Quantum Computing

Claudio Tessa - 2024/2025

1 Introduction

1.1 Complex Numbers

In the realm of complex numbers, a number z can be expressed in different forms:

$$z = x + iy = r(\cos\varphi + i\sin\varphi) = re^{i\varphi}$$

where

- x is the real part
- y is the imaginary part
- r is the length of the vector
- φ is the radius between the vector and the real axis

A complex number can be **rotated by an angle** ψ by multiplying it with $e^{i\psi}$, which geometrically corresponds to rotating z by an angle ψ within the complex plane.

We define the **conjugate** of a complex number z as

$$\bar{z} = x - iy = re^{-i\varphi}$$

that is, changing the sign of the imaginary part.

We can now define the **Hermitian** of a vector of complex number $z = \begin{bmatrix} a \\ b \end{bmatrix}$, where a and b are complex. From here, the **conjugate transpose** of z is the vector $z^H = \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix}$.

1.2 Dirac's notation

Dirac notation (also knows as **bra-ket** notation), provides a way to represent quantum states. A central element of this notation is the **ket**, denoted as $|v\rangle = \vec{v}$, which corresponds to a **unitary column vector**.

The ket is used to represents a quantum state, characterized as a complex unit vector (i.e., with a length of one). Kets are used in conjunction with **bras**, which are row vectors denoted by $\langle v| = \vec{v}^H$. The bra $\langle v|$ represents the conjugate transpose of the ket $|v\rangle$.

On kets and bras we can perform multiplications:

- The scalar product between two kets $|x\rangle$ and $|y\rangle$ (that is, between two vectors $\vec{x}^H$ and $\vec{y}$) is represented as $\langle x|y\rangle = \vec{x}^H \cdot \vec{y}$.

- We often need to multiply a ket $\vec{v}$ (a column vector) with a matrix M. This is denoted as $M|v\rangle = M \cdot \vec{v}$.
- We can also concatenate multiplications, for example $\langle x|M|y\rangle = \vec{x}^H \cdot M \cdot \vec{y}$.

2 Qubits

Quantum bits (or **qubits**) are the fundamental units in quantum information processing, in the same way that bits are the fundamental units of information for classical processing. Just like classical bits, there are several ways to realize quantum bits physically. A qubit, however, has infinite possible values, differently from classical bits that can be either 0 or 1.

A qubit state is represented by a unit vector $|v\rangle$ of two complex numbers a and b:

$$|v\rangle = \begin{pmatrix} a \\ b \end{pmatrix} = a|0\rangle + b|1\rangle$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. These two vectors are called the **standard basis**, while the complex numbers a and b are called the **amplitudes**. When a and b are both non-zero, $|v\rangle$ is said to be a **superposition**.

When describing the state qubit, it is possible to use any pair of **orthonormal basis** $|u\rangle$ and $|u^\perp\rangle$:

$$|v\rangle = a|u\rangle + b|u^\perp\rangle$$

Remember that two vectors $|u\rangle$ and $|u^\perp\rangle$ are orthonormal if they are orthogonal and both unitary.

The most used basis, however, are the standard basis. Another set of useful basis are the Hadamard basis, denoted with labels $|+\rangle$ and $|-\rangle$:

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

2.1 Single-Qubit Measurements

Any device that measures a qubit must have two preferred states whose representative vectors $|u\rangle$ and $|u^\perp\rangle$ form an orthonormal basis (we will generally assume $|u\rangle = |0\rangle$ and $|u^\perp\rangle = |1\rangle$). The measurement outcome is always one of the two basis vectors $|u\rangle$ or $|u^\perp\rangle$. This behavior of measurement is an **axiom** of quantum mechanics.

Consider the qubit $|v\rangle = a|u\rangle + b|u^\perp\rangle$. The probability that the state of the qubit is measured as $|u\rangle$ is $|a|^2$. Similarly, The probability that the state is measured as $|u^\perp\rangle$ is $|b|^2$.

Measurement of a qubit changes its state. If a qubit $|v\rangle = a|u\rangle + b|u^\perp\rangle$ is measured as $|u\rangle$, then the state changes to $|v\rangle = 1|u\rangle + 0|u^\perp\rangle = |u\rangle$. A second measurement with respect to the same basis will return $|u\rangle$ with probability 1.

While the mathematics of measuring a qubit in the superposition state $a|0\rangle + b|1\rangle$ with respect to the standard basis is clear, measurement brings up questions as to the meaning of a superposition. Superposition is basis dependent: all states are in superpositions with respect to some basis and not with respect to others

Because the result of measuring a superposition is probabilistic, some people are tempted to think of the state $|v\rangle = a|0\rangle + b|1\rangle$ as a probabilistic mixture of $|0\rangle$ and $|1\rangle$. **It is not**. In particular, it is not true that the state is either $|0\rangle$ or $|1\rangle$ and that we just do not happen to know which. Rather, $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results.

Given that qubits can take one of infinitely many states, one might hope that a single qubit could store lots of classical information. However, information about a qubit can be obtained only by measurement, and any measurement result in one of only two states. Thus, a single measurement yields at most a single classical bit of information. Because the measurement changes the state, one cannot make two measurements on the original state of a qubit.

> Note that if you have a qubit in state $|v\rangle = a|0\rangle + b|1\rangle$ with a and b unknown, **is is impossible to measure a and b**. Furthermore, a quantum state cannot be cloned. It is not possible to measure a qubit's state twice, even indirectly by copying the qubit's state and measuring the copy

2.2 Global Phase of a Qubit

Let's consider two qubits:

$$|v\rangle = a|0\rangle + b|1\rangle \qquad\qquad |v'\rangle = e^{i\varphi}|v\rangle$$

where $e^{i\varphi}$ is a unitary complex number (of length 1). Therefore, the amplitudes of v' and v have the same "lengths". Then, the two vectors $|v\rangle$ and $|v'\rangle$ describe **the same qubit**. To denote this, we write

$$|v\rangle = |v'\rangle$$

$|v\rangle$ and $|v'\rangle$ differ only from a rotation φ which is called **global phase** and has no physical meaning.

Apparently, there are four degrees of freedom (independent parameters needed to fully describe the state) in a qubit $|v\rangle = a|0\rangle + b|1\rangle$, as a and b are complex numbers (and therefore made up of 2 parameters each). However, one degree of freedom is removed by the **normalization constraint** $|a|^2 + |b|^2 = 1$.

We can therefore rewrite the qubit as

$$|v\rangle = e^{i\alpha}\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\beta}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

then, multiplying by $e^{-i\alpha}$ (the **global phase** has no consequences) and setting $\varphi = \beta - \alpha$, we can rewrite $|v\rangle$ in **spherical coordinates** (Bloch sphere):

$$|v\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$\varphi = \beta - \alpha$ is called **relative phase** and it is physically meaningful. It is a measure of the angle in the complex plane between the two complex numbers a and b.

3 Single-Qubit Gates

Quantum logic gates are the fundamental components of quantum circuits, analogous to classical logic gates. These gates operate on single or multiple qubits, manipulating their quantum states and, in the case of multi-qubit gates, creating entanglement. A key characteristic of quantum logic gates is their reversibility, meaning the input state can always be recovered from the output state.

Mathematically, while qubits are vectors, gates are matrices. The action of the gare on the qubit is found by multiplying vector $|v\rangle$, which represents the state of the qubit, by matrix U, representing the gate. The result is a qubit in a new state:

$$|v'\rangle = U|v\rangle$$

In particular, a gate is a 2x2 **unitary** matrix U. Unitary, in the case of a matrix, means that

$$U^H U = UU^H = UU^{-1} = I$$

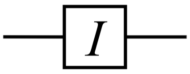
The matrix is unitary because it must satisfy some principles of quantum mechanic:

- **No-cloning**: qubits cannot be copied.
- **No-delete**: state transformation of a qubit is reversible, $|v\rangle = U^H|v'\rangle$

There exist many types of quantum gates. However, it is possible to identify the minimum number of gates such that, combining them, one can obtain all other gates. These make up the **universal set** of gates. Any quantum computer has to at least implement the universal set of gates.

All quantum gates are equivalent to rotations, since all qubits are on the Bloch sphere, and a gate is transforming a qubit into another qubit (therefore into another point on the sphere).

3.1 Identity gate

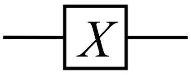


$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$|v\rangle = I|v\rangle$$

Apparently useless, but it is not. It is useful with multiple qubits circuits.

3.2 Pauli-X gate (Not)



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

Amplitudes a and b are **exchanged**. If $|v\rangle = a|0\rangle + b|1\rangle$ we have

$$X|v\rangle = b|0\rangle + a|1\rangle$$

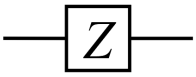
It is equivalent to a **rotation around the *x*-axis by π radians**. This rotation requires $\theta \to \pi - \theta$ and $\varphi = -\varphi$. Therefore, with $|v\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ we obtain

$$|v'\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle + e^{-i\varphi}\cos\left(\frac{\theta}{2}\right)|1\rangle$$

then, if we multiply $|v'\rangle$ by $e^{i\varphi}$ (unit vector, same qubit), we can see that $|v'\rangle$ is the same as $|v\rangle$ with a and b swapped:

$$|v'\rangle = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle$$

3.3 Pauli-Z gate (Phase Flip)



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

Changes the sign of b. If $|v\rangle = a|0\rangle + b|1\rangle$ we have

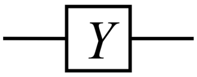
$$Z|v\rangle = a|0\rangle - b|1\rangle$$

It is equivalent to a **rotation around the *z*-axis by π radians**. This rotation requires $\varphi \to \varphi + \pi$ ($e^{i(\varphi+\pi)} = -e^{i\varphi}$). Therefore, with $|v\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ we obtain

$$|v'\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle - e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

We can see that $|v'\rangle$ is the same as $|v\rangle$ with b negative:

3.4 Pauli-Y gate



$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

It is equivalent to a **rotation around the *y*-axis by π radians**. Moreover, $Y = iXZ$ (i is a global phase and can be neglected). X and Z are two π rotations around the *x*-axis and the *y*-axis, which is equivalent to a π rotation around the *y*-axis.

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

$$\implies Y = \begin{bmatrix} 0 & -1 \\ i & 0 \end{bmatrix} = -i \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iXZ$$

3.5 Phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

It is equivalent to a **rotation around the *z*-axis by $\frac{\pi}{2}$ radians**. If you perform two consecutive rotations with gate S, it is equivalent to one rotation with gate Z:

$$S \cdot S - \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

3.6 Hadamard gate

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

It is equivalent to a **rotation around the *y*-axis by $\frac{\pi}{2}$ radians, followed by a rotation around the *x*-axis by π radians**. Note that:

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

$|+\rangle$ and $|-\rangle$ are relevant states (Hadamard states), since for both of them $|a|^2 = |b|^2 = \frac{1}{2}$. This gives the qubit equal probability of being measured as $|0\rangle$ or $|1\rangle$ (**maximum superposition**). It is often used to prepare qubits in superposition states.

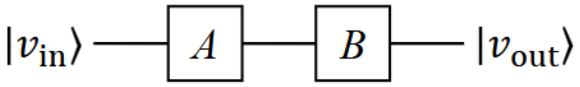
Note that all quantum gates are equivalent to rotations on the Bloch sphere. If you apply twice the same Pauli gate you go back to the initial qubit:

$$X^2 = Y^2 = Z^2 = I$$

Moreover, for a gate to create a superposition from a base state, all elements of the gate must be different from zero.

4 Single-Qubit quantum circuits

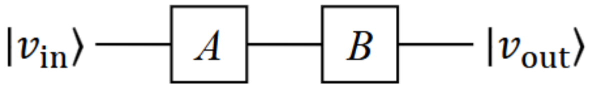
Quantum circuits are a model for quantum computation. They are a sequence of initializations of qubits to known values, gates, measurements, and possibly other actions.



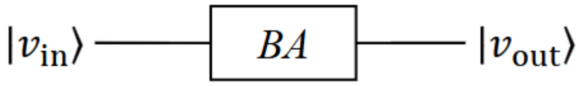
Here, lines define the sequence of events. Horizontal lines are qubits, while the objects connected by lines are operations (gates, measurements) performed on qubits. Double lines represent classical bits instead. Note that **lines are not physical connections**.

4.1 Serial gates

Consider the following quantum circuit.



with gates B directly after gate A. Then, the effect of the two gates can be described as a single gate $C = BA$:



Note that the multiplication is **from right to left** with respect to the order in which gates appear in the circuit:

$$|v_{\text{out}}\rangle = C|v_{\text{in}}\rangle = BA|v_{\text{in}}\rangle$$

4.2 Bra-ket notation: outer product of kets

The **outer product** between kets $|a\rangle = \begin{bmatrix}a_1\\a_2\end{bmatrix}$ and $|b\rangle = \begin{bmatrix}b_1\\b_2\end{bmatrix}$ is a 2×2 matrix represented with the notation $|a\rangle\langle b|$ and defined as:

$$|a\rangle\langle b| = \vec{a} \otimes \vec{b}^H = \begin{bmatrix}a_1\\a_2\end{bmatrix} \otimes \begin{bmatrix}\bar{b}_1 & \bar{b}_2\end{bmatrix} = \begin{bmatrix}a_1\bar{b}_1 & a_1\bar{b}_2\\ a_2\bar{b}_1 & a_2\bar{b}_2\end{bmatrix}$$

The outer product is an element-by-element product between the first vector and the Hermitian of the second vector. $\otimes$ is the **tensor product** operator.

The outer and scalar product have this useful property:

$$(|a\rangle\langle b|)|c\rangle = |a\rangle\,\langle b|c\rangle = \langle b|c\rangle|a\rangle$$

Remember that $|a\rangle\langle b|$ is a matrix, and $\langle b|c\rangle$ is a scalar.

Proof

We want to prove that $(|a\rangle\langle b|)|c\rangle = |a\rangle\,\langle b|c\rangle = \langle b|c\rangle|a\rangle$, where $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$, $|b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$, and $|c\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$.

Use the definition of outer product and apply the inner product:

$$(|a\rangle\langle b|)|c\rangle = \begin{bmatrix} a_1\bar{b}_1 & a_1\bar{b}_2 \\ a_2\bar{b}_1 & a_2\bar{b}_2 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a_1\bar{b}_1c_1 + a_1\bar{b}_2c_2 \\ a_2\bar{b}_1c_1 + a_2\bar{b}_2c_2 \end{bmatrix}$$

observe that $\begin{bmatrix} a_1\bar{b}_1c_1 + a_1\bar{b}_2c_2 \\ a_2\bar{b}_1c_1 + a_2\bar{b}_2c_2 \end{bmatrix} = \begin{bmatrix} a_1(\bar{b}_1c_1 + \bar{b}_2c_2) \\ a_2(\bar{b}_1c_1 + \bar{b}_2c_2) \end{bmatrix}$, and $(\bar{b}c_1 + \bar{b}c_2)$ is the inner product $\langle b|c\rangle$. Therefore, we can rewrite the result as

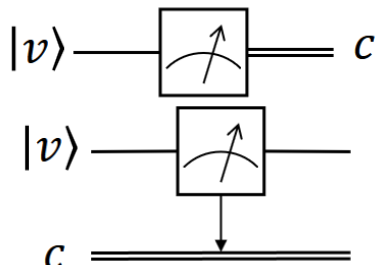
$$(|a\rangle\langle b|)|c\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \langle b|c\rangle = |a\rangle\,\langle b|c\rangle$$

4.3 Measurement of a Qubit

The **measurement** (or **projection**) operator is a special **non-unary** (and **non-invertible**) 2×2 matric M_k such that

$$M_k = |k\rangle\langle k|$$

which projects a qubit $|v\rangle$ along a vector $|k\rangle$.



After the projection, the resulting state **could be** (probabilistic)

$$|v\rangle_k = \frac{M_k|v\rangle}{\langle v|M_k|v\rangle}$$

which does **not** correspond to a rotation.

The **probability** of the measurement to be $|v_k\rangle$ is

$$p_k = \langle v|M_k|v\rangle$$

in the standard basis $M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

4.3.1 Property of the Measurement Operator

Once applied, M_k does not change the vector anymore, if it is applied twice:

$$M_k^2 = M_k M_k = M_k$$

Proof 1

Define $|k\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$. Now compute:

- $M_k = |k\rangle\langle k| = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix}$
- $M_k^2 = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} = \begin{bmatrix} a^4 + a^2b^2 & a^3\bar{b} + a\bar{b}b^2 \\ b\bar{a}a^2 + b^3\bar{a} & b^4 + a^2b^2 \end{bmatrix} = \begin{bmatrix} a^2 \cancel{(a^2 + b^2)} & a\bar{b}\cancel{(a^2 + b^2)} \\ b\bar{a}\cancel{(a^2 + b^2)} & b^2\cancel{(a^2 + b^2)} \end{bmatrix}$

Remembering that $a^2 + b^2 = 1$, thus

$$M_k^2 = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} = M_k$$

Proof 2

We want to prove that the application of M_k to ket $|v\rangle$ projects $|v\rangle$ on vector $|k\rangle$.

From the definition of $M_k = |k\rangle\langle k|$, apply M_k to $|v\rangle$:

$$M_k|v\rangle = |k\rangle\langle k||v\rangle = \langle k|v\rangle|k\rangle$$

remember that $\langle k|v\rangle$ is the cosine of the angle between $|k\rangle$ and $|v\rangle$. Therefore, the resulting vector has the same direction of $|k\rangle$, scaled by $\langle k|v\rangle$.

5 Multiple-Qubits States

Given two qubits

$$|v_A\rangle = a_0|0\rangle + a_1|1\rangle, \qquad |v_B\rangle = b_0|0\rangle + b_1|1\rangle$$

we with to know their combined state. In other words, we want to know the probability for the two qubits to be

- both in state $|0\rangle$; or
- the first one in state $|0\rangle$ and the second one in state $|1\rangle$; or
- the first one in state $|1\rangle$ and the second one in state $|0\rangle$; or
- both in state $|1\rangle$.

The two qubits do not necessarily interact with each other.

The state of the two qubits $|v_A\rangle$ and $|v_B\rangle$ is described with their **tensor product**

$$|v_A\rangle \otimes |v_B\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

for this, we can introduce a new compact notation:

$$|v_A v_B\rangle = |v_A\rangle \otimes |v_B\rangle$$

Note that the opposite is not always true. A vector of 4 element cannot always be decomposed into the tensor product of 2 qubits.

We can rewrite $|v_A v_B\rangle$ as

$$\begin{aligned} |v_A v_B\rangle &= a_0 b_0 \underbrace{(|0\rangle \otimes |0\rangle)}_{|00\rangle} + a_0 b_1 \underbrace{(|0\rangle \otimes |1\rangle)}_{|01\rangle} + a_1 b_0 \underbrace{(|1\rangle \otimes |0\rangle)}_{|10\rangle} + a_1 b_1 \underbrace{(|1\rangle \otimes |1\rangle)}_{|11\rangle} \\ &= a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle \end{aligned}$$

So we have:

- $(a_0 b_0)^2$ probability of being in state $|00\rangle$
- $(a_0 b_1)^2$ probability of being in state $|01\rangle$
- $(a_1 b_0)^2$ probability of being in state $|10\rangle$
- $(a_1 b_1)$ probability of being in state $|11\rangle$

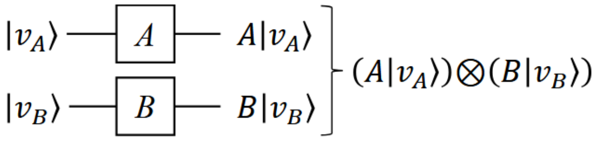
Moreover, the combined amplitudes also normalize to 1. In fact, we can rewrite the sum of the square of the amplitudes as

$$a_0^2 b_0^2 + a_0^2 b_1^2 + a_1^2 b_0^2 + a_1^2 b_1^2 = a_0^2 \underbrace{(b_0^2 + b_1^2)}_{1} + a_1^2 \underbrace{(b_0^2 + b_1^2)}_{1} = a_0^2 + a_1^2 = 1$$

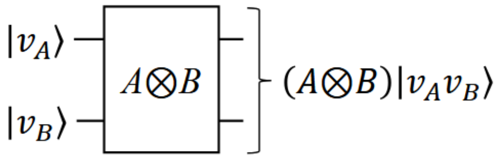
5.1 Multiple-Qubits Circuits (Parallel Gates)

Applying single gates to two independent qubits, corresponds to

Applying single gates A and B to two independent qubits, initially in states $|v_A\rangle$ and $|v_B\rangle$ respectively, corresponds to applying the tensor product of those gates, $A \otimes B$, to the combined state of the two qubits, $|v_A\rangle \otimes |v_B\rangle$. The resulting state is $(A \otimes B)(|v_A \otimes |v_B\rangle\rangle)$, which is equivalent to the tensor product of the individual resulting states, $(A|v_A\rangle) \otimes (B|v_B\rangle)$:

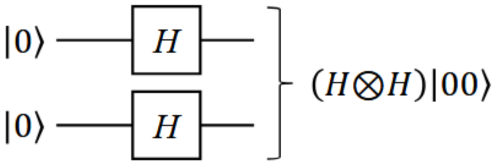


This is represented as a single composite gate $A \otimes B$:



5.1.1 The $H^{\otimes n}$ Hadamard Transform

A particular case is the one with the Hadamard gate:



this case is so common that we define a particular notation for this **Hadamard transform**:

$$H^{\otimes n}$$

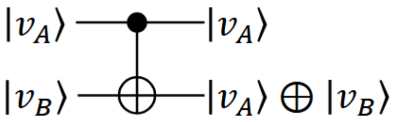
is the Hadamard transform of n qubits. The example in the previous figure shows the $H^{\otimes 2}$, Hadamard transform of 2 qubits.

The Hadamard transform places the state in a **uniform** superposition (equal probability of being in any state).

6 Multiple-Qubits Gates

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

Controlled NOT (CNOT)



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

where $\oplus$ is the XOR operator.

If the control qubit $|v_A\rangle$ is $|1\rangle$, then the target qubit v_B is flipped. In other words, if we apply the CNOT gate to $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$, that is

$$|v_A v_B\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle$$

we invert the last two amplitudes:

$$CNOT|v_A b_A\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_1 \\ a_1 b_0 \end{bmatrix}$$

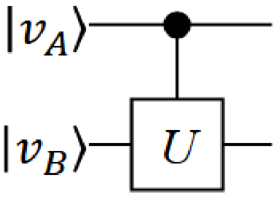
More **in general**, if we apply the CNOT gate to

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

we invert the two amplitudes c_2 and c_3

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

Generic Controlled Gate



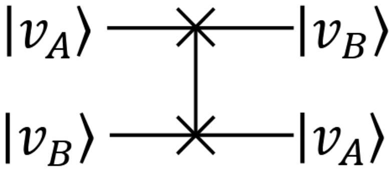
$$C_U = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$$

If control qubit $|v_A\rangle$ is $|1\rangle$, then target gate U is applied to qubit $|v_B\rangle$. In other words, if we apply the generic controlled gate C_U to $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$ we obtain

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

Note that $\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$ is **not equivalent** to $I \otimes U$.

SWAP



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

The state of $|v_A\rangle = a_0|0\rangle + a_1|1\rangle$ and $|v_B\rangle = b_0|0\rangle + b_1|1\rangle$, described with their tensor product

$$|v_A v_B\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle$$

is swapped after we apply the SWAP gate:

$$SWAP|v_A v_B\rangle$$

fino a pag 31