QUBITS

QUÉLARD Xavier

5 novembre 2017

Résumé

...

Table des matières

Introduction

...

1. Historique : mécanique quantique et Qu-Bit

...

2. Comment réaliser un QuBit ?

2.1 Photons polarisés

...

2.2 Pièges à ions / technologie NMR

...

2.3 Pièges à ions / technologie NMR

...

2.4 Solid State QuBit (supraconductor technology)

...

3. Simulation informatique

3.1 Rappels mathématiques

3.1.1 Loi de composition interne et groupe

Une loi de composition interne $\star$ sur l'ensemble X est une aplication de la forme :

$$\star : X \times X \to X$$

Soit G un ensemble non vide, muni d'une loi de composition interne $\oplus$. (G, $\oplus$) est un groupe abélien $\Leftrightarrow$

- $\oplus$ associative : $\forall (x, y) \in G^2, (x \oplus y) \oplus y = x \oplus (y \oplus z)$
- $\exists e \in G / x \oplus e = e \oplus x = x$ (e est le neutre du groupe G selon la loi $\oplus$)
- $\oplus$ commutative : $\forall (x, y) \in G^2, x \oplus y = y \oplus x$

3.1.2 Anneaux et corps

Disposant de la définition d'un corps commutatif, nous pouvons maintenant donner la définition d'un anneau commutatif. Soit A un ensemble non vide, muni de deux lois de compositions interne $\oplus$ et $\otimes$.

Alors $(A, \oplus, \otimes)$ anneau commutatif $\Leftrightarrow$

- $(A, \oplus)$ est un groupe commutatif
- la loi $\otimes$ est associative
- la loi $\otimes$ est distributive par rapport à la loi $\oplus$, c'est-à-dire que :

$$\forall (x, y, z) \in A^3, (x \oplus y) \otimes z = x \otimes (y \oplus z)$$

- la loi $\otimes$ est commutative : $\forall (x1, x2) \in A^2, x1 \otimes x2 = x2 \otimes x1$

Un corps commutatif est alors simplement un anneau commutatif dont tous les éléments sont inversibles, exceptés le neutre pour l'opération $\oplus$. Il est alors aisé de remarquer que l'ensemble $\mathbb{R}$ ou bien $\mathbb{C}$ sont, munis des opérations $(+, \times)$, des corps.

3.1.3 espace vectoriel et produit scalaire

Soit E un ensemble non vide et $(\mathbb{K}, +, \times)$ un corps de neutre $0_{\mathbb{K}}$ pour $+$ et $1_{\mathbb{K}}$

pour $\times$. On note $(E, +, \cdot)$ l'ensemble E muni de la même loi $+$ que $\mathbb{K}$ (c'est donc une loi interne à E), et d'une loi externe $\cdot : \mathbb{K} \times E \to E$.

Alors E est un espace vectoriel $\Leftrightarrow$

- $(E, +)$ est un groupe commutatif
- $\forall \lambda \in \mathbb{K}, \forall (x, y) \in E^2, \lambda \cdot (x + y) = (\lambda \cdot x) + (\lambda \cdot y)$ (distributivité)
- $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall x \in E, (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
- $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall x \in E, (\lambda \times \mu) \cdot x = \lambda \cdot (\mu \cdot x)$
- $\forall x \in E, 1_{\mathbb{K}} \cdot x = x$

On appele les éléments de E des vecteurs, les éléments de $\mathbb{K}$ des scalaires, et le vecteur $0_{\mathbb{K}}$ est appelé le vecteur nul. En résumé, un espace vectoriel est un espace E consitué d'éléments appelés vecteurs, qui sont stables par addition et par multiplication d'un scalaire. Les espaces $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont donc des espaces vectoriels (le second est appelé espace vectoriel complexe).

On appele produit scalaire sur E (espace vectoriel) toute forme bilinéaire symétrique et définie positive, c'est-à-dire :

- forme : c'est une application du type $\langle \cdot / \cdot \rangle : \begin{cases} E \times E \to \mathbb{K} \\ (u, v) \mapsto \langle u/v \rangle \end{cases}$
- symétrie : $\forall (u, v) \in E^2, \langle u/v \rangle = \langle v/u \rangle$
- linéarité à droite : $\forall (u, v, w) \in E^3, \langle u/v+w \rangle = \langle u/v \rangle + \langle u/w \rangle$ (de la symétrie et la linéarité découle alors la bi-linéarité)
- defini positif : $\forall u \in E, \langle u/u \rangle \geq 0$ et $\forall u \in E, \langle u/u \rangle = 0u = 0_E$

Il est important de remarquer que s'il l'on se place dans un espace vectoriel complexe, le produit scalaire donne un nombre complexe, tandis qu'en se plaçant dans un espace vectoriel sur le corps des réels, le produit scalaire donnera lui même un réel. De manière générale, il associe à vecteur un élément du corps $\mathbb{K}$.

3.1.4 norme induite, suites de Cauchy et espace de Hilbert

Une norme est une application $N : E \to \mathbb{R}_+$ et qui satisfait l'hypothèse de séparation ($\forall u \in E, N(u) = 0 \Rightarrow u = 0_E$), d'absolue homogénéité ($\forall \lambda \in \mathbb{K}, \forall u \in E, N(\lambda \cdot u) = \lambda \cdot N(u)$), et l'inégalité triangulaire ($\forall (u, v) \in E^2, N(u + v) \leq N(u) + n(v)$).

A chaque produit scalaire est associé une norme, que l'on appele norme induite par le produit scalaire. Elle est définie par :

$$N(\cdot) : \begin{cases} E \to \mathbb{R}_+ \\ u \mapsto \sqrt{\langle u/u \rangle} \end{cases} \tag{3.1}$$

Une fois que nous possédons une norme, il est possible d'introduire la notion de convergence, mais aussi de définir les suites de Cauchy. Soit $(U)_n$ une suite de vecteurs de E. Alors $(U)_n$ suite de Cauchy $\Leftrightarrow$

$$\forall \varepsilon \in \mathbb{R}_+^*, \exists N \in \mathbb{N} / \forall (p,q) \in \mathbb{N}^2, |u_p - u_q| < \varepsilon \tag{3.2}$$

Une suite de Cauchy est donc simplement une suite dont les termes se rapprochent uniformément les uns des autres en l'infini. Un espace vectoriel, muni d'une norme découlant d'un produit scalaire, et dont toutes les suites de Cauchy convergent, est appelé un espace de Hilbert. La convergence d'une suite vers une valeur $l \in \mathbb{K}$ se traduit par la propriété (3.3) .

$$\forall \varepsilon \in \mathbb{R}_+^*, \exists N \in \mathbb{N} / \forall n \in \mathbb{N}, n \geq N \Rightarrow |u_n - l| < \varepsilon \tag{3.3}$$

C'est dans un tel espace que nous allons travailler pour définir nos QuBits.

3.2 Application aux QuBits

3.2.1 Définition d'un QuBit

Notons dans toute la suite $\mathbb{H}_n$ un espace de Hilbert complexe et de dimension n. Un vecteur quelconque de l'espace $\mathbb{H}_2$ est donc défini par : $|\mathbf{\Phi}\rangle = \lambda|\mathbf{0}\rangle + \mu|\mathbf{1}\rangle$, où λ et μ sont des coefficient complexes, et où $|\mathbf{0}\rangle$ ainsi que $|\mathbf{1}\rangle$ sont deux vecteurs formant une base orthonormée de $\mathbb{H}_2$ (les deux vecteurs sont orthogonaux et de norme 1). Le produit scalaire de deux vecteurs est alors défini par (3.4), et la norme induite sera (3.5).

$$\langle \Phi / \Psi \rangle = \langle\ \lambda|\mathbf{0}\rangle + \mu|\mathbf{1}\rangle\ /\ \nu|\mathbf{0}\rangle + \sigma|\mathbf{1}\rangle\ \rangle = \lambda^*\nu + \mu^*\sigma = \langle \Phi / \Psi \rangle^* \tag{3.4}$$

$$||\Phi||^2 = \langle \Phi / \Phi \rangle = \langle\ \lambda|\mathbf{0}\rangle + \mu|\mathbf{1}\rangle\ /\ \lambda|\mathbf{0}\rangle + \mu|\mathbf{1}\rangle\ \rangle = |\lambda|^2 + |\mu|^2 \tag{3.5}$$

Un QuBit isolé est alors défini comme un vecteur de cet espace $\mathbb{H}_2$ (voir 3.6) auquel on ajoute une condition sur la norme : la condition de normalisation (3.7). Si cette dernière n'est pas indispensable, elle est commode et constamment utilisé dans la littérature, nous l'adopterons donc également.

$$|\boldsymbol{Q}\rangle = \alpha \cdot |\mathbf{0}\rangle + \beta \cdot |\mathbf{1}\rangle \tag{3.6}$$

$$(\alpha, \beta) \in \mathbb{C}^2\ /\ |\alpha|^2 + |\beta|^2 = 1 \tag{3.7}$$

3.2.2 QuBit et mesure

La mesure d'un QuBit corresponds à une application $\mathbb{M} : \mathbb{H}_2 \to \{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$: on choisis un QuBit quelconque, et la mesure nous donnera soit l'état $|\mathbf{0}\rangle$, soit l'état $|\mathbf{1}\rangle$. Mais comme vu dans la première partie de ce rapport, la mesure en mécanique quantique n'est pas une opération déterministe : en effet, si le QuBit était de la forme $|\boldsymbol{Q}\rangle = |\mathbf{0}\rangle$, et que l'on mesure la probabilité que ce dernier soit dans l'état $|\mathbf{0}\rangle$, nous obtiendrons bel et bien 100%. De même, si $|\boldsymbol{Q}\rangle = |\mathbf{1}\rangle$, nous obtiendrons

une probabilité de 0%. En revanche, dans le cas général, tout se complique. Soit $|\boldsymbol{\omega}\rangle$ un vecteur de $\mathbb{H}_2$. Nous voulons connaître la probabilité selon laquelle notre QuBit sera mesuré dans l'état $|\boldsymbol{\Omega}\rangle$. Elle est définie par (3.8).

$$P(\ M(|\boldsymbol{Q}\rangle) = |\boldsymbol{\Omega}\rangle\ ) = |\langle\ |\boldsymbol{Q}\rangle\ /\ |\boldsymbol{\Omega}\rangle\ \rangle|^2 = P(\ M(Q) = \Omega\ ) \tag{3.8}$$

La conséquence logique des dernières affirmations est que pour un QuBit de la forme $|\boldsymbol{Q}\rangle = \alpha \cdot |\mathbf{0}\rangle + \beta \cdot |\mathbf{1}\rangle$, sa probbilité d'être mesuré dans l'état $|\mathbf{0}\rangle$ est de λ^2, et celle d'être mesuré dans l'état $|\mathbf{1}\rangle$ est de μ^2. la condition de normalisation (3.7) prends alors tout son sens : la somme des probabilités de deux évènements formant un ensemble complet vaut 1. Ce résultat se généralise pour n'importe quel couple d'etats , tant que ces derniers forment une base orthonormée.

3.2.3 Visualisation avec la sphère de Bloch

L'objectif de cette section est de donner un aperçu visuel au lecteur d'un état quantique. C'est à cette problématique que la sphère de Bloch, nommée après le brillant mathématicien, apporte une réponse. Pour présenter cette dernière, il est d'abord nécessaire de définir les relations et classes d'équivalences.

$R : E \to E$ relation d'équivalence $\Leftrightarrow$
- R refléxive : $\forall x \in E, xRx$ (x est en relation avec lui même)
- R symétrique : $\forall (x, y) \in E^2, xRy \Rightarrow yRx$
- R transitive : $\forall (x, y, z) \in E^3, xRy$ et $yRz \Rightarrow xRz$

Une classe d'équivalence d'un élément x, notée $[x]$, est alors simplement défini comme le sous ensemble de E contenant tous les éléments de E en relation avec x, soit plus formellement : $x \in E, \forall y \in E, y \in [x] \Leftrightarrow yRx$. Avec ceci en tête, examinons maintenant la relation $R : \mathbb{H}^2 \to \mathbb{H}^2$

$$|\boldsymbol{\Psi}\rangle R |\boldsymbol{\Psi'}\rangle \Leftrightarrow \exists z \in \mathbb{C} / \begin{cases} |\boldsymbol{\Psi}\rangle R |\boldsymbol{\Psi'}\rangle \Leftrightarrow |\boldsymbol{\Psi}\rangle = z|\boldsymbol{\Psi'}\rangle \\ |z| = 1 \end{cases} \tag{3.9}$$

R est une relation d'équivalence (la réfléxivité, la symétrie et la transitivité sont toutes trivialement vérifiées). Deux QuBit appartenant à une même classe d'équivalence sont égaux, à une multiplication par un complexe z de module 1. Un tel $z = e^{i\theta}$ est appelé un facteur de phase. Un QuBit pur est alors simplement un représentant d'une classe d'équivalence de la relation d'équivalence évoquée ci-dessus. Multiplier un état par un facteur de phase ne changera par la probabilité d'être mesuré dans un état $|\boldsymbol{\alpha}\rangle$ donné. En effet :

$$P(\ M(z|\boldsymbol{\Psi}\rangle) = |\boldsymbol{\alpha}\rangle\ ) = \langle z|\boldsymbol{\Psi}\rangle / |\boldsymbol{\alpha}\rangle\rangle \tag{3.10}$$

$$= |e^{i\theta}| \langle |\boldsymbol{\Psi}\rangle / |\boldsymbol{\alpha}\rangle\rangle \tag{3.11}$$

$$= P(\ M(|\boldsymbol{\Psi}\rangle) = |\boldsymbol{\alpha}\rangle\ ) \tag{3.12}$$

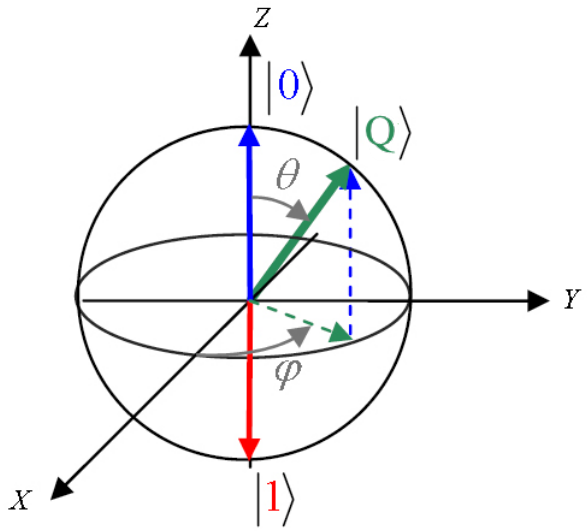

FIGURE 3.1 – *Visualisation d'un état quantique dans la sphère de Bloch.*

On peux alors supposer que deux vecteurs de $\mathbb{H}^2$ sont équivalents s'ils ne différent que par un facteur de phase, ce qui amène à la réécriture suivante :

$$\forall |\mathbf{\Psi}\rangle \in \mathbb{H}^2, \exists \theta \in [0,\pi] \ / \ |\mathbf{\Psi}\rangle = \cos(\theta/2) \cdot |\mathbf{0}\rangle + \sin(\theta/2) e^{i(\varphi)} \cdot |\mathbf{1}\rangle \quad (3.13)$$

$$\equiv \cos(\theta/2) e^{-i(\varphi/2)} \cdot |\mathbf{0}\rangle + \sin(\theta/2) e^{i(\varphi/2)} \cdot |\mathbf{1}\rangle \quad (3.14)$$

Sous cette nouvelle forme, il est possible de représenter tout QuBit pur comme point sur une sphère, où θ et φ font office de colatitude et longitude (voir figure 3.1). La correspondance entre l'espace des QuBit purs et une sphère de Bloch est un isomorphisme : une application bijective entre deux espaces, dont la réciproque est également bijective. On constate cependant sur la figure 3.1 que la linéarité n'est pas préservée (en effet, $|\mathbf{0}\rangle \neq -|\mathbf{1}\rangle$). Il faut ainsi considérer cette relation comme une occasion de visualiser plus simplement l'état des QuBits, mais ne permettant pas nécessairement d'interprétations graphiques cohérentes.

3.2.4 extension à plusieurs QuBits

Le passage de un à deux QuBit apporte de nombreuses nouveautés et dévoile une complexité qui pourrait sembler à priori innatendue. Mais c'est cette dernière qui donne tout son potentiel à l'informatique quantique. Pour expliquer ce dernier, il est nécessaire de définir le produit tensoriel $\otimes$ de deux QuBits (3.15) .

$$(\cdot)\otimes(\cdot):\begin{cases}\mathbb{H}^2\times\mathbb{H}^2\to\mathbb{H}^4\\ (|\boldsymbol{\varphi}\rangle,|\boldsymbol{\Psi}\rangle)\mapsto|\boldsymbol{\varphi}\rangle\otimes|\boldsymbol{\Psi}\rangle=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}\lambda\\ \mu\end{pmatrix}=\begin{pmatrix}\alpha\lambda\\ \alpha\mu\\ \beta\lambda\\ \beta\mu\end{pmatrix}\end{cases}\tag{3.15}$$

Le produit tensoriel de deux espaces $\mathbb{H}^2$, qui corresponds à l'espace dans lequel deux QuBits existent, est défini par un espace dont la base est égale à toutes les combinaisons possibles de produit tensoriels entre les vecteurs de bases des deux espaces de départ. C'est donc un espace de dimension 4 ayant pour base orthonormée :

$$\{|\mathbf{0}_{\boldsymbol{A}}\otimes\mathbf{0}_{\boldsymbol{B}}\rangle,|\mathbf{0}_{\boldsymbol{A}}\otimes\mathbf{1}_{\boldsymbol{B}}\rangle,|\mathbf{1}_{\boldsymbol{A}}\otimes\mathbf{0}_{\boldsymbol{B}}\rangle,|\mathbf{1}_{\boldsymbol{A}}\otimes\mathbf{1}_{\boldsymbol{B}}\rangle\}=\{|\mathbf{00}\rangle,|\mathbf{01}\rangle,|\mathbf{10}\rangle,|\mathbf{11}\rangle\}\tag{3.16}$$

$$=\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}\tag{3.17}$$

$$=\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}\tag{3.18}$$

On définit les états quantiques purs comme étant ceux pouvant s'écrire $|\boldsymbol{\varphi}\rangle\otimes|\boldsymbol{\Psi}\rangle$. En reprenant les coefficients utilisés dans l'equation (3.15), on en déduit que les états quantiques purs sont ceux de la forme :

$$|\boldsymbol{\varphi}\rangle\otimes|\boldsymbol{\Psi}\rangle=\alpha\lambda\cdot|\mathbf{00}\rangle+\alpha\mu\cdot|\mathbf{01}\rangle+\beta\lambda\cdot|\mathbf{10}\rangle+\beta\mu\cdot|\mathbf{11}\rangle\tag{3.19}$$

Les états quantiques n'étant pas purs sont dits intriqués, et l'existence de ces derniers a remis en cause le principe de localité que nous avons évoqués dans la partie 1. En effet, si l'on considère l'état de Bell : $|\boldsymbol{\Psi}\rangle=\frac{1}{\sqrt{2}}\cdot(\ |\mathbf{00}\rangle+|\mathbf{11}\rangle\ )$, alors une mesure de l'un des deux QuBit dans sa base respective nous donnera immédiatement l'information de la mesure du second QuBit dans sa propre base, même si les deux QuBit, après intrication, sont séparés d'un potentielle très grande distance [1].

Il semblerait tentant de faire un parallèle à l'informatique classique : deux bits peuvent ainsi former un registre dans seulement 4 états possibles : $00, 01, 10, 11$. Cependant, là où il n'y a que quatre possibilités fixes en informatique classiques, il

1. Des tests expérimentaux confirme de nos jours cet effet pour une distance supérieure à 10km.

est nécessaire de se rappeler que dans $\mathbb{H}^4$, les vecteurs / registres de deux QuBits sont des combinaisons linéaires des vecteurs $\{|\mathbf{00}\rangle, |\mathbf{01}\rangle, |\mathbf{10}\rangle, |\mathbf{11}\rangle\}$. Cela veut donc dire qu'avant une mesure, un registre de QuBit effectue simultanément les calculs pour **chacune** des quatre possibilitées. Pour un registre de deux QuBit, nous avons donc $4 = 2^2$ calculs effectués en parallèle. Un registre de trois QuBits réaliserait ainsi $8 = 2^3$ calculs en parallèle. Ainsi, chaque ajout de QuBit augmente exponentiellement (en 2^n, où n est le nombre de QuBits du registre quantique concerné) la puissance de calcul comparé à l'équivalent registre composé de bits classiques.

Il convient en revanche de clarifier les affirmations faites précédemment. Un registre quantique de taille n fera effectivement 2^n calculs en parallèle. En revanche, avant une mesure, il nous est impossible d'exploiter cette puissance de calcul, et post-mesure, nous n'obtiendrons qu'un seul résultat. C'est pour cela que la puissance quantique ne s'applique pas à tout type de problème, et qu'il est si dur de créer de nouveaux algorithme quantiques : en plus d'obéir à une nouvelle forme de logique, il est nécessaire de créer un algorithme utilisant cette puissance de calcul en parallèle, mais dont le résultat final ne nécessite qu'une seule valeur [2].

3.3 Portes logiques

3.3.1 évolution dans le temps d'un QuBit

Les relations établies dans les parties précédentes ont été écrites dans un espace $\mathbb{H}^2$ concernant un unique QuBit, puis généralisées à un ensemble de deux QuBit. Le passage à un nombre supérieur de QuBit s'effectuera exactement de la même manière, avec le produit tensoriel, défini de manière légèrement plus généralisée, pour pouvoir s'appliquer à deux espaces $\mathbb{H}_1$ et $\mathbb{H}_2$ de dimension quelconque.

Nous pouvons donc désormais considérer un état quantique appartenant à un espace $\mathbb{H}^{2^n}$, c'est-à-dire un registre composé de n QuBits. Notons cet espace plus simplement $\mathbb{H}^{\otimes n}$. Il est alors possible de donner l'équation de Schrödinger, qui décrit l'évolution dans le temps de tout état quantique précédant une mesure par :

$$\frac{d\Psi(t)}{dt} = -iH\Psi(t) \tag{3.20}$$

Où H est l'opérateur Hamiltonien. Dans ce cas particulier de la résolution de l'équation de Schrödinger **(pour l'instant, j'ai du mal à comprendre parfaitement d'où sortent les hypothèses menant aux simplifications donnant l'equation ci-dessus)**, nous avons tout simplement une solution de la forme $\Psi(t) = U(t)\Psi(0)$, où $U(t) = e^{-itH}$. Notons que cette évolution temporelle ne modifie pas la norme de l'état quantique Ψ.

2. Dans la dernière section sont rapidement présentés quelques algorithmes quantiques réputés.

3.3.2 algèbre des portes logiques

Faire fonctionner un ordinateur classique requiert de savoir créer des bits (de nos jours, il s'agit de transistors de quelques dizaines de nanomètres), mais également de pouvoir utiliser des opérations sur ces derniers. Ainsi, avec des portes NOT, AND, OR, XOR etc, il est possible de fabriquer toutes les opérations indispensables à un algèbre de base, donnnant ainsi à l'ordinateur une grande puissance de calcul.

L'analogie avec l'ordinateur quantique est parfaitement justifiée : il nous faut créer des portes logiques quantiques pouvant agir sur des QuBits afin de pouvoir faire d'un ordinateur quantique une réalité. De manière générale, une porte logique est une application de la forme :

$$L(...) : \begin{cases} \mathbb{H}^{\otimes n} \times \mathbb{H}^{\otimes n} \times \mathbb{H}^{\otimes n} \times ... & \to \mathbb{H}^{\otimes n} \times \mathbb{H}^{\otimes n} \times \mathbb{H}^{\otimes n} \times ... \\ (|\boldsymbol{\varphi}\rangle, |\boldsymbol{\Psi}\rangle, |\boldsymbol{\Omega}\rangle, ...) & \mapsto (L(\varphi), L(\Psi), L(\Omega), ...) \end{cases} \tag{3.21}$$

C'est donc simplement une application linéaire qui a un nombre donné de QuBit tous de même dimension, renvoi un même nombre de QuBits dans un état potentiellement différent. Une porte quantique n'effectuant pas de mesure, il est nécessaire que la transformation maintienne la condition de normalité. Au final, pour représenter une porte logique, il suffira d'utiliser une matrice M de norme 1. L'état de chaque QuBit après passage dans L sera ainsi facilement calculé par $L(\Psi) = M \cdot \Psi$. Par définition, il apparait que le calcul quantique est spontanément réversible. On en déduit ainsi que toute matrice définissant une porte logique quantique sera inversible (donc de déterminant non nul).

3.3.3 portes logiques à 1 QuBit

Nous allons maintenant nous intéresser à plusieurs portes quantiques classiques, en commençant bien sur par le niveau le plus bas : les portes agissant sur un registre d'un seul QuBit. Nous allons définir deux porte quantiques, phase L_Φ et rotation L_α, à partir desquelles il est possible de reconstruire toutes les portes de "dimension 1". Notons $Mat()$ l'application qui à une porte quantique associe l'unique matrice la représentant (on se positionne dans la base orthonormée $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$). Alors :

$$Mat(L_\Phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \tag{3.22}$$

$$Mat(L_\alpha) = \begin{pmatrix} cos(\alpha) & sin(\alpha) \\ -sin(\alpha) & cos(\alpha) \end{pmatrix} \tag{3.23}$$

La première porte ajoute un vecteur de phase à la composante en $|\mathbf{1}\rangle$, tandis que la seconde effectue une rotation de α du QuBit. Ces transformations rappellent exactement la définition d'un point sur la sphère de Bloch (equation 3.13), ce qui nous permet d'affirmer qu'il est effectivement possible d'aboutir à n'importe

quelle transformation à partir de ces deux portes logiques. On peux ainsi définir la classique porte NOT (négation du QuBit) et la porte de Hadamard :

$$Mat(NOT) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.24}$$

$$Mat(HADAMARD) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.25}$$

Si l'interprétation de la porte NOT est immédiate, il convient de revenir rapidement sur la porte de $HADAMARD$. C'est une porte indispensable en programmation quantique : en effet, elle sert souvent de première étape lors d'un algorithme, pour faire passer un registre d'un état initial $|\mathbf{0}\rangle_i$ pour chacun de ses QuBit à un état final de superposition des 2^n états $|\mathbf{0}\rangle_i$ et $|\mathbf{1}\rangle_i$ de norme toutes égales.

3.3.4 portes logiques à 2 QuBit (j'ai choisi de pas parler de la porte CU)

Certaines portes logiques à deux QuBit suivent une certaine logique : l'un des deux QuBit est appelé QuBit contrôle (d'où $CNOT = Controlled\ NOT$), et l'autre QuBit cible (usuellement, nous les "positionnons" dans cet ordre). L'idée est alors de vérifier l'état du QuBit de contrôle, et d'agir -ou non- sur le QuBit cible en fonction da la valeur du QuBit de contrôle.

Nous pouvons alors très facilement définir deux premières portes quantiques sur deux QuBits : la porte $CNOT$ qui appliquera ou non la transformation NOT sur le QuBit cible, et la porte $CPHASE$ qui appliquera potentiellement une phase au QuBit ciblé. Enfin, la porte $SWAP$ va simplement échanger les composantes $|\mathbf{01}\rangle$ et $|\mathbf{10}\rangle$. Voici leur matrices :

$$Mat(CNOT) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.26}$$

$$Mat(CPHASE) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\Phi} \end{pmatrix} \tag{3.27}$$

$$Mat(SWAP) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.28}$$

3.3.5 Ensemble universel

Un ensemble universel est un ensemble de portes quantiques tel que tout calcul quantique soit décomposable en opération composées de ces différentes portes. Les ensembles $\{PHASE, ROTATION, CPHASE\}$ et $\{PHASE, ROTATION, CNOT\}$ **(PREUVE ? !)** sont de tels ensembles universels. En effet, avec les deux premières portes, toute opération sur un unique QuBit est réalisable, tandis qu'avec la porte $CPHASE$ ou $CNOT$, une intrication est possible, ce qui permet de "descendre en dimension" et donc assurer que tout calcul est réalisable.

4. Simulation d'algorithme quantiques

4.1 Algorithme de Shor

4.2 Algorithme de Grover

Conclusion

...

Bibliographie

...

Annexe