

Chapitre 1 : Bases de l'informatique quantique

Informatique quantique pour la recherche opérationnelle

Dimitri Watel - ENSIIE

Quelques définitions et résultats.

2022

1 qbit et n -qbit

Définition 1. Un *qbit* $|\varphi\rangle$ est une superposition de deux états, les états $|0\rangle$ et $|1\rangle$. Il existe $\alpha, \beta \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$$

On peut également utiliser la notation vectorielle $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

Exemples :

$$\alpha = 1 \text{ et } \beta = 0 \quad |\varphi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\alpha = 0 \text{ et } \beta = -2i \quad |\varphi\rangle = -2i |1\rangle = \begin{pmatrix} 0 \\ -2i \end{pmatrix}$$

$$\alpha = \frac{2}{\sqrt{2}} \text{ et } \beta = \frac{-2i}{\sqrt{2}} \quad |\varphi\rangle = \frac{2}{\sqrt{2}}(|0\rangle - i|1\rangle) = \begin{pmatrix} 2/\sqrt{2} \\ -2i/\sqrt{2} \end{pmatrix}$$

Définition 2. Un n -qbit est une superposition de 2^n états, les états $|0\dots 000\rangle, |0\dots 001\rangle, |0\dots 010\rangle, |0\dots 011\rangle, \dots$, et $|1\dots 111\rangle$. Il existe $\alpha_0, \alpha_1, \dots, \alpha_{2^n-1} \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha_0 \cdot |0\dots 000\rangle + \alpha_1 \cdot |0\dots 001\rangle + \dots + \alpha_{2^n-1} \cdot |1\dots 111\rangle$$

On peut aussi noter

$$|\varphi\rangle = \alpha_0 \cdot |\underline{0}\rangle + \alpha_1 \cdot |\underline{1}\rangle + \dots + \alpha_{2^n-1} \cdot |\underline{2^n-1}\rangle$$

avec $\underline{i}$ la représentation binaire de i avec n bits, ou la représentation vectorielle

$$|\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \alpha_{2^n-1} \end{pmatrix}$$

2 Opérations de base

Soient $|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$, $|\varphi\rangle = \sum_{i=0}^{2^m-1} \beta_i \cdot |\underline{i}\rangle$ et $a, b \in \mathbb{C}$.

- **Combinaison linéaire** (si $n = m$):

$$a \cdot |\phi\rangle + b \cdot |\varphi\rangle = \sum_{i=0}^{2^n-1} (a \cdot \alpha_i + b \cdot \beta_i) \cdot |\underline{i}\rangle$$

- **Norme :**

$$\| |\varphi\rangle \| = \sqrt{\sum_{i=0}^{2^n-1} |\alpha_i|^2}$$

- **Produit scalaire** (si $n = m$):

$$\langle \phi | \varphi \rangle = \langle \phi | \cdot |\varphi\rangle = |\phi\rangle^\dagger \cdot |\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i^* \beta_i$$

La notation $*$ est pour le conjugué complexe. La notation $\langle \phi |$ ou $|\phi\rangle^\dagger$ correspond au vecteur $|\phi\rangle$ transposé et conjugué.

- **Produit tensoriel :**

$$\begin{aligned} |\phi\rangle \otimes |\varphi\rangle &= \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \alpha_{2^n-1} \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \\ \dots \\ \beta_{2^m-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \cdot \beta_0 \\ \alpha_0 \cdot \beta_1 \\ \dots \\ \alpha_{2^n-1} \cdot \beta_{2^m-2} \\ \alpha_{2^n-1} \cdot \beta_{2^m-1} \end{pmatrix} \\ &= \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^m-1} \alpha_i \cdot \beta_j \cdot |\underline{i}\rangle \otimes |\underline{j}\rangle \end{aligned}$$

Si $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ et $|\varphi\rangle = \gamma |0\rangle + \delta |1\rangle$ alors le résultat est

$$\begin{aligned} |\phi\rangle \otimes |\varphi\rangle &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \cdot \gamma \\ \alpha \cdot \delta \\ \beta \cdot \gamma \\ \beta \cdot \delta \end{pmatrix} \\ &= (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle) \\ &= \alpha \cdot \gamma \cdot |0\rangle \otimes |0\rangle + \alpha \cdot \delta \cdot |0\rangle \otimes |1\rangle \\ &\quad + \beta \cdot \gamma \cdot |1\rangle \otimes |0\rangle + \beta \cdot \delta \cdot |1\rangle \otimes |1\rangle \\ &= \alpha \cdot \gamma \cdot |00\rangle + \alpha \cdot \delta \cdot |01\rangle + \beta \cdot \gamma \cdot |10\rangle + \beta \cdot \delta \cdot |11\rangle \end{aligned}$$

Attention! Ce produit n'est pas commutatif.

Définition 3. Un n -qbit est intriqué s'il n'est pas le produit tensoriel de deux autres qbits.

Par exemple $|00\rangle + |11\rangle$ est intriqué.

3 Porte quantique et circuit quantique

Définition 4. Une porte quantique est un opérateur linéaire et unitaire qui transforme un n -qbit en un autre n -qbit. Toute porte quantique peut être encodée avec une matrice unitaire A de taille $2^n \times 2^n$, c'est-à-dire une matrice inversible, dont l'inverse est la matrice conjuguée de la transposée (ou adjointe) : $A^{-1} = A^\dagger = {}^t A^*$.

Appliquer une porte A sur $|\varphi\rangle$ revient à effectuer le produit $A|\varphi\rangle$. On peut aussi appliquer la porte sur les états de base et calculer le résultat par linéarité.

Les matrices unitaires : sont inversibles et préservent le produit scalaire.

Voici quelques portes classiques :

Porte de Hadamard $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ 
 Effet sur $|0\rangle$ $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 Effet sur $|1\rangle$ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Porte X ou NOT $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 
 Effet sur $|0\rangle$ $|1\rangle$
 Effet sur $|1\rangle$ $|0\rangle$

Porte Y $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ 
 Effet sur $|0\rangle$ $i|1\rangle$
 Effet sur $|1\rangle$ $-i|0\rangle$

Porte Z $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 
 Effet sur $|0\rangle$ $|0\rangle$
 Effet sur $|1\rangle$ $-|1\rangle$

Porte CNOT $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ 
 Effet sur $|00\rangle$ $|00\rangle$
 Effet sur $|01\rangle$ $|01\rangle$
 Effet sur $|10\rangle$ $|11\rangle$
 Effet sur $|11\rangle$ $|10\rangle$

Porte SWAP $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ 
 Effet sur $|00\rangle$ $|00\rangle$
 Effet sur $|01\rangle$ $|10\rangle$
 Effet sur $|10\rangle$ $|01\rangle$
 Effet sur $|11\rangle$ $|11\rangle$

Un circuit quantique est une succession de portes, ce circuit prend en entrée un n -qbit et renvoie en sortie un n -qbit. Par exemple

$$\left. \begin{array}{c} |1\rangle \\ |0\rangle \end{array} \right\} \begin{array}{c} \text{---} \text{H} \text{---} \\ \text{---} \text{X} \text{---} \end{array} \left. \begin{array}{c} \text{---} \\ \text{---} \end{array} \right\} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Dans la représentation graphique d'un circuit,

$$\left. \begin{array}{c} |1\rangle \\ |0\rangle \end{array} \right\} \begin{array}{c} \text{---} \text{---} \\ \text{---} \text{---} \end{array} \text{ se simplifie en } |10\rangle \left\{ \begin{array}{c} \text{---} \\ \text{---} \end{array} \right.$$

$$|\varphi\rangle \text{---} \text{A} \text{---} \text{B} \text{---} \text{ est équivalent à } |\varphi\rangle \text{---} \text{BA} \text{---}$$

$$\left\{ \begin{array}{c} |\varphi\rangle \\ \text{---} \text{A} \text{---} \\ \text{---} \text{B} \text{---} \end{array} \right\} \text{ est équivalent à } |\varphi\rangle \left\{ \begin{array}{c} \text{---} \text{A} \otimes \text{B} \text{---} \end{array} \right.$$

$$\text{où } A \otimes B = \begin{pmatrix} a_{00} \cdot B & a_{01} \cdot B & \cdots & a_{02^{n-1}} \cdot B \\ a_{10} \cdot B & a_{11} \cdot B & \cdots & a_{12^{n-1}} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{2^{n-1}0} \cdot B & a_{2^{n-1}1} \cdot B & \cdots & a_{2^{n-1}2^{n-1}} \cdot B \end{pmatrix}$$

4 Mesurer un qbits

On ne peut pas observer un qbit sous sa forme superposée. Il faut le mesurer.

Définition 5. Mesurer un n -qbit de norme 1 le transforme en un des états de bases, que l'on peut ensuite observer.

Mesurer $\alpha|0\rangle + \beta|1\rangle$ renvoie 0 avec une probabilité $|\alpha|^2$, et renvoie 1 avec une probabilité $|\beta|^2$.

Mesurer $\sum_{i=0}^{2^n-1} \alpha_i \cdot |i\rangle$ renvoie i avec une probabilité $|\alpha_i|^2$.

Une fois le qbit mesuré, il perd sa superposition.

Définition 6. Deux n -qbits sont équivalents si on ne peut les distinguer par la mesure.

Par exemple

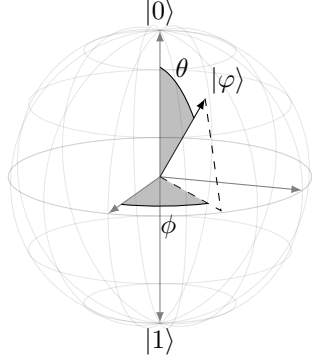
- $|0\rangle$ et $i|0\rangle$
- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et $\frac{-1}{\sqrt{2}}|00\rangle + \frac{1+i}{2}|11\rangle$

On note $|\varphi\rangle \simeq |\phi\rangle$ si ces deux qbits sont équivalents.

5 qbits équivalents et sphère de Bloch

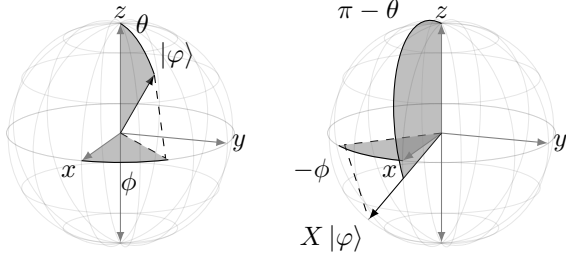
Théorème 5.1. Pour tout 1-qbit $|\varphi\rangle$, il existe θ et ϕ tels que $|\varphi\rangle$ est équivalent $\cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2}) \cdot e^{i\phi}|1\rangle$.

La sphère de Bloch est une représentation de toutes les classes d'équivalences de qbits.



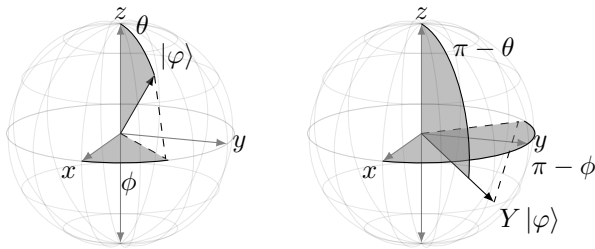
On peut observer l'effet des portes X, Y et Z sur la sphère.

$$\begin{aligned} |\varphi\rangle &\simeq \cos(\theta/2)|0\rangle + \sin(\theta/2) \cdot e^{i\phi}|1\rangle \\ X|\varphi\rangle &\simeq \sin(\theta/2) \cdot e^{i\phi}|0\rangle + \cos(\theta/2)|1\rangle \\ X|\varphi\rangle &\simeq \cos(\pi/2 - \theta/2)|0\rangle + \sin(\pi/2 - \theta/2) \cdot e^{-i\phi}|1\rangle \end{aligned}$$



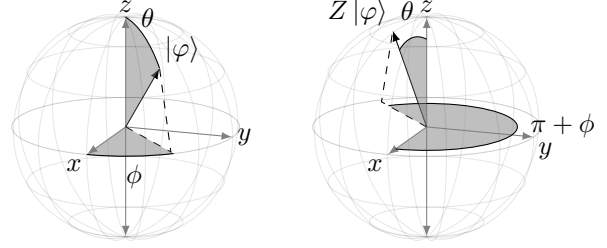
C'est une rotation d'un demi-tour autour de l'axe X .

$$\begin{aligned} Y|\varphi\rangle &\simeq i \sin(\theta/2) \cdot e^{i\phi}|0\rangle - i \cos(\theta/2)|1\rangle \\ Y|\varphi\rangle &\simeq \cos(\pi/2 - \theta/2)|0\rangle + \cos(\pi/2 - \theta/2) \cdot e^{i(\pi-\phi)}|1\rangle \end{aligned}$$



C'est une rotation d'un demi-tour autour de l'axe Y .

$$\begin{aligned} Z|\varphi\rangle &\simeq \cos(\theta/2)|0\rangle - \sin(\theta/2) \cdot e^{i\phi}|1\rangle \\ Z|\varphi\rangle &\simeq \cos(\theta/2)|0\rangle + \sin(\theta/2) \cdot e^{\pi+i\phi}|1\rangle \end{aligned}$$



C'est une rotation d'un demi-tour autour de l'axe Z .

6 Base, changement de base

Définition 7. Une base de n -qbits est un ensemble linéairement indépendant de 2^n qbits ; il s'agit d'une base de $(\mathbb{C}^{2^n}, +, \cdot)$.

Définition 8. Une base de n -qbits est *orthonormale* si, pour tout vecteur $|\varphi\rangle$ de la base, $\| |\varphi\rangle \| = 1$ et pour tout couple $|\phi\rangle$ et $|\varphi\rangle$ de vecteurs de la base, $\langle \phi | \varphi \rangle = 0$.

Les états de bases forment une base orthonormale.

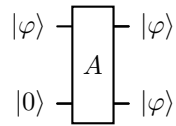
Théorème 6.1. Toute porte quantique transforme une base en une base et une base orthonormale en une base orthonormale.

Exemples de bases orthonormales:

- $|0\rangle$ et $|1\rangle$
- Base de Hadamard :
 - $|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 - $|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Base de Bell (obtenue avec $(H \otimes I_2) \cdot CNOT$):
 - $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
 - $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
 - $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
 - $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

7 Non clonage

Théorème 7.1. *Il n'existe pas de porte A dont l'effet est de cloner un qbit.*



Preuve : tester sur $|0\rangle$, $|1\rangle$ et $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ et constater une incohérence.

Théorème 7.2. *Pour toute base de 1-qbits $(|e_0\rangle, |e_1\rangle)$ orthonormale, il existe un circuit qui*

- clone les états de la base $|e_0\rangle, |e_1\rangle$
- ne clone pas les autres

$A \cdot (|\varphi\rangle \otimes |0\rangle) = |\varphi\rangle \otimes |\varphi\rangle$ si et seulement si $|\varphi\rangle = |e_0\rangle$ ou $|\varphi\rangle = |e_1\rangle$.

Preuve : il suffit de trouver A pour la base $(|0\rangle, |1\rangle)$, de trouver la matrice de passage B entre les deux bases et de mettre les portes B et B^{-1} au bon endroit dans le circuit.