ICGM

Institut Charles Gerhardt Montpellier

CHEMISTRY: MOLECULES TO MATERIALS

cnrs · Université de Montpellier · enscm Chimie Montpellier · MUSE Pôle Chimie Montpellier Université d'Excellence · Institut Carnot Chimie Balard Cirimat

Introduction to Quantum Computation

Bruno Senjean
ICGM, Université de Montpellier, CNRS

Quizz session:
`http://www.quizzoodle.com/session/1c507ea8389e4e5fba8b8c6de8739a75`

November 2, 2024

Table of contents

Classical Computation

Classical circuit

Classical bits

The basic component of classical information is the ***classical bit*** (binary digit) which can take the value 1 or 0, experimentally corresponding to the state of a transistor, a voltage, or a flux of photons in an optic fiber.

Although the electronic components which create, store and manipulate classical bits rely on quantum mechanics (***first quantum revolution***), the classical bit states are described by classical mechanics, essentially because they involve a huge number of particles.

Classical bits

The basic component of classical information is the ***classical bit*** (binary digit) which can take the value 1 or 0, experimentally corresponding to the state of a transistor, a voltage, or a flux of photons in an optic fiber.

Although the electronic components which create, store and manipulate classical bits rely on quantum mechanics (***first quantum revolution***), the classical bit states are described by classical mechanics, essentially because they involve a huge number of particles.

Information is stored as a succession of bits, encoding integer numbers and real numbers. For N bits:

$$n = \sum_{i=0}^{N-1} a_i 2^i \xrightarrow{\text{digitization}} a_{N-1} a_{N-2} \dots a_1 a_0.$$

With N bits, one can encode 2^N **integer numbers** (*one* at a time).

Classical bits: examples

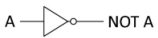
QUESTION 1

Classical logical gates

A logic gate is an idealized or physical device implementing a ***Boolean function***, a logical operation performed on one or more binary inputs that produces a single binary output.

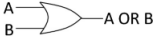
Classical logical gates

A logic gate is an idealized or physical device implementing a ***Boolean function***, a logical operation performed on one or more binary inputs that produces a single binary output.



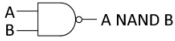
A	NOT A
0	1
1	0

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

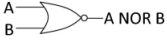


A	B	A OR B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0



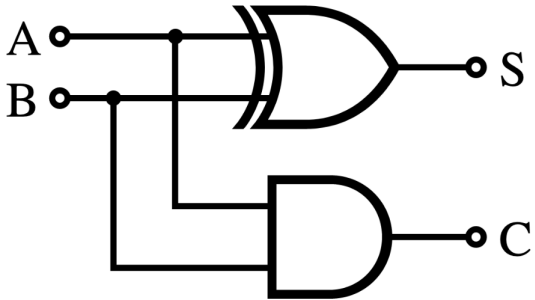
A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0



A	B	A NOR B
0	0	1
0	1	0
1	0	0
1	1	0

Classical circuit: model of classical computation

Example: the half adder circuit



A	B	S A + B	C Retenu
0	0	**0**	**0**
0	1	**1**	**0**
1	0	**1**	**0**
1	1	**0**	**1**

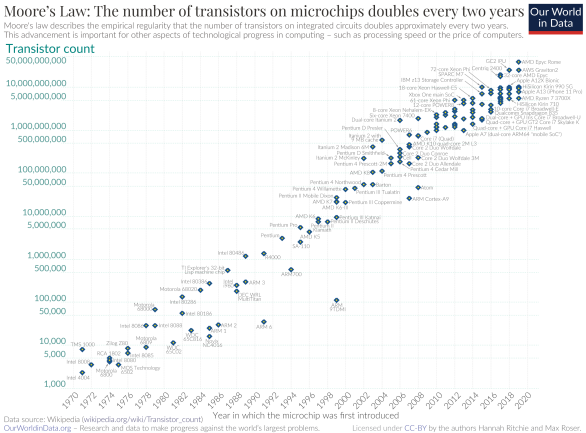
Toward Second Quantum Revolution

Moore's law

The calculation power of a computer is related to the number of transistor in the processor, which has been observed to double about every two years.

Moore's law

The calculation power of a computer is related to the number of transistor in the processor, which has been observed to double about every two years.



The end of Moore's law?

Transistors are reaching a size where ***quantum effects*** are ***not negligible*** anymore ! ~ 2 nm

The end of Moore's law?

Transistors are reaching a size where ***quantum effects*** are ***not negligible*** anymore ! ~ 2 nm

There might be different solutions: 3D stacking, new emergent technologies (post-silicon era), ...

The end of Moore's law?

Transistors are reaching a size where ***quantum effects*** are ***not negligible*** anymore ! ~ 2 nm

There might be different solutions: 3D stacking, new emergent technologies (post-silicon era), ...

But why not a change of paradigm ? Exploit the quantum effects instead of dealing with them !

QUESTION 2

Quantum Mechanics

Postulates

Postulate 1a: Quantum state of a system

*Associated to any isolated physical system is a complex vector space with inner product (***Hilbert space***) known as the* **state space** *of the system. The system is completely described by its* **state vector***, which is a unit vector in the system's state space.*

Postulate 1a: Quantum state of a system

*Associated to any isolated physical system is a complex vector space with inner product (**Hilbert space**) known as the **state space** of the system. The system is completely described by its **state vector**, which is a unit vector in the system's state space.*

Consider an orthonormal basis $\{|a_i\rangle\}$ for a N-dimensional state space. An arbitrary state vector in the state space can be written as:

$$|\psi\rangle = \sum_{i=1}^{N} a_i |a_i\rangle$$

We say that $|\psi\rangle$ is a ***superposition*** of the states $|a_i\rangle$ with associated ***amplitude*** a_i.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle\psi|\psi\rangle = 1 \longleftrightarrow \sum_{i=1}^{N} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta}|\psi\rangle$ is also normalized.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle\psi|\psi\rangle = 1 \longleftrightarrow \sum_{i=1}^{N} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta}|\psi\rangle$ is also normalized.

States that differ by this ***global phase factor*** are said to be ***equivalent***.

States that differ by a ***relative phase*** are distinct.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle\psi|\psi\rangle = 1 \longleftrightarrow \sum_{i=1}^{N} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta}|\psi\rangle$ is also normalized.

States that differ by this ***global phase factor*** are said to be ***equivalent***.

States that differ by a ***relative phase*** are distinct.

What about a composite system made up of two (or more) distinct physical systems ?

Postulate 1b: Quantum state of composite systems

The state space of **composite** system is the **tensor product** of the state spaces of the **component** physical systems A and B, i.e. $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Postulate 1b: Quantum state of composite systems

The state space of **composite** system is the **tensor product** of the state spaces of the **component** physical systems A and B, i.e. $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

For component physical systems A and B, prepared in the state $|\psi_A\rangle$ and $|\psi_B\rangle$, respectively, then the **joint state** is a state of the total system:

$$|\psi\rangle \quad = \quad |\psi_A\rangle \otimes |\psi_B\rangle \equiv |\psi_A\rangle\,|\psi_B\rangle \equiv |\psi_A\psi_B\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{N_A} \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{N_B} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_1 b_{N_B} \\ a_2 b_1 \\ \vdots \\ a_{N_A} b_{N_B} \end{pmatrix} = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} a_i b_j \, |a_i\rangle \otimes |b_j\rangle$$

Postulate 1b: Quantum state of composite systems

QUESTION 3

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |a_i\rangle \otimes |b_j\rangle$ and

$$|\Psi\rangle = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \mu_{ij} |\mu_{ij}\rangle \xrightarrow{\mu_{ij}=a_i b_j} |\psi\rangle = |\psi_a\rangle \otimes |\psi_b\rangle$$

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |a_i\rangle \otimes |b_j\rangle$ and

$$|\Psi\rangle = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \mu_{ij} |\mu_{ij}\rangle \xrightarrow{\mu_{ij}=a_i b_j} |\psi\rangle = |\psi_a\rangle \otimes |\psi_b\rangle$$

Examples of a composite system of two two-level component systems: **QUESTION 4**

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\Big(|a_1 b_2\rangle + |a_2 b_1\rangle \Big)$$

$$|\Psi_2\rangle = \frac{1}{2}\Big(|a_1 b_1\rangle + |a_1 b_2\rangle + |a_2 b_1\rangle + |a_2 b_2\rangle \Big)$$

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |a_i\rangle \otimes |b_j\rangle$ and

$$|\Psi\rangle = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \mu_{ij} |\mu_{ij}\rangle \xrightarrow{\mu_{ij}=a_i b_j} |\psi\rangle = |\psi_a\rangle \otimes |\psi_b\rangle$$

Examples of a composite system of two two-level component systems: **QUESTION 4**

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\Big(|a_1 b_2\rangle + |a_2 b_1\rangle \Big)$$

$$|\Psi_2\rangle = \frac{1}{2}\Big(|a_1 b_1\rangle + |a_1 b_2\rangle + |a_2 b_1\rangle + |a_2 b_2\rangle \Big) = \frac{1}{2}\Big(|a_1\rangle + |a_2\rangle \Big) \otimes \Big(|b_1\rangle + |b_2\rangle \Big) = |\psi\rangle$$

Entangled states are interesting because they exhibit ***correlations*** that have ***no classical analog***.

Postulate 2: Measurement of physical observable

Every measurable physical quantity $\mathcal{M}$ is described by a **Hermitian** *operator $\hat{\mathcal{M}}$ acting on the states of the state space $\mathcal{H}$. This operator is an* **observable**, *and its eigenvectors form a basis of $\mathcal{H}$. The result of measuring a physical quantity $\mathcal{M}$* **must be one of the eigenvalues** *of the corresponding operator $\hat{\mathcal{M}}$.*

Postulate 2: Measurement of physical observable

Every measurable physical quantity $\mathcal{M}$ is described by a **Hermitian** *operator $\hat{\mathcal{M}}$ acting on the states of the state space $\mathcal{H}$. This operator is an* **observable**, *and its eigenvectors form a basis of $\mathcal{H}$. The result of measuring a physical quantity $\mathcal{M}$* **must be one of the eigenvalues** *of the corresponding operator $\hat{\mathcal{M}}$.*

Consider the ***spectral decomposition*** of $\hat{\mathcal{M}}$:

$$\hat{\mathcal{M}} = \sum_m m\hat{P}_m = \sum_m m\,|m\rangle\langle m|$$

where $\hat{P}_m$ is the ***projector*** onto the eigenspace of $\hat{\mathcal{M}}$ with eigenvalue m.

The possible outcomes of the measurement are the **eigenvalues** m of the observable.

Postulate 2: Projective measurement on state $|\psi\rangle$

Consider a state $|\psi\rangle \in \mathcal{H}$, which can always be written in the eigenbasis of $\hat{\mathcal{M}}$:

$$|\psi\rangle = \sum_m \psi_m |m\rangle$$

The ***probability*** of getting the eigenvalue m upon measuring $\hat{\mathcal{M}}$ in the state $|\psi\rangle$ is given by

$$p_\psi(m) = \langle\psi| \hat{P}_m |\psi\rangle = |\langle\psi|m\rangle|^2 = |\psi_m|^2 \quad \text{(Born rule)}$$

Given that outcome m occurred, $|\psi\rangle$ ***collapses*** immediately to

$$|\psi\rangle \longrightarrow \frac{\hat{P}_m |\psi\rangle}{\sqrt{p_\psi(m)}} = |m\rangle$$

Postulate 2: Projective measurement, expectation value

One can easily calculate **average values** for projective measurements,

$$\begin{aligned}
\mathbf{E}_\psi(\hat{\mathcal{M}}) &= \sum_m m\, p_\psi(m) \\
&= \sum_m m \langle\psi| \hat{P}_m |\psi\rangle \\
&= \langle\psi| \left(\sum_m m \hat{P}_m \right) |\psi\rangle \\
&= \langle\psi| \hat{\mathcal{M}} |\psi\rangle \equiv \langle\hat{\mathcal{M}}\rangle_\psi
\end{aligned}$$

It follows a formula for the standard deviation

$$\Delta_\psi \hat{\mathcal{M}} = \sqrt{\langle\hat{\mathcal{M}}^2\rangle_\psi - \langle\hat{\mathcal{M}}\rangle_\psi^2}$$

which is a measure of the typical spread of the observed values upon measurement of $\hat{\mathcal{M}}$.

Postulate 3: Time evolution of a system

The time evolution of the state vector $|\psi(t)\rangle$ is governed by the **Schrödinger equation**, *where $H(t)$ is the (time-dependent)* **Hamiltonian** *(observable associated with the total energy of the system),*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

Postulate 3: Time evolution of a system

The time evolution of the state vector $|\psi(t)\rangle$ is governed by the **Schrödinger equation**, *where $H(t)$ is the (time-dependent)* **Hamiltonian** *(observable associated with the total energy of the system),*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

or, equivalently:

The time evolution of a closed system is described by a **unitary transformation** *on the initial state,*

$$|\psi(t)\rangle = U(t;t_0)|\psi(t_0)\rangle$$

Operations are ***unitary*** to preserve the norm of the quantum state in time.

Quantum Computation

Quantum Bit or Qubit

Quantum bit: a mathematical object

A ***quantum bit (qubit)*** is the basic component of quantum computers and is the simplest quantum system: a ***two-level system***.

Quantum bit: a mathematical object

A ***quantum bit (qubit)*** is the basic component of quantum computers and is the simplest quantum system: a ***two-level system***.

Any state of the state space will be decomposed in the ***computational basis*** made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

Quantum bit: a mathematical object

A ***quantum bit (qubit)*** is the basic component of quantum computers and is the simplest quantum system: a ***two-level system***.

Any state of the state space will be decomposed in the ***computational basis*** made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

In contrast with a classical bit, the state can be something else than $|0\rangle$ and $|1\rangle$, it can be a ***superposition*** of $|0\rangle$ and $|1\rangle$.

Quantum bit: a mathematical object

A ***quantum bit (qubit)*** is the basic component of quantum computers and is the simplest quantum system: a ***two-level system***.

Any state of the state space will be decomposed in the ***computational basis*** made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

In contrast with a classical bit, the state can be something else than $|0\rangle$ and $|1\rangle$, it can be a ***superposition*** of $|0\rangle$ and $|1\rangle$.

A qubit follows the law of quantum mechanics. It ***cannot be examined*** to determine its quantum state, but its measurement outcome will be $|0\rangle$ with probability $|\psi_0|^2$ or $|1\rangle$ with probability $|\psi_1|^2$.

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

4-qubit: $|\psi\rangle = \psi_0 |0000\rangle + \psi_1 |0001\rangle + \psi_2 |0010\rangle + \psi_3 |0011\rangle \psi_4 |0100\rangle + \psi_5 |0101\rangle + \psi_8 |0110\rangle + \psi_7 |0111\rangle$
$+\psi_8 |1000\rangle + \psi_9 |1001\rangle + \psi_{10} |1010\rangle + \psi_{11} |1011\rangle \psi_{12} |1100\rangle + \psi_{13} |1101\rangle + \psi_{14} |1110\rangle + \psi_{15} |1111\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

4-qubit: $|\psi\rangle = \psi_0 |0000\rangle + \psi_1 |0001\rangle + \psi_2 |0010\rangle + \psi_3 |0011\rangle \psi_4 |0100\rangle + \psi_5 |0101\rangle + \psi_8 |0110\rangle + \psi_7 |0111\rangle$
$+\psi_8 |1000\rangle + \psi_9 |1001\rangle + \psi_{10} |1010\rangle + \psi_{11} |1011\rangle \psi_{12} |1100\rangle + \psi_{13} |1101\rangle + \psi_{14} |1110\rangle + \psi_{15} |1111\rangle$

The number of binary strings that are encoded on the qubit register ***doubles for every additional qubit***.

That's the **Quantum corollary** to Moore's law

Not performing any measurements, Nature conceals a great deal of ***hidden quantum information***, which grows ***exponentially*** with the number of qubits ($N = 500 > n_{\text{atoms}}$ in the universe !).

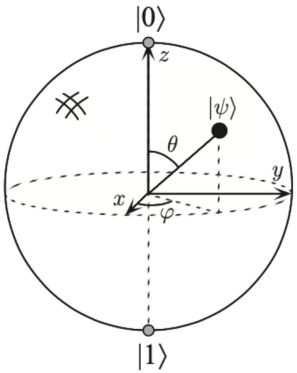
Quantum Computation

Quantum gates

Single-qubit gates: Bloch Sphere representation

Because $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$, one can rewrite the qubit state as follows:

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



Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a ***rotation on the Bloch sphere.*** It corresponds to a 2×2 matrix which can be expressed as a function of **four basis operators**.

Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a ***rotation on the Bloch sphere.*** It corresponds to a 2×2 matrix which can be expressed as a function of **four basis operators**.

A commonly used basis consists in ***Pauli's matrices***:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a ***rotation on the Bloch sphere.*** It corresponds to a 2×2 matrix which can be expressed as a function of **four basis operators**.

A commonly used basis consists in ***Pauli's matrices***:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Alternative notations:

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

Properties: $\hat{X}^2 = \hat{Y}^2 = \hat{Z}^2 = \hat{I}$ and $\boldsymbol{\sigma}_i \boldsymbol{\sigma}_j = i\varepsilon_{ijk}\boldsymbol{\sigma}_k + \delta_{ij}\mathbb{I}$

Single-qubit gates: Pauli generators for rotations

Any rotation around the direction $\vec{n} = (n_x, n_y, n_z)$ $(|\vec{n}| = 1)$ can be expressed as the exponential matrix of a superposition of Pauli's matrices, with $\hat{\vec{\sigma}} = (\hat{X}, \hat{Y}, \hat{Z})$,

$$
\begin{aligned}
e^{i\frac{\theta}{2}(\vec{n}\cdot\hat{\vec{\sigma}})} &= \sum_{k=0}^{\infty} \frac{i^k \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^k}{k!} \\
&= \sum_{p=0}^{\infty} \frac{(-1)^p \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^{2p}}{(2p)!} + i\sum_{q=0}^{\infty} \frac{(-1)^q \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^{2q+1}}{(2q+1)!} \\
&= \mathbb{I}\sum_{p=0}^{\infty} \frac{(-1)^p \left(\frac{\theta}{2}\right)^{2p}}{(2p)!} + i\left(\vec{n}\cdot\hat{\vec{\sigma}}\right)\sum_{q=0}^{\infty} \frac{(-1)^q \left(\frac{\theta}{2}\right)^{2q+1}}{(2q+1)!} \\
&= \cos\frac{\theta}{2}\mathbb{I} + i\sin\frac{\theta}{2}(n_x\hat{X} + n_y\hat{Y} + n_z\hat{Z}) = R_{\vec{n}}(\theta)
\end{aligned}
$$

Single-qubit gates

$$\hat{X} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{matrix}, \quad \hat{Z} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{matrix}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{matrix}, \quad \hat{T} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \end{matrix},$$

Single-qubit gates

$$\hat{X} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{matrix}, \quad \hat{Z} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{matrix}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{matrix}, \quad \hat{T} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \end{matrix},$$

Alternatively:

$$\hat{X} = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad \hat{H} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|, \quad \hat{T} = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$$

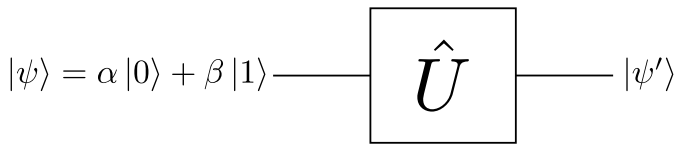
Single-qubit gates

$$\hat{X} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{matrix}, \quad \hat{Z} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{matrix}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{matrix}, \quad \hat{T} = \begin{matrix} \\ |0\rangle \\ |1\rangle \end{matrix} \begin{matrix} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \end{matrix},$$

Alternatively:

$$\hat{X} = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad \hat{H} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|, \quad \hat{T} = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$$

Circuit representation:



QUESTION 5

Controlled multi-qubit gate C-U

Single-qubit gates cannot create entanglement, one requires **multi-qubit gates**.

Controlled multi-qubit gate C-U

Single-qubit gates cannot create entanglement, one requires **multi-qubit gates**.

Consider a register of N qubits, where a quantum operation $\hat{U}$ is applied to the last $(N-1)$ qubits, controlled by the first qubit.

This gate is called a singly-controlled multi-qubit gate (can be easily generalized to a multi-controlled multi-qubit gate) and is given by

$$\text{C-U} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}^{\otimes^{N-1}} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \hat{U}$$

such that $\hat{U}$ is only applied if the first qubit is in state $|1\rangle$.

Controlled multi-qubit gate C-U

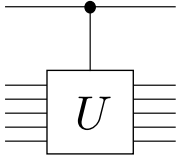
Single-qubit gates cannot create entanglement, one requires **multi-qubit gates**.

Consider a register of N qubits, where a quantum operation $\hat{U}$ is applied to the last $(N-1)$ qubits, controlled by the first qubit.

This gate is called a singly-controlled multi-qubit gate (can be easily generalized to a multi-controlled multi-qubit gate) and is given by

$$\text{C-U} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}^{\otimes^{N-1}} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \hat{U}$$

such that $\hat{U}$ is only applied if the first qubit is in state $|1\rangle$.



Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array}, \quad \text{SWAP} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array}, \quad \text{SWAP} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Alternatively:

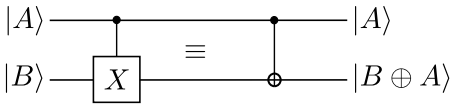
$$\text{C-}\hat{\text{N}}\text{OT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|, \quad \text{S}\hat{\text{W}}\text{AP} = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$

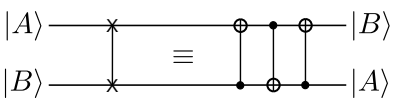
Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array}, \quad \text{SWAP} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Alternatively:

$$\text{C-}\hat{\text{NOT}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|, \quad \text{S}\hat{\text{WAP}} = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$





Toffoli gate

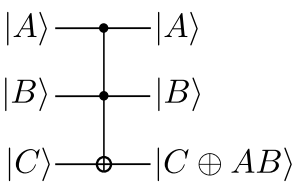
The Toffoli gate is a multi-controlled 3-qubit gate (controlled-controlled NOT gate), which was originally devised as a ***universal, reversible classical logic gate*** by Toffoli.

$$
\begin{array}{c}
 \\
|000\rangle \\
|001\rangle \\
|010\rangle \\
|011\rangle \\
|100\rangle \\
|101\rangle \\
|110\rangle \\
|111\rangle
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
|000\rangle & |001\rangle & |010\rangle & |011\rangle & |100\rangle & |101\rangle & |110\rangle & |111\rangle
\end{array} \\
\left(\begin{array}{cccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0}
\end{array}\right)
\end{array}
$$

Toffoli gate

The Toffoli gate is a multi-controlled 3-qubit gate (controlled-controlled NOT gate), which was originally devised as a ***universal, reversible classical logic gate*** by Toffoli.

$$
\begin{array}{c}
 \\
|000\rangle \\
|001\rangle \\
|010\rangle \\
|011\rangle \\
|100\rangle \\
|101\rangle \\
|110\rangle \\
|111\rangle
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
|000\rangle & |001\rangle & |010\rangle & |011\rangle & |100\rangle & |101\rangle & |110\rangle & |111\rangle
\end{array} \\
\left(\begin{array}{cccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0}
\end{array}\right)
\end{array}
$$

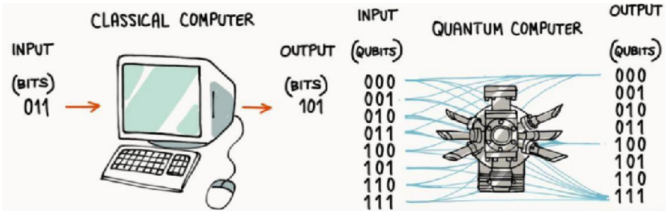


Quantum Computation

Quantum Circuit

Quantum circuit: model of quantum computation

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$



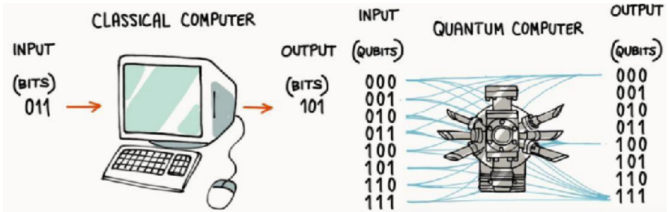
$|0\rangle$ ——————————————————

$|0\rangle$ ——————————————————

$|0\rangle$ ——————————————————

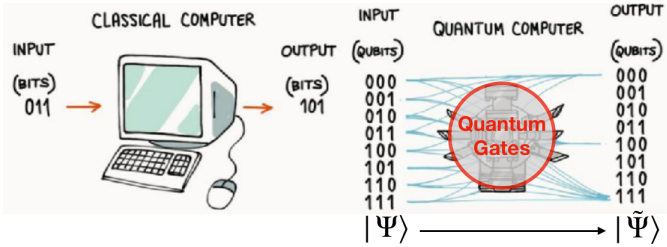
Quantum circuit: model of quantum computation

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$



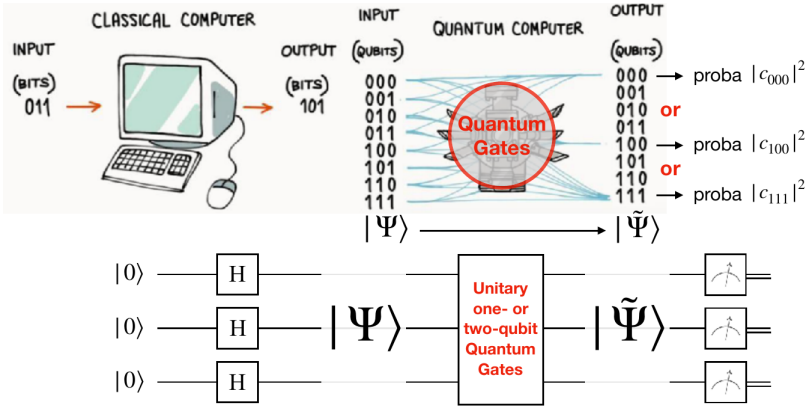
Quantum circuit: model of quantum computation

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$



Quantum circuit: model of quantum computation

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$



Quantum Computation

Examples

Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

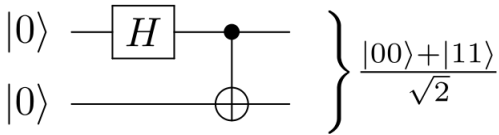
$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

They can be prepared with an Hadamard gate and a CNOT gate:

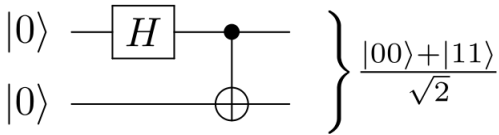


Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

They can be prepared with an Hadamard gate and a CNOT gate:



$$|00\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \xrightarrow{\mathrm{CNOT}_{12}} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Einstein, Podolski and Rosen (EPR, 1935)

Quantum mechanics:

1. An ***unobserved*** particle does no possess physical properties that exist ***independent*** of observation. Rather, such physical properties ***arise as a consequence of measurements*** performed upon the system.
2. For an ***entangled*** state of a composite system of A and B, the action performed on system A will ***modify*** the description of system B.

Einstein, Podolski and Rosen (EPR, 1935)

Quantum mechanics:

1. An ***unobserved*** particle does no possess physical properties that exist ***independent*** of observation. Rather, such physical properties ***arise as a consequence of measurements*** performed upon the system.
2. For an ***entangled*** state of a composite system of A and B, the action performed on system A will ***modify*** the description of system B.

EPR wanted to show that any ***complete*** physical theory should fulfill the sufficient condition that a value of a physical property can be predicted with certainty **immediately before measurement**.

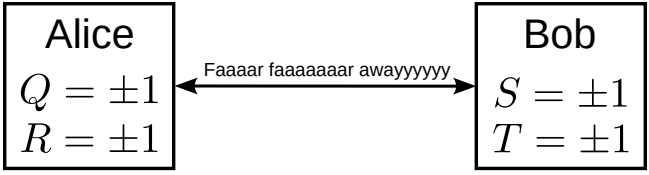
Hence, quantum mechanics is incomplete and one is missing a *local hidden variable*, according to their assumption of ***local realism***.

Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).

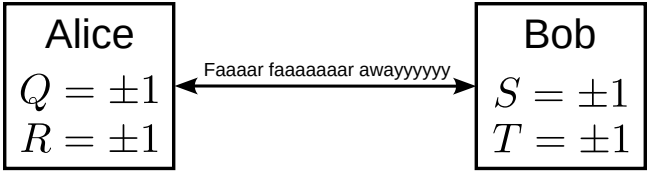
Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).



Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).



Bell inequality:

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2$$

And if Charlie prepares two entangled qubits ?

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \frac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \frac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

we have

$$\langle Q \otimes S \rangle_\psi = \langle R \otimes S \rangle_\psi = \langle R \otimes T \rangle_\psi = -\langle Q \otimes T \rangle_\psi = \frac{1}{\sqrt{2}}$$

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \dfrac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

we have

$$\langle Q \otimes S \rangle_\psi = \langle R \otimes S \rangle_\psi = \langle R \otimes T \rangle_\psi = -\langle Q \otimes T \rangle_\psi = \frac{1}{\sqrt{2}}$$

such that

$$\langle QS \rangle_\psi + \langle RS \rangle_\psi + \langle RT \rangle_\psi - \langle QT \rangle_\psi = 2\sqrt{2} > 2.$$

Hence, the fact that two spatially separate particles can form an ***unseparable system violates Bell inequality***.

And indeed, Bell inequality (1964) are not obeyed by Nature (Alain Aspect experiment, 1982).

Example: Quantum teleportation

Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

Example: Quantum teleportation

Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

But:

1. Alice doesn't know the state of the qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
2. She cannot look at it or it will collapse...
3. She can only communicate with Bob once...

Example: Quantum teleportation

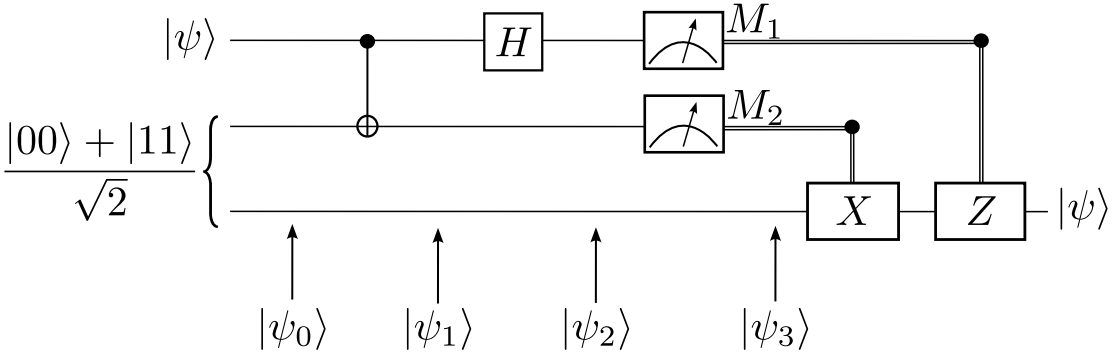
Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

But:

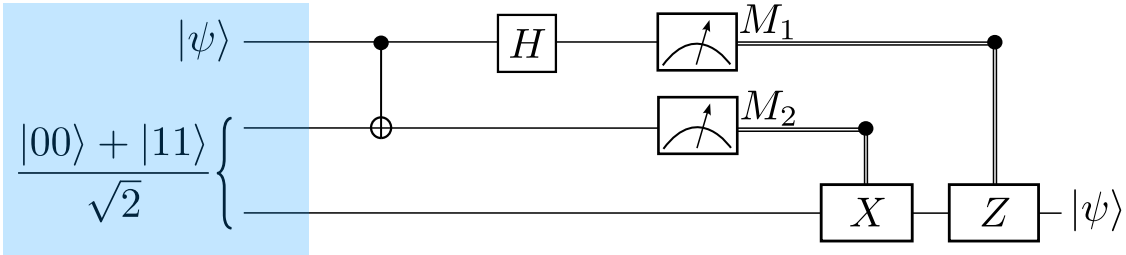
1. Alice doesn't know the state of the qubit, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
2. She cannot look at it or it will collapse...
3. She can only communicate with Bob once...

Fortunately, their EPR pair can be used to send $|\psi\rangle$ to Bob ! (Experiment by Bennett *et al.*, 1993)

Example: Quantum teleportation

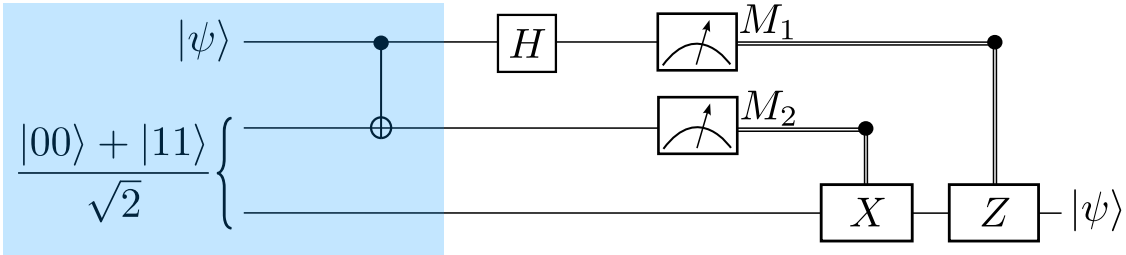


Example: Quantum teleportation



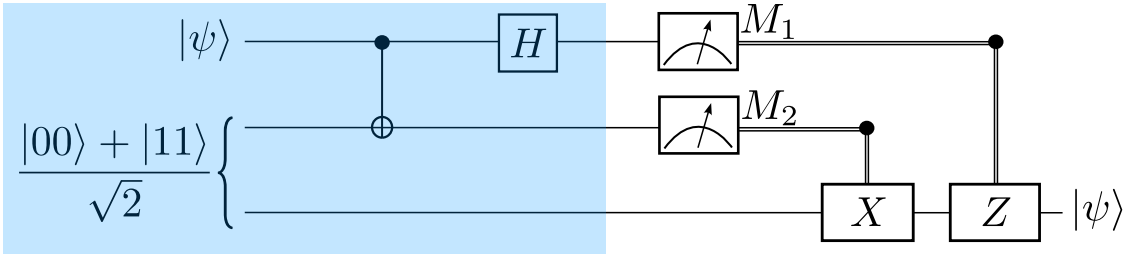
$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\Big)$$

Example: Quantum teleportation



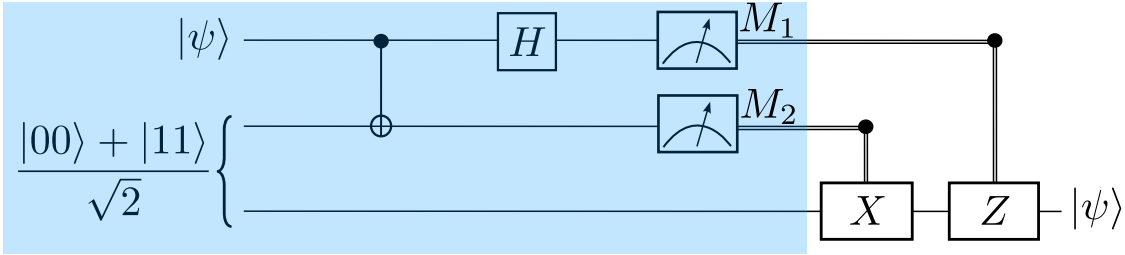
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\Big)$$

Example: Quantum teleportation



$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\Big(\alpha\,(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle) + \beta\,(|0\rangle - |1\rangle)\,(|10\rangle + |01\rangle)\Big) \\
&= \frac{1}{2}\Big(|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\Big)
\end{aligned}
$$

Example: Quantum teleportation



$$
\begin{aligned}
00 \longrightarrow |\psi_3(00)\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\
01 \longrightarrow |\psi_3(01)\rangle &= \alpha\,|1\rangle + \beta\,|0\rangle \\
10 \longrightarrow |\psi_3(10)\rangle &= \alpha\,|0\rangle - \beta\,|1\rangle \\
11 \longrightarrow |\psi_3(11)\rangle &= \alpha\,|1\rangle - \beta\,|0\rangle
\end{aligned}
$$

Example: Quantum teleportation

Only the information about the quantum state and not the state itself (no matter or energy) passes from Alice to Bob.

The teleportation is not faster than light, as Alice has to pass the information to Bob by a classical channel.

Classical versus Quantum

QUESTION 6

Irreversibility versus Reversibility

Quantum gates are ***unitary***, and hence ***reversible***.

Irreversibility versus Reversibility

Quantum gates are ***unitary***, and hence ***reversible***.

Classical logical gates are not all reversible, but ***any*** **irreversible** classical algorithm can be transformed into a **reversible** algorithm at the expense of having a higher volume of information and the introduction of the ***Toffoli*** gate.

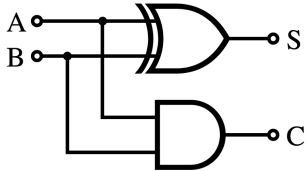
Irreversibility versus Reversibility

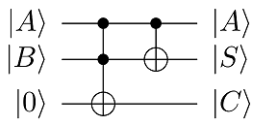
Quantum gates are ***unitary***, and hence ***reversible***.

Classical logical gates are not all reversible, but ***any* irreversible** classical algorithm can be transformed into a **reversible** algorithm at the expense of having a higher volume of information and the introduction of the ***Toffoli*** gate.

Toffoli gate is a ***universal reversible*** gate for classical computing. As it is reversible, it has a quantum analog, and **any classical algorithm has a quantum analog as well**.

Example of the half-adder circuit:





Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Quantum computing: Beyond Clifford gate set (CNOT + S + H)

1. Toffoli + H
2. CNOT, H and T
3. Clifford + T gates ($S = T^2$)

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Quantum computing: Beyond Clifford gate set (CNOT + S + H)

1. Toffoli + H
2. CNOT, H and T
3. Clifford + T gates ($S = T^2$)

Note: quantum algorithms that is written with Clifford gates can be simulated ***efficiently*** **on classical computers** (Gottesman-Knill theorem)

Non-Clifford relative phase gates are very important !

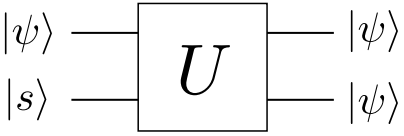
Making copy?

QUESTION 7

No cloning theorem

Copies are *everywhere* in the classical world, they are one of the most ***powerful*** means of spreading and preserving information.

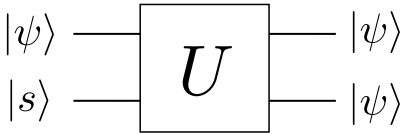
Can we make a copy of an ***unknown*** quantum state ?



No cloning theorem

Copies are *everywhere* in the classical world, they are one of the most ***powerful*** means of spreading and preserving information.

Can we make a copy of an ***unknown*** quantum state ?



Suppose the procedure works for two particular pure states $|\psi\rangle$ and $|\varphi\rangle$, thus

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,, \qquad U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

The inner product of the two states give $\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \longrightarrow |\psi\rangle$ and $|\varphi\rangle$ are either equal or orthogonal.

Hence, a general quantum cloning device is **impossible**.

Fault-Tolerant era

QUESTION 8

What is the Fault-Tolerant era ?

- The Fault-tolerant era is the era of **error corrected** (**logical**) qubits.
- Quantum components are **inevitably noisy** in **any** Quantum era ! NISQ and Fault-tolerant.
- Can we use **noisy** (**physical**) qubits to simulate an **error-free** computation ?

YES !

↓

Threshold Theorem

Threshold Theorem

- Theorem: a quantum computer with a physical error rate **below a certain threshold** can, through application of **quantum error correction** schemes, suppress the **logical error** rate to **arbitrarily low levels**

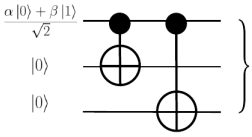
- Requirements: each **error correction** circuit will reduce the error probability from p to $cp^2 < p$, for some constant c

- We can **increase the gain** we get from one round of error correction ($p \to cp^2$) by **concatenation of codes**

level 0		level 1		level 2	$\cdots$		level k
p	$\to$	cp^2	$\to$	$c(cp^2)^2$	$\cdots$	$\to$	$c^{-1}(cp^2)^k$

Quantum Error Correction (Encoding and Transversality) 41 / 46

- Core idea of QEC → **redundant qubits** which correlation tells us something about noise

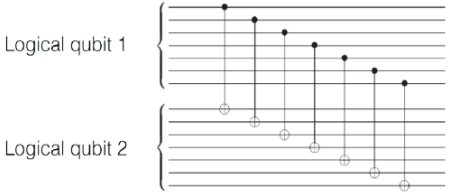


$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle = \alpha|0\rangle_{\mathrm{L}} + \beta|1\rangle_{\mathrm{L}}$$

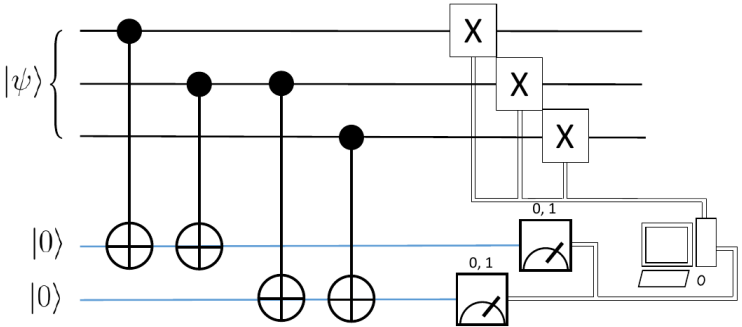
Single logical-qubit gate

$$X_L|\psi\rangle = X_1 \otimes X_2 \otimes X_3|\psi\rangle = \alpha|1\rangle_L + \beta|0\rangle_L$$
$$Z_L|\psi\rangle = Z_1 \otimes Z_2 \otimes Z_3|\psi\rangle = \alpha|0\rangle_L - \beta|1\rangle_L$$

Transversality (CNOT)



Example: Bitflip error correction code (level 1)[1]

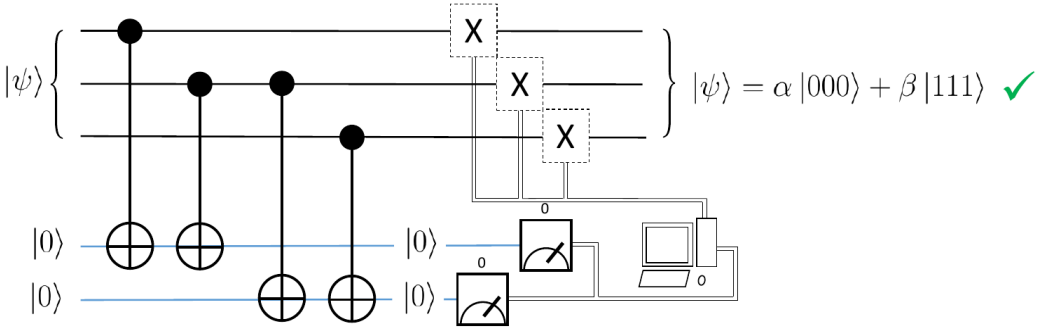


These three physical qubits make one logical qubit and we will have many such logical qubits in a circuit, which must be corrected independently.

The ancilla qubits used to detect the syndromes (errors) can be reused after measurement.

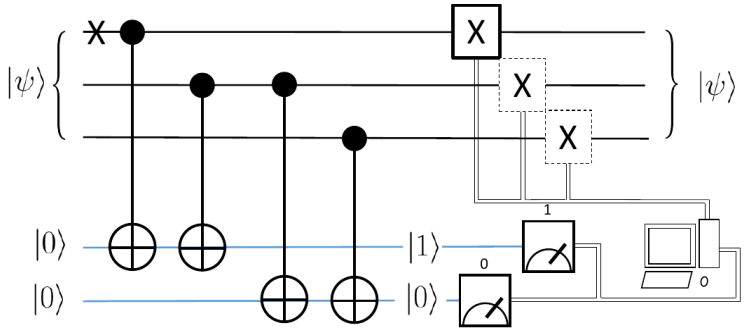
[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

Example: Bitflip error correction code (level 1)[1]



[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

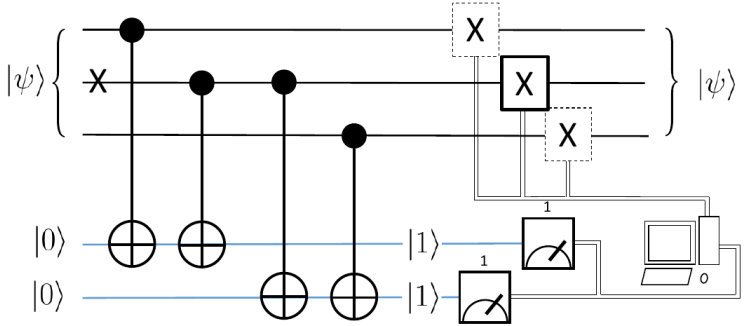
Example: Bitflip error correction code (level 1)[1]



$$|\psi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$ ✓

[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

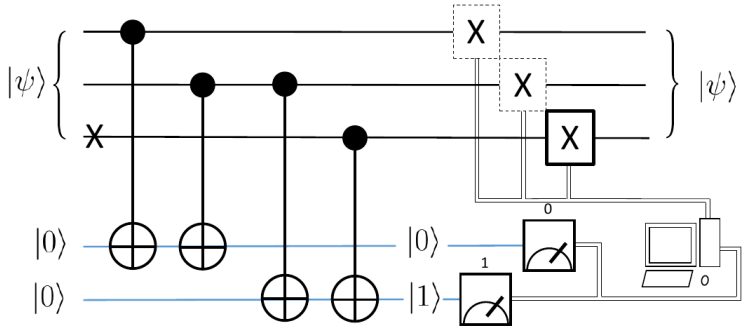
Example: Bitflip error correction code (level 1)[1]



$$|\psi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$ ✓

[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

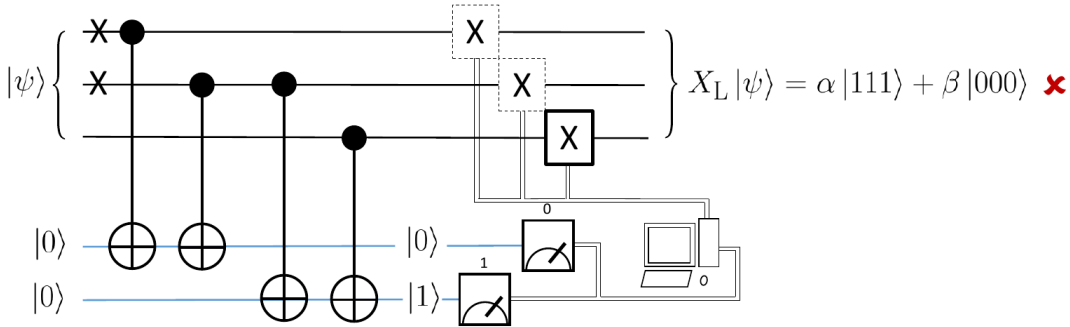
Example: Bitflip error correction code (level 1)[1]



$$|\psi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$ ✓

[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

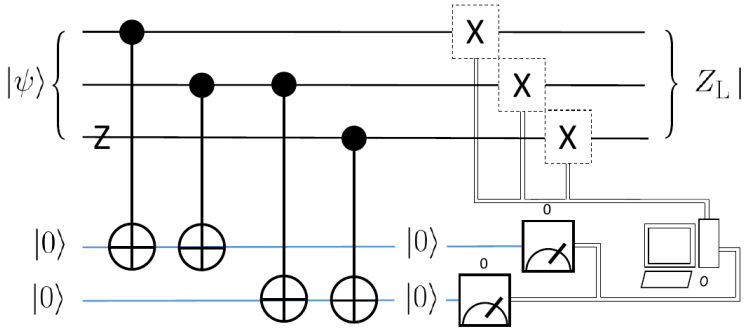
Example: Bitflip error correction code (level 1)[1]



$$X_{\mathrm{L}}\,|\psi\rangle = \alpha\,|111\rangle + \beta\,|000\rangle$$ ✘

[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

Example: Bitflip error correction code (level 1)[1]

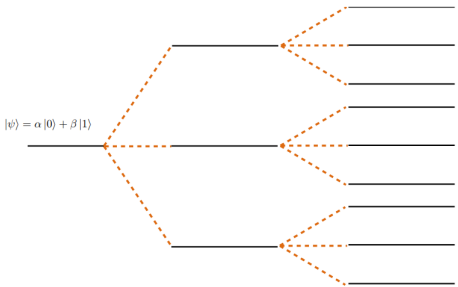


$$Z_{\mathrm{L}}\,|\psi\rangle = \alpha\,|000\rangle - \beta\,|111\rangle$$ ✘

[1] QCPC2023, David Herrera Martí and Zach Blunden-Codd

Correction to arbitrary precision: Concatenation

level 0		level 1		level 2	⋯		level k
p	$\rightarrow$	cp^2	$\rightarrow$	$c(cp^2)^2$	⋯	$\rightarrow$	$c^{-1}(cp^2)^k$



Universal Fault-tolerance

- Is that all ? Let's just use **transversability** to apply any operations between our logical qubits !
- Universal Quantum Computing = Universal set of gates **(Clifford (S, H, CNOT) + T gates)**
- Eastin-Knill (no-go) theorem[2]: **no** quantum error correcting code can **transversely** implement a **universal** gate set

SOLUTIONS ?

↓

Magic State Distillation or T-state distillation factories

Requires many many ⋯ many physical qubits and operations[3]

[2] B. Eastin, E. Knill, PRL 102 (11), 110502 (2009)

[3] J. O'Gorman and E. T. Campbell, PRA 95, 032338 (2017) ; C. Gidney and A. G. Fowler, Quantum 3, 135 (2019)

Take Home Messages

Take Home messages

Quantum computing differs from classical computing due to:

- Superposition
- Entanglement
- Measurement (collapse)
- No-cloning
- Reversibility (unitary operations)

Other important information:

- Any Clifford circuit is classically simulatable
- No QEC can act transversely on physical qubits (Eastin-Knill no-go theorem)

Developing ***efficient*** quantum algorithms for practical relevant (industrial or societal) tasks is not trivial, as it requires a radical change of vision of computing.

ICGM
Institut Charles Gerhardt Montpellier

Enjoy the tutorials!

CHEMISTRY: MOLECULES TO MATERIALS

cnrs · Université de Montpellier · enscm Chimie Montpellier · MUSE Pôle Chimie Montpellier Université d'Excellence · Institut Carnot Chimie Balard Cirimat