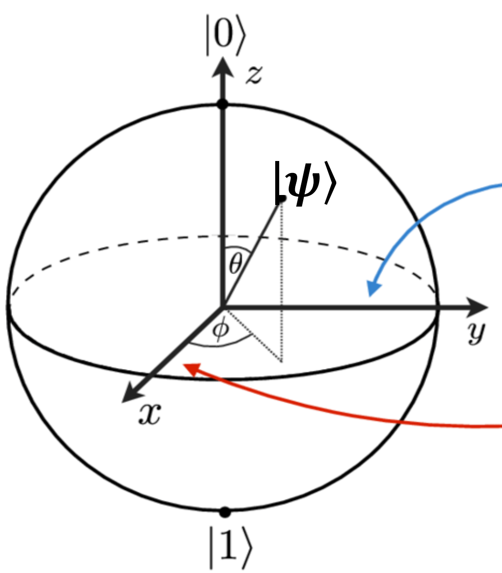
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Qubit

- Hence, the Z-basis is not the only basis we can use
- The **X-basis** is given by the two **vectors $|+\rangle$ and $|-\rangle$**:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$



$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

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

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

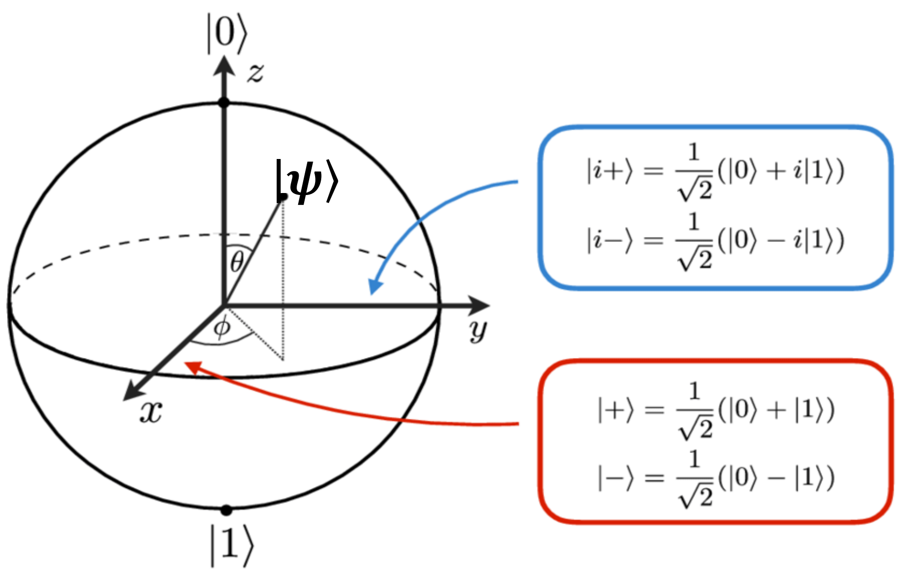
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Qubit

- Another (less commonly used) basis is

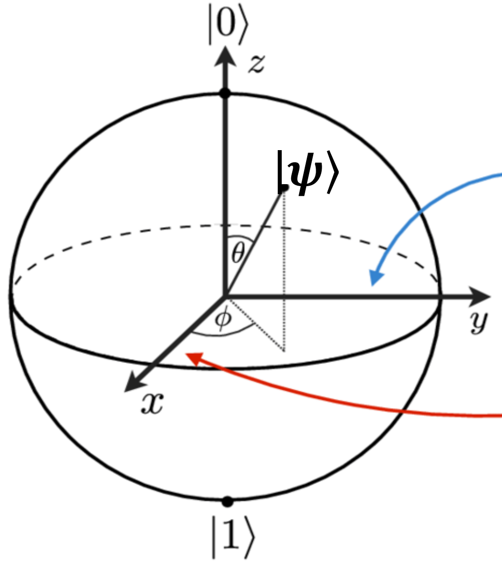
$$|i+\rangle = |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}$$

$$|i-\rangle = |\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -i\end{bmatrix}$$



Qubit

- Summing up, we have three pairs of basis elements:
- $\{|0\rangle, |1\rangle\}$ Computational basis (Bloch sphere *Z*-axis)
- $\{|+\rangle, |-\rangle\}$ Hadamard basis (Bloch sphere *X*-axis)
- $\{|↺\rangle, |↻\rangle\} = \{|i\rangle, |-i\rangle\}$ Circular basis (Bloch sphere *Y*-axis)



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

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

MULTI-QUBIT

Multi-Qubit

- The mathematical structure of a qubit generalizes to higher dimensional quantum systems
- The state of any quantum system is a normalized vector (a vector of norm one) in a complex vector space
  - The normalization is necessary to ensure that the total probability of all the outcomes of a measurement sum to one

- The joint state of a system of qubits is described using an operation known as the **tensor product**, $\otimes$, that mathematically is the same as taking the Kronecker product of their vectors

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad |b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \quad |ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_0 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \\ b_1 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{bmatrix}$$

Multi-Qubit

- A single **bit** has ***two** possible states* and a **qubit** state has ***two** complex amplitudes*
- Similarly, **two bits** have ***four** possible states* (00, 01, 10, 11) and the state of **two qubits** requires ***four** complex amplitudes*
- These amplitudes are stored in a 4D-vector:

$$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

- The rules of measurement still work in the same way:

$$p(|00\rangle) = |\langle 00|a\rangle|^2 = |a_{00}|^2$$

- And the same normalisation condition holds:

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

Multi-Qubit

- If we have ***n* qubits**, we will need to keep track of **2^n complex amplitudes**
- **Vectors** representing more qubits grow exponentially with the number of qubits

- This is the reason quantum computers with large numbers of qubits are so difficult to simulate
- A modern laptop can easily simulate a general quantum state of around 20 qubits, but simulating 100 qubits is too difficult for the largest supercomputers

Multi-Qubit

- The state of any ***n* qubit system** can be written as a normalized linear combination of the **2^n bit-string states** (states formed by the tensor products of $|0\rangle$'s and $|1\rangle$'s)
- The orthonormal basis formed by the 2^n bit-string states is called the computational basis

- A system of **two** qubits, e.g. $|\psi_1\psi_2\rangle$, whose complete state is the tensor product of two different single qubit states , e.g. $|\psi_1\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)$ and $|\psi_2\rangle = (\beta_0|0\rangle + \beta_1|1\rangle)$, can be described by an equation in the form

$$|\psi_1\psi_2\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle =$$

$$= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

Multi-Qubit

- It is possible for two qubits to be in a state that **cannot** be written as the tensor product of two single qubit states
- States of a system of which **cannot** be expressed as a tensor product of states of its individual subsystems, that is are not separable, are called **entangled states**
- Instead, states separable into the tensor product of states from the constituent subsystems are referred to as **separable states**

Multi-Qubit

Exercises

1. Write down the kronecker product of the qubits:
   a) $|0\rangle \otimes |1\rangle$
   b) $|0\rangle \otimes |+\rangle$
   c) $|+\rangle \otimes |1\rangle$
   d) $|1\rangle \otimes |+\rangle$
   e) $|-\rangle \otimes |+\rangle$
2. Write the state: $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|01\rangle$ as two separate qubits

Multi-Qubit

- The state $|00\rangle + |11\rangle$ is an example of a quantum state that cannot be described in terms of the state of each of its components (qubits) separately

- In other words, we cannot find a_1, a_2, b_1, b_2 such that

$$(a_1|0\rangle + b_1|1\rangle)\otimes(a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$$

since

$$(a_1|0\rangle + b_1|1\rangle)\otimes(a_2|0\rangle + b_2|1\rangle)$$

$$= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

and $a_1b_2 = 0$ implies $a_1a_2 = 0$ or $b_1b_2 = 0$

Multi-Qubit

- **Bell states** are a very famous example of **entangled states**:

$$|\psi_1\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \qquad |\psi_2\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$

$$|\psi_3\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}} \qquad |\psi_4\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

- Take as example $|\psi_1\rangle$:
  - If the first qubit is measured, and the result is $|0\rangle$, then also the measurement of the second qubit will give $|0\rangle$ as a result
- In general, for entangled states, it holds that measured one of the two qubits, also the state of the other qubit is well determined

Multi-Qubit

- There exist entangled states also for three and more qubits
- Entanglement is a form of quantum mechanical correlation which tells that the state of a single quantum system could depend **instantly** on the state of other quantum systems
- In other words, entanglement tells that not always a complex system can be understood in terms of its constituents

- Without the existence of entangled states, **quantum computers would be no more powerful** than their classical counterparts
- Entanglement makes it possible to create a complete 2^n dimensional complex vector space to do computations in, using just n physical qubits

QUANTUM LOGIC GATES

Quantum logic gates

- A **quantum logic gate** is a basic quantum circuit operating on a small number of qubits
- Quantum gates are the building blocks of **quantum circuits**, like classical logic gates are for conventional digital circuits

- **Quantum gates** are **unitary operators**, and are described as unitary matrices relative to some basis
  - An (invertible) complex square matrix U is called **unitary** if its adjoint (conjugate transpose) and its inverse coincide, i.e.:

$$U^{\dagger}U = UU^{\dagger} = I$$

  where I is the identity matrix

Quantum logic gates

- Quantum gates can be used to manipulate the state of one or more qubits by changing the state vector $|\psi\rangle$, with the normalization condition continuing to be valid

- **Quantum gates** must be **reversible**, i.e. when an operator is applied to a given state, it must be always possible to reconstruct the input state starting from the output

- A gate which acts on $\boldsymbol{n}$ **qubits** is represented by a $\mathbf{2^n \times 2^n}$ **unitary matrix**, and the set of all such gates with the group operation of matrix multiplication is the symmetry group $\mathrm{U}(2^n)$

Quantum logic gates

- To see the **effect of a gate on a qubit**, we simply **multiply** the qubit's statevector by the gate represented as a matrix **2x2**, whereas for n qubits we have a statevector of size 2^n and a matrix (gate) of size $2^n \times 2^n$
- The most common quantum gates operate on vector spaces of **one or two qubits**, just like the common classical logic gates operate on one or two bits
- There are two different conventions regarding the order in which the qubits in a quantum circuit have to be read:
  - The **traditional notation** where the **top** qubit is the **most** significant one
  - The **IBM notation** where the **top** qubit is the **least** significant one

ONE QUBIT GATES

One-Qubit gates: the Pauli gates

The Pauli gates: X-gate

- The **X-gate** is the quantum equivalent of the classical not gate
- It is able to flip the $|0\rangle$ state in $|1\rangle$ state (and vice versa)

- The X-gate is represented by the **Pauli-X matrix**:

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

- The X-gate switches the amplitudes of the states $|0\rangle$ and $|1\rangle$:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

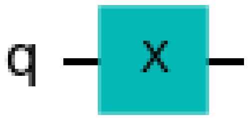
- Because of the its effect on a qubit, it is also called **bit-flip** gate

One-Qubit gates: the Pauli gates

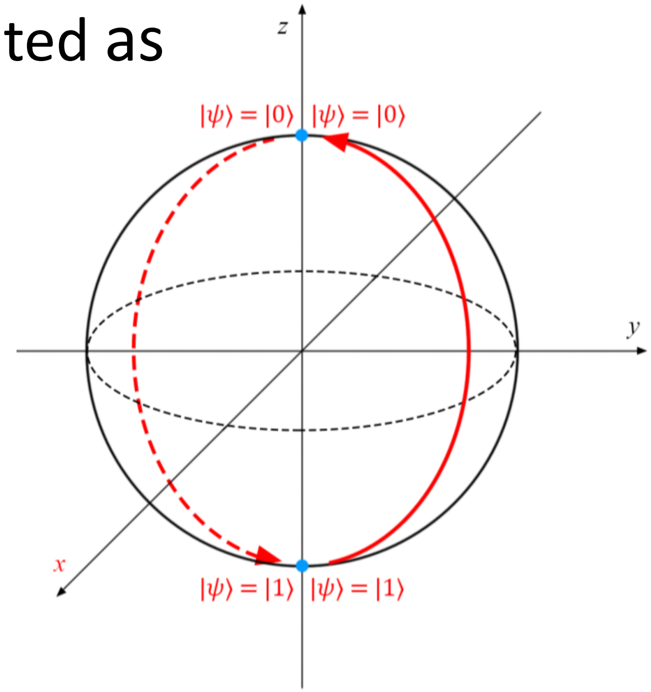
The Pauli gates: X-gate

- In general: $$|\psi'\rangle = X|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

- In quantum circuits, the X-gate is represented as



- By looking at the Bloch sphere, it is possible to interpret the action of X gate in terms of a rotation around the x-axis of π radians (180°)
- The poles are flipped and points in the lower hemisphere move to the upper and vice versa



Pauli X

One-Qubit gates: the Pauli gates

The Pauli gates: Z-gate

- The **Z-gate** is able to swap $|+\rangle$ and $|-\rangle$ state as well as $|i\rangle$ and $|-i\rangle$
- The Z-gate is represented by the **Pauli-Z matrix**:

$$\mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

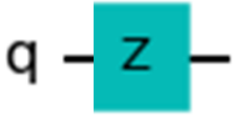
- Z-gate do not change the probabilities of measuring $|0\rangle$ and $|1\rangle$
  - $Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$ and $Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = -\begin{bmatrix} 0 \\ 1 \end{bmatrix} = -|1\rangle$
  - the states $|0\rangle$ and $|1\rangle$ are the two *eigenstates* of the Z-gate
  - In fact, the *computational basis* formed by the states $|0\rangle$ and $|1\rangle$ is often called the Z-basis

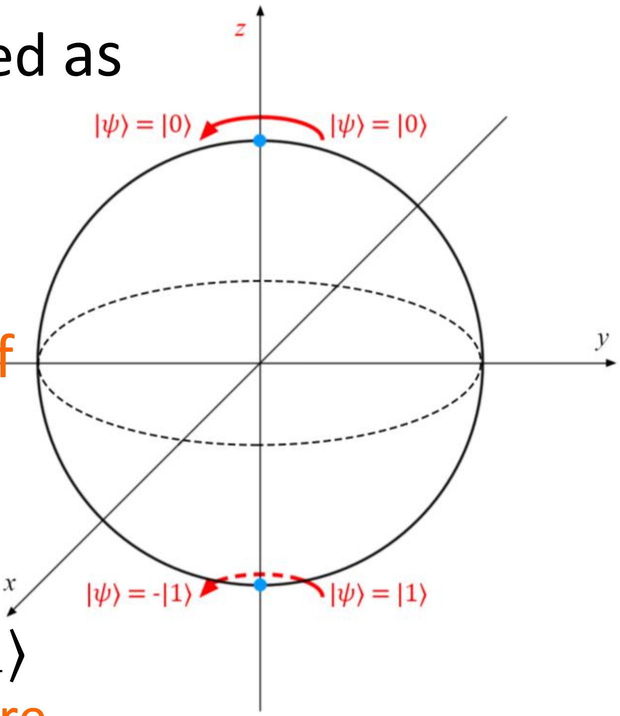
One-Qubit gates: the Pauli gates

The Pauli gates: Z-gate

- In general: $|\psi'\rangle = \mathrm{Z}|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$

- In quantum circuits, the Z-gate is represented as





Pauli Z

- By looking at the Bloch sphere, the action of this gate is a rotation around the z-axis of π radians (180°)
- It is also called **phase-flip** gate
- It has no effect on $|0\rangle$ but transforms $|1\rangle$ to $-|1\rangle$ which are the same point $|1\rangle$ on the Bloch sphere

One-Qubit gates: the Pauli gates

The Pauli gates: Y-gate

- The **Y-gate** is represented by the **Pauli-y matrix**:

$$\mathrm{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

- The final state has both a different relative phase and a different amplitude probability

- Since its action on the qubit state corresponds to the one that can be achieved by combining a Pauli X gate and a Pauli Z gate, it is usually called **bit-phase-flip** gate

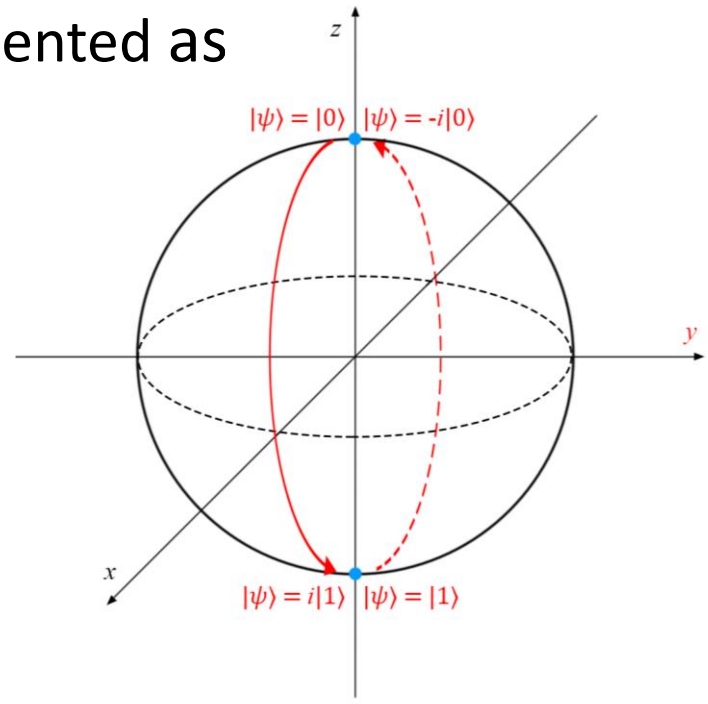
One-Qubit gates: the Pauli gates

The Pauli gates: Y-gate

- In general: $|\psi'\rangle = Y|\psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\,\beta \\ i\,\alpha \end{bmatrix} = -i\begin{bmatrix} \beta \\ -\alpha \end{bmatrix}$

- In quantum circuits, the X-gate is represented as

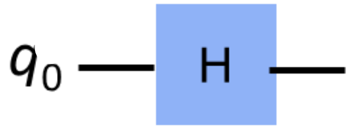
- By looking at the Bloch sphere, it is possible to interpret the action of this gate in terms of a rotation around the y-axis of π radians (180°)



Pauli Y

One-Qubit gates: the Hadamard Gate

- The **Hadamard gate** (H-gate) is a fundamental quantum gate
- It allows us to move away from the poles of the Bloch sphere and create a superposition of $|0\rangle$ and $|1\rangle$
- It has the matrix: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- In quantum circuits, the H-gate is represented as



- We can see that the H-gate performs the transformations:

$$H|0\rangle = |+\rangle \text{ and } H|1\rangle = |-\rangle$$

- The action of Hadamard gate is a rotation around the y-axis of $\pi/2$ radians, followed by a rotation around the x-axis of π radians

One-Qubit gates

Exercises

- Verify that all gates introduced so far are their **own inverse**
  - Note that gates introduces so far are **unitary** matrices, then the inverse is equal to the conjugate transpose
  - Note also that if a complex square matrix is equal to its own conjugate transpose, then it is a **Hermitian matrix** (or self-adjoint matrix)

- Verify that you can **create an X-gate** by sandwiching a Z-gate between two H-gates, that is $X = HZH$
  - Starting in the Z-basis, the H-gate switches our qubit to the X-basis, the Z-gate performs a NOT in the X-basis, and the final H-gate returns our qubit to the Z-basis

One-Qubit gates: the Pauli gates

Exercises - solutions

- Verifying $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}, \boldsymbol{H}$ are their own inverse
  - $XX = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
  - $YY = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} -i^2 & 0 \\ 0 & -i^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
  - $ZZ = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
  - $HH = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

- Verifying $\boldsymbol{HZH}$ behaves like an X-gate
  - $HZH = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$

One-Qubit gates: Arbitrary rotations

- There are three gates that allow to do an **arbitrary rotation** around the x, y and z axis, respectively
- These operators are R_x, R_y and R_z, and are defined as:

$$R_x(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \quad R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \quad R_z(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

- Notice that while R_x and R_y change the probabilities of the system states, R_z does not (i.e. the probability of measuring $|0\rangle$ rather than $|1\rangle$ remains the same)
- What R_z changes is the relative phase of the qubit

One-Qubit gates

Exercises

- Apply $R_x(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$ and $R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$

  to $|0\rangle$, $|1\rangle$ and $|q_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ and verify that the probabilities of the state change

- Apply $R_z(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$ to $|0\rangle$, $|1\rangle$ and $|q_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ and verify that the probabilities of the state do not change

One-Qubit gates: Arbitrary rotations

- R_z performs a rotation of φ around the Z-axis direction and changes the relative phase of the qubit

- R_z is a **parametrized** gate and is also called **P-gate**
- It needs a real number φ to tell it exactly what to do

- Notice that the Z-gate, that is $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, is a special case of the P-gate $P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$, with $\varphi = \pi$:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix}$$

One-Qubit gates: the S-gate

- The **S-gate**, also known as $\sqrt{Z}$-gate, is a P-gate with $\varphi = \pi/2$ around the Z-axis direction
- The **S-gate** does a quarter-turn around the Bloch sphere

- The matrix is: $$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix}$$

- The name $\sqrt{Z}$-gate is due to the fact that two successively applied S-gates has the same effect as one Z-gate:

$$SS|q\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} |q\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} |q\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} |q\rangle$$
$$= Z|q\rangle$$

One-Qubit gates: the S-gate

- Unlike other gates introduced so far, the **S-gate is not its own inverse**
- We can have $S^\dagger$-gate (or $\sqrt{Z}^\dagger$-gate)
- The $S^\dagger$-gate is clearly a P-gate with $\varphi = -\pi/2$
- The matrix is: $S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{bmatrix}$
- It holds

$$SS^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i(\frac{\pi}{2}-\frac{\pi}{2})} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

One-Qubit gates: the T-gate

- The **T-gate** is a P-gate with $\varphi = \pi/4$

- The matrices for T and $T^\dagger$ are:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \qquad T^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{bmatrix}$$

- As with the S-gate, the T-gate is sometimes also denoted as the $\sqrt[4]{Z}$-gate

One-Qubit gates: the U-gate

- The **U-gate** is the most general of all single-qubit quantum gates
- It is a parametrised gate of the form:

$$U(\theta,\phi,\lambda) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)}\cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

- Every gate could be specified as $U(\theta,\phi,\lambda)$, but it is unusual to see this in a circuit diagram
- As an example, we see the **U-gate** for representing the **H-gate** and **P-gate** respectively

$$U(\frac{\pi}{2},0,\pi) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and } U(0,0,\lambda) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix} = P$$

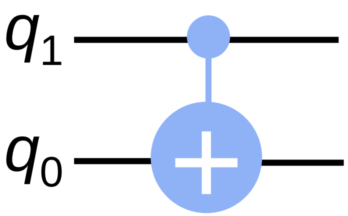
MULTI-QUBIT GATES

Multi-Qubit gates

- Among the **multiple-qubit gates**, there is a wide range of gates which is based on the same principle: **controlled gates**
- A given number of **control qubits** decide if a given operation must be performed on another set of qubits or not
- In the case of a two-qubit, there is one **control** qubit and one **target** qubit

Multi-Qubit gates: CNOT gate

- An important two-qubit gate is the **CNOT-gate**
- It is a conditional gate that performs an X-gate on the second qubit, **target** bit, if the state of the first qubit, **control** bit is $|1\rangle$
- In the picture q1 is the control qubit and q0 is the target qubit

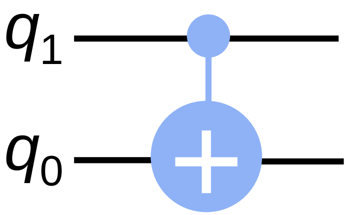


Multi-Qubit gates: CNOT gate

- The matrix of the CNOT gate is $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

- This matrix **swaps the amplitudes of $|10\rangle$ and $|11\rangle$** in the statevector:

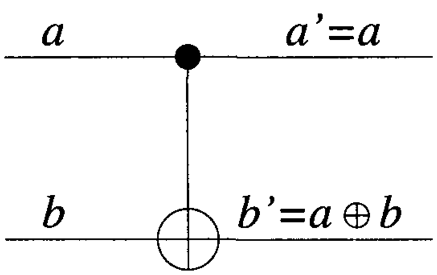
$$|a\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} \quad \mathrm{CNOT}|a\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{11} \\ a_{10} \end{bmatrix}$$



Multi-Qubit gates: CNOT gate

- The CNOT, or **controlled-NOT**, or Feynman gate is a **reversible** gate and perform **the XOR**, as shown in the true table below

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

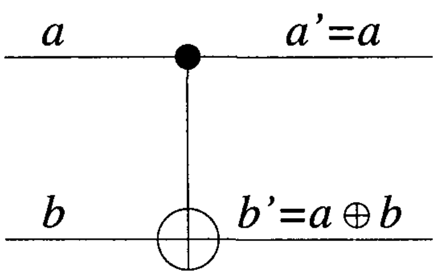


- The **second bit**, or target bit, is flipped if and only if the first bit is set to one and therefore $b' = a \oplus b$

Multi-Qubit gates: CNOT gate

- Note that, if we set the **target bit to 0**, the CNOT gates becomes the **FANOUT gate**: $(a, 0) \rightarrow (a, a)$

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



- It is easy to check that **CNOT is self-inverse**:
  - Indeed, the application of two CNOT gates, leads to

$$(a, b) \rightarrow (a, a \oplus b) \rightarrow \big(a, a \oplus (a \oplus b)\big) = (a, b)$$

  - Therefore, $(\text{CNOT})^2 = I$, that is $\text{CNOT}^{-1} = \text{CNOT}$

Multi-Qubit gates: Controlled gates

Generic controlled gates

- The operation performed by the generic single-qubit gate U can be represented by using the generic matrix

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

- If the action of U on the target qubit must be taken only if the first qubit is equal to $|1\rangle$, the controlled-U gate it holds that:

$$\text{controlled } U = CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

- Note that all the single qubit gates previously presented can be theoretically implemented in the ***controlled version***

Multi-Qubit gates: Controlled gates

- We can write the action of CU for all the four possible input patterns and observe the action when the control qubit is $|1\rangle$

$$\boldsymbol{CU|00\rangle} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle \quad \boldsymbol{CU|01\rangle} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

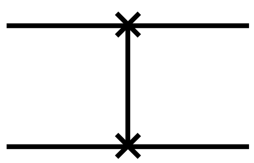
$$\boldsymbol{CU|10\rangle} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ u_{00} \\ u_{10} \end{bmatrix} = |1\rangle \otimes U|0\rangle$$

$$\boldsymbol{CU|11\rangle} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ u_{01} \\ u_{11} \end{bmatrix} = |1\rangle \otimes U|1\rangle$$

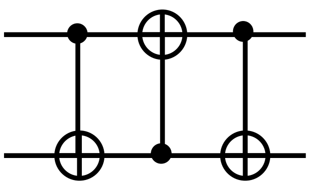
Multi-Qubit gates: Swap gate

- The **Swap gate** allows to swap two qubits
- It is defined as follows:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



- In general, the action is: $|\psi'\rangle = SWAP|\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a \\ c \\ b \\ d \end{bmatrix}$
- The **SWAP gate** is that it can be implemented, for example, using **three CNOT gates**



Multi-Qubit gates: CCNOT gate

- It is possible to show that two-bit reversible gates are not enough for **universal computation**

- Instead, a universal gate is the **controlled-controlled-NOT** (**CCNOT**) or **Toffoli gate**, which is a three-bit gate

- The Toffoli gate has **two** control qubits and **one** target qubit

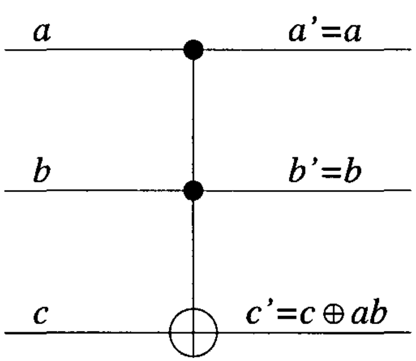
- The X operation is applied to the target qubit if and only if both control qubits are set to $|1\rangle$

Multi-Qubit gates: CCNOT gate

- The **CCNOT** gate acts as follows:
  - the **two control bits are unchanged**, that is $a' = a$ and $b' = b$
  - the **target bit is flipped** if and only if the two control bits are set to 1, that is $c' = c$ xor ab

Table and circuit of the CCNOT

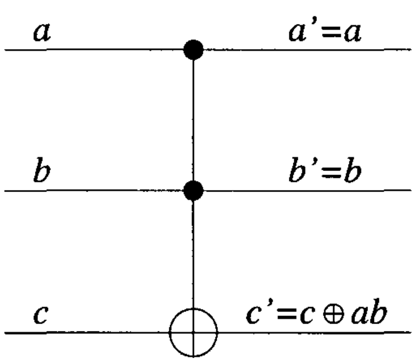
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Multi-Qubit gates: CCNOT gate

- The **CCNOT** gate (Toffoli gate) is **universal**
- To prove the CCNOT **universality**, we show how to use it to construct **both NAND and FANOUT gates**
  - If we set a = 1, the Toffoli gate acts on the other two bits as a CNOT and we have seen that the FANOUT gate can be constructed from the CNOT
  - Since $c' = c \oplus ab = \bar{c}\, ab + c\, \overline{ab}$, if we set $c = 1$, then $c' = 1 \oplus ab = 0\, ab + 1\, \overline{ab} = \overline{ab}$

a	*b*	*c*	*a'*	*b'*	*c'*
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

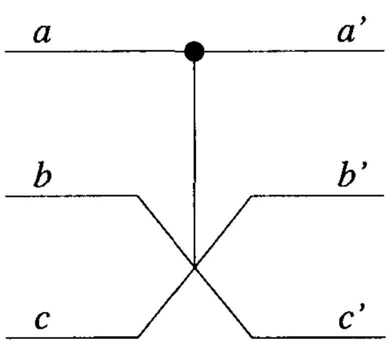


Multi-Qubit gates: CSWAP gate

- Another universal reversible gate is the **controlled-EXCHANGE gate** or **CSWAP gate** or **Fredkin gate**
- The SWAP operation is performed if and only if the control bit ***a*** **is set to 1** and the two target qubits b and c e are **swapped**

Table and circuit of the controlled-EXCHANGE

a	*b*	*c*	*a'*	*b'*	*c'*
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1



Multi-Qubit gates

- Both the Toffoli and Fredkin gates are **self-inverse**
- The price to pay to have **irreversible gates** is the introduction of additional bits and on output this produces **garbage** bits
- **Garbage bits**
  - are **not reused** during the computation
  - are needed to **store the information** that would allow us **to reverse the operations**
  - For instance, if we set c = 1 at the input of the Toffoli gate, we obtain $c' = \overline{ab}$ plus two garbage bits $a' = a$ and $b' = b$

QUANTUM CIRCUITS

Quantum circuit

- **Quantum operators** are described by means of **unitary matrices**
- A **quantum circuit** can be seen as **set of gates** connected to each other, where each gate is represented by a unitary matrix
- There can be two kinds of connections between gates belonging to the same circuit: **series** and **parallel** connections

- To understand the **behavior of a given circuit**, it is necessary to understand how to compute the **overall unitary matrix** describing the action of gates placed in parallel or in series

Quantum circuit

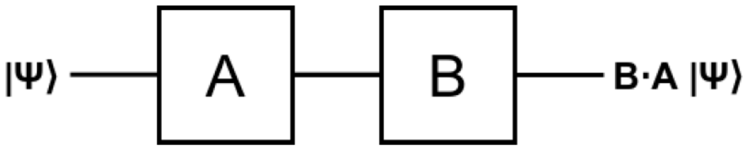
- The **time-flow in a circuit** is represented **from left to right**
- This means that the **evolution of the state of a qubit** has a physical meaning if considered from left to right

- However, when the matrix transfer function of the whole (or a part of the) circuit has to be computed, **unitary matrices must be written from right to left**
  - The **leftmost gate** in the circuit is described by the **rightmost unitary matrix**

Quantum circuit

Gates Connected in Series

- The overall transfer function of two generic one-qubit quantum gates connected in series can be computed as shown in the figure below



- The output after the input passed through gate A and B is:

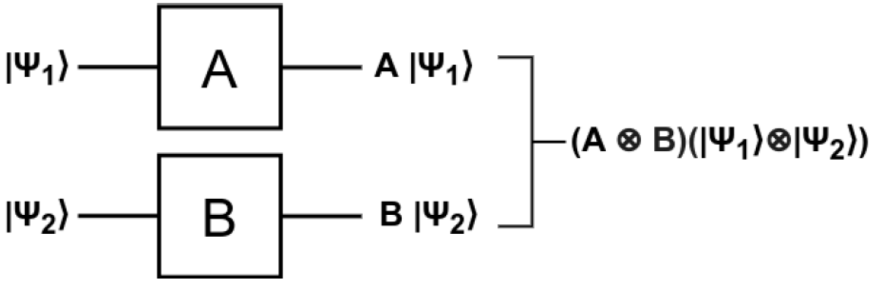
$$|\psi\rangle = BA|\psi\rangle$$

- The method can be extended to an arbitrary number of gates

Quantum circuit

Gates Connected in Parallel

- When two gates are placed in parallel, the **overall unitary matrix** acting on the **two qubits** is obtained using the **Kronecker product**, as shown in the figure below



- The output after the inputs passed through gates A and B is: $\boldsymbol{A|\psi_1\rangle \otimes B|\psi_2\rangle = (A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A \otimes B)|\psi_1\psi_2\rangle}$

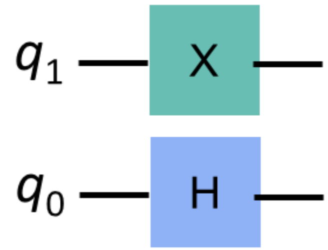
- The method can be extended to an arbitrary number of gates

One-Qubit gates on multi-Qubit

Example

- We have that a single bit gate acts on a qubit in a multi-qubit vector using the **tensor product** to calculate matrices that act on multi-qubit statevectors
- For example, if on q_1 acts the **X-gate** (NOT) and on q_0 acts the **H-gate** we can represent the simultaneous operations *X and H* using their **Kronecker product**:

$$X|q_1\rangle \otimes H|q_0\rangle = (X \otimes H)|q_1 q_0\rangle$$

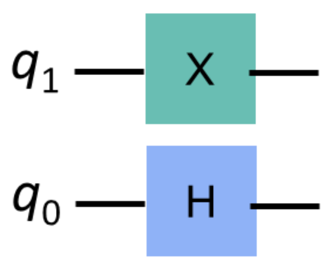


One-Qubit gates on multi-Qubit

- The **operation** $X|q_1\rangle \otimes H|q_0\rangle = (X \otimes H)|q_1 q_0\rangle$ is given by:

$$X \otimes H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

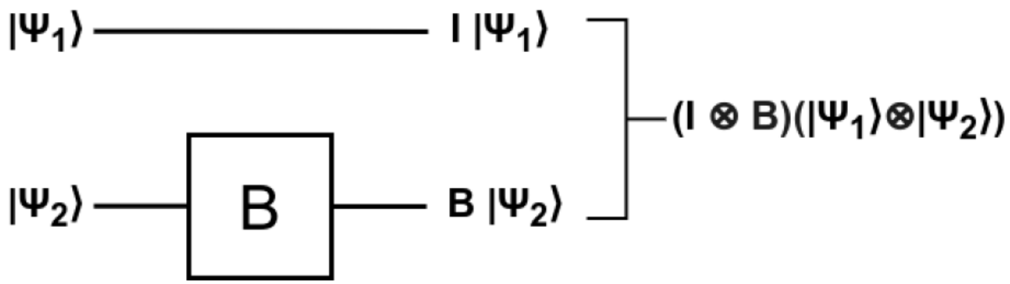
$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & 1 \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ 1 \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & 0 \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & H \\ H & 0 \end{bmatrix}$$



One-Qubit gates on multi-Qubit

Gates Connected in Parallel

- If gates are applied only to a subset of the inputs, qubits where no gates are acting can be treated as operated by an identity, as shown in the figure below

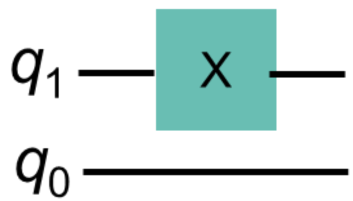


- The output after the inputs passed through gate B is:
$|\psi_1\rangle \otimes B|\psi_2\rangle = (I \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (I \otimes B)|\psi_1\psi_2\rangle$

One-Qubit gates on multi-Qubit

Example

- We need to **apply a gate to only one qubit** at a time, such as in the circuit below where on q_1 acts the **X-gate** (NOT)



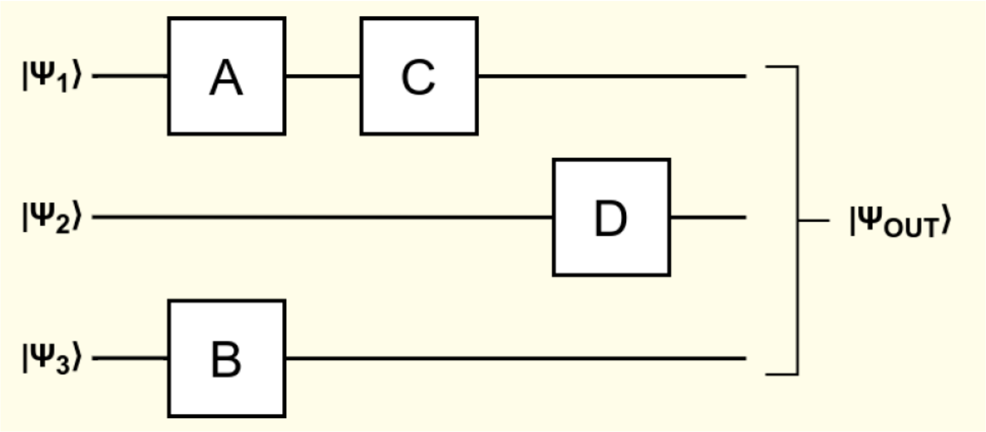
- In such a case, we describe the operation using **Kronecker product with the identity matrix**, e.g.: $X \otimes I$, giving

$$X \otimes I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

HOW TO ANALYZE QUANTUM CIRCUITS

Example of a circuit

- Let us consider the following circuit, where A, B, C and D represent generic gates



- To analyze this circuit, two steps have to be followed

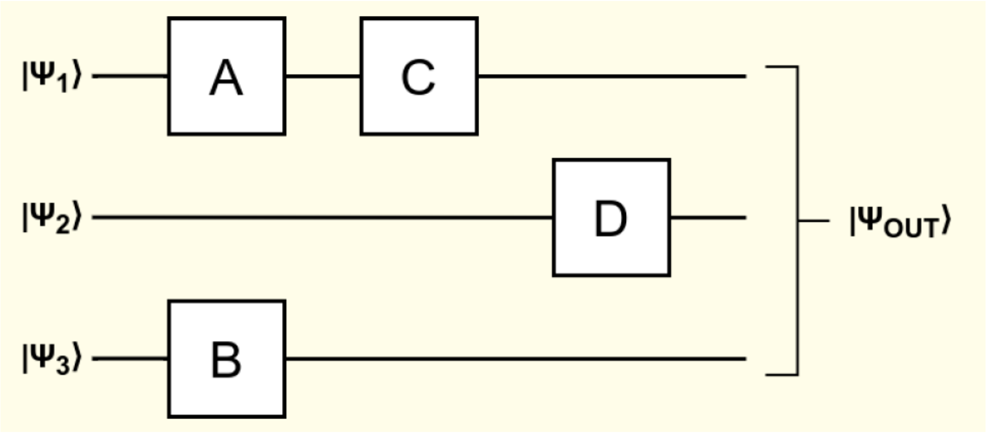
Example of a circuit

1) Write a unique expression for the three input qubits by performing the tensor product among them:

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle = |\psi_1\psi_2\psi_3\rangle$$

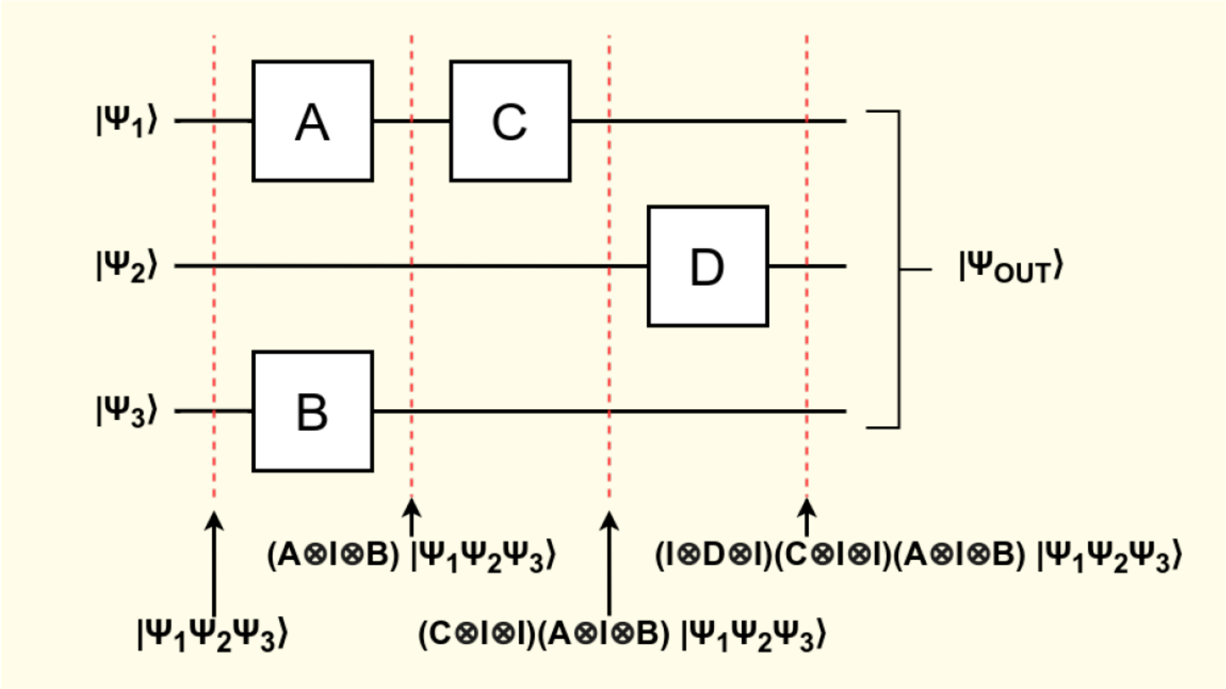
2) Compute the overall matrix function considering the gates from right to left (where I_k is the identity matrix of order k):

$$|\psi_{out}\rangle = (I_2 \otimes D \otimes I_2) \cdot (C \otimes I_4) \cdot (A \otimes I_2 \otimes B)\ |\psi_1\psi_2\psi_3\rangle$$



Example of a circuit

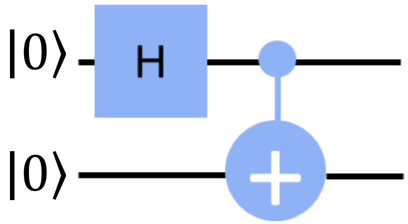
- The step-by-step analysis is shown here below



Example with H and CNOT gates

- In real quantum circuit analysis, we can follow two different strategies:
  - Exploiting the **matrix calculation**, as done before
  - Adopting a method based on **truth tables** of different gates, that can be faster

- Let us consider the circuit below



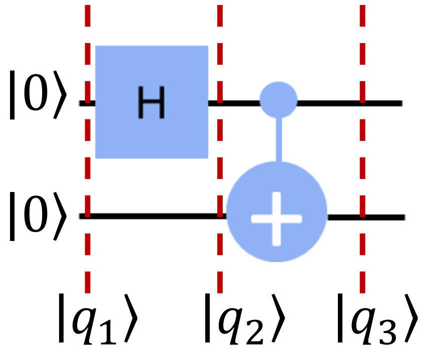
Example with H and CNOT gates

Matrix multiplication

- In this circuit we have two operators: the Hadamard gate and the CNOT gate, represented by the two unitary matrices

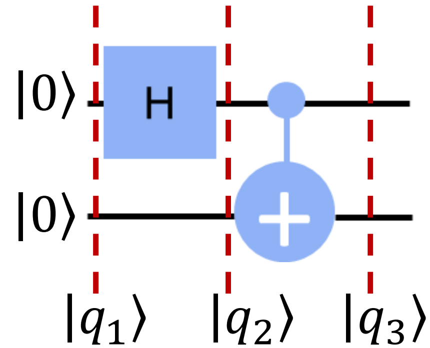
$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- We compute $|q_1\rangle$, $|q_2\rangle$ and $|q_3\rangle$ corresponding to the values shown in the figure



Example with H and CNOT gates

Matrix multiplication



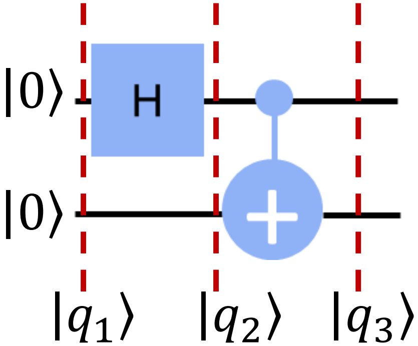
- $|q_1\rangle = |0\rangle \otimes |0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

- $|q_2\rangle = (H \otimes I)|00\rangle = \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} =$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Example with H and CNOT gates

Matrix multiplication



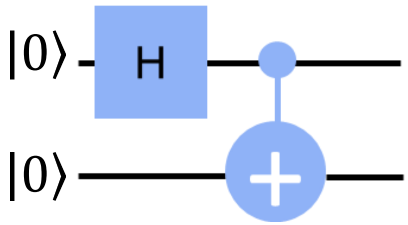
- $|q_3\rangle = CNOT \cdot \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) =$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} =$$

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

Example with H and CNOT gates

- We can look at this circuit also in a different way



- Applying the H gate to $|0\rangle$ we obtain state $|+\rangle$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

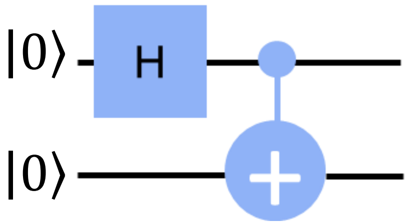
- So, we can see how CNOT gate acts on a qubit in superposition given by the state $|+\rangle$

Example with H and CNOT gates

- Before we apply the CNOT we have

$$|{+}0\rangle = |{+}\rangle \otimes |0\rangle = \mathrm{H}|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \times \begin{bmatrix}1\\0\end{bmatrix}\\ 1 \times \begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$



- When we **apply the CNOT gate**, we have the state

$$\mathrm{CNOT}|{+}0\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right)$$

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

Example with H and CNOT gates

Truth tables

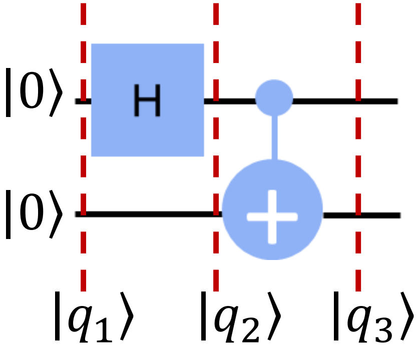
- The approach based on **truth tables** exploits the precomputed results that are listed in a table, as shown here below for the involved operators H and CNOT

Hadamard	CNOT
$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) = \|+\rangle$	$\mathrm{CNOT}\|0x\rangle = \|0x\rangle$
$H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) = \|-\rangle$	$\mathrm{CNOT}\|1x\rangle = \|1\bar{x}\rangle$

- It is typically much quicker to apply than the matrix method

Example with H and CNOT gates

Truth tables



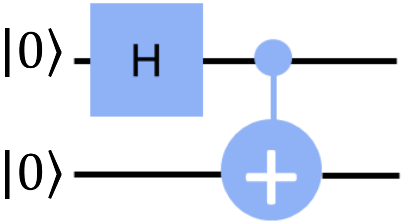
- $|q_1\rangle = |0\rangle \otimes |0\rangle = |00\rangle$
- $|q_2\rangle = H|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
- $|q_3\rangle = CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(CNOT|00\rangle + CNOT|10\rangle) =$

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

Entanglement with H and CNOT gates

- The circuit considered in the example produces one of the four ***Bell* states**

$$\text{CNOT}|+0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



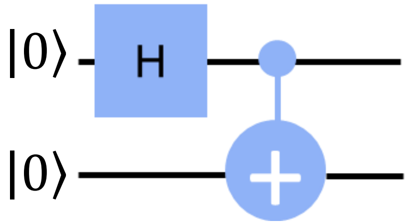
- As we said, this is an interesting state because the result is that the two qubits are ***entangled*** and we have:
  - **50%** probability of being measured in the state $|00\rangle$
  - **50%** probability of being measured in the state $|11\rangle$
  - And, most interestingly, it has a **0%** probability of being measured in the states $|01\rangle$ or $|10\rangle$
  - This combined state ***cannot*** be written as two separate qubit states

Entanglement with H and CNOT gates

- Although our qubits are in superposition, measuring one will tell us the state of the other and **collapse its superposition**

- For example, if we measured the top qubit and got the state $|1\rangle$ the **collective state of our qubits** changes like

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{\text{measure}} |11\rangle$$



- Even ***if we separated these qubits*** light-years away, measuring one qubit collapses the superposition and appears to have an *immediate effect on the other*