

Quantum Computing

Intensive Computation

Annalisa Massini
2022-2023

Lecture 18

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 $v = [v_0 \ \cdots \ v_{N-1}]^T$ and $w = [w_0 \ \cdots \ w_{N-1}]^T$ (T denotes transpose so v and w are vectors column vectors) is given by $\sum_0^{N-1} w_i^* v_i$ 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 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 transformations** 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: $\langle x| = [x_0 \quad x_1]$

- Any ket $|x\rangle$ has a corresponding bra $\langle x|$
- We can **convert** between them using the **conjugate transpose** (denoted by the $*$ 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

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

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

- The vectors $|0\rangle$ and $|1\rangle$
 - 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 **$|0\rangle$** or **$|1\rangle$**
- Since the **states $|0\rangle$ and $|1\rangle$ 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 $|0\rangle$ and $|1\rangle$ – 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:
- $$\begin{aligned} |q_0\rangle &= \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{i}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{i}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix} \end{aligned}$$

Qubit

- As we already 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:

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

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 $|1\rangle$ 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 $i|1\rangle$ are identical to those 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 $|\gamma| = 1$ as ***global phase***
- **States that differ only by a global phase ($|a\rangle$ 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 $|0\rangle$
 - 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**
$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \xrightarrow{\text{measure } |0\rangle} |\psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
- 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, since the absolute value of a complex number $z = a + ib$ is $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$, **all complex number with absolute value 1** can be expressed as $e^{i\gamma} = \cos \gamma + i \sin \gamma$ and it holds that $|e^{i\gamma}| = 1$
- 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

$$|\psi\rangle = r_1|0\rangle + r_2e^{i\varphi}|1\rangle$$

- with:

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

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

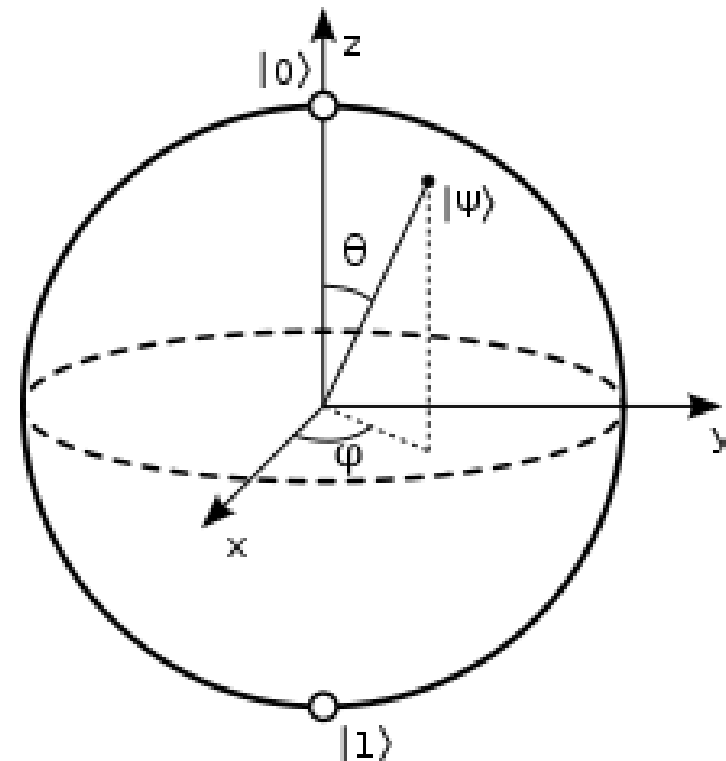
$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2} |1\rangle$$

Qubit

- We can describe the **state of any qubit** using the two **variables φ and θ** :

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

- 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**

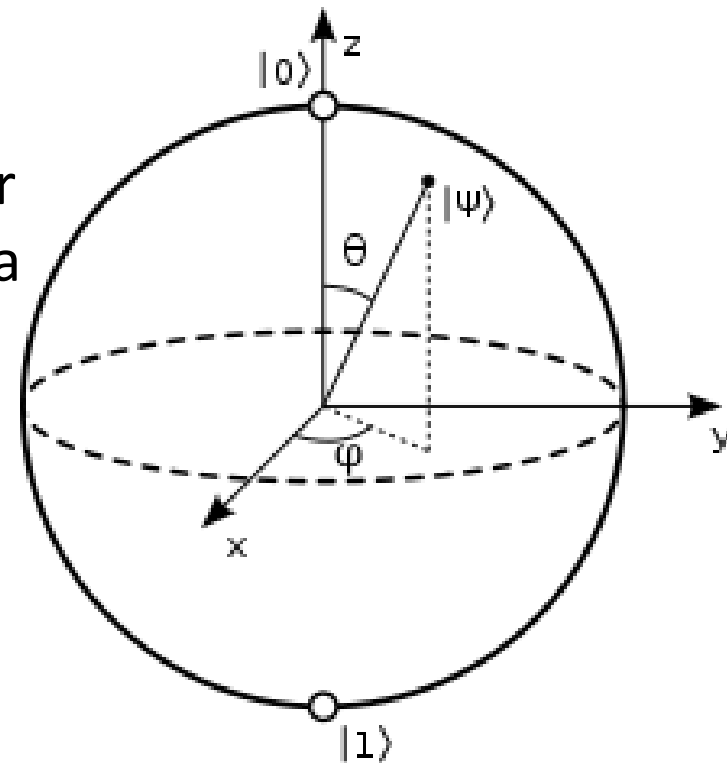


Qubit

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

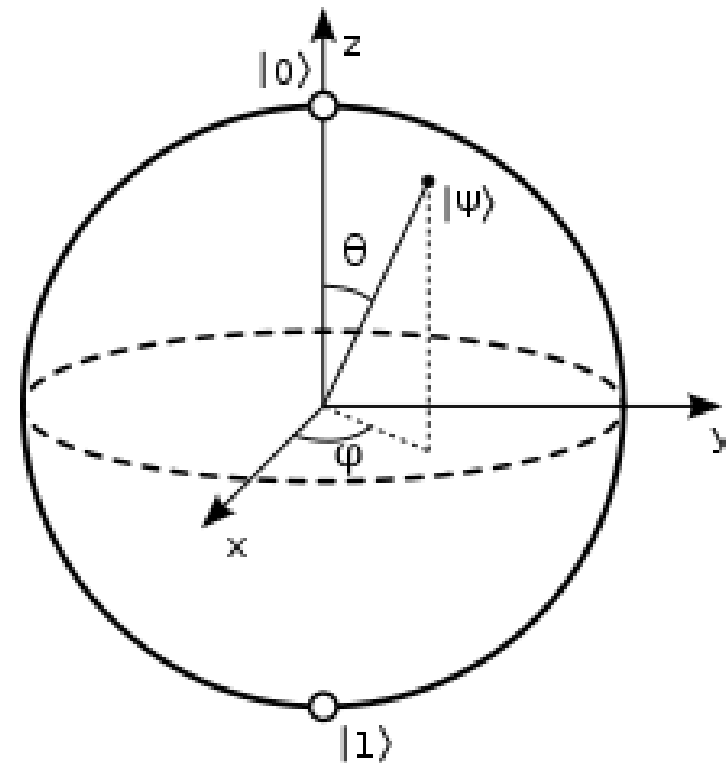
$$\begin{cases} x = \cos\phi \sin\theta \\ y = \sin\phi \sin\theta \\ z = \cos\theta \end{cases}$$

- 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 $x^2 + y^2 + z^2 = 1$



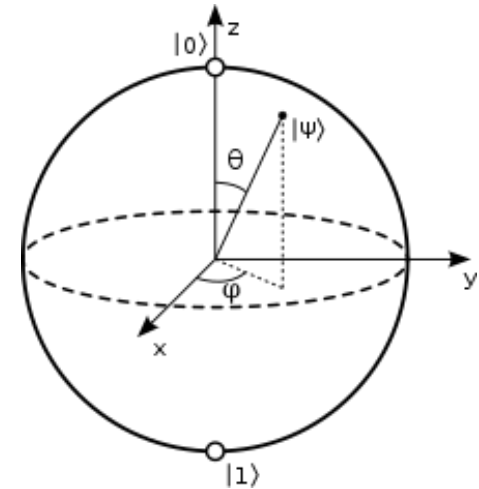
Qubit

- 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

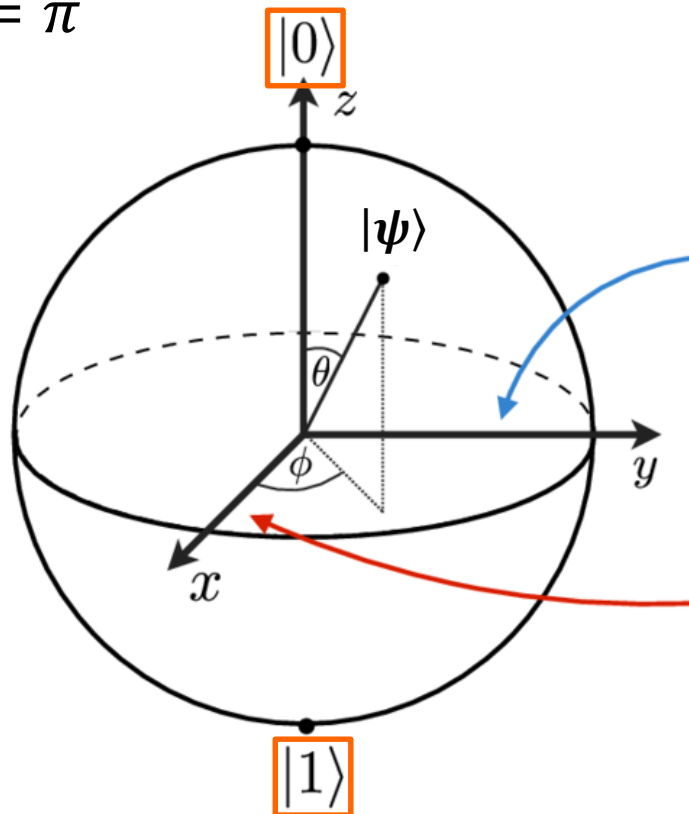
- For the generic state $|\psi\rangle$ we can write:



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

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 $\theta = \pi$



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

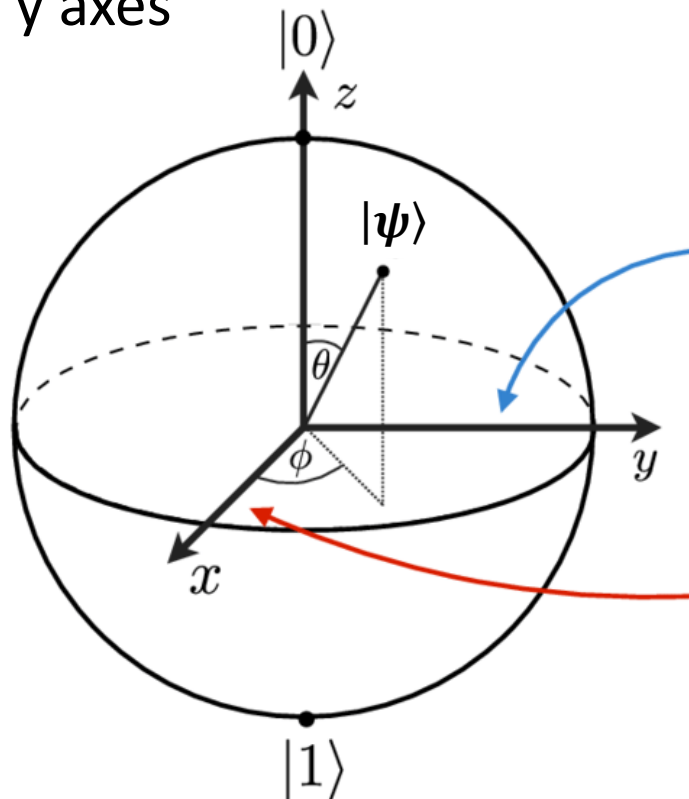
$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

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

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

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



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

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

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

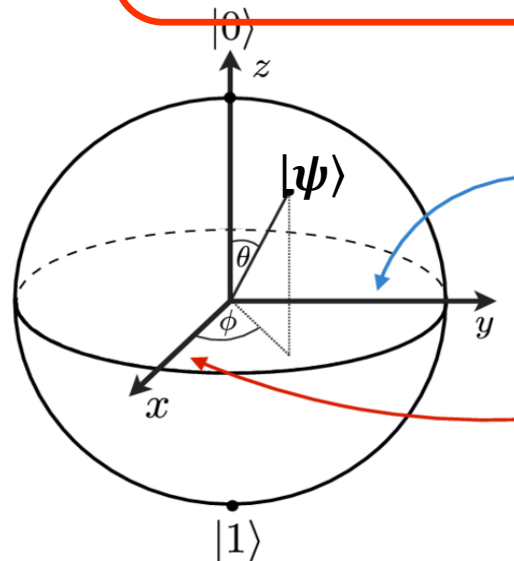
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Qubit

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

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

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



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

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

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

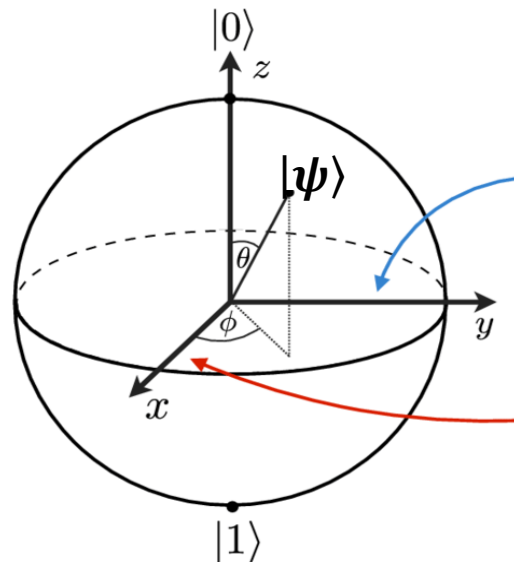
$$|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Qubit

- Another less commonly used basis is that formed by the eigenstates of the Y-gate:

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

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



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

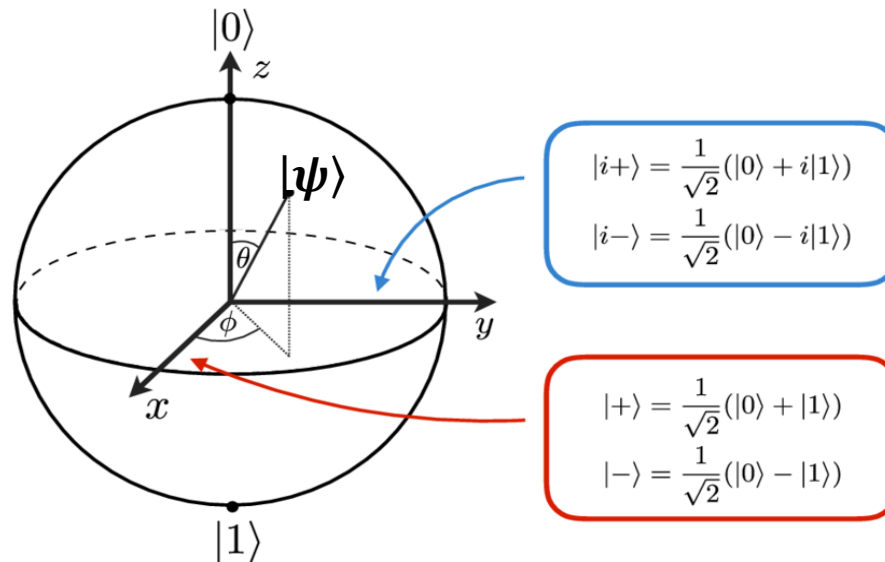
$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

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

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

Qubit

- Three pairs of basis elements:
 - $\{|0\rangle, |1\rangle\}$ Computational basis (Bloch sphere Z-axis)
 - $\{|+\rangle, |-\rangle\}$ Hadamard basis (Bloch sphere X-axis)
 - $\{|i+\rangle, |i-\rangle\} = \{|i+\rangle, |i-\rangle\}$ Circular basis (Bloch sphere Y-axis)



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

$$\begin{aligned} |\psi_1\psi_2\rangle &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle = \\ &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \end{aligned}$$

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

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

since

$$\begin{aligned} & (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \\ &= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle \end{aligned}$$

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**:

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

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

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

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

- 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
 - A complex square matrix U is called **unitary** if its **adjoint** and its **inverse** coincide, i.e.:

$$U^\dagger U = U U^\dagger = I$$

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 **n qubits** is represented by a **$2^n \times 2^n$ unitary matrix**, and the set of all such gates with the group operation of matrix multiplication is the symmetry group $U(2^n)$

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 2×2** , 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: 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**:

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

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

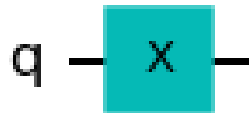
$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

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

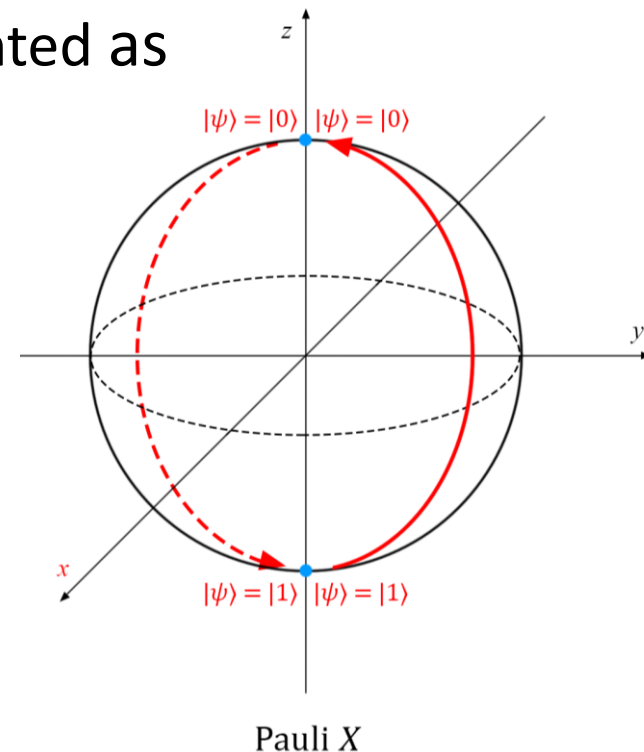
One-Qubit gates: the Pauli gates

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 this gate** in terms of a **rotation around the x-axis of π radians (180°)**



One-Qubit gates: the Pauli gates

The Pauli gates: Z-gate

- The **Z-gate** is able to flip the $|+\rangle$ state in $|-\rangle$ state (and vice versa)
- The **Z-gate** is represented by the **Pauli-Z matrix**:

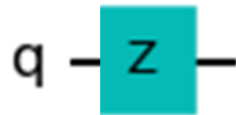
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

- Z-gate appears to have no effect on our qubit when it is in either of these two states
 - $Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$
 - This is because 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

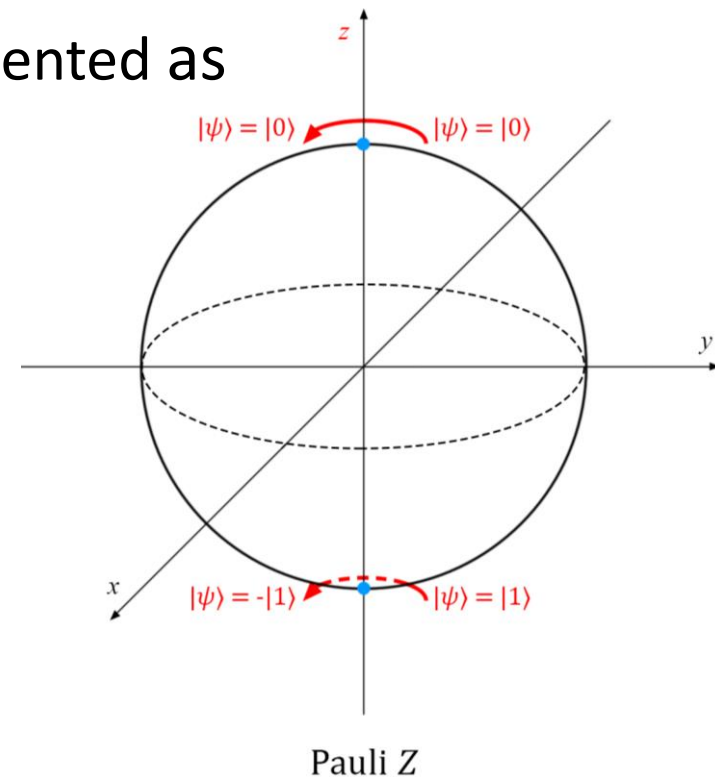
One-Qubit gates: the Pauli gates

The Pauli gates: Z-gate

- In general:
$$|\psi'\rangle = Z|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$
- In quantum circuits, the Z-gate is represented as



- By looking at the Bloch sphere, it is possible to interpret the action of this gate in terms of a rotation around the z -axis of π radians (180°)
- It has no effect on $|0\rangle$ but transforms $|1\rangle$ to $-|1\rangle$



One-Qubit gates: the Pauli gates

The Pauli gates: Y-gate

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

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

- 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

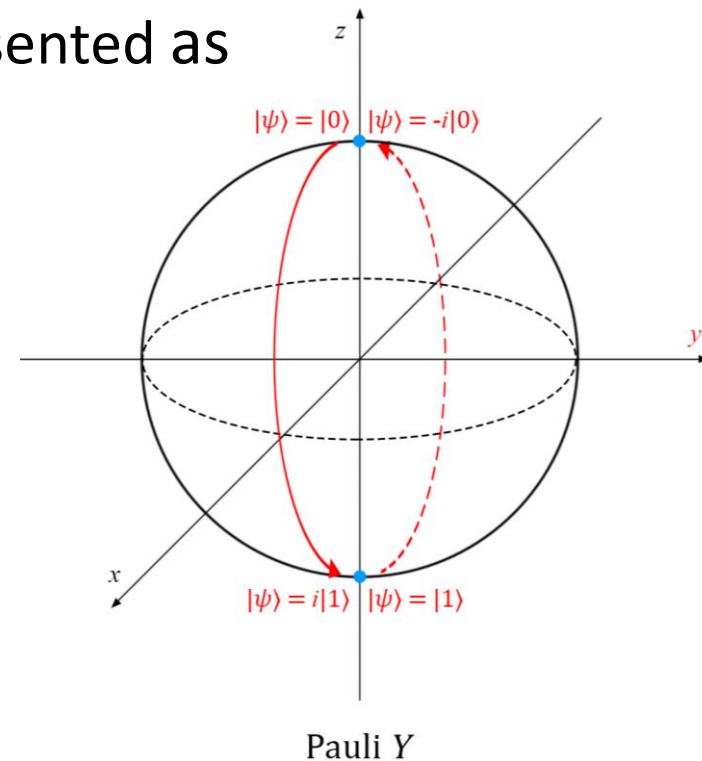
One-Qubit gates: the Pauli gates

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 Y-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°)**

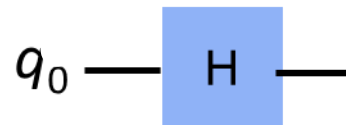


One-Qubit gates: the Hadamard Gate

- 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**
- 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