Quantum Computing
A Practical Perspective

Marco Venere

marco.venere@polimi.it

November 7th, 2024
Politecnico di Milano

Who I am

- Second-year PhD student in Information Techology

- MSc in Computer Science and Engineering at PoliMi

- Research Interests:

  - Quantum Computing

  - High-Performance Computing

  - Hardware Design

Course Objectives

- Design, develop, and analyze algorithms for quantum computers

- Visualize and analyze quantum circuits and their output

- Practical examples of well-known algorithms belonging to State of the Art

- Exploit MathWorks MATLAB Support Package for Quantum Computing to study algorithms and design new circuits

Agenda

- Lecture 1 → Theory Recap on Quantum Computing

- Lecture 2 → Initial Setup and First Experiments

- Lecture 3 → Grover's Algorithm

- Lecture 4 → Combinatorial Optimization

- Lecture 5 → VQE, QNN, QMC

- Lecture 6 → Quantum Error Correction & Mitigation – Projects Presentation

Online Material

Material is uploaded online in the following Dropbox folder: link

Here you can find:

- slides for the lectures

- live scripts for the tutorial sessions

- recordings of the lectures

MATLAB OnRamp

In case you don't know how to use MATLAB, please follow this easy tutorial: link

You will find useful material and basics on programming with MATLAB.

Quantum Computing: A New Paradigm

Quantum Computing is a new paradigm of computation, exploiting laws of quantum mechanics to achieve an exponential speedup w.r.t. classical computation
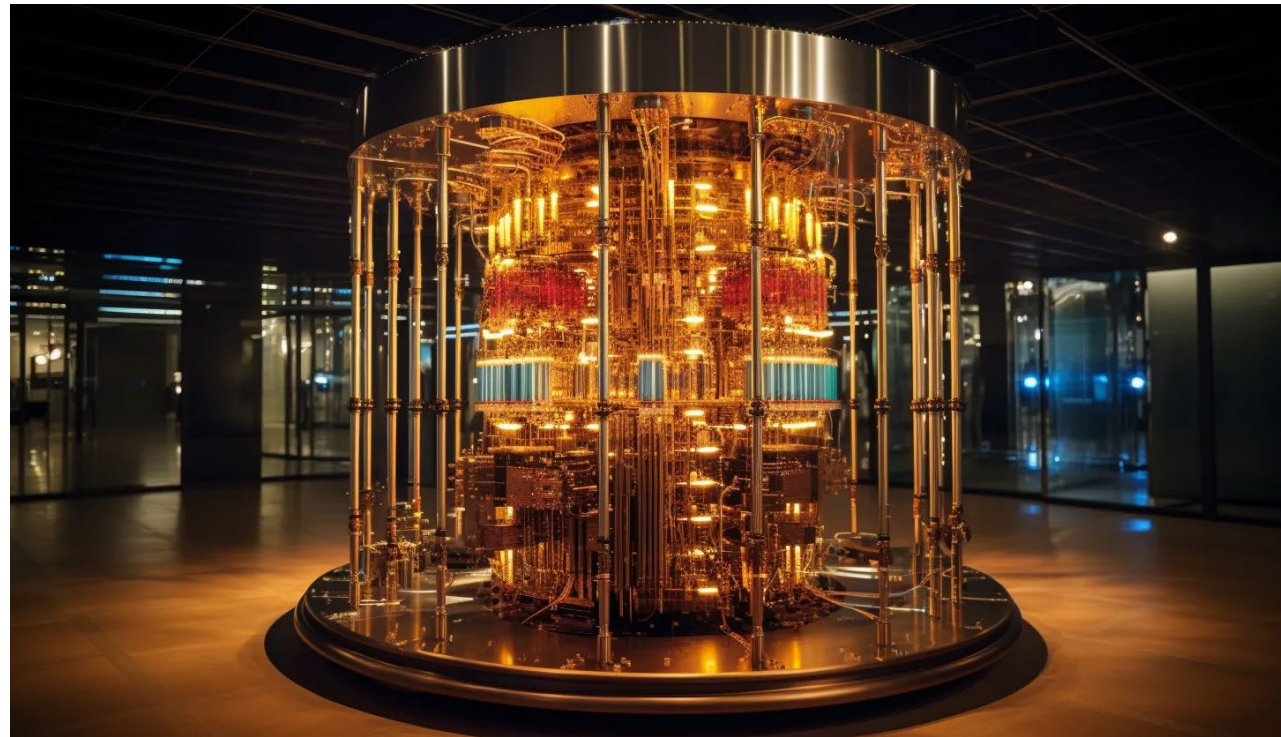
Quantum Computing: Several Use Cases

A great number of use cases is rapidly growing up:

- Combinatorial Optimization

- Machine Learning

- Drug Design and Test

- Physical Systems Simulation

- Secure Communications

Qubits

The basic unit of information is the **qubit**. A qubit can be represented as a vector with two complex components:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

(Dirac) **bra-ket** notation

$$\alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

Since they are vectors, they belong to a vector space. One of the possible basis is:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(a.k.a. **computational basis**)

We can think of these two qubits as the quantum version of the classical bits **0** and **1**!

Quantum Superposition

In classical computation, every bit can only have **one** possible state: either 0 or 1.

In quantum computing, a generic qubit can represent a **superposition** of two states:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle \qquad \begin{array}{l} \alpha, \beta \in \mathbb{C} \\ |\alpha|^2 + |\beta|^2 = 1 \end{array}$$

Quantum physics allows for superposition, often used to get **exponential speedup**!

From the perfect superposition of $|0\rangle$ and $|1\rangle$, we get:

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ and } |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \qquad \text{(a.k.a. \textbf{Hadamard basis})}$$

Bra-Ket Notation

The most commonly used notation for qubits is the Dirac Bra-Ket notation.

Every qubit is represented as a **ket** (column vector in $\mathbb{C}^2$):

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Its Hermitian transpose (a.k.a. complex conjugate transpose) is the **bra** (row vector in $\mathbb{C}^2$):

$$\langle\phi| = |\phi\rangle^\dagger = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

Bras do not represent qubits, but they are useful tools that we can use for specific cases.

Inner Product Between Qubits

Qubits are vectors, and they support inner product.

Let's assume that we want to compute $|0\rangle \cdot |\psi\rangle$. We are going to exploit bra-ket notation:

$$\langle 0||\psi\rangle = \langle 0 | \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \langle 0 |(\alpha|0\rangle + \beta|1\rangle) = \alpha\langle 0||0\rangle + \beta\langle 0||1\rangle$$

Due to their definition, $|0\rangle$ and $|1\rangle$ are orthonormal (and their bra versions are as well):

$$\alpha\langle 0||0\rangle + \beta\langle 0||1\rangle = \alpha \cdot 1 + \beta \cdot 0 = \alpha$$

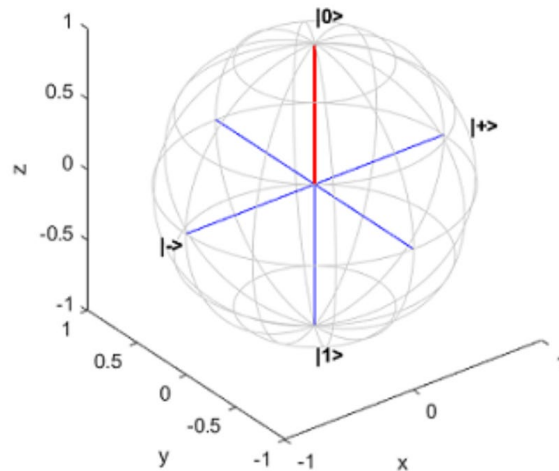It makes sense: we are projecting $|\psi\rangle$ over $|0\rangle$, thus the result is simply α.

Usually, $\langle\phi||\psi\rangle$ is abbreviated in $\langle\phi|\psi\rangle$.

Bloch Sphere

Qubits can be represented in spherical coordinates on the **Bloch Sphere**:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi \leq 2\pi$$

You can see that $|+\rangle$ and $|-\rangle$ are the perfect superposition of $|0\rangle$ and $|1\rangle$!

https://it.mathworks.com/help/matlab/math/introduction-to-quantum-computing.html

Physical Qubit Implementation

Qubits can be physically implemented in a number of possible ways:

- Superconducting qubits are artificial atoms. They encode $|0\rangle$ and $|1\rangle$ as a **ground state** and an **excited state**. They require very low temperature (about 15 mK), and are usually built via superconducting material, often using **LC circuits**.

- Quantum Dots are semiconductor particles that are illuminated by UV light. Doing so, an electron in the quantum dot can get excited to represent a change in quantum information.

- Neutral Atom and trapped-ion QCs trap and place particles in a magnetic field. Their energy level encodes quantum information.

Operations on 1 qubit

In classical computing, given one bit, the following operations can be performed:

Constant 0: $0 \rightarrow 0, \ 1 \rightarrow 0$ **Constant 1:** $0 \rightarrow 1, \ 1 \rightarrow 1$

Identity: $0 \rightarrow 0, \ 1 \rightarrow 1$ **Negation**: $0 \rightarrow 1, \ 1 \rightarrow 0$

In quantum computing, we can perform **infinite** possible operations on one qubit:

$|\psi\rangle \rightarrow U|\psi\rangle$ where U is a **unitary matrix**: $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ $\alpha, \beta, \gamma, \delta \in \mathbb{C}$

Unitary: its inverse U^{-1} equals its transpose conjugate $U^{\dagger}$.

Operations on qubits are also called **gates**. They must be **reversible**.

Important Gates on 1 qubit

Here are some very important gates you should remember:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

X, Y, and Z are also called **Pauli** matrices: in quantum mechanics, they describe the interaction of the spin of a particle with an external electromagnetic field.

The four matrices I, X, Y, and Z form a basis for the vector space of the 1-qubit gates: every gate U can be represented as a linear combination of these 4 matrices!

The effect of these gates

Let's see what happens when we apply these operations to one qubit:

$$I: \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

This is an **identity** gate!

$$X: \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

This is the quantum equivalent of the **negation**! Indeed:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \text{ and } X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

The effect of these gates – cont'ed

$$Z: \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

We are changing the sign of the second component: this is a **phase flip**! Indeed:

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \text{ and } Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

Finally, we can show that $Y = i\,XZ$.

Important Gates on 1 qubit – cont'ed

Other important gates:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ is the Hadamard gates

This gate is very useful to create perfect superpositions:

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

The two components of the qubit are now identical!

Important Gates on 1 qubit – cont'ed

Other important gates:

These gates perform a generic rotation around x, y, and z axes.

$$R_X = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$R_Y = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ -\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$R_Z = \begin{pmatrix} \exp\left(-i\frac{\theta}{2}\right) & 0 \\ 0 & \exp\left(i\frac{\theta}{2}\right) \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(i\frac{\pi}{2}\right) \end{pmatrix}$$

Measurement of a Qubit: Observable Z

Unfortunately, we cannot directly access the state of a qubit, i.e., α and β.

Instead, we need to perform a **measurement**. Using quantum jergon, we say that we measure an **observable**, which is a physical property of the quantum system.

Usually, we measure the observable Z ($|0\rangle$ and $|1\rangle$), and the output of the measurement is:

$$m = \begin{cases} +1 \text{ with probability } |\langle 0|\psi\rangle|^2 = |\alpha|^2 \\ -1 \text{ with probability } |\langle 1|\psi\rangle|^2 = |\beta|^2 \end{cases} \qquad (\textbf{Born Rule})$$

For this reason, α and β are also called **probability amplitudes**.

Measurement of a Qubit: Observable X

We can also measure observable X ($|+\rangle$ and $|-\rangle$), exploiting the Born rule:

$$m = \begin{cases} +1 \text{ with probability } |\langle+|\psi\rangle|^2 = \frac{|\alpha+\beta|^2}{2} \\ -1 \text{ with probability } |\langle-|\psi\rangle|^2 = \frac{|\alpha-\beta|^2}{2} \end{cases}$$

Quantum Circuit
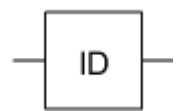
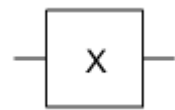We can represent a flow of operations with a **quantum circuit**.

$$|0\rangle - \boxed{H} -$$

This circuit shows an Hadamard gate H applied to a qubit $|0\rangle$.

Other blocks:

$\boxed{\text{ID}}$ identity I gate	$\boxed{\text{X}}$ Pauli X gate	$\boxed{\text{RX}_\theta}$ R_X gate	$\boxed{\text{RZ}_\theta}$ R_Z gate
$\boxed{\text{Y}}$ Pauli Y gate	$\boxed{\text{Z}}$ Pauli Z gate	$\boxed{\text{RY}_\theta}$ R_Y gate	measurement

https://it.mathworks.com/help/matlab/math/types-of-quantum-gates.html
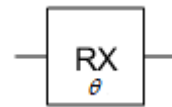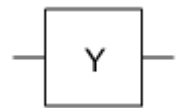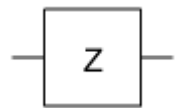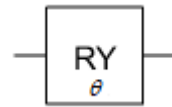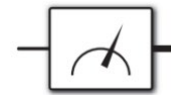
# Physical Operations on Qubits

Physical qubits need to be:

- **Initialized** into a specific state, e.g., $|00\dots00\rangle$.

- **Processed**: operations need to be applied to the qubit. For example, lasers may be used to change the spin of the electron and apply generic rotations.

- **Measured**: also in this case, lasers may be used. Measurement apparati are strictly technology-dependent, and the basis states that can be measured may change across different platforms.

All these operations may introduce **noise**. Quantum Error Correction and Mitigation are used to mitigate such effects and correct errors in the computation.
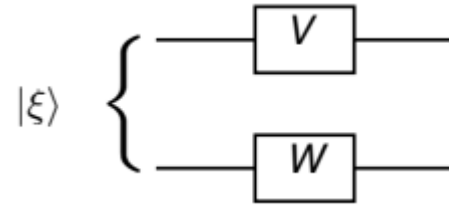
Multiple Qubits

We can perform computation using multiple qubits. Look at the following quantum circuit:
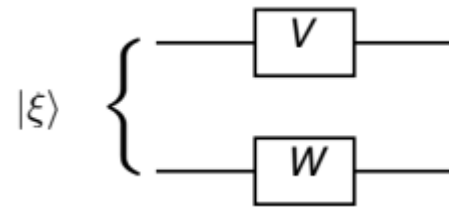
$|\xi\rangle$ is a quantum **register** of two qubits. It can be represented by a vector of $2^2 = 4$ complex components. For n qubits, the state vector consists of 2^n components!

Multiple Qubits

The operation performed onto $|\xi\rangle$ can be described by a matrix product, just like 1-qubit operations. But what is the matrix U that we multiply with $|\xi\rangle$?

$$U = V \otimes W$$

where $\otimes$ is the tensor product between V and W.

Image credits: Quantum Information Processing 101 course

Tensor Product

Given two matrices A and B, the tensor product is defined as:

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

To make it more clear: imagine that you move B over all components of A, and you multiply every element of B by the element of A you are currently moving over.

Common Gates

Among the most common gates used with multiple qubits, we have:
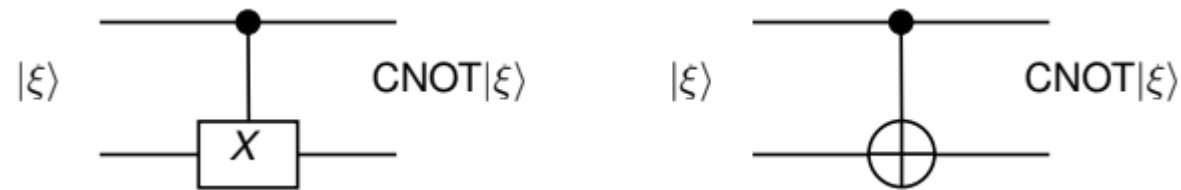
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

This is a controlled-NOT (CNOT) gate: the first qubit is used as a control qubit for the X operation. X is only applied if the control qubit is in the $|1\rangle$ state.

Image credits: Quantum Information Processing 101 course

Common Gates
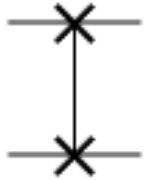
This is the SWAP gate. It swaps the state of two qubits.
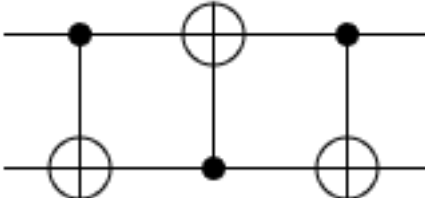
This is an alternative way to implement a swap.

NO CLONING THEOREM: we can swap states of qubits, but **we CANNOT copy** the state of one qubit into another one.

Entanglement

Look at the following circuit:

Let's compute its final state:

$$|0\rangle|0\rangle \to H_0|0\rangle|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} \to CNOT_{0,1} \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$$
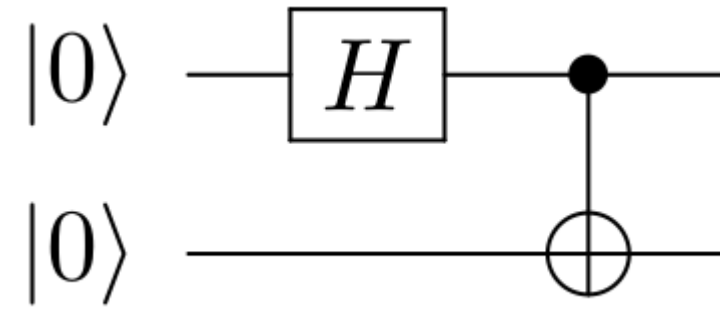
Such a state is called **Bell State** (or **EPR Pair**). Qubits in such a state are said to be **entangled**: their state cannot be described as a tensor product between the states of the single qubits. They only have a **shared** state. Entanglement is exploited by quantum algorithms and quantum communication of information.

If we measure one of the two qubits, the other one will collapse on the same state as the first one!

The Bell States

The Bell States are the most important entangled states:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad |\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \quad |\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

The Bell States form an orthonormal basis.

Starting from $|\Phi^+\rangle_{AB}$, the others can be produced as: $\left|\Phi^{ZX}\right\rangle_{AB} = Z_A^Z X_A^X |\Phi^+\rangle_{AB}$, where the suffixes are binary variables.

Entangled qubits are shared to create communication channels, as we can see now.

Quantum Super-Dense Coding

Alice and Bob share a pair of entangled qubits.

Alice generates one of $|\Phi^+\rangle_{AB}$, $|\Phi^-\rangle_{AB}$, $|\Psi^+\rangle_{AB}$ or $|\Psi^-\rangle_{AB}$: she starts with $|\Phi^+\rangle_{AB}$ and may then apply a Z and/or X operation to achieve the state $\left|\Phi^{ZX}\right\rangle_{AB} = Z_A^Z X_A^X |\Phi^+\rangle_{AB}$.

Then, she transmits her qubit to Bob. Bob measures, using the $\{|\Phi^+\rangle_{AB}$, $|\Phi^-\rangle_{AB}$, $|\Psi^+\rangle_{AB}$, $|\Psi^-\rangle_{AB}\}$ basis set.

Based on what he measures, he finds out the values for X and Z. Thus, Alices communicates two bits by only sending one qubit!

Quantum Teleportation

Alice and Bob share a pair of entangled qubits $|\Phi^+\rangle_{AB}$.

Alice also possesses a qubit $|\psi\rangle_{A'} = \alpha|0\rangle_{A'} + \beta|1\rangle_{A'}$

The joint state of the qubits is:

$$|\psi\rangle_{A'}|\Phi^+\rangle_{AB} = \left(\alpha|0\rangle_{A'} + \beta|1\rangle_{A'}\right)\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{A'AB} + \beta|100\rangle_{A'AB} + \alpha|011\rangle_{A'AB} + \beta|111\rangle_{A'AB}\right)$$

$$= \frac{1}{2}\left(\alpha\left(|\Phi^+\rangle_{A'A} + |\Phi^-\rangle_{A'A}\right)|0\rangle_B + \beta\left(|\Psi^+\rangle_{A'A} - |\Psi^-\rangle_{A'A}\right)|0\rangle_B\right) +$$

$$\frac{1}{2}\left(\alpha\left(|\Psi^+\rangle_{A'A} + |\Psi^-\rangle_{A'A}\right)|1\rangle_B + \beta\left(|\Phi^+\rangle_{A'A} - |\Phi^-\rangle_{A'A}\right)|1\rangle_B\right)$$

Quantum Teleportation

$$= \frac{1}{2}\left(|\Phi^+\rangle_{A'A}(\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{A'A}(\alpha|0\rangle_B - \beta|1\rangle_B)\right) +$$

$$\frac{1}{2}\left(|\Psi^+\rangle_{A'A}(\alpha|1\rangle_B + \beta|0\rangle_B) + |\Psi^-\rangle_{A'A}(\alpha|1\rangle_B - \beta|0\rangle_B)\right)$$

$$= \frac{|\Phi^+\rangle_{A'A}|\psi\rangle_B + |\Phi^-\rangle_{A'A}Z|\psi\rangle_B + |\Psi^+\rangle_{A'A}X|\psi\rangle_B + |\Psi^-\rangle_{A'A}XZ|\psi\rangle_B}{2}$$

At this point, Alice performs a Bell measurement of the qubits $A'A$. The state collapses to one of these four states: $\{|\Phi^+\rangle_{A'A}|\psi\rangle_B, |\Phi^-\rangle_{A'A}Z|\psi\rangle_B, |\Psi^+\rangle_{A'A}X|\psi\rangle_B, |\Psi^-\rangle_{A'A}XZ|\psi\rangle_B\}$

Quantum Teleportation

Since Alice knows the state of $A'A$, due to the entanglement she also finds out what the state is for Bob's qubit: $|\psi\rangle_B, Z|\psi\rangle_B, X|\psi\rangle_B, XZ|\psi\rangle_B$

Therefore, Alice sends two classical bits to Bob, to identify one of these four states. Given these bits, Bob applies the inverse operations to get $|\psi\rangle_B$ back (he undoes Z and/or X, if necessary).

This means that qubit $|\psi\rangle$ moved from Alice to Bob, by only exploiting a shared pair of entangled qubits, and by only transmitting two classical bits!

This process does **not** clone the qubit: after the measurements, Alice destroys it from her side, and Bob gets it.

Quantum Key Distribution

One of the use cases for Quantum Computing is **secure communication**.

There are several scenarios where users need to authenticate. They often rely on the need to generate a **secret key** which is shared among the two parties.

Such a key is used to encode a message on one side, and then decode it when it reaches the other side. In this way, an eavesdropper cannot decrypt it!

Quantum Computing can be really helpful in generating secret keys!

Quantum Key Distribution

The **BB84** protocol is a Quantum Key Distribution protocol that exploits a public quantum channel to communicate a secret key.

Alice starts by generating two random bitstrings: $a = a_1 a_2 \dots a_n$ and $b = b_1 b_2 \dots b_n$.

Then, she encodes them in n qubits. Given qubit k and a_k and b_k, $|\psi_k\rangle$ will be encoded as:

$a_k \, b_k = 00 \rightarrow |\psi_k\rangle = |0\rangle,$ $\qquad a_k \, b_k = 01 \rightarrow |\psi_k\rangle = |+\rangle,$

$a_k \, b_k = 10 \rightarrow |\psi_k\rangle = |1\rangle,$ $\qquad a_k \, b_k = 11 \rightarrow |\psi_k\rangle = |-\rangle.$

We can notice that, if $b_k = 0$, she is encoding using the Z basis (computational basis), while, if $b_k = 1$, she is encoding in the X basis (Hadamard basis).

Quantum Key Distribution

If we measure $|\psi_k\rangle = |0\rangle$ in the computational basis, we get +1 all the time, which is correct!

If we measure $|\psi_k\rangle = |+\rangle$ in the computational basis, we get +1 half of the time, and -1 for the other half.

Therefore, given a single measurement, we cannot distinguish $|0\rangle$ from $|+\rangle$. The same thing happens in the Hadamard basis.

This indistinguishability is at the basis of the protocol!

Quantum Key Distribution

Example of encoding:

string a	0	1	1	0	1
string b	1	1	0	0	1
basis	X	X	Z	Z	X
encoded qubit	$|+\rangle$	$|-\rangle$	$|1\rangle$	$|0\rangle$	$|-\rangle$

Quantum Key Distribution

Alice sends the encoded qubits over the channel to Bob.

Bob receives the qubits, but does not know the string b necessary to measure them in the correct basis.

Bob generates his own string: $b' = b'_1 b'_2 \ldots b'_n$

He then measures the qubits according to b', i.e., if $b'_k = 0$ then he uses the Z basis. Otherwise, he uses the X basis.

Given the measurements, he generates his own bitstring a': if the $k^{th} = +1$, $a'_k = 0$. Otherwise, $a'_k = 1$.

Quantum Key Distribution

At this point, both Alice and Bob have two bitstrings.

They both communicate to each other bitstrings b and b'.

When $b_k = b'_k$, they keep the bits a_k and a'_k. Otherwise, they discard them.

Finally, they use the bits they kept to compose their secret key!

Quantum Key Distribution
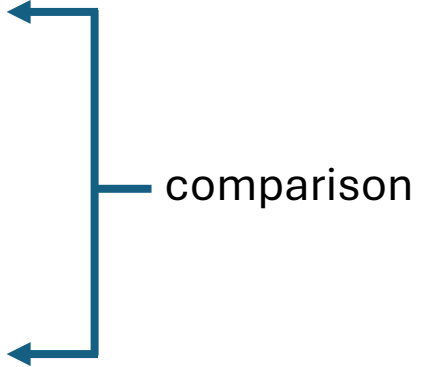
Example of complete secret key generation:

string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubit	$|-\rangle$	$|0\rangle$	$|+\rangle$	$|-\rangle$	$|1\rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
String a'	1	0/1	0	0/1	1

Based on slides from Quantum Information Processing 101

Quantum Key Distribution

Example of complete secret key generation:

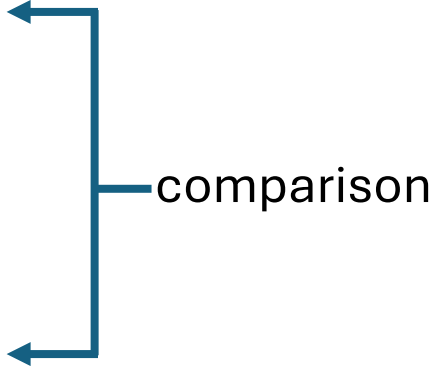| string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubit	$|-\rangle$	$|0\rangle$	$|+\rangle$	$|-\rangle$	$|1\rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
String a'	1	0/1	0	0/1	1

comparison

Based on slides from Quantum Information Processing 101

Quantum Key Distribution

Example of complete secret key generation:

string a	1	0	0	1	1
string b	1	0	1	1	0
basis	X	Z	X	X	Z
encoded qubit	$\lvert-\rangle$	$\lvert 0\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert 1\rangle$
string b'	1	1	1	0	0
Bob's basis	X	X	X	Z	Z
String a'	1	0/1	0	0/1	1

comparison

secret key

Based on slides from Quantum Information Processing 101

Quantum Key Distribution

What if an eavesdropper tries to interfere?

1. Due to the **no cloning theorem**, no eavesdropper can clone the qubits sent by Alice over the public quantum channel

2. The only thing an eavesdropper can do is a **measurement**, but for each qubit transmitted by Alice, he does not know the correct measurement basis!

Quantum Key Distribution

Therefore, when the eavesdropper measures the qubit, he may disturb them!

Example:

Alice's basis	X	Z	X	Z
Eave's basis	X	X	Z	Z
Disturbance	No	Yes	Yes	No

Based on slides from Quantum Information Processing 101

Quantum Key Distribution

When Alice and Bob share their bitstrings, if the eavesdropper's basis is different from Alice's basis, and Bob's basis is the same as Alice's basis, Alice and Bob can detect the existence of the eavesdropper!

This happens with probability $\frac{1}{4}$.

In a communication of n qubits, the probability of successful detection is $P(n) = 1 - \left(\frac{3}{4}\right)^n$, which becomes close to 1 (around 0.999) after $n = 25$.

Physical Operations on Multiple Qubits

Every QPU has a specific **topology**, describing which qubits are interconnected. 2-qubit operations can only be applied if the corresponding qubits are interconnected in the topology.

This means that, once a developer designs a generic quantum circuit, the **transpilation** process must be performed: it converts the circuit to another form, using only the gate set supported by the QPU, and every operation will respect the underlying topology of the QPU.

The **coupling graph** of a QPU contains the topology of a QPU and the **error rates** for every supported operation, including measurements.

Physical Operations on Multiple Qubits

IBM Q16 Melbourne Coupling Graph

error rates
for a 1-qubit operation
and readout

error rates
for a 2-qubit operation
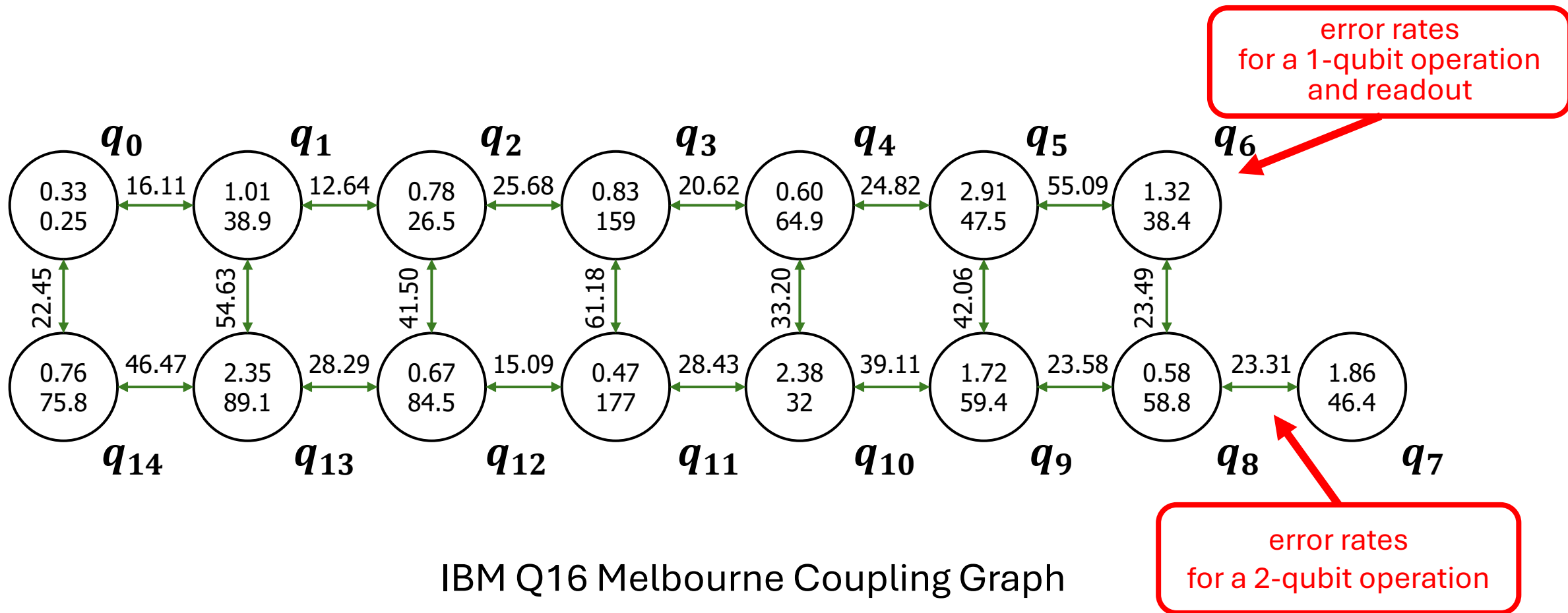
Nikita Acharya, Miroslav Urbanek, Wibe A. De Jong, and Samah Mohamed Saeed. 2021. Test Points for Online Monitoring of Quantum Circuits. J. Emerg. Technol. Comput. Syst. 18, 1, Article 14 (January 2022), 19 pages, https://doi.org/10.1145/3477928

End of the General Overview

This course is supported by MathWorks, which provides MATLAB Support Package for Quantum Computing!

In the next lesson, we will prepare our environment and do our first experiments!

Please bring your PC, with a valid MATLAB setup and install this package.

Also, register on this platform: https://quantum.ibm.com/login

We will use IBM Quantum to access real quantum hardware!

Exercises

1. Try to compute: $\langle +|\psi\rangle$ and $\langle -|\psi\rangle$. This will tell you how to move from the computational basis to the Hadamard basis!

2. Try to figure the matrix representation of the SWAP gate.

3. Try to figure out what matrix representation to use for a **Permutation** operation that permutes the coefficients of 2 qubits.

Thank you for your attention!

Quantum Computing
A Practical Perspective

Marco Venere

marco.venere@polimi.it

November 7th, 2024
Politecnico di Milano