QCOMP103-A: Architecture Quantique

Qubits, portes quantique et savoir modéliser leurs opérations

Présenté par Jean-Adrien DUCASTAING
Sous la supervision de Nicolas BOUTRY, PhD

Plan du cours

- ❖ Bits et qubits
- ❖ De la porte logique classique à la porte quantique
- ❖ Représenter les opérations sur un qubit avec la sphère de Bloch

Un **qubit** (ou bit quantique) est une unité d'information représentant un **système quantique à deux états**.

Un **système quantique à deux dimensions** peut être dans les états 0 et 1 simultanément, on décrit donc son état par le **vecteur d'état de dimension 2**:

$$|\psi\rangle = \begin{array}{c} \mathbf{0} \\ \mathbf{1} \end{array} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

Notre **qubit s'effondre sur un bit classique** au moment de la **mesure.**

On remarque qu'**un bit classique est un cas particulier du qubit** lorsque $|c_0|^2 = 1$ ou $|c_1|^2 = 1$.

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = c_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = c_0 |0\rangle + c_1 |1\rangle$$

Considérons le **byte** (soit 8 bits) suivant: **01101011**

$$\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}$$

Notre système à 8 bits est donc représenté par le vecteur d'état:

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{array}{c} \mathbf{00000000} \\ \mathbf{00000001} \\ \vdots \\ \mathbf{01101010} \\ \mathbf{01101011} \\ \mathbf{01101100} \\ \vdots \\ \mathbf{11111110} \\ \mathbf{11111111} \end{array} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

En considérant que **le qubit est une généralisation du bit classique**, on considère donc que ce byte peut être représenté par un **qubyte** appartenant a l'**espace vectoriel complexe**:

$$(\mathbb{C}^2)^{\otimes 8} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$$

De dimension $\mathbf{2^8 = 256}$

De manière plus générale **un qubyte est en superposition de ses états de base** et peut être écrit sous la forme de:

$$\begin{array}{c} 00000000 \\ 00000001 \\ \vdots \\ 01101010 \\ 01101011 \\ 01101100 \\ \vdots \\ 11111110 \\ 11111111 \end{array} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{106} \\ c_{107} \\ c_{108} \\ \vdots \\ c_{254} \\ c_{255} \end{pmatrix}$$

On remarque donc que **8 qubits peuvent s'effondrer au moment de la mesure sur l'une des 2^8 = 256 combinaisons de bits classiques**.

On appelle tout **assemblage** de **deux qubits ou plus** un **registre quantique**.

$$\begin{array}{c} \mathbf{00000000} \\ \mathbf{00000001} \\ \vdots \\ \mathbf{01101010} \\ \mathbf{01101011} \\ \mathbf{01101100} \\ \vdots \\ \mathbf{11111110} \\ \mathbf{11111111} \end{array} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{106} \\ c_{107} \\ c_{108} \\ \vdots \\ c_{254} \\ c_{255} \end{pmatrix}$$

L'assemblage de deux qubit $|0\rangle \otimes |1\rangle$

Peut être écrit de manière équivalente $|0 \otimes 1\rangle$ ou $|01\rangle$

$$|\psi\rangle = c_{0,0}\,|00\rangle + c_{0,1}\,|01\rangle + c_{1,0}\,|10\rangle + c_{1,1}\,|11\rangle$$

ATTENTION: Le produit de Kronecker de deux états n'est pas commutatif

$$|0 \otimes 1\rangle = |01\rangle \neq |10\rangle = |1 \otimes 0\rangle$$

Kahoot

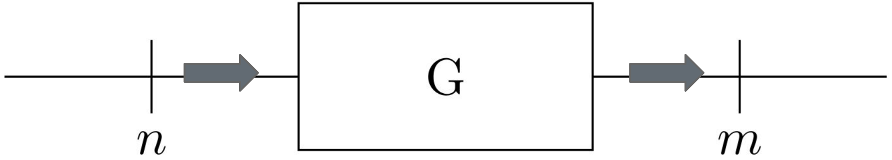
1. Prenez votre téléphone ou votre laptop
2. Allez à l'adresse **kahoot.it**
3. Rentrez le code PIN donné au tableau
4. Tenez vous prêt à jouer

Une **porte logique G** prenant en entrée **n bits** et retournant **m bits** peut être représentée par une matrice **2^m-par-2^n**

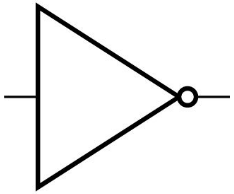
$$S_{input} = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2^n-1} \end{pmatrix} \in \underbrace{(\overbrace{\mathbb{C}^2}^{\text{Dimension de 1 qubit}})^{\otimes n}}_{\text{Dimension de n qubits}} = \mathbb{C}^{2^n}$$

$$G = \left.\underbrace{\begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,2^n} \\ g_{1,0} & \ddots & \cdots & g_{1,2^n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{2^m,0} & g_{2^m,1} & \cdots & g_{2^m,2^n} \end{pmatrix}}_{2^n \text{ colonnes}}\right\} 2^m \text{ lignes}$$

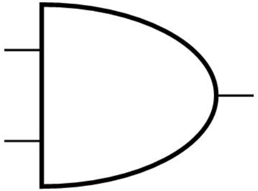
$$G * \overbrace{S_{input}}^{\text{Registre de n qubits}} = \underbrace{S_{output}}_{\text{Registre de m qubits}} \in \mathbb{C}^{2^m}$$



LE SENS DE LECTURE SE FAIT DE GAUCHE À DROITE

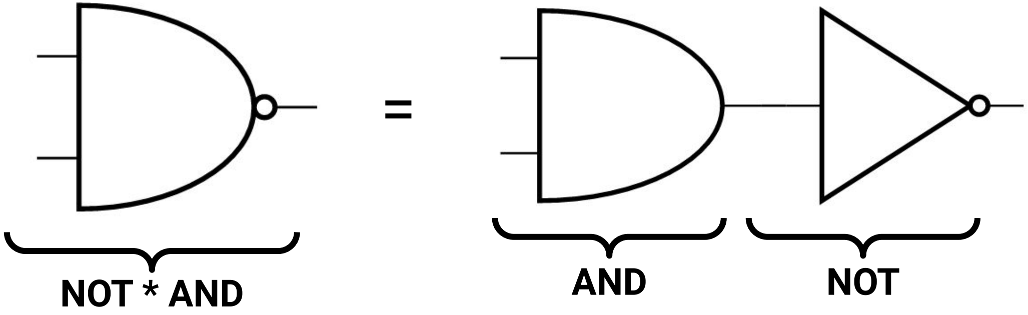


$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$



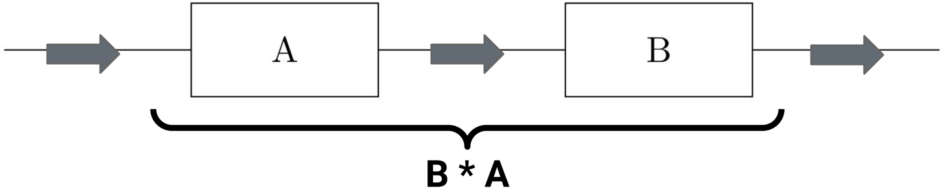
$$AND = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$AND\,|11\rangle = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad AND\,|01\rangle = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$



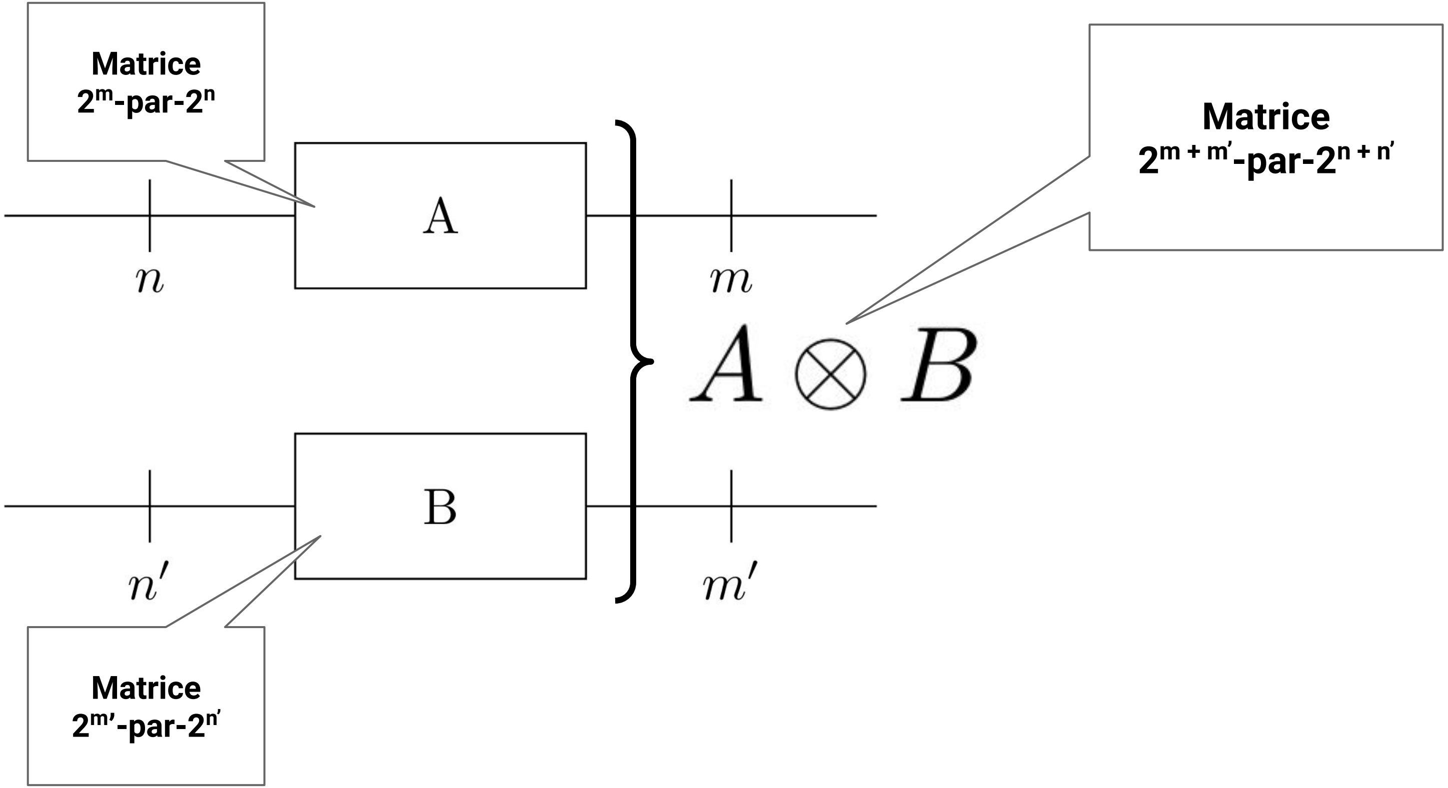
$$NOT * AND = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = NAND$$

Operations sequentielles



B * A et pas A * B

Qu’en est-il pour des **opérations parallèles** ?



Une porte est dite réversible si on peut déterminer l'état de ses bits d'entrée à partir de l'état de ses bits de sortie.

Le **principe de Landauer**:
- **Ecrire** de l'information est **réversible**.
- **Effacer** de l'information est **irreversible**.

Pour **ne pas perdre d'énergie** on utilise des portes **qui ne détruisent pas d'information**, c'est à dire des **portes réversibles**.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

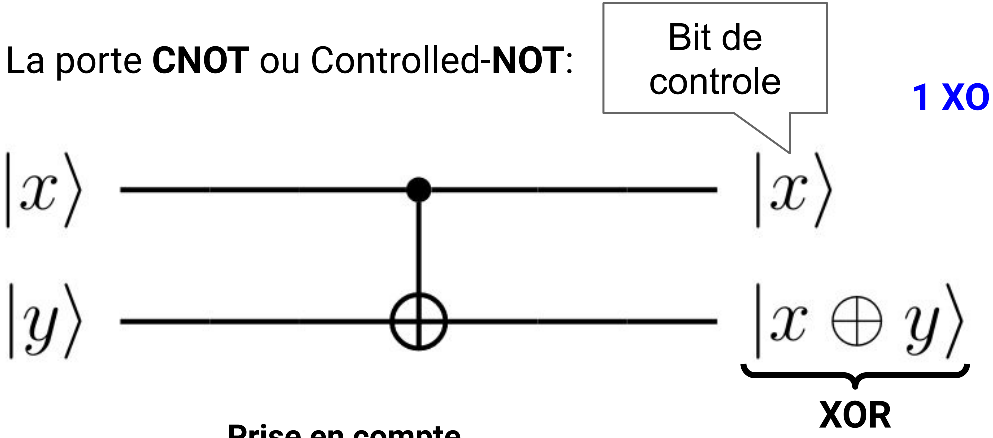
NOT est une porte **réversible**, car l'on peut déterminer l'état des bits d'entrée à partir de l'état des bits de sortie.

$$AND = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

AND n'est pas une porte réversible, car on ne peut pas déterminer l'état des bits d'entrée a partir de l'état des bits de sortie.

AND * 00 = 0   AND * 01 = 0   AND * 10 = 0

La porte **CNOT** ou Controlled-**NOT**:



1 XOR 0 = 1   1 XOR 1 = 0   0 XOR 0 = 0   0 XOR 1 = 1

- Si $|x\rangle = |0\rangle$

alors le bit de sortie sera **égal** à $|y\rangle$

- Si $|x\rangle = |1\rangle$

alors le bit de sortie sera **l'opposé** de $|y\rangle$

Prise en compte du bit de contrôle

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

Opération à exécuter (NOT)

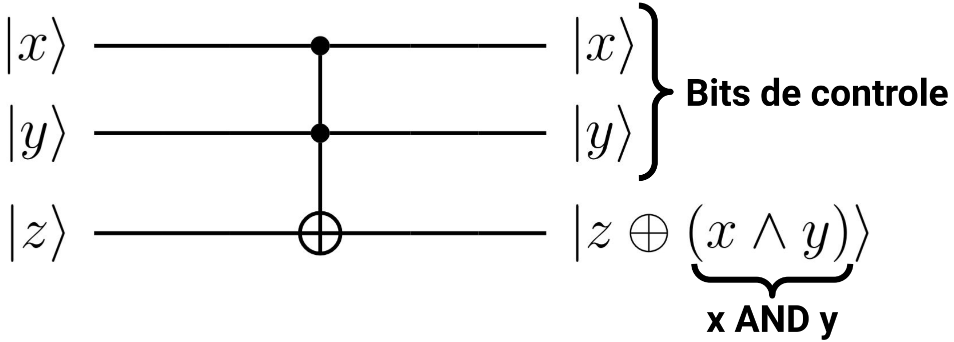
Plus généralement, a quoi correspond **l'opposé** d'un qubit ?

$$|\psi\rangle = \boxed{c_0}|0\rangle + \boxed{c_1}|1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

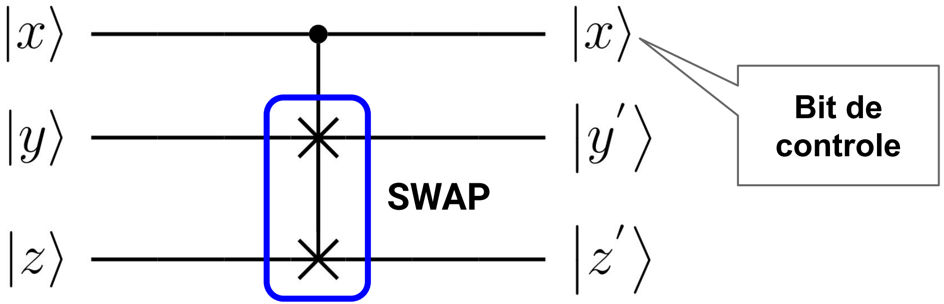
$$NOT * |\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix} = \boxed{c_1}|0\rangle + \boxed{c_0}|1\rangle$$

D'autres portes réversibles:

La porte de **Toffoli** ou CCNOT (Controlled-CNOT):



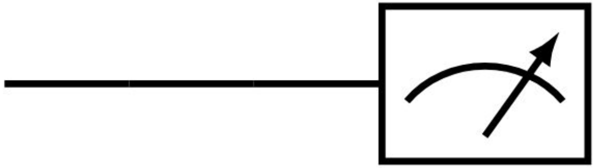
La porte de **Fredkin** ou CSWAP (Controlled-SWAP):



$$|0, y, z\rangle \longrightarrow |0, y, z\rangle$$

$$|1, y, z\rangle \longrightarrow |1, z, y\rangle$$

Finalement on a l'opération de **mesure**

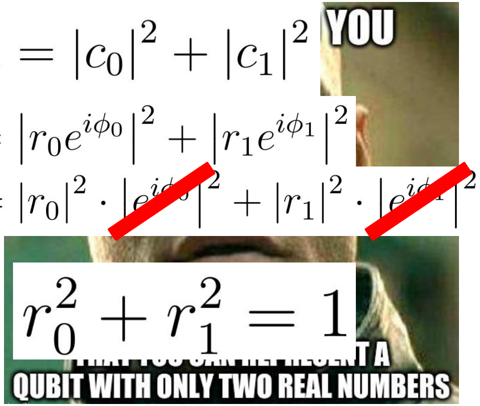


L'opération de mesure n'est pas réversible

Kahoot

1. Prenez votre téléphone ou votre laptop
2. Allez à l'adresse **kahoot.it**
3. Rentrez le code PIN donné au tableau
4. Tenez vous prêt à jouer

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = c_0\,|0\rangle + c_1\,|1\rangle = \underbrace{(a_0 + ib_0)}_{c_0}\,|0\rangle + \underbrace{(a_1 + ib_1)}_{c_1}\,|1\rangle \longrightarrow (\boxed{a_0}, \boxed{b_0}, \boxed{a_1}, \boxed{b_1}) \in \mathbb{R}^4$$



$$1 = |c_0|^2 + |c_1|^2$$

$$= \left|r_0 e^{i\phi_0}\right|^2 + \left|r_1 e^{i\phi_1}\right|^2$$

$$= |r_0|^2 \cdot \cancel{\left|e^{i\phi_0}\right|^2} + |r_1|^2 \cdot \cancel{\left|e^{i\phi_1}\right|^2}$$

$$r_0^2 + r_1^2 = 1$$

$$cos(\theta)^2 + sin(\theta)^2 = 1$$

$$r_0 = cos(\theta)$$

$$r_1 = sin(\theta)$$

$$|\psi\rangle = \boxed{r_0} e^{i\boxed{\phi_0}} \cdot |0\rangle + \boxed{r_1} e^{i\boxed{\phi_1}} |1\rangle$$ **or** $$c \cdot |\psi\rangle \sim |\psi\rangle$$

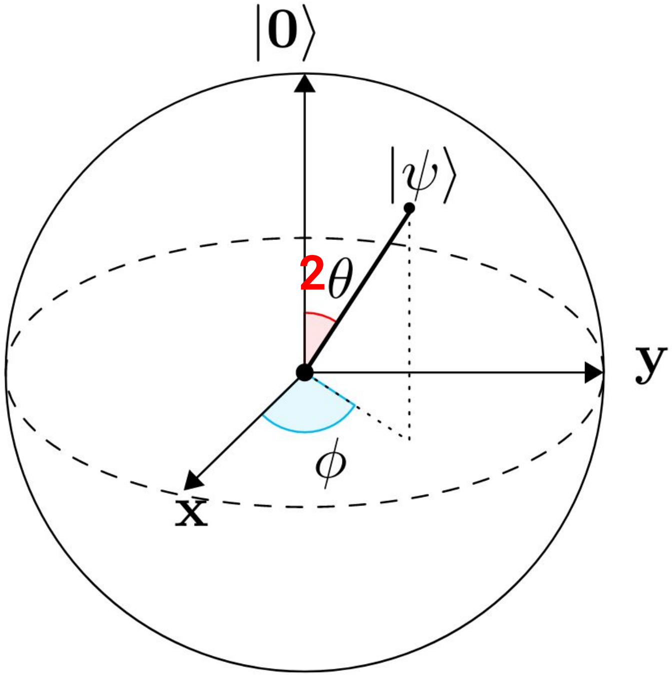
$$e^{-i\phi_0}\,|\psi\rangle = e^{-i\phi_0}\left(r_0 e^{i\phi_0} \cdot |0\rangle + r_1 e^{i\phi_1} \cdot |1\rangle\right)$$

$$= r_0 \underbrace{e^{i(\cancel{\phi_0 - \phi_0})}}_{= 1} \cdot |0\rangle + r_1 e^{i(\phi_1 - \phi_0)} \cdot |1\rangle$$

$$= \boxed{r_0} \cdot |0\rangle + \boxed{r_1} e^{i\underbrace{\boxed{(\phi_1 - \phi_0)}}_{\phi}} \cdot |1\rangle$$

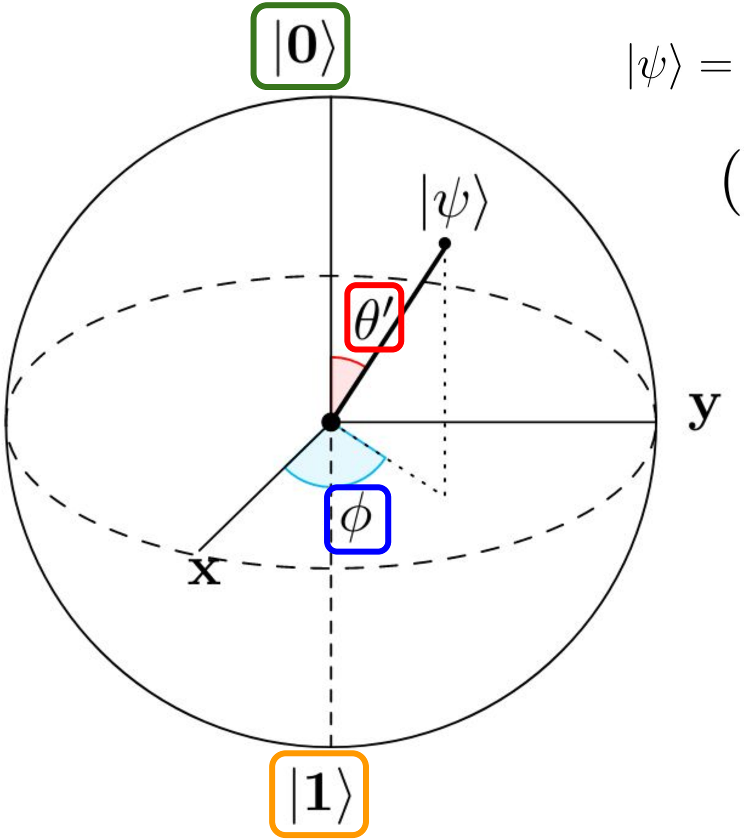
$$= cos(\boxed{\theta}) \cdot |0\rangle + sin(\boxed{\theta}) e^{i\boxed{\phi}} \cdot |1\rangle \longrightarrow (\boxed{\theta}, \boxed{\phi}) \in \mathbb{R}^2$$

$$|\psi\rangle = cos(\boxed{\theta}) \cdot |0\rangle + sin(\boxed{\theta})e^{i\boxed{\phi}} \cdot |1\rangle \qquad 0 \leq \boxed{\theta} \leq \frac{\pi}{2} \qquad 0 \leq \boxed{\phi} < 2\pi$$



$$\cancel{\begin{aligned} x &= cos(\phi)sin(\theta) \\ y &= sin(\phi)sin(\theta) \\ z &= cos(\theta) \end{aligned}} \qquad \begin{aligned} x &= cos(\phi)sin(\underline{2}\theta) \\ y &= sin(\phi)sin(\underline{2}\theta) \\ z &= cos(\underline{2}\theta) \end{aligned}$$

$$\underbrace{(\theta,\ \phi)}_{\text{Qubit}} \xrightarrow{Bloch} \underbrace{(2\theta,\ \phi)}_{\text{Représentation sur la sphère}}$$



$$|\psi\rangle = cos(\theta) \cdot |0\rangle + sin(\theta)e^{i\phi} \cdot |1\rangle \qquad 0 \leq \theta \leq \frac{\pi}{2} \qquad 0 \leq \phi < 2\pi$$

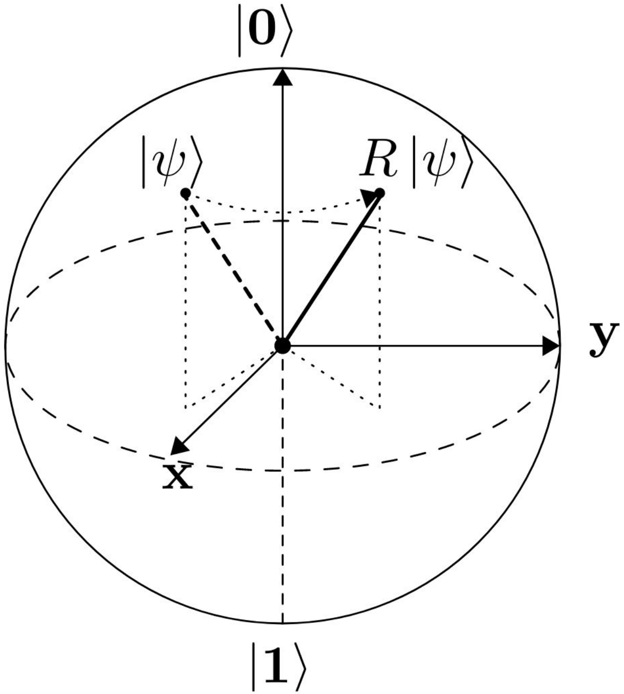
$$(\theta,\ \phi) \xrightarrow{Bloch} (2\theta,\ \phi) = (\theta',\ \phi)$$

$\boxed{|0\rangle}$ est le **pôle nord**.

$\boxed{|1\rangle}$ est le **pôle sud**.

$\boxed{\theta'} = 2\theta$ est la **latitude** du point.

$\boxed{\phi}$ est la **longitude** du point.



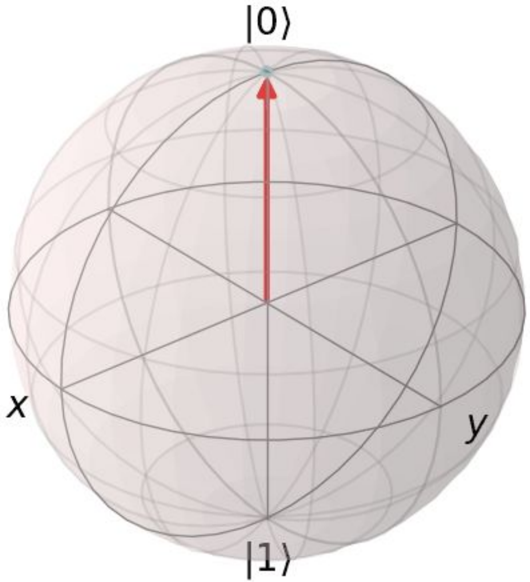
Changement de phase

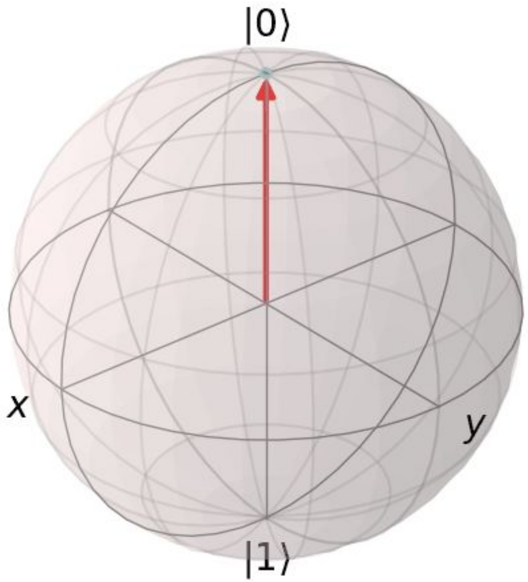
$$R(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

$$\begin{pmatrix} cos(\theta) \\ e^{i\phi} sin(\theta) \end{pmatrix} \xrightarrow{R(\alpha)} \begin{pmatrix} cos(\theta) \\ e^{i\alpha} e^{i\phi} sin(\theta) \end{pmatrix} = \begin{pmatrix} cos(\theta) \\ e^{i(\boxed{\alpha+\phi})} sin(\theta) \end{pmatrix}$$

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

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$





3 - Représenter les opérations sur un qubit avec la sphère de Bloch (cf. polycopié page 18)

Kahoot

1. Prenez votre téléphone ou votre laptop
2. Allez à l'adresse **kahoot.it**
3. Rentrez le code PIN donné au tableau
4. Tenez vous prêt à jouer