Modélisation d'un système quantique.

1 Bit probabiliste.

On considère un système physique X avec des niveaux distinguables[1] dans $\Sigma = \{0, 1\}$. L'état de connaissance de ce système est un vecteur

$$v = \begin{pmatrix} a \\ b \end{pmatrix},$$

où a représente la probabilité que l'on ait un 0, et b la probabilité que l'on ait un 1. Ceci implique que l'on ait $a, b \in \mathbb{R}^+$ et $a + b = 1$.

On peut considérer des *transformations du système* X, passant d'un état à un autre :

- ▷ $\mathsf{INIT}_0 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ qui initialise à l'état 0 ;
- ▷ $\mathsf{INIT}_1 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ qui initialise à l'état 1 ;
- ▷ $\mathsf{NOT} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ qui inverse l'état.

On demande que ces opérations soient *linéaires* :

$$\mathsf{NOT} \begin{pmatrix} a \\ b \end{pmatrix} = a\, \mathsf{NOT} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\, \mathsf{NOT} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

1. On peut distinguer de l'état physique deux états : un état 0 (par exemple, pas de courant), et un état 1 (par exemple, avoir du courant)

On peut représenter une telle opération par une matrice stochastique : c'est une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

telle que $a, b, c, d \geq 0$ et $a + c = b + d = 1$. Ainsi, INIT_0 et INIT_1 ne sont pas des transformations valides.

Lorsqu'on « observe » le système X, on change l'état de nos connaissances :

$$\begin{pmatrix} 1/4 \\ 3/4 \end{pmatrix} \xrightarrow{1/4} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{après avoir vu 0}$$
$$\begin{pmatrix} 1/4 \\ 3/4 \end{pmatrix} \xrightarrow{3/4} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{après avoir vu 1.}$$

2 Bit quantique.

On considère un système physique X avec des niveaux distinguables dans $\Sigma = \{0, 1\}$. L'état de connaissance de ce système est un vecteur

$$v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

où $\alpha, \beta \in \mathbb{C}$ sont les *amplitudes* et vérifient $|\alpha|^2 + |\beta|^2 = 1$.

Les transformations de X sont des opérations linéaires en v et préservent la norme, représentations les matrices *unitaires*, c'est-à-dire des matrices $U^\dagger U = \mathbb{1}$,[2] qui généralise les matrices orthogonales pour les matrices complexes. Quelques exemples de matrices unitaires sont :

- la matrice identité $\mathbb{1}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

2. L'opération $-^\dagger$ est la *transconjuguasion* qui correspond à la transposée de la conjugaison composante par composante.

- la matrice **NOT** $:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;
- la matrice de Hadamard $\mathbf{H} := \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$;
- la matrice $\mathbf{Y} := \begin{pmatrix} 0 & \mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix}$;
- la matrice de rotation $\mathbf{R}_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$;
- mais les matrices des opérations INIT_i ne sont pas unitaires.

Lorsqu'on « observe » le système X (que l'on appellera une *mesure*), on change l'état de nos connaissances :

$$\begin{pmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \begin{array}{ll} \xrightarrow{\frac{1}{2}=\left|-\frac{1}{\sqrt{2}}\right|^2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{après avoir vu 0} \\ \xrightarrow{\frac{1}{2}=\left|\frac{1}{\sqrt{2}}\right|^2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \text{après avoir vu 1.} \end{array} .$$

3 Plusieurs qubits.

On considère deux systèmes X_1, X_2 avec 4 niveaux $\Sigma = \{00, 01, 10, 11\}$. On peut distinguer un vecteur probabiliste « classique » et un état quantique :

$$\begin{pmatrix} 1/8 \\ 1/2 \\ 0 \\ 3/8 \end{pmatrix} \leftarrow/\rightarrow \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/2 \\ 1/2 \end{pmatrix} .$$

Un système à n qubits sera représenté par un espace à 2^n dimensions.

L'opération importante est le *produit tensoriel*. Si l'on a deux matrices $A \in \mathbb{C}^{k\times\ell}$ et $B \in \mathbb{C}^{m\times n}$ alors on a une matrice $A \otimes B \in \mathbb{C}^{km\times\ell n}$.

Définition 1 (Construction du produit tensoriel)**.** Si on a :

- ▷ un espace vectoriel V avec une base $\{e_1, \dots, e_n\}$;
- ▷ un espace vectoriel V' avec une base $\{e'_1, \dots, e'_m\}$;

alors l'espace vectoriel $V \otimes V'$ a pour base

$$\{e_i \otimes e'_j \mid i \in [\![1, n]\!] \text{ et } j \in [\![1, m]\!]\}.$$

Ainsi,

$$V \otimes V' = \text{vect}\{v \otimes v' \mid v \in V \text{ et } v' \in V\}.$$

On a quelques propriétés sur le produit tensoriel.

Proposition 1. On a :

- ▷ $\lambda \otimes A = \lambda A$ où l'on identifie $\mathbb{C}^{1\times 1}$ et $\mathbb{C}$;
- ▷ $(A \otimes B) \otimes C = A \otimes (B \otimes C)$;
- ▷ $(A \otimes B)(C \otimes D) = AC \otimes BD$;
- ▷ $A \otimes (B + C) = A \otimes B + A \otimes C$.

On suppose ici que les matrices respectent les bonnes conditions de dimension pour que ces opérations aient du sens. □

Attention ! En général, on a $A \otimes B \neq B \otimes A$.

4 Notation de Dirac.

On adopte les notations suivantes :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

que l'on appelle *ket* $|-\rangle$. Cette notation est linéaire dans le sens où l'on a

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta 1.$$

L'écriture des produits tensoriels est plus simple $|0\rangle \otimes |0\rangle = |00\rangle$. L'avantage est que l'on peut écrire

$$\frac{1}{\sqrt{2}} |0000\rangle + \frac{1}{\sqrt{2}} |1111\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ \vdots \\ 0 \\ 1/\sqrt{2} \end{pmatrix}.$$

On a la notion de *dualité* : $|\psi\rangle \leftrightarrow \langle\psi| = (|\psi\rangle)^\dagger$.

Avec $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ et $|\varphi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, on peut définir des notations sympathiques :

$$\langle\varphi| |\psi\rangle = \begin{pmatrix} \bar{\gamma} & \bar{\delta} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\bar{\gamma} + \beta\bar{\delta} = \langle\varphi|\psi\rangle .$$

On peut aussi définir $|-\rangle \langle-|$. On peut ainsi interpréter $|\psi\rangle \langle\psi|$ comme la projection sur vect $|\psi\rangle$.