Principes fondamentaux de l'information quantique

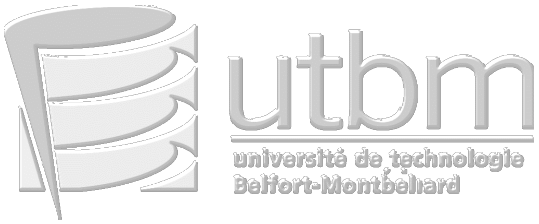
En vue de l'obtention de l'unité de valeur

AC20

Écrit le : *22/06/2014* **par :**

Budai Lucas, Jaffali Hamza, Nounouh Ismaël

Semestre de printemps 2014



Établissement :
Université Technologique de Belfort Montbéliard
Président du jury :
BRIAND Michel
Professeur encadrant :
HOLWECK Frédéric

Remerciements

C'est avec grand plaisir que nous souhaitons adresser ici toute notre reconnaissance à Frédéric Holweck, qui nous a accompagné durant tout ce semestre pendant lequel il a été notre suiveur dans cette UV d'acquisition de connaissances. Nous le remercions particulièrement de nous avoir fait découvrir les fondements de la théorie de l'information quantique, et de nous avoir proposé ce sujet d'AC20. Il convient également de remercier les professeurs de mathématiques du Tronc Commun de l'UTBM, ainsi que ceux de l'enseignement secondaire, qui nous ont fourni les outils nécessaires à la compréhension des calculs et des concepts mathématiques relatifs à ce sujet.

Nous tenons également à remercier l'UTBM, notamment son directeur, Pascal Brochet, de nous permettre d'étudier durant toute l'année dans cette école. Ces remerciements ne seraient pas complets sans un remerciement à Michel Briand, responsable de l'UV AC20, permettant aux édutiants, chaque semestre, d'approfondir des sujets qui les tiennent à cœur.

Enfin, nous remercions notre famille et nos proches de nous avoir soutenu durant ce semestre, et durant nos études en général.

Table des matières

Chapitre 1

Introduction aux Qubits

Dans ce chapitre nous définirons tous d'abord ce qu'est un qubit par rapport à un bit classique et les 3 grands postulats qui régissent la théorie de l'information quantique. Nous poursuivrons avec l'introduction d'états composés de deux ou plusieurs qubits. Enfin, nous verrons quelles sont les différentes manières de manipuler un état à un ou plusieurs qubits.

1.1 Bits classiques vs Bits quantiques dit Qubits

L'information la plus simple d'un ordinateur est le bit (Bynary digit originellement). Le bit est la quantité minimale d'information d'un message et est l'unité de mesure de base en informatique. Celui-ci ne peut prendre que deux valeurs : 0 ou 1. Les bits sont manipulés par nos ordinateurs au moyen de processus physiques simples et véhiculants des informations binaires : vrai/faux, on/off, 0/1... Le bit quantique ou qubit est l'analogue quantique du bit classique et représente un système quantique à 2 états de base : $|0\rangle$ et $|1\rangle$. Pour distinguer les états quantiques des états classiques on les note : $|0\rangle$ ou$|1\rangle$ suivant une convention introduite dans les années 1930 par le physicien Paul Dirac [1]. La principale différence avec un bit classique est que le qubit, étant un bit quantique, peut se trouver dans une infinité d'états entre $|0\rangle$ et $|1\rangle$. On note généralement un qubit $|\psi\rangle$ dans la base $\{|0\rangle$,$|1\rangle\}$.

La notation usuelle pour un qubit $|\psi\rangle$ dans la base $\{|0\rangle, |1\rangle\}$ est

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

α et β sont des nombres complexe, α, $\beta \in \mathbb{C}$. Ainsi $|\alpha|^2$ et $|\beta|^2$ sont en fait les probabilités pour $|\psi\rangle$ de se trouver dans les états $|0\rangle$ ou $|1\rangle$ avant d'avoir été mesurés. On a alors $|\alpha|^2 + |\beta|^2 = 1$.

1.1.1 Le chat de Schrödinger

Pour clarifier l'infinité d'états que peut prendre un qubit prenons l'exemple du chat de Schrödinger [2]. Le chat de Schrödinger est une expérience imaginée en 1935 par le physicien Erwin Schrödinger, elle met en avant un important postulat de la mécanique quantique qui est celui de la mesure mais permet aussi de comprendre la capacité d'un état quantique à avoir une

1. 1902-1984 Il est considéré comme l'un des "pères" de la mécanique quantique et il a aussi prévu l'existence de l'antimatière.

2. Erwin Schrödinger (1887-1961) est physicien et théoricien autrichien. Il a permis le développement du formalisme théorique de la mécanique quantique.

infinité d'états superposés. Par le biais de cette expérience nous espèrons vous faire comprendre qu'un état quantique est assimilable ici à un qubit et est une superposition d'états tant que celui-ci n'a pas été mesuré. On peut ainsi introduire un premier postulat quantique.

Un chat est enfermé dans une boîte avec un flacon de gaz mortel et une source radioactive. Un compteur Geiger mesure les radiations dans la boite. A un certain seuil le flacon est brisé et le chat meurt. Selon l'interprétation de Copenhague [3], le chat est à la fois vivant et mort. Pourtant, en ouvrant la boîte, et donc en effectuant une mesure, nous pourrons observer que le chat est soit mort, soit vivant. On pose $|0\rangle$ = chat mort et $|1\rangle$ = chat vivant avec $|\alpha|^2$ la probabilité de mort et $|\beta|^2$ la probabilité d'être vivant. Alors on note $|\psi\rangle$ représentant l'état du chat, on obtient alors le système suivant :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

Notre intuition nous dit que les phrases " le chat est mort " et " le chat est vivant " sont chacune la négation de l'autre. En fait, il existe une troisième possibilité : le chat peut être dans un état de superposition, dans lequel il cumule plusieurs états classiques incompatibles, vivant et mort. Cela illustre parfaitement la superposition des qubits car tant que la mesure n'est pas faite, pour l'observateur, le chat est dans une superposition des ces états incompatibles. Bien qu'illogique au niveau macroscopique (le chat), ce principe de superposition des états, pour les particules telles que les électrons ou les photons, est à ce jour la meilleure formalisation pour décrire les résultats expérimentaux en mécanique quantique [4].

"I think I can safely say that nobody understands quantum mechanics."
-Richard Feynman

1.2 Les postulats quantiques et les qubits

Nous allons maintenant préciser les quelques postulats de la mécanique quantique. Ceux-ci serviront de base à la théorie de l'information quantique.

1.2.1 Postulat de l'état d'un système quantique

Les états d'un système quantique sont des éléments d'un espace vectoriel aussi appelé espace de Hilbert noté $\mathbb{H}$. La dimension de cet espace peut être finie ou infinie selon les cas étudiés.

Les états du sytème quantique d'un qubit sont les éléments d'un espace à deux dimensions, engendrés par les états de base $|0\rangle$ et $|1\rangle$. Tous les états seront donc de la forme (1.1) dans la base $\{|0\rangle\ ,|1\rangle\}$. La notation abstraite de Dirac (1.1) pour l'état $|\psi\rangle$ peut conduire à plusieurs représentations mathématiques : l'état peut être représenté par une fonction ψ(r,t). Par une matrice (le plus souvent dans le cas où l'espace étudié est de dimension fini). Ou bien par une matrice de fonctions.
Prenons le cas d'un espace à deux dimensions.
Notre espace est ici fini il est donc plus simple d'utiliser une repésentation matricielle :

$$|0\rangle \rightarrow \begin{pmatrix}1\\0\end{pmatrix}; |1\rangle \rightarrow \begin{pmatrix}0\\1\end{pmatrix} \tag{1.3}$$

3. Interprétation de la physique quantique de plusieurs physicien dont Niels Bohr, Werner Heisenberg, Pascual Jordan, Max Born. Schrödinger inventa son expérience du chat de Schrödinger pour se moquer gentillement de leur interprétation.

4. Pour plus d'explication sur la superposition des états physiques, voir Chapitre 2

et ainsi :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{1.4}$$

Rappelons des bases d'algèbre linéaire exprimées dans la notation de Dirac. Celles-ci nous serons utiles par la suite dans des exemples et démonstrations.
-le *produit scalaire hermitien* de deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ est noté $\langle\psi|\phi\rangle$.
Le produit scalaire hermitien satisfait $\langle\psi|\phi\rangle = \overline{\langle\phi|\psi\rangle}$ et $\langle\psi|\lambda_1\phi_1 + \lambda_2\phi_2\rangle = \lambda_1\langle\psi|\phi_1\rangle + \lambda_2\langle\psi|\phi_2\rangle$.
Les états $\langle 0|$, $\langle 1|$ et $\langle\psi|$ sont représentés par des matrices lignes :

$$\langle 0| \rightarrow \begin{pmatrix}1 & 0\end{pmatrix}; \langle 1| \rightarrow \begin{pmatrix}0 & 1\end{pmatrix}; \langle\psi| \rightarrow \begin{pmatrix}\bar{\alpha} & \bar{\beta}\end{pmatrix} \tag{1.5}$$

-la *norme* d'un vecteur $|\psi\rangle$ est : $||\psi|| = \sqrt{\langle\psi|\psi\rangle}$. Les états de base sont orthonormés ce qui équivaut à :

$$\langle 0|1\rangle = 0\,;\ \langle 0|0\rangle = \langle 1|1\rangle = 1 \tag{1.6}$$

Avec des états $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$ la représentation matricielle conduit à

$$\langle\psi|\phi\rangle = \begin{pmatrix}\bar{\alpha} & \bar{\beta}\end{pmatrix}\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \bar{\alpha}\gamma + \bar{\beta}\delta \tag{1.7}$$

1.2.2 Postulat de la mesure

Nous l'avons déjà partiellement évoqué avec l'expérience du chat de Schrödinger, nous allons maintenant expliquer plus en détail le principe de la mesure en information quantique.
Prenons un état :
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dans un espace $\mathbb{H}$ il est donc dans une superposition de 2 états dans notre cas. On soumet cet état à une mesure, on le projette donc dans une base $\{|0\rangle, |1\rangle\}$. Le résultat de la mesure est obtenu avec une certaine probabilité dont l'amplitude est définie par :

$$|\alpha|^2 = |\langle 0|\psi\rangle|^2 \tag{1.8}$$

amplitude de probabilité d'obtenir l'état $|0\rangle$ après mesure.

$$|\beta|^2 = |\langle 1|\psi\rangle|^2 \tag{1.9}$$

amplitude de probabilité d'obtenir l'état $|1\rangle$ après mesure.
Le point important à retenir est qu'effectuer une mesure transforme le qubit. Si nous avons un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et que l'on effectue une mesure sur celui-ci alors dans ce cas $|\psi\rangle = |0\rangle$ ou $|1\rangle$, autrement dit le qubit $|\psi\rangle$ a été projetté dans la base $\{|0\rangle, |1\rangle\}$. Imaginons que la mesure nous donne le résultat $|0\rangle$ et bien il est maintenant impossible d'effectuer la moindre opération sur l'état $|\psi\rangle$ car la mesure a modifié notre état et l'a transformé en $|\psi\rangle = |0\rangle$. Il est alors impossible de retirer des informations supplémentaires sur ce qubit.

1.2.3 Postulat d'évolution

Est-ce que l'état quantique évolue avec le temps ou bien reste-t-il constant tant que l'on ne le modifie pas par mesure ou opération ?

L'évolution d'un système quantique fermé, c'est à dire sans interaction extérieure, est décrit par

une transformation unitaire. Cette évolution de l'état provient de l'application d'un opérateur linéaire, nommé l'opérateur d'évolution. Prenons un état $|\psi\rangle$ d'un système quelconque au temps t_1, et bien cet état est lié à l'état $|\psi'\rangle$ du système au temps t_2 par l'opérateur d'évolution U qui dépend seulement du temps entre t_1 et t_2.

$$|\psi'\rangle = U|\psi\rangle \tag{1.10}$$

Le problème étant que l'on ne connait pas l'opérateur d'évolution U. En fait l'évolution du système est gouvernée par l'équation de Shrödinger :

$$i\bar{h}|\psi(t)\rangle = H|\psi(t)\rangle \tag{1.11}$$

avec H l'opérateur hamiltonien, qui est l'opérateur quantique associé à l'énergie totale du système. Nous verrons plus en détails cette équation dans la suite du rapport durant la manipulation d'états et les opérateurs sur un qubits.

1.3 Système d'états à un ou plusieurs qubits

Nous avons pu voir précédemment que les qubits se différencient des bits classiques entre autres par leurs états. En effet, les bits élémentaires ne peuvent jouir que de 2 états différents : 0 et 1 , à l'inverse des qubits qui eux peuvent se trouver dans d'autres états (une infinité) que les états $|0\rangle$ et $|1\rangle$.
De ce fait, l'état d'un qubit peut être assimilé à un vecteur dans un espace à deux dimensions :

- l'un des états de base $|0\rangle$ ou $|1\rangle$

- ou plus généralement une superposition de ces états de base : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

De même, l'état d'un système à 2 qubits est un vecteur dans un espace à 4 dimensions :

- l'un des 4 états de base : $|00\rangle$,$|01\rangle$,$|10\rangle$ ou $|11\rangle$

- ou une superposition d'états de base : $|\psi\rangle$=$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ avec $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$;
où l'état $|00\rangle$ signifie l'état $|0\rangle$ du premier qubit et l'état $|0\rangle$ du deuxième qubit.

Par ailleurs, cette représentation du système, constituée des 2 qubits, par un vecteur pourrait être mise sous forme d'un produit tensoriel (voir annexe) des états des 2 qubits en question. Cependant nous verrons par la suite qu'il existe des systèmes d'états qui ne peuvent pas être mis sous cette forme : ce sont les états intriqués (ou encore enchevêtrés). C'est cette particularité qui est le plus souvent exploitée dans les algorithmes quantiques.

1.3.1 Produit de deux qubits (états séparables)

Tout d'abord, nous allons définir ce qu'est un système à 2 qubits (obtenu comme "produit" de 2 systèmes à 1 qubit). Soient deux qubits dont les états sont représentés par $|\psi_A\rangle$ et $|\psi_B\rangle$, tels que :

$$|\psi_A\rangle = a|0_A\rangle + b|1_A\rangle$$

$$|\psi_B\rangle = c|0_B\rangle + d|1_B\rangle$$

avec : $|a|^2 + |b|^2 = 1$ et $|c|^2 + |d|^2 = 1$

L'état du système à 2 qubits est donc défini par le produit tensoriel (voir annexe) des deux états des qubits :

$$|\psi_A\rangle \otimes |\psi_B\rangle \iff (a|0_A\rangle + b|1_A\rangle) \otimes (c|0_A\rangle + d|1_A\rangle)$$

$$\iff |\psi_{AB}\rangle = a_1|0_A0_B\rangle + a_2|0_A1_B\rangle + a_3|1_A0_B\rangle + a_4|1_A1_B\rangle \; ; avec \sum_{i=1}^{4} |a_n|^2 = 1 \tag{1.12}$$

Un état à 2 qubits peut être représenté par une matrice de dimension 2x2 dans la base constituée des éléments $|0_A\rangle|0_B\rangle, |0_A\rangle|1_B\rangle, |1_A\rangle|0_B\rangle, |1_A\rangle|1_B\rangle$, qui est tout simplement l'analogie de la représentation de l'état d'un qubit par une matrice de dimension 2x1 dans la base $(|0\rangle, |1\rangle)$. Pour simplifier les notations, dans la plupart des cas, on note $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

D'où, $|\psi_A\rangle \sim \begin{pmatrix} a \\ b \end{pmatrix}$ et $|\psi_B\rangle \sim \begin{pmatrix} c \\ d \end{pmatrix}$

Et enfin, $|\psi_{AB}\rangle \sim \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$

Par ailleurs, cette représentation de l'état d'un système à 2 qubits est une forme particulière. En effet, il existe des systèmes à 2 qubits qui ne peuvent pas être mis sous la forme de l'équation 1.12 , on les nomme états intriqués.

Exemple de système à 2 qubits

On prend $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi_B\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. On obtient l'état du système de ces 2 qubits en calculant :

$$|\psi_A\rangle \otimes |\psi_B\rangle$$

.

On a donc,

$$|\psi_{AB}\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Remarque 1.1 *Dans cet exemple, nous avons commencé par choisir les états de deux qubits pour former un système d'état à deux qubits. Ceci étant dit, nous aurions pu faire l'inverse, c'est-à-dire choisir directement un système d'état à deux qubits, mais nous n'aurions pas eu la certitude de pouvoir retrouver une forme factorisée.*

1.3.2 Etats intriqués (non séparables)

Petite fable : [5] Nous sommes en 2100. Un de vos amis physicien, qui aime animer les soirées avec des tours de passe-passe, vous apporte une série de paires de dés. Il vous demande de les jeter une paire après l'autre. Vous gardez un souvenir cuisant du mini-trou noir de Noël dernier, et vous manipulez la première paire avec une extrême précaution. Finalement, vous vous risquez à la lancer, et vous obtenez un double 3. Vous jetez alors la deuxième paire : double 6. Enfin la suivante : double 1. Toujours des doubles. Les dés de cette fable se comportent comme des particules quantiques "intriquées". Chaque dé pris séparément est aléatoire et non truqué, mais son double intriqué donne toujours le même résultat que le premier ...

Comme nous avons pu le voir précédemment, les systèmes d'états à deux qubits peuvent être mis soit sous forme factorisable, c'est-à-dire sous la forme d'un produit tensoriel de deux états de

5. Pour la Science N°272 - juin 2000 - Anton Zeilinger

qubits, ou soit sous forme non factorisable, nommés états intriqués. En effet, la définition même d'un état intriqué est l'impossibilité d'écrire l'état du système sous forme d'un produit tensoriel de 2 système à un qubit.

Pour pouvoir distinguer ces deux formes de systèmes, nous allons voir la notion de rang d'une matrice. En effet le système d'état à 2 qubits peut être assimilé à une matrice de dimension 2x2 dans la base $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ (vu dans 1.1.2). De ce fait, $|\psi_{AB}\rangle$ est factorisable ssi le $rang(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}) = 1$. De même, $|\psi_{AB}\rangle$ n'est pas factorisable ssi le $rang(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}) = 2$.

Maintenant, arrive à notre esprit cette question : comment calculer le rang d'une matrice (dans notre cas de dimension 2x2) ? Et bien, ceci est très simple. Il suffit de savoir ce qu'est le rang d'une matrice. Par définition, le rang d'une matrice est égal au nombre de ses vecteurs lignes (respectivement ses vecteurs colonnes) sauf si l'une d'entre elles est combinaison linéaire des autres. De plus, on sait que le déterminant d'une matrice est nul si et seulement si les vecteurs colonnes (respectivement les vecteurs lignes) sont liés. Ainsi, pour savoir si $|\psi_{AB}\rangle$ est factorisable, il nous faudra calculer le determinant de sa matrice correspondante et par conséquent :

$$\begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix} = 0 \iff rang(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}) = 1 \iff |\psi_{AB}\rangle \text{ est factorisable} \iff |\psi_{AB}\rangle$$

est un <u>état séparable</u>

$$\begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix} \neq 0 \iff rang(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}) = 2 \iff |\psi_{AB}\rangle \text{ n'est pas factorisable} \iff |\psi_{AB}\rangle$$

est un <u>état intriqué</u>

Exemple d'état intriqué

Le premier état de Bell défini par $|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ est un état intriqué. En effet, $|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \sim \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Et $\frac{1}{\sqrt{2}} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = \frac{1}{2} \neq 0 \iff \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est une matrice de rang 2 et donc cet état est bien intriqué.

Remarque 1.2 *Dans cet exemple, nous parlons du premier état de Bell. Il en existe plusieurs, plus exactement 4. En effet, ces états sont obtenus en injectant les états basiques, c'est-à-dire,* $|00\rangle$ *;*$|01\rangle$ *;*$|10\rangle$ *ou* $|11\rangle$ *dans une porte logique particulière que nous verrons dans le chapitre suivant.*

Particularité des états intriqués

Comme nous avons pu le remarquer, les états intriqués ne font pas apparaître directement l'état individuel de deux qubits mais seulement l'état du système à deux qubits. Par ailleurs, on les nomme parfois états enchevêtrés pour bien mettre en relief l'existence d'une certaine corrélation entre les deux qubits. En effet, la mesure d'un des deux états des qubits permet de savoir directement (par simple déduction et sans aucun calcul) l'état du deuxième qubit. Effectivement, lorsque l'on effectue la mesure de l'état d'un qubit, qui quitte donc son état de superposition pour se stabiliser sur l'état $|0\rangle$ ou $|1\rangle$, nous en déduisons l'état du système à deux qubits et, par conséquent, ceci entraine la déduction de l'état du deuxième qubit. Ainsi, tant qu'aucune mesure n'est effectuée sur le système, l'état de chaque qubit n'est pas défini. C'est

tout particulièrement cette spécificité (corrélation) que l'on exploite pour la mise en œuvre de certains algorithmes en information quantique.

Exemple : Mesure d'un état intriqué à 2 qubits

Nous allons, encore une fois, utiliser le fameux état de Bell défini par, nous vous le rappelons, $|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Maintenant, supposons que nous mesurons l'état d'un des qubits et que nous trouvons l'état $|1\rangle$. Alors l'état du système à 2 qubits, c'est-à-dire, $|\psi_{Bell}\rangle$ serait projeté sur l'état $|11\rangle$. Et par conséquent, l'état du deuxième qubit serait obligatoirement dans l'état $|1\rangle$.

$$\text{Mesure sur le } 1^{er} \text{ qubit} \rightarrow |\psi_1\rangle = |1\rangle \Rightarrow |\psi_{Bell_2}\rangle = |11\rangle \Rightarrow \text{Etat du } 2^{eme}\text{qubit } \rightarrow |\psi_2\rangle = |1\rangle$$

Ceci n'est pas valable pour tous les systèmes à deux qubits. En effet, la différence avec un système à deux qubits factorisable (celui défini par l'équation 1.12) est que nous aurions eu comme état du système (avec la même supposition que précédemment) :

$$|\psi_{Factorisable}\rangle = \frac{a_1}{|a_1|^2 + |a_2|^2}|10\rangle + \frac{a_2}{|a_1|^2 + |a_2|^2}|11\rangle) = |1\rangle \otimes (\frac{a_1}{|a_1|^2 + |a_2|^2}|0\rangle + \frac{a_2}{|a_1|^2 + |a_2|^2}|1\rangle)$$

.

1.3.3 Système à n-qubits

Un système de n-qubits évolue dans un espace de Hilbert $\mathbb{H}_N$ à 2^n dimensions. C'est l'espace vectoriel engendré par le produit des vecteurs de base. Un système à n-qubits correspond au produit tensoriel de chacun de ses qubits :

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$$

Il existe deux façons de représenter la base dans laquelle s'exprime l'état d'un système à n-qubits. En effet, prenons pour illustration n=3. On obtient ainsi $2^n = 2^3 = 8$ éléments qui constituent la base, dans laquelle s'exprime l'état du système à 3 qubits, que l'on peut noter sous forme "binaire" : $|000\rangle, |001\rangle, ..., |111\rangle$. Par ailleurs, nous pouvons aussi noter ces éléments sous forme "décimale". De fait, les 2^3 états de base seront notés :

$$\begin{array}{ll} |000\rangle \rightarrow |0\rangle & |100\rangle \rightarrow |4\rangle \\ |001\rangle \rightarrow |1\rangle & |101\rangle \rightarrow |5\rangle \\ |010\rangle \rightarrow |2\rangle & |110\rangle \rightarrow |6\rangle \\ |011\rangle \rightarrow |3\rangle & |111\rangle \rightarrow |7\rangle \end{array}$$

Généralisons cette manière de representer les états basiques. Ainsi, pour un sytème à n-qubits, les 2^n états de la base seront notés $|x\rangle$ avec $x \in [0, 2^n - 1]$. On obtient donc :

$$|000...0\rangle \rightarrow |0\rangle$$

$$|000...1\rangle \rightarrow |1\rangle$$

$$|x_1x_2x_3...x_n\rangle \rightarrow |x\rangle \text{ avec } x = x_1 2^{n-1} + x_2 2^{n-2} + x_3 2^{n-3} + ... + x_n 2^0$$

Remarque 1.3 *Toutes les notions vues précédemment restent vraies pour les systèmes à n qubits.*

1.4 Théorème de non-clonage

Ce théorème de non-clonage élaboré par Wooters [6] et Zurek [7] en 1982 [8] énonce que l'on ne peut pas effectuer une copie d'un qubit qui se trouve dans un état de superposition, du moins une copie parfaite. Encore une fois, l'information quantique se différencie nettement de l'information classique qui elle peut effectuer l'opération "copie".

Remarque 1.4 *Nous verrons par la suite que l'on peut effectuer la copie des éléments basiques* $|0\rangle$ *ou* $|1\rangle$ *(l'analogie des bits classiques) et par conséquent l'information quantique n'est pas désavantagée par rapport à l'information classique.*

1.4.1 Démonstration

Le théorème dit qu'il n'existe pas d'opérateur unitaire U (voir section précédente) tel que $|\psi\rangle|b\rangle \xrightarrow{U} |\psi\rangle|\psi\rangle$. Nous allons voir que l'on peut démontrer ce théorème par l'absurde.

Hypothèse : Il existe U tel que $U|\psi\rangle|b\rangle=|\psi\rangle|\psi\rangle$ avec $|b\rangle$ l'état initial du qubit copié.
On a donc $\forall\psi$, $U|\psi\rangle|b\rangle=|\psi\rangle|\psi\rangle$

Prenons donc $|\beta\rangle$ tel que $|\beta\rangle \neq |\psi\rangle$. On a alors $U|\beta\rangle|b\rangle=|\beta\rangle|\beta\rangle$ avec U inchangé. Effectuons maintenant le produit hermitien de ces deux expressions (les deux résultats). On obtient :

$$\langle\beta|\langle\beta|\psi\rangle|\psi\rangle = \langle b|\langle\beta|U\dagger U|\psi\rangle|b\rangle$$

$$(\langle\beta|\psi\rangle)^2 = \langle b|b\rangle\langle\beta|\psi\rangle = \langle\beta|\psi\rangle$$

L'ensemble des solutions de cette équation est $\langle\beta|\psi\rangle = 0$, c'est-à-dire que les deux états doivent être orthogonaux, et $\langle\beta|\psi\rangle = 1$ ce qui équivaut à $|\beta\rangle = |\psi\rangle$.

Ainsi, la copie parfaite d'un état en superposition est impossible mais la copie d'un état basique tel que $|0\rangle$ ou $|1\rangle$ est faisable. On retrouve l'analogue classique de la porte COPY.

Remarque 1.5 *On peut également appliquer ce théorème pour des systèmes à 2 qubits. En effet, nous pouvons seulement effectuer la COPIE des éléments* $|00\rangle$,$|01\rangle$,$|10\rangle$ *ou* $|11\rangle$ *mais pas des états en superposition.*

Enfin, nous verrons qu'il existe tout de même un moyen de réaliser une copie sur un état superposé, mais que cela impliquera en pratique une augmentation du volume d'information traité.

1.5 Manipulation d'états à un ou plusieurs qubits

1.5.1 Opérateurs sur un qubit

Tant qu'un qubit n'est pas soumit à une mesure, ce dernier peut évoluer dans son état, de par l'éventuelle intéraction qu'il connaît avec son environnement. Cette transformation du qubit est en effet régie par le postulat d'évolution, explicité précedemment. En effet, l'évolution de cet état résulte en fait de l'application d'un opérateur linéaire, appelé opérateur d'évolution. Le postulat nous apprend, en outre, que cet opérateur jouit d'une propriété particulière : c'est un

6. William Kent Wootters est un physicien théoricien américain, et l'un des fondateurs du domaine de la théorie de l'information quantique.

7. Wojciech Hubert Zurek (né en 1951) est un physicien de premier plan du Los Alamos National Laboratory travaillant dans le domaine de la physique quantique, et en particulier sur la décohérence.

8. Nature Vol. 299 28 October 1982

opérateur unitaire (voir Annexe). Géométriquement, une transformation unitaire est une rotation d'un "solide indéformable" dans l'espace de Hilbert, c'est à dire, une transformation du vecteur représentant l'état du qubit, sans en changer sa norme.

Contrairement aux opérateurs classiques, par exemple les opérateurs logiques sur des bits classiques, qui ne sont pas toujours réversibles, les opérateurs unitaire, eux, le sont toujours. En effet, la réversiblilité d'une opération consiste à trouver l'opérateur inverse qui nous donne l'atécédent de l'image d'un objet, par l'application de l'opérateur. Ceci n'est pas toujours trivial pour des opérateurs logiques, mais pour des opérateurs unitaires, il suffira seulement d'inverser une matrice (voir plus loin).

Détermination de l'opérateur

Un qubit évolue donc (dans le temps) selon une transformation unitaire, par application sur ce deriner d'un opérateur. Il serait intéressant de se demander, dans la mesure où l'évolution de l'état est connue, quel est cet opérateur unitaire. En mécanique quantique, l'état à l'instant t d'un système est décrit par un élément $|\psi(t)\rangle$ de l'espace complexe de Hilbert. L'évolution temporelle de $|\psi(t)\rangle$ est en fait décrite par l'équation de Schrödinger :

$$\frac{\hat{\vec{\mathbf{p}}}^2}{2m}|\psi(t)\rangle + V(\hat{\vec{\mathbf{r}}},t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle \tag{1.13}$$

avec :

— i est l'unité imaginaire

— $\hbar$ est la constante de Planck réduite, $\hbar = \frac{h}{2\pi}$

— $\mathcal{H} = \frac{\hat{\vec{\mathbf{p}}}^2}{2m} + V(\hat{\vec{\mathbf{r}}},t)$ est l'opérateur hamiltonien, associé à l'observable "énergie totale du système"

— $\hat{\vec{\mathbf{r}}}$ est l'observable de position

— $\hat{\vec{\mathbf{p}}}$ est l'observable impulsion

L'équation de Schrödinger est une équation différentielle du premier ordre par rapport au temps. Ce qui signifie que la donnée d'un état initial $|\psi(t_0)\rangle$ suffit à déterminer $|\psi(t)\rangle$ à tout instant ultérieur t. Ceci n'est valable que si l'évolution n'est pas interrompue par une mesure d'une grandeur physique du système.

Cette équation est également linéaire et homogène. Ses solutions sont donc linéairement superposables. Si $|\psi_1(t)\rangle$ et $|\psi_2(t)\rangle$ sont deux solutions de l'équation (1.1) et si l'état initial du système est défini par $|\psi(t_0)\rangle = \lambda_1|\psi_1(t_0)\rangle + \lambda_2|\psi_2(t_0)\rangle$ alors l'état du système au temps t est donné par $|\psi(t)\rangle = \lambda_1|\psi_1(t)\rangle + \lambda_2|\psi_2(t)\rangle$. Il existe donc une correspondance linéaire entre $|\psi(t_0)\rangle$ et $|\psi(t)\rangle$.

Du fait de la correspondance linéaire entre $|\psi(t_0)\rangle$ et $|\psi(t)\rangle$, il existe un opérateur linéaire $U(t,t_0)$ tel que :

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

En réinjectant ceci dans l'équation (1.1), et après une succession d'opérations effectuées, on en déduit la solution formelle :

$$U(t,t_0) = \exp(-i\frac{(t-t_0)}{\hbar}\mathcal{H}\,)$$

On peut "ajuster" physiquement l'opérateur hamiltonien par un choix approprié d'interactions du système avec son environnement ce qui nous permettra donc de *piloter* l'évolution de son état quantique (voir Chapitre 2).

Exemple d'opérateurs unitaires

Comme explicité dans la première sous-partie, il est toujours possible d'exprimer un qubit sous forme d'un vecteur, en notation matricielle, dans la mesure où l'on a préalablement choisi une base. Ainsi, un opérateur unitaire sur un qubit ordinaire prendra la forme d'une matrice carrée d'ordre 2, qui plus est, unitaire (voir Annexe).

Etudions, dans un premier temps, et pour nous habituer à la notion d'opérateur, l'exemple de l'opérateur logique NON (NOT) connu pour les bits classiques. L'application NOT : $x \to \overline{x}$, réalise en effet :

$$0 \to 1$$
$$1 \to 0$$

Il serait intéressant dans notre cas de se demander s'il existe une opération unitaire analogue de NOT, qui réalise la même opération, mais sur des qubits, à savoir :

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to |0\rangle$$

On se place ici dans la base $|0\rangle, |1\rangle$. Nous pouvons ainsi utiliser la représentation matricielle des ces états de base. En effet :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Nous allons raisonner par analyse-synthèse pour vérifier que l'opérateur NOT est bien un opérateur unitaire. Supposons que l'opérateur NOT est un opérateur unitaire, donc linéaire. L'opérateur NOT peut ainsi être représenté par une matrice carrée, dépendante de la base choisie. En effet, cette matrice décrit comment l'on transforme par l'opérateur NOT, les vecteurs de la base. Posons alors X, la matrice de l'application NOT dans la base $|0\rangle, |1\rangle$.

On a donc :

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

On vérifie facilement que :

$$X|0\rangle = |1\rangle \text{ et } X|1\rangle = |0\rangle$$

La matrice X réalise donc bien l'opération de négation. Vérifions à présent que l'opérateur NOT est bien un opérateur unitaire. Pour ce faire, on vérifie que la matrice X est unitaire. Vérifions donc que $X\,{}^{\mathrm{t}}\overline{X} = I_2$.

Tout d'abord comme X est une matrice à coeffcients réels, $X = \overline{X}$. Or X est une matrice symétrique ($X = {}^{\mathrm{t}}X$). Il ne reste donc plus qu'à vérifier que $X^2 = I_2$. Et en effet :

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

Ainsi l'opérateur NOT est bien un opérateur unitaire. Si on applique cet opérateur à un état quelconque, on obtient :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{NOT} |\psi\rangle_N = \alpha|1\rangle + \beta|0\rangle$$

Par ailleurs, il existe d'autres matrices, autre que X ci-dessus, qui représentent une opération sur un qubit. En fait, toute matrice unitaire est susceptible de représenter une porte logique, ou un opérateur quelconque, à un qubit. Parmi celles qui sont particulièrement utilisées citons :

- la porte Y définie par la matrice $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ dont la table de vérité est :

$$|0\rangle \to i|1\rangle$$
$$|1\rangle \to -i|0\rangle$$

- la porte Z définie par la matrice $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ou opérateur de $flip$ dont la table de vérité est :

$$|0\rangle \to |0\rangle$$
$$|1\rangle \to -|1\rangle$$

- la porte de Hadamard définie par la matrice $H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ dont la table de vérité est :

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- la porte U_θ définie par la matrice $U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, rotation d'angle θ, dont la table de vérité est :

$$|0\rangle \to \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$$
$$|1\rangle \to \cos(\theta)|1\rangle - \sin(\theta)|0\rangle$$

Les quatres matrices X, Y, Z et H sont en effet étroitement liées. On peut ainsi rapidement établir les relations suivantes :

— $X^2 = Y^2 = Z^2 = H^2 = I_2$ (car matrices unitaires, à coefficients réels)

— $XY = iZ$, $YZ = iX$ et $ZX = iY$

— $HXH = Z$, $HYH = -Y$ et $HZH = X$

1.5.2 Opérateurs sur un état à deux (ou plusieurs) qubits

Tout comme un système à un qubit, un système à deux qubits évolue selon une transformation unitaire. Une matrice unitaire et carrée d'ordre 4 représente donc une transformation possible. De façon générale, toute opération unitaire sur un système à n-qubits peut être représentée par une matrice carée d'ordre 2^n. On pourra ainsi manipuler des états à plusieurs qubits, et réaliser des opérations plus complexes sur ces derniers.

En pratique, l'augmentation du nombre de qubits traités "simultanement" permettra de retranscrire un opérateur classique irréversible, en un opérateur quantique réversible. Ceci servira directement la mise en place d'algorithmes et circuits quantiques, notion qui sera introduite dans la prochaine sous-section 1.5.3.

Il apparaît donc intéressant d'étudier les principales portes logiques réversibles agissant sur des états à plusieurs qubits.

Porte c-NOT

La porte c-NOT, ou *controlled* NOT est souvent utilisée pour remplacer la porte NOT. Elle fonctionne de la manière suivante :

Etat d'entrée	Etat de sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

La porte c-NOT agit en effet sur un système à deux qubits. Le premier bit sert de contrôle (bit de *contrôle*) et le second bit (bit *cible*) subit ou pas une négation, en fonction de l'état du bit de *contrôle*. Sachant comment l'opérateur c-NOT tranforme les vecteurs de la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, on peut alors le représenter par une matrice, dans cette même base :

$$\text{c-NOT} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Ainsi, la valeur du bit *cible* est inchangée, si le bit de *contrôle* vaut 0 et la valeur du bit *cible* est changée, si le bit de *contrôle* vaut 1. En fait, le bit *cible* vaut à la sortie la somme, modulo 2, des deux bits d'entrée, tandis que le bit de *contrôle* reste inchangé. On note alors, c-NOT : $(x, y) \to (x, x \oplus y)$.

En plus de la notation matricielle, on peut introduire la représentation sous forme de circuit des opérateurs :

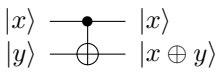


FIGURE 1.1 – Porte c-NOT

On voit donc ici que la porte c-NOT prend en entrée deux qubits simples : $|x\rangle$ et $|y\rangle$ formant à eux deux un système à deux qubits. Le système passe donc la porte c-NOT et cette dernière retourne le résultat attendu, à savoir : on retroune l'identité du premier qubit d'entrée sur le premier qubit de sortie, et on retourne une somme binaire entre les deux premiers qubits sur le second qubit de sortie.

La porte c-NOT est très utilisée dans les algortihmes quantiques. Elle peut d'ailleurs être ré-adaptée en prenant le premier bit comme *cible* et le second comme bit de *contrôle*.

Enfin, l'application de l'opérateur c-NOT à un état quelconque $|\psi\rangle$ donne :

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \xrightarrow{c-NOT} |\psi\rangle_S = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle$$

Porte SWAP

La porte SWAP, comme son nom l'indique, échange la place les deux qubits passés en paramètre : SWAP : $(x, y) \to (y, x)$. La porte SWAP se compose d'une succession de 3 portes c-NOT, avec alternance du bit de *contrôle* :

Vérifions que ce circuit realise bien l'opération d'échange des deux qubits $|x\rangle$ et $|y\rangle$.

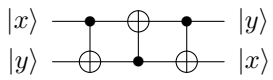
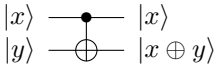


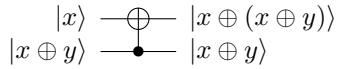
FIGURE 1.2 – Porte SWAP

Utilisation des circuits

En effet, après un passage sur la première porte c-NOT, avec premier qubit en contrôle, on obtient ceci :



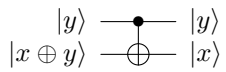
Ensuite, on applique une seconde porte c-NOT, avec second qubit en contrôle, et on obtient cela :



Or la somme binaire est associative et commutative, donc :

$$|x \oplus (x \oplus y)\rangle = |(x \oplus x) \oplus y\rangle = |y\rangle$$

Enfin, on passe par une troisième porte c-NOT, avec premier qubit en contrôle, et le résultat final donne :



Le circuit est donc bien valide.

Utilisation des matrices

Il est aisé de déterminer comment l'opérateur SWAP transforme les états de base d'un système à deux qubits :

Etat d'entrée	Etat de sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$

Cela nous permet alors d'écrire la matrice représentant l'opérateur SWAP :

$$\text{SWAP} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Le circuit nous dit que la porte SWAP est en fait une triple application de la porte c-NOT, en alternant la place du bit de *contrôle*. On appellera c-NOT$_1$ la porte c-NOT avec premier qubit en bit de *contrôle*, et c-NOT$_2$ la porte c-NOT en prenant l'autre qubit en *contrôle*. On a donc :

$$\text{c-NOT}_1 : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ et c-NOT}_2 : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

On sait que SWAP = c-NOT$_1$ $\circ$ c-NOT$_2$ $\circ$ c-NOT$_1$ d'après le circuit. On peut vérifier, grâce au produit matriciel suivant, que le circuit est bien valide :

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

Enfin, l'application de l'opérateur SWAP à un état quelconque $|\psi\rangle$ donne :

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \xrightarrow{SWAP} |\psi\rangle_S = \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle$$

Porte TOF

L'opérateur TOF, mis en place par Tommaso Toffoli [9] en 1980, peut être considéré comme un c-c-NOT (*controledcontroled* NOT). Cette porte apporte une grande aide dans la résolution du problème de réversibilité des portes logiques classiques, et nous verrons, sous peu, dans quelle mesure justement cette porte consitue une solution.

Tout d'abord, cette porte prend 3 qubits en entrée : les deux premiers servants pour le *contrôle* et le troisième étant le qubit *cible*. Cet opérateur réalise ainsi l'application unitaire suivante, TOF : $(x, y, z) \to (x, y, z \oplus xy)$. Le circuit correspondant à la porte de Toffoli est donc le suivant :

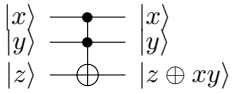


FIGURE 1.3 – Porte TOF

La porte TOF transforme les états de base d'un système à trois qubits comme suit :

9. Tommaso Toffoli (né en 1943 à Montereale Valcellina) est un scientifique et un universitaire italien. Il est professeur de génie électronique et d'informatique à l'université de Boston depuis 1995.

Etat d'entrée	Etat de sortie
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$
$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$

Ainsi :

$$\text{TOF} : \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Cette porte s'avèrera utile pour adapter et rendre réversible certaines portes logiques classiques.

1.5.3 Premieres applications

Générateur d'états de Bell

Il existe en effet une porte logique créant des états de Bell. Il suffit de lui introduire l'un des états de base d'un système à deux qubits ($|00\rangle, |01\rangle, |10\rangle$ ou $|11\rangle$) pour obtenir un des quatre états de Bell. Le circuit en question est le suivant :

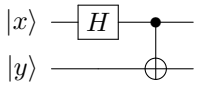
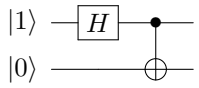


FIGURE 1.4 – Une porte créant des états de Bell

On applique la porte d'Hadamard au premier qubit du système, puis on utilise le résultat comme bit de *contrôle* dans la porte c-NOT, avec le second qubit du système comme bit *cible*. Si l'on introduit par exemple l'état $|00\rangle$ dans le circuit, on notera β_{00} l'état de Bell correspondant. Les quatres états de Bell seront donc : β_{00}, β_{01}, β_{10} et β_{11}.

Etudions le cas où l'état de base $|10\rangle$ est introduit à l'entrée du circuit. On a :



Appliquons la porte de Hadamard au premier qubit :

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Grâce au produit tensoriel, on reforme un système à 2 qubits, avec le second qubit inchangé depuis le départ :

$$H|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

Enfin, on applique la porte c-NOT à cet état à 2 qubits :

$$cNOT(H|1\rangle \otimes |0\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

Ainsi on obtient l'état de Bell associé à l'état de base $|10\rangle$:

$$\beta_{10} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

De la même manière, on construit les 3 autres états de Bell :

$$\begin{aligned} \beta_{00} &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ \beta_{01} &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ \beta_{11} &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

Il pourrait être intéressant de vérifier que ces états de Bell sont orthogonaux. Pour ce faire, on construit une matrice B en mettant les 4 vecteurs représentant les 4 états de Bell dans la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, dans chacune des colonnes de la matrice.

$$\mathrm{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

Il s'avère que la matrice B est une matrice unitaire, vérfiant ainsi : $B^{\mathrm{t}}\overline{B} = I_4$. Comme B est une matrice unitaire, ses colonnes forment une base orthonormée dans l'espace de *Hilbert* (voir Annexe). Donc les états de Bell sont deux à deux orthogonaux.

Théorème de non-clonage

Comme énoncé au chapitre précédent, l'opération COPY : $(x, b) \to (x, x)$ ne peut être effectuée sur un état de superposition $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ grâce à un simple opérateur sur 2 qubits. Néanmoins, on peut aisément copier les éléments de base $|0\rangle$ et $|1\rangle$. Pour ce faire, on utilise la célèbre porte c-NOT. On se propose donc de revérifier ces assertions.

On appelle $|b\rangle = \alpha|0\rangle + \beta|1\rangle$ la page blanche utilisée pour y copier le qubit $|x\rangle$. On se propose de vérifier pour quelles valeurs du qubit $|b\rangle$ la copie avec l'opérateur c-NOT est possible.

Prenons dans un premier temps $|x\rangle = |0\rangle$:
On cherche $|b\rangle$ tel que $cNOT|x\rangle|b\rangle = |x\rangle|x\rangle$. Or on a :

$$cNOT|x\rangle|b\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{pmatrix} \text{ et } |x\rangle|x\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

On en déduit donc que $\alpha = 1$ et $\beta = 0$. Donc on peut copier l'élément de base $|0\rangle$, losque l'on prend comme page blanche $|b\rangle = 0$. De la même manière, on peut copier l'élément de base $|1\rangle$ en prenant $|b\rangle = 0$.

Par contre, en prenant un état de superposition pour $|x\rangle = \lambda|0\rangle + \mu|1\rangle$, on peut montrer que la copie n'est pas possible. On pose toujours $|b\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$cNOT|x\rangle|b\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda\alpha \\ \lambda\beta \\ \mu\alpha \\ \mu\beta \end{pmatrix} = \begin{pmatrix} \lambda\alpha \\ \lambda\beta \\ \mu\beta \\ \mu\alpha \end{pmatrix} \text{ et } |x\rangle|x\rangle = \begin{pmatrix} \lambda^2 \\ \lambda\mu \\ \lambda\mu \\ \mu^2 \end{pmatrix}$$

Après simplification de l'égalité vectorielle, on obtient le système suivant :

$$\begin{cases} \alpha = \lambda \\ \beta = \mu \\ \beta = \lambda \\ \alpha = \mu \end{cases}$$

Pour copier l'état superposé $|x\rangle = \lambda|0\rangle + \mu|1\rangle$, il faut donc que $\alpha = \beta = \lambda = \mu$. Si cette condition est validée, cela implique que $|x\rangle = |b\rangle$, et donc que l'on ne peut pas considérer cette opération comme un clonge, puisque les deux états sont égaux dès le départ. Si cette condition n'est pas validée, alors la copie grâce à la porte c-NOT est impossible.

On voit donc que la porte c-NOT ne nous permet que de copier des éléments de base, mais pas d'états formés par une superposition de ces derniers.

Du circuit classique au circuit quantique

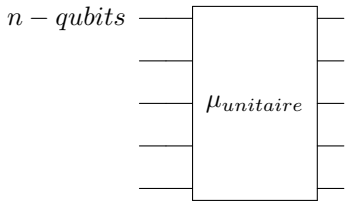
La principale différence entre les circuits classiques et quantiques, en plus de la différence de nature des objets manipulés, est le caractère réversibile ou non des opérations associées.

Définition 1 *Une porte logique L est réversible (ou inversible) si, pour toute sortie y, il existe une unique entrée x telle que L(x) = y. Si une porte L est réversible, il existe une porte inverse L' pour laquelle L'(y) = x. Selon le principe des tiroirs (voir Annexe), toute porte réversible doit avoir le même nombre de bits en entrée et en sortie.*

Un circuit classique peut être modélisé sous la forme d'une application f : $Z_2^n \to \{0, 1\}$. Cependant, cette application n'est pas inversible si n est différent de 1 (par exemple : NOT est inversible, mais pas NAND). En effet, une application inversible doit avoir le même nombre de bit en entrée et en sortie. Ainsi, tout circuit quantique réversible pourra être représenté par une application f : $Z_2^n \to Z_2^n$. Un circuit quantique prendrait donc la forme suivante :

Rappelons maintenant un théorème fondamental de la logique classique, qui nous sera utile pour la suite :

Théorème 1 *Toute porte logique peut être construite à partir de l'opération NAND et COPY.*



Remarque 1.6 *On dit que les portes NAND et COPY forment un jeu de portes logiques universelles. La porte NAND n'est pas inversible.*

En raison du caractère réversible des opération quantiques d'une part, et du théorème de non-clonage d'autre part, ni l'une ni l'autre de ces deux portes portes classiques (universelles), n'est directement transposable à l'information quantique. Il est cependant possible de transformer les algorithmes classiques irréversibles en algorithmes quantiques réversibles. Pour ce faire, une augmentation du volume d'information à traiter est indispensable. Cela se traduira en pratique par l'ajout de bits *auxiliaires* au traitement, en plus des bits indispensables en entrée.

Prenons l'exemple de la porte NAND. Cette porte, en effet irréversible, réalise l'opération suivante, NAND : $(x, y) \rightarrow \overline{xy}$. Cette porte prend donc initialement 2 bits en entrée. Nous allons démontrer qu'il est possible de modéliser la porte NAND grâce à la porte de Toffoli, manipulant ainsi trois bits au lieu de deux, dont un bit *auxiliaire*.

En imposant la valeur du troisième bit de la porte TOF (bit *cible*) à 1, la porte se comportera comme l'opération NAND. Faisons varier la valeur du couple formé par les deux premiers bits en entrée, en fixant le troisième bit à 1 :

Etat d'entrée	Etat de sortie
$\|001\rangle$	$\|001\rangle$
$\|011\rangle$	$\|011\rangle$
$\|101\rangle$	$\|101\rangle$
$\|111\rangle$	$\|110\rangle$

On remarque aisément que le troisième bit de sortie correspond en effet à la négation du produit binaire des deux premiers bits, même résultat après application de la porte NAND. On a donc :

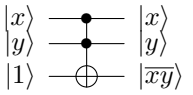


FIGURE 1.5 – Porte TOF modélisant NAND

La restranscription de la porte NAND irréversible grâce à la porte TOF réversible nécessite ici un seul bit auxiliaire.

Il est par ailleurs également possible de modéliser la porte COPY à l'aide de la porte TOF, mais le nombre de bit auxiliaires nécessaires à cette opération augmente considérablement cette fois-ci. Voici, sans détailler, le circuit permettant une telle modélisation :

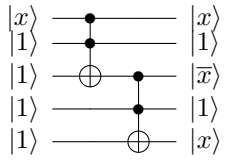


FIGURE 1.6 – Porte TOF modélisant COPY

On voit donc que la porte TOF permet à la fois de modéliser la porte NAND et COPY. Elle permet donc, d'après le théorème précédent, la modélisation de toutes les portes logiques classiques. Néanmoins, on pourrait se demander quelle serait l'analogie de ce théroème pour les portes réversibles. Cette analogie existe et en voici son énoncé :

Théorème 2 (Bennet [10] -Landauer [11] -Toffoli [12]) *Soit $N \geq 2, N := 2^n$. Toute application booléenne inversible $f : \mathbb{B}^N \to \mathbb{B}^N$ est calculable (avec variables auxiliaires) sur l'ensemble des portes $\{NOT, SWAP, TOF\}$.*

La traduction quantique $\{\hat{NOT}, \hat{SWAP}, \hat{TOF}\}$ des portes $\{NOT, SWAP, TOF\}$ nous permet une généralisation du précédent théorème à toutes les opérations unitaires :

Théorème 3 (Kitaev-Shen-Vialyi) *Soit $n \geq 2, n := 2^n$. Toute matrice unitaire $U_N \in SU(N)$, vue comme une porte à n-qubits, est calculée par un circuit sur l'ensemble de portes :*

$$\{\hat{NOT}, \hat{SWAP}, \hat{TOF}\} \cup \{U \mid U \in U(2)\}$$

Ce théorème nous informe donc que les portes réversibles de base (traduites en transformations unitaires) ainsi que toutes les portes à 1 qubit suffisent pour calculer n'importe quelle transformation unitaire sur N qubits.

Ainsi, à tout circuit classique irréversible, on pourra associer un circuit quantique réversible.

Chapitre 2

Représentation des qubits et Spin de l'électron

Dans ce chapitre, nous étudierons la représentation des qubits dans un espace à 3 dimensions ainsi que le spin de l'électron et sa manipulation avec la mécanique quantique.

2.1 La Sphère de Bloch

La sphère de Bloch, du nom du physicien et mathématicien Félix Bloch [1], est une représentation géométrique d'un état pur d'un système quantique à deux niveaux ; c'est donc, entre autre, une représentation d'un qubit. Celle-ci nous permet de représenter un qubit qui est initialement un état complexe dans un espace à trois dimensions tel que $\mathbb{R}^3$. Il est possible de généraliser la construction de cette sphère à un système à n niveaux. Nous allons tout d'abord exprimer cette sphère avec un seul qubit pour que cela soit plus facile puis nous essayerons de faire un rapprochement entre un qubit dans la sphère de Bloch et le spin d'un électron.

2.1.1 Représentation dans la Sphère de Bloch

On prend un état :$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ que l'on commence maintenant à connaitre.

On pose : $r_1 e^{i\theta_1}$ la forme exponentielle de α et $r_2 e^{i\theta_2}$ respectivement la forme exponentielle de β, avec $r_1, r_2 > 0$ et $0 < \theta < 2\pi$.

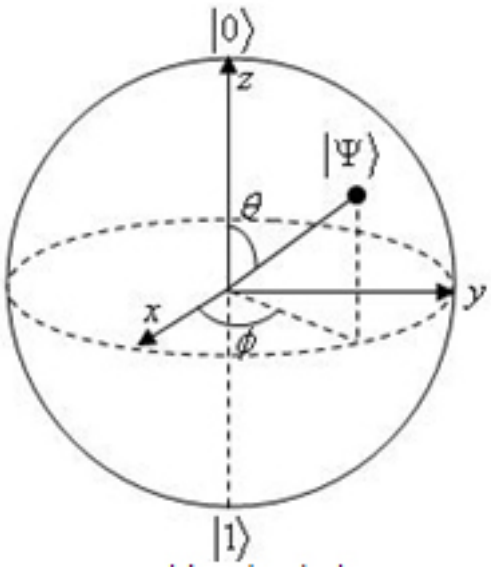
Donc :
$|\psi\rangle = r_1 e^{i\theta_1}|0\rangle + r_2 e^{i\theta_2}|1\rangle \Longleftrightarrow e^{i\theta_1}(r_1|0\rangle + r_2 e^{i(\theta_2-\theta_2)}|1\rangle)$

$On\, pose\, \phi = \theta_1 + \theta 2$ d'où :

$$|\psi'\rangle = e^{i\theta_1}(cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\phi}|1\rangle)$$

1. Felix Bloch (23 octobre 1905 – 10 septembre 1983) était un physicien suisse, il fut récompensé du prix Nobel de physique en 1952.

Nous allons maintenant représenter cet état dans la Sphère de Bloch qui est une représentation à trois dimensions :



Pour expliquer la différence de phase nous allons prendre deux états $|\psi\rangle$ et $|\psi'\rangle$ avec :
$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi'\rangle = e^{i\phi}|\psi\rangle = \frac{e^{i\phi}}{\sqrt{2}}(|0\rangle + |1\rangle)$ avec ϕ un réel.
Nous allons montrer que, dans n'importe qu'elle base, les deux états sont physiquement indiscernables.
Pour cela nous allons utiliser une autre base que celle que $\{|0\rangle; |1\rangle\}$. Nous allons prendre la base $\{|U\rangle; |U^{\perp}\rangle\}$.

On pose donc : $|U\rangle = \alpha|0\rangle + \beta|1\rangle$
et : $|U^{\perp}\rangle = \bar{\beta}|0\rangle - \bar{\alpha}|1\rangle$
On évalue $|\psi\rangle et |\psi'\rangle$:

$$\langle U|\psi\rangle = (\bar{\alpha}\langle 0| + \bar{\beta}\langle 1|)(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}} \Rightarrow |\psi\rangle = \frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}}|U\rangle + \frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}}|U^{\perp}\rangle$$

Et la probabilité d'observer $\langle U|\psi\rangle$ est :

$$|\langle U|\psi\rangle|^2 = \frac{|\bar{\alpha}+\bar{\beta}|^2}{2}$$

$$\langle U|\psi'\rangle = (\bar{\alpha}\langle 0| + \bar{\beta}\langle 1|)(e^{i\phi}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = e^{i\phi}\frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}} \Rightarrow |\psi'\rangle = e^{i\phi}\frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}}|U\rangle + e^{i\phi}\frac{\bar{\alpha}+\bar{\beta}}{\sqrt{2}}|U^{\perp}\rangle$$

La probabilité d'observer $\langle U|\psi'\rangle$ est :

$$|\langle U|\psi'\rangle|^2 = |e^{i\phi}|^2\frac{|\bar{\alpha}+\bar{\beta}|^2}{2}$$

Or $|e^{i\phi}|^2 = 1$ donc la probabilité d'observer $|U\rangle$ pour $|\psi\rangle$ est la même que la probabilité d'observer $|U\rangle$ pour $|\psi\rangle$.

Cela nous prouve que des états sont indiscernables à une phase globale près, cette phase étant $e^{i\phi}$.
Nous allons maintenant montrer qu'au contraire deux états : $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ sont discernable en leurs appliquant l'opérateur de Hadamard.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} avec\ |0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} et\ |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

Donc :

$$H|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}[|0\rangle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} + |1\rangle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}] = \frac{1}{2}[\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix}] = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle \tag{2.2}$$

et

$$H|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}[|0\rangle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} - |1\rangle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}] = \frac{1}{2}[\begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \end{pmatrix}] = \frac{1}{2} \begin{pmatrix} 0 \\ 2 \end{pmatrix} = |1\rangle \tag{2.3}$$

On voit donc que $|\psi\rangle \neq |\psi'\rangle$. Cela nous prouve qu'au contraire deux états qui diffèrent par une phase relative sont discernables.

2.1.2 Propriétés de la Sphère de Bloch

Nous allons maintenant montrer les propriétés de la sphère de Bloch. Dans un premier temps, nous verrons que le produit hermitien de deux vecteurs opposés est nul puis nous verrons l'effet que produit une porte quantique sur un vecteur.

Produit scalaire de deux vecteurs opposés

Prenons un vecteur $|\psi\rangle$ et son opposé dans la sphère, $|\phi\rangle$ avec :

$|\psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\varphi}|1\rangle$
et
$|\phi\rangle = cos(\frac{\pi-\theta}{2})|0\rangle + sin(\frac{\pi-\theta}{2})e^{i(\varphi+\pi)}|1\rangle$

Nous allons maintenant calculer le produit scalaire de $\langle\phi|\psi\rangle$:

$\langle\phi|\psi\rangle = cos(\frac{\pi-\theta}{2})cos(\frac{\theta}{2})\langle 0|0\rangle + e^{i\varphi}e^{i(-\varphi-\pi)}sin(\frac{\pi-\theta}{2})sin(\frac{\theta}{2})\langle 1|1\rangle$

Or : $cos(\frac{\pi-\theta}{2}) = sin(\frac{\theta}{2}),\ sin(\frac{\pi-\theta}{2}) = cos(\frac{\theta}{2})$ et $e^{i(\varphi-\pi)} = e^{i\varphi}e^{-i\pi}$ *et* $e^{-i\pi} = -1$.

Donc : $\langle\phi|\psi\rangle = sin(\frac{\theta}{2})cos(\frac{\theta}{2})\langle 0|0\rangle - e^{i\varphi}e^{-i\varphi}cos(\frac{\theta}{2})sin(\frac{\theta}{2})\langle 1|1\rangle = 0$.

Ce résultat nous démontre donc la première propriété de la sphère de bloch : deux vecteurs opposés ont un produit scalaire nul.

Rotation dans la Sphère de Bloch

Nous allons maintenant voir comment les actions des portes quantique X,Y,Z s'interprètent sur la sphère de Bloch. Pour cela nous allons nous servir d'un qubit $|\psi\rangle$et des portes quantiques X,Y et Z qui sont respectivement :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad et \ \ |\psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\varphi}|1\rangle \tag{2.4}$$

Nous allons tout d'abord passer $|\psi\rangle$ en vecteur afin de pouvoir le représenter sur la sphère avec les coordonnés (θ, φ).

Le vecteur $|\psi\rangle$ a donc pour coordonnées : $(cos(\frac{\theta}{2}), e^{i\varphi}sin(\frac{\theta}{2}))$.

Nous allons donc calculer le produit de la matrice X avec le qubit $|\psi\rangle$:

$$X.|\psi\rangle = \begin{pmatrix} 0 + e^{i\varphi}sin(\frac{\theta}{2}) \\ cos(\frac{\theta}{2}) + 0 \end{pmatrix} \Rightarrow \ |\psi'\rangle = e^{i\varphi}sin(\frac{\theta}{2})|0\rangle + cos(\frac{\theta}{2})|1\rangle \tag{2.5}$$

Nous allons chercher a retrouver une forme du type : $|\psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\varphi}|1\rangle$. Donc nous allons factoriser par $e^{i\varphi}$:

$|\psi'\rangle = e^{i\varphi}[sin(\frac{\theta}{2})|0\rangle + e^{-i\varphi}cos(\frac{\theta}{2})|1\rangle]$

Grâce à l'équivalence des qubits à une phase [2] près nous allons pouvoir supprimer la phase $e^{i\varphi}$, de plus nous savons que $sin(\frac{\theta}{2}) = cos(\frac{\pi-\theta}{2})$ et $cos(\frac{\theta}{2}) = sin(\frac{\pi-\theta}{2})$. Nous pouvons donc écrire :

$|\psi'\rangle = cos(\frac{\pi-\theta}{2})|0\rangle + e^{-i\varphi}sin(\frac{\pi-\theta}{2})|1\rangle$

Notre état initial $|\psi\rangle$ avait comme coordonnées $(\theta, \varphi) \rightarrow (sin(\theta)cos(\theta), sin(\theta)sin(\varphi), cos(\theta))$ dans $\mathbb{R}^3$.

Alors que notre état final a comme coordonnés :

$$(\pi - \theta, -\varphi) \rightarrow$$

$(sin(\pi-\theta)cos(\pi-\varphi), sin(\pi-\theta)sin(\pi-\varphi), cos(\pi-\theta)) = (-sin(\theta)cos(\varphi), sin(\theta)sin(\varphi), -cos(\theta))$

Ce qui équivaut à chercher l'image de notre premier vecteur :$(sin(\theta)cos(\theta), sin(\theta)sin(\varphi), cos(\theta))$ par la matrice :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Qui correspond a la matrice suivante dans $\mathbb{R}$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\theta) & -sin(\theta) \\ 0 & sin(\theta) & -cos(\theta) \end{pmatrix}$$

2. Voir Réprésentation dans la Sphère de Bloch

Ce qui nous prouve que la matrice X a imposé une rotation autour de l'axe x au qubit $|\psi\rangle$. La matrice X agit donc sur $\mathbb{C}^2$ (l'espace de Hilbert) ce qui revient à agir par rotation sur $\mathbb{R}^3$ (la sphère de Bloch).

Nous allons maintenant rapidement regarder les résultats que donne le produit du qubit $|\psi\rangle$ avec les portes Y et Z mais nous détaillerons moins les calculs car ceux-ci sont similaires dans les étapes à celui avec la porte X.

$$Y.|\psi\rangle = \begin{pmatrix} 0 - ie^{i\varphi}sin(\frac{\theta}{2}) \\ icos(\frac{\theta}{2}) + 0 \end{pmatrix} \Rightarrow |\psi'\rangle = -ie^{i\varphi}sin(\frac{\theta}{2})|0\rangle + icos(\frac{\theta}{2})|1\rangle \tag{2.6}$$

De nouveau nous allons chercher a retomber sur une forme :
$|\psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\varphi}|1\rangle$.
Au final nous devrions trouver :
$|\psi'\rangle = cos(\frac{\pi-\theta}{2})|0\rangle + e^{i(\pi-\varphi)}sin(\frac{\pi-\theta}{2})|1\rangle$

Ce qui prouve que Y agit comme une rotation de π autour de l'axe y.

Maintenant avec la porte Z :

$$Z.|\psi\rangle = \begin{pmatrix} 0 + cos(\frac{\theta}{2}) \\ -e^{i\varphi}sin(\frac{\theta}{2}) + 0 \end{pmatrix} \Rightarrow |\psi'\rangle = cos(\frac{\theta}{2})|0\rangle - e^{i\varphi}sin(\frac{\theta}{2})|1\rangle \tag{2.7}$$

Nous allons encore une fois chercher a retomber sur une forme :
$|\psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\varphi}|1\rangle$.
Au final nous devrions trouver :
$|\psi'\rangle = cos(\frac{\pi-\theta}{2})|0\rangle + e^{i(\pi+\varphi)}sin(\frac{\pi-\theta}{2})|1\rangle$

Ce qui prouve que Z agit comme une rotation de π autour de l'axe z.

La Sphère de Bloch permet donc de représenter des qubits dans un espace à 3 dimensions, elle respecte les particularité des qubits [3] et propose une représentation simple en ouvrant des axes de réfléxion quand à la manipulation de qubit [4].

2.2 Le Spin de l'électron

Dans cette partie, nous allons tenter de comprendre ce qu'est le spin de l'électron et de faire le lien entre la partie mathématique et physique de l'information quantique.

Définition

L'électron est une particule élémentaire constituant la partie externe d'un atome, celui-ci est chargé négativement. L'électron est à la fois un corps et une onde quantique c'est à dire qu'il se comporte à la fois comme une onde et une particule tout comme la lumière.

Le spin est une quantité quantique attaché à une particule (comme la charge par exemple). Le spin est un concept abstrait de la physique et il n'a pas d'équivalent classique. Le spin caractérise le "moment magnétique intrinsèque" de la particule.
Le spin à été mis en évidence par l'expérience de Stern-Gerlach en 1922.

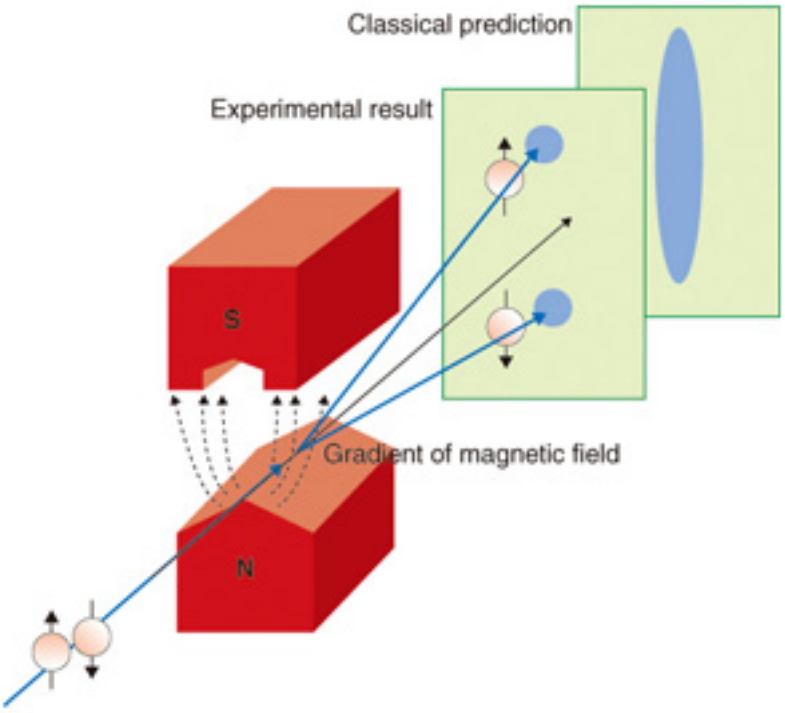
3. voir le produit scalaire de vecteur opposés
4. voir les matrices de rotation

2.2.1 L'expérience de Stern-Gerlach

Existence des qubits et possibilité de mesure

L'expérience de Stern et Gerlach est une expérience de mécanique quantique qui a longtemps été l'expérience qui illustrait le mieux les propriétés du spin de l'électron. Elle a été mise au point par Otto Stern et Walther Gerlach [5] en février 1922.

L'expérience réalisée en 1922 consistait à projeter des atomes d'argent aux travers d'un champ magnétique non-homogène sur un écran.



Les physicien ont été surpris du résultat de l'expérience car l'interprétation de la physique classique laissait à penser que les atomes d'argent allaient se répartir verticalement sur l'écran de mesure de la même manière que le feraient des aimants, or il n'en fut rien puisque les scientifiques observèrent deux point distincts. Un premier dévié vers le haut par rapport à la trajectoire initiale des atomes et un second dévié vers le bas.

Nous allons maintenant tenter de comprendre l'interprétation quantique de ce phénomène. L'énergie potentiel est ici donnée par : E = -$\vec{\mu}$. $\vec{B}$ avec $\vec{B}$ le champ magnétique et $\vec{\mu}$ le moment magnétique de la particule.

Or si la particule possède un moment magnétique, comme c'est le cas ici, elle sera soumise à une force :
On pose l'orientation du champ magnétique $\vec{B}$ vers l'axe z c'est à dire $\vec{B}$ =(0,0,b(z)) vecteur de l'orientation du champ magnétique. Mais la démonstration est la même pour n'importe quel

5. Walther Gerlach (1er août 1889 - 10 août 1979) et Otto Stern (17 février 1888 - 17 août 1969) sont tous deux des physiciens allemands connus pour avoir mis en évidence l'existence du spin de l'électron. Otto Stern est aussi connu pour avoir été lauréat du prix Nobel de physique de 1943 "pour ses contributions au développement de l'épitaxie par jet moléculaire et sa découverte du moment magnétique du proton".

autre spin et n'importe quel autre champ magnétique celà est fait afin de simplifier les calculs.

$$F_z = E'(z).\begin{pmatrix}0\\0\\1\end{pmatrix}$$

Si $B = (0, 0, b(z))$ alors :

$$E(z) = -(x_\mu, y_\mu, z_\mu).\begin{pmatrix}0\\0\\b(z)\end{pmatrix} = -z_\mu b(z)$$

Ainsi la force exercée sur notre particule par le champ magnétique est :

$$F_z = E'(z).\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\-z_\mu b(z)\end{pmatrix}$$

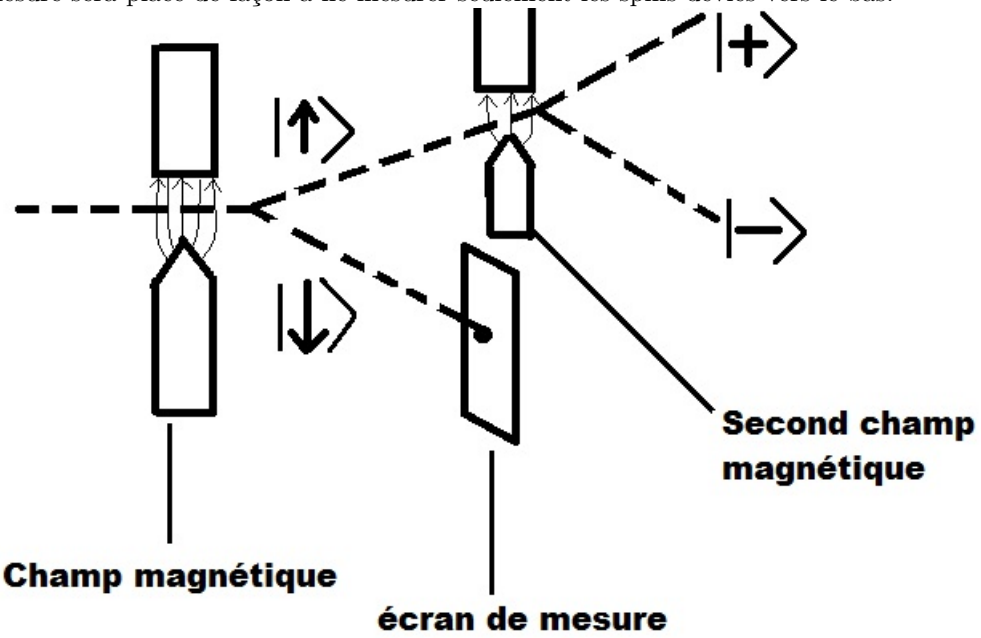
Si le moment magnétique est orienté vers le haut : $|\uparrow\rangle$ alors la particule est déviée vers le haut.

Si le moment magnétique est orienté vers le bas : $|\downarrow\rangle$ alors la particule est déviée vers le bas. Et si le moment magnétique est orienté n'importe où : $|\nearrow\rangle = \alpha|0\rangle + \beta|1\rangle$ alors la particule est déviée suivant un pourcentage donc $|\uparrow\rangle = |\alpha|^2$ et $|\downarrow\rangle = |\beta|^2$. Cependant nous ne pouvons savoir la position de la particule qu'après l'avoir mesurée sur l'écran, ce qui signifie que la particule suit les deux trajectoires simultanément jusqu'à ce qu'elle soit mesurée, on peut faire le rapprochement avec la superposition d'état du qubit. Cette observation implique que les qubits comme le spin existent et que nous pouvons les mesurer.

Cette expérience permet aussi de préparer des états quantiques. Nous allons maintenant rapidement expliquer comment préparer un état quantique.

Préparation d'un état quantique

Dans une premier temps on reprend le dispositif de Stern-Gerlach sauf que l'écran qui permet la mesure sera placé de façon à ne mesurer seulement les spins déviés vers le bas.



Une fois que notre particule a franchis le premier champ magnétique, nous connaissons sans le mesurer son état car les particules déviées vers la bas sont arrêtée par l'écran. Ainsi nous savons que toute les particules qui passerons par le second champ magnétique auront comme spin $|\uparrow\rangle = |0\rangle$. Nous avons donc initialisé notre état à $|0\rangle$.

En passant le second champ magnétique notre état sera de nouveau dévié ce qui le modifie de nouveau. Ainsi si l'on effectue une mesure nous aurons deux états possible : un état $|+\rangle$ et un état $|-\rangle$ en supposant que le second champ magnétique n'ait pas la même orientation que le premier car sinon nous aurions les mêmes résultats qu'après le passage du premier champ magnétique. Nous avons donc notre nouvel état initialisé avec :

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ ou \ \ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.8}$$

Ainsi nous avons réussi à préparer un état quantique qui est physiquement utilisable pour d'autre expérience.

2.2.2 Résonance Magnétique Nucléaire

La résonance magnétique nucléaire (RMN) désigne une propriété de certains noyaux atomiques possédant un spin nucléaire, placés dans un champ magnétique. Dans cette partie nous allons démontrer comment réalisé appliquer physiquement une porte quantique à un spin.

Avant propos :

Avant de débuter l'explication de la résonance nous allons voir une démonstration mathématique qu'il est possible d'étudier en MT28.

Nous allons résoudre une équation différentiel de type : $X'(t) = AX(t)$ avec X(t) $\in \mathbb{R}^2$ et A $\in \mathbb{M}_{2\times 2}$. On suppose la matrice A diagonalisable avec deux valeurs propres $\lambda_1 \neq \lambda_2$ et deux vecteurs propres v_1 et v_2.

On a alors Av_1 =$\lambda_1 v_1$ et $Av_2 = \lambda_2 v_2$.

La solution de cette équation différentielle est :

$$X(t) = C_1 e^{\lambda_1 t} v_1 + C_2 e^{\lambda_2 t} v_2 \ avec \ C_1 \ et \ C_2 \in \mathbb{R} \tag{2.9}$$

En effet

$$X'(t) = \lambda_1 C_1 e^{\lambda_1 t} v_1 + \lambda_2 C_2 e^{\lambda_2 t} v_2 \tag{2.10}$$

et on a bien

$$AX(t) = C_1 e^{\lambda_1 t} A v_1 + C_2 e^{\lambda_2 t} A v_2 = C_1 e^{\lambda_1 t} \lambda_1 v_1 + C_2 e^{\lambda_2 t} \lambda_2 v_2 \tag{2.11}$$

Cette démonstration nous servira plus tard pour expliquer le fonctionnement de la résonance magnétique nucléaire.

Le vif du sujet

Comme nous l'avons vu plus haut le spin est une quantité quantique qui peut se mesurer dans une direction de l'espace et ne peut prendre que deux valeurs selon la direction, haut ou bas assimilables aux $|0\rangle$ et $|1\rangle$ d'un qubit. Cependant le spin n'est donc pas un vecteur représentant une direction mais un vecteur de matrice (ou un observable si l'on veut s'exprimer dans le langage

de la mécanique quantique) dont chaque matrice représente les issues possibles de la mesure. Ainsi on définit le moment magnétique de spin comme étant :

$$\vec{\mu}_{spin} = \frac{e\hbar}{2m}(X, Y, Z)$$

Avec X,Y,Z qui sont les matrices que nous connaissons aussi appelée matrices de Pauli [6]. Elles représentent les résultats possibles de mesure du spin dans les directions x, y et z.

La mesure d'un spin ou d'un état$|\psi\rangle$ dans la direction z dont la base est $\{|0\rangle; |1\rangle\}$ est caractérisée par un opérateur qui a deux vecteurs propres $|0\rangle$ et $|1\rangle$ de valeurs propres +1 et -1.

L'énergie potentielle de la particule est donc :

$$E = -\vec{\mu}_{spin}.\vec{B}$$

Cependant notre particule est immobile [7] et soumis à un champ magnétique orienté ce qui modifie son expression quantique. *On supposera toujours $\vec{B}$ orienté sur l'axe z* Donc l'hamiltonien s'écrit :

$$\mathcal{H} = -\vec{\mu}.\vec{B} = \frac{e\hbar}{2m}(X, Y, Z).\begin{pmatrix} 0 \\ 0 \\ B_0 \end{pmatrix} = \frac{e\hbar}{2m}B_0 Z = \frac{w_0}{2}Z$$

Avec w_0=$\frac{-e\hbar}{2m}B_0$ qui est constant.

Ainsi, le champ potentiel, c'est-à-dire, l'hamiltonien auquel est soumis la particule dans $\vec{B}$ est :

$$\mathcal{H} = \frac{\omega_0}{2}.Z$$

Nous pouvons donc résoudre l'équation de Schrödinger associée à notre Hamiltonien pour déterminer l'évolution du spin dans le champ magnétique (ce qui implique une résonance magnétique).

D'après l'équation de Schrödinger, nous avons :

$$i\hbar|\psi'(t)\rangle = \mathcal{H}|\psi(t)\rangle \Rightarrow |\psi'(t)\rangle = \frac{i}{\hbar}\mathcal{H}|\psi(t)\rangle$$

Les vecteurs propres de $\frac{i}{\hbar}\mathcal{H}$ sont : $|0\rangle \rightarrow \frac{-i}{\hbar}\frac{\omega_0}{2}$ et $|1\rangle \rightarrow \frac{i}{\hbar}\frac{\omega_0}{2}$.

Ainsi nous obtenons une équation différentielle. En réutilisant la méthode vu dans l'avant propos on trouve :

$$|\psi(t)\rangle = C_1 e^{\frac{-i\omega_0 t}{2\hbar}}|0\rangle + C_2 e^{\frac{i\omega_0 t}{2\hbar}}|1\rangle \tag{2.12}$$

Si $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ alors $C_1 = \alpha$ *et* $C_2 = \beta$. (état initial)

Ainsi :

$$|\psi(t)\rangle = \alpha e^{\frac{-i\omega_0 t}{2\hbar}}|0\rangle + \beta e^{\frac{i\omega_0 t}{2\hbar}}|1\rangle$$

On factorise par l'exponentielle d'où :

$$|\psi(t)\rangle = e^{\frac{-i\omega_0 t}{2\hbar}}(\alpha|0\rangle + \beta e^{\frac{i\omega_0 t}{\hbar}}|1\rangle)$$

6. Wolfgang Ernst Pauli (25 avril 1900- 15 décembre 1958) était un physicien autrichien connu pour sa définition du principe d'exclusion en mécanique quantique, ce qui lui valut le prix Nobel de physique de 1945.

7. Ce qui implique que l'énergie cinétique est nul, celà nous permet d'avoir un développement simplifié.

Comme nous l'avons vu avec la sphère de Bloch, nous pouvons simplifier l'expression en supprimant la première exponentielle grâce à l'équivalence des phases :

$$|\psi(t)\rangle = \alpha|0\rangle + \beta e^{\frac{i\omega_0 t}{\hbar}}|1\rangle$$

On projette dans un espace à 3 dimensions et nous passons en coordonnées sphériques :

$$|\psi(t)\rangle = cos(\frac{\theta}{2})|0\rangle + e^{\frac{i\omega_0 t}{\hbar}} e^{i\varphi} sin(\frac{\theta}{2})|1\rangle$$

$$\Rightarrow |\psi(t)\rangle = cos(\frac{\theta}{2})|0\rangle + e^{i(\varphi + \frac{\omega_0 t}{\hbar})} sin(\frac{\theta}{2})|1\rangle$$

Notre équation est donc résolue et nous connaissons l'évolution de l'état de spin de la particule dans le temps. Si on souhaite modifier notre particule en lui faisant faire un demi tour, on pose alors :

$$t = \pi \frac{\hbar}{\omega_0}$$

D'où :

$$|\psi(\pi \frac{\hbar}{\omega_0})\rangle = Z|\psi(0)\rangle$$

Ce qui correspond a utiliser la matrice de rotation Z sur notre particule. Nous avons donc modifié notre spin au moyen d'un champ magnétique, celle-ci est quantique et nous pouvons la manipuler aussi bien théoriquement avec nos matrices X,Y,Z que réellement, en la projetant dans des champs magnétiques. Ce modèle nous montre que la porte Z réalisée peut être implémentée physiquement sur un qubit (le spin de l'électron) à l'aide de technique expérimentale et physique telle que la Résonance Magnétique Nucléaire.

Chapitre 3

Communication quantique

Une des premières applications de la théorie de l'information quantique fut la communication quantique. L'intrication et la superposition des systèmes quantiques, le postulat de la mesure et les opérateurs unitaires permettent en effet de mettre en place les protocoles et les architectures d'information quantique qui peuvent être utilisés pour transmettre de l'information à travers des canaux quantiques. Nous tenterons donc, dans ce chapitre, de ne nous intéresser à ces protocles de communication. Nous aborderons dans un premier temps la téléportation quantique. Nous poursuivrons avec le codage "superdense" aussi appelé Superdense coding. Enfin, nous irons voir de plus près quelques protocoles de cryptographie quantique.

3.1 Téléportation quantique

Encore une fois, dans cette partie, nous allons voir que le phénomène "mystique" de l'intrication est fondamental et très important pour l'élaboration d'algorithmes ou encore de protocole de communications quantiques. Plus particulièrement, ici, dans la conception d'un protocole qui permettrait la "téléportation" d'états quantiques. Cette appellation, qui pourrait laisser croire à de le science-fiction, est plus qu'envisageable dans le domaine de l'information quantique. Néanmoins, il ne s'agit pas d'une téléportation à proprement parlé, qui pourrait laisser penser au transfert de matière d'un point A vers un point B, mais seulement d'un transfert d'état quantique. En effet, nous allons voir comment transmettre une information connue ou inconnue (c'est-à-dire l'état inconnu d'un qubit, par exemple) d'un point A vers un point B sans pour autant transporter le système physique porteur du qubit (et par conséquent sans aucun transport de matière). En language courant, nous pouvons résumer le problème par la situation suivante :

Un agent secret (ou pas) remet à Anne une enveloppe (ici, le qubit) qui contient un message (l'état du qubit) très important destiné à un autre agent, Benoît situé à quelques kilomètres de là (mais cela pourrait être des milliards de kilomètres). L'agent demande à Anne de ne pas prendre connaissance du message (état inconnu du qubit) et, n'ayant pas confiance dans les services postaux, de ne pas envoyer l'enveloppe à Benoît (c'est-à-dire ici, de ne pas envoyer le qubit en lui même, mais seulement l'information qu'il contient). Dans ces conditions comment Anne parviendra-t-elle à transmettre le message à Benoît ?

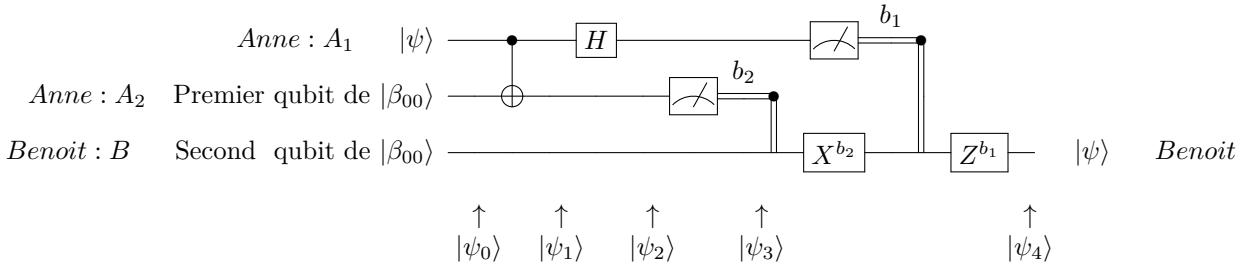


FIGURE 3.1 – Circuit de téléportation

3.1.1 Protocole

Dans tout ce protocole, nous supposons qu'Anne et Benoît se sont rencontrés précédemment et se sont partagés à l'amiable un système à deux qubits intriqué, plus exactement l'état de Bell (qui nous le rappelons est défini par $|\psi_{Bell}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$). De plus, Anne détient un deuxième qubit dont l'état lui est inconnu $|\psi_{A_1}\rangle = \alpha|0\rangle + \beta|1\rangle$, qui par ailleurs veut être transmis à Benoît (nous parlons bien, ici, de l'état du qubit). Nous obtenons donc un système à 3 qubits dont l'état est décrit par :

$$|\psi_0\rangle = |\psi_{Bell}\rangle \otimes |\psi_{A_1}\rangle = \frac{1}{\sqrt{2}}(\underbrace{\alpha|0\rangle + \beta|1\rangle}_{|A_1\rangle})(\underbrace{|00\rangle + |11\rangle}_{|A_2B\rangle})$$

$$= \frac{1}{\sqrt{2}}\{\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)\} \text{ avec } \underbrace{|...\rangle}_{|A_1A_2B\rangle}$$

1. La première étape de la téléportation consiste à appliquer la porte C-Not sur le système à 2 qubits constitué par la paire des qubits que détient Anne : A_1 et A_2. Ainsi, Anne obtient :
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\{\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)\}$$

2. Ensuite, la deuxième étape consiste à envoyer le premier qubit d'Anne, noté A_1, sur une porte de Hadamard. De fait, l'état $|\psi_1\rangle$ devient :
$$|\psi_2\rangle = \frac{1}{2}\{\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |011\rangle - |101\rangle)\}$$
$$= \frac{1}{2}\{|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle + \beta|0\rangle)$$
Ici, nous pouvons voir que l'état du qubit inconnu est complétement déterminé par l'état du système à 2 qubits définit par $|A_1A_2\rangle$. Ce phénomène est du à l'intrication quantique.
3. Anne mesure l'état du sytème $|A_1A_2\rangle$ et transmet le resultat de cette mesure, appelé mesures de Bell, à Benoît par n'importe quel moyen de communication (ex : telephone,...) : cette étape montre bien que la relativité n'est pas remise en question dans le principe de téléportation.
4. Benoît reçoit le résultat d'Anne noté $|a_1a_2\rangle$. Il effectue enfin l'opération $Z^{a_1}X^{a_2}$, avec "Z" et "X" les portes logiques quantiques définies précédemment, sur son qubit. Le résultat de cette manipàulation donnera, avec certitude, l'état du qubit inconnu noté $|A_1\rangle$.

Remarque 3.1 *Nous pourrions penser que ce protocole théorique que nous venons de voir nous permettrait de construire aisément un téléporteur ; il n'en est rien, le défi expérimental est immense.*

3.1.2 Petit historique

Pour téléporter, il fallait des particules intriquées. Depuis les années 1980, et après les expériences pionnières de l'Américain John Clauser et du Français Alain Aspect, ils avaient appris à produire assez simplement des paires de photons intriqués.

Principe d'intrication :

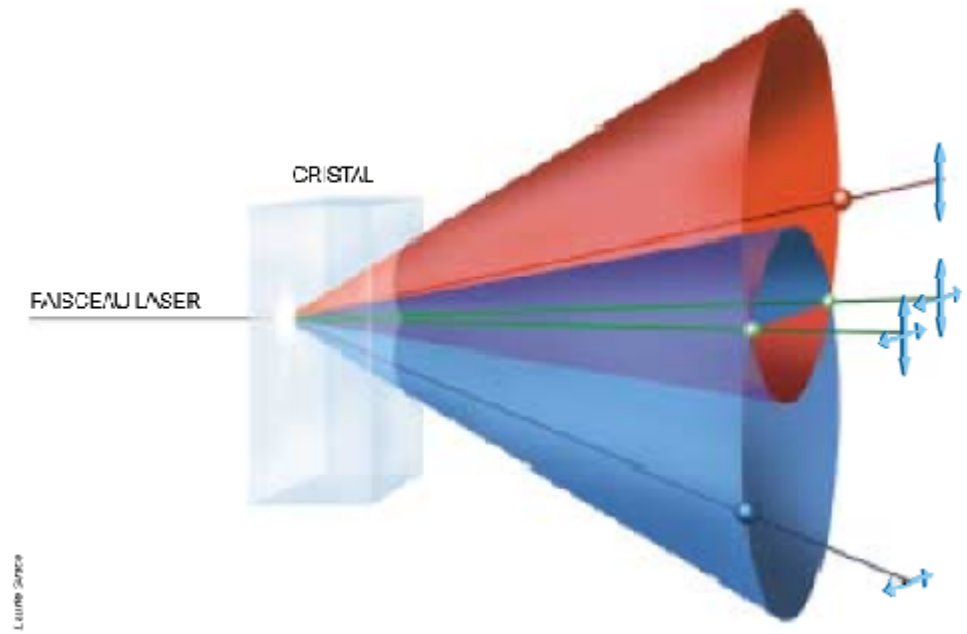


FIGURE 3.2 – Construction d'une paire intriqué de photons

Les paires de photons intriqués sont créées par un faisceau laser qui traverse un cristal (le borate de baryum, par exemple). Le cristal convertit un photon ultraviolet en deux photons de moindre énergie, l'un polarisé verticalement (sur le cône rouge), l'autre horizontalement (sur le cône bleu). Si les photons se propagent le long de l'intersection des cônes (en vert), il est impossible de connaître a priori la polarisation de chacun, mais ils sont intriqués. La mesure de la polarisation de l'un détermine celle de l'autre, qui lui est perpendiculaire.

Durant l'été 1997, à l'Université de Rome, l'équipe de Francesco De Martini fut la première à réaliser la téléportation d'un photon. Les chercheurs avaient toutefois légèrement "triché", en utilisant le même photon, à la fois comme support pour l'état quantique à téléporter et pour former le canal virtuel de téléportation. Viens ensuite, en 1997, l'équipe du physicien Anton Zeilinger (Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl et Harald Weinfurter), alors à l'université d'Innsbruck, qui réalise pour la première fois une expérience de téléportation à trois photons.

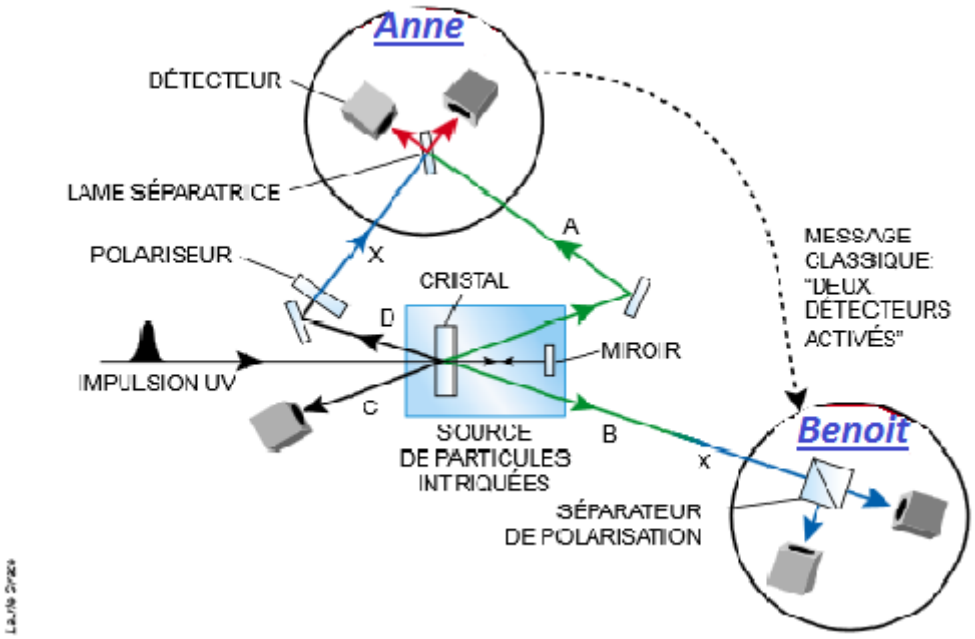


FIGURE 3.3 – Principe de téléportation

L'expérience d'Innsbruck utilise une impulsion de lumière laser ultraviolette. En se propageant dans le cristal, cette impulsion produit la paire de photons intriqués A et B , qui vont respectivement vers Anne et vers Benoit. L'impulsion, réfléchie par un miroir, retraverse le cristal et crée deux autres photons, C et D. Un polariseur impose au photon D un état donné, X (inconnu). Le photon C est détecté, ce qui confirme que le photo X a été envoyé à Anne. Anne combine les photons A et X avec une lame séparatrice de faisceau (voir la figure). Si elle détecte un photon dans chaque détecteur (dans 25 % des cas), le photon de Benoit devient instantanément une copie du photon d'origine X de Anne et la téléportation est un succès, et par l'intermédiaire d'un message classique elle en avertit Benoit, qui utilise un séparateur de polarisation pour vérifier que son photon a acquis la polarisation de X.

L'expérience autrichienne de téléportation implique ici trois photons : un photon original et une paire de photons intriqués, mais elle est imparfaite puisqu'on ne téléporte qu'un quart des photons en moyenne (25%). Le procédé a même été amélioré en 2002, par Francesco De Martini et ses collègues, qui ont été porté à 50 % la probabilité de succès de la mesure de Bell.

Remarque 3.1 *Des chercheurs de l'université de Vienne et de l'académie autrichienne des Sciences sont parvenus en septembre 2004 à réaliser une téléportation quantique de photons d'une rive à l'autre du Danube, sur une distance de 800 mètres, à l'aide d'une liaison optique. Récemment, on apprenait qu'une équipe chinoise avait battu le record de distance pour la téléportation quantique avec 97 km. Mais Anton Zeilinger et ses collègues ont déjà "pulvérisé" ce record en faisant de la téléportation quantique sur une distance de 143 km.*

3.2 Superdense coding

3.2.1 Principe de base

Notre second exemple d'application de l'intrication pour la communication sera le Superdense coding. Ce moyen de communication introduit pour la première fois en 1992 [1], permet de mettre en place un codage et une transmission des informations plus "dense" que les protocoles classiques. En effet, le principe est le suivant :

Alice et Bob partagent initialement l'état de Bell β_{00} : chacun d'entre eux possède un qubit de cet état intriqué. Comment Alice peut elle transmettre deux bits classiques d'information à Bob, ***en ne lui envoyant qu'un seul qubit ?***

Alice voudrait donc transmettre à Bob l'un des état basiques suivant : $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Les étapes du protocole de Superdense coding sont les suivantes :

— Alice choisit les 2 bits qu'elle veut transmettre
— En fonction de ces derniers, elle agit sur son qubit appartenant à l'état de Bell partagé
— Alice envoie son qubit de l'état de Bell après manipulation
— Bob réceptionne ce qubit, et applique alors une porte à tout le système intriqué
— L'état de base à 2 qubits ainsi récupéré correspond aux 2 bits choisis par Anne

En fonction de l'état de base à 2 qubits choisi par Alice, la manipulation sur le premier qubit de $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ sera différente :

Choix de Anne	Manipulation associée sur β_{00}
$\|00\rangle$	I
$\|01\rangle$	X_1
$\|10\rangle$	Z_1
$\|11\rangle$	$(ZX)_1$

Il en resulte donc la transformation suivante, en fonction de chacun des choix de Alice.

$$\begin{aligned}
|00\rangle : &\quad \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{I} \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= |\omega_1\rangle \\
|01\rangle : &\quad \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{X_1} \tfrac{1}{\sqrt{2}}(|10\rangle + |01\rangle) &= |\omega_2\rangle \\
|10\rangle : &\quad \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{Z_1} \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &= |\omega_3\rangle \\
|11\rangle : &\quad \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{(ZX)_1} \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= |\omega_4\rangle
\end{aligned}$$

Une fois son qubit manipulé, elle l'envoie à Bob. Il possède donc désormais l'état intriqué dans son intégralité. Il applique alors la porte inverse de la porte génératrice des états de Bell à savoir : une porte c-NOT contrôlée par le premier qubit, suivie d'une porte de Hadamard sur le premier qubit également.

Bob applique donc ce circuit-ci :
C'est à la sortie de ce circuit que l'on retrouve l'état initialement choisi pour être transmit par Alice. Vérifions cela pour chacun des cas de figure :

1. C. H. Bennett and Stephen J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992)

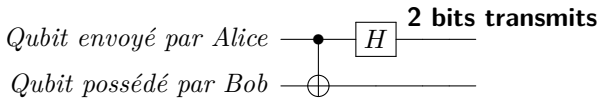


FIGURE 3.4 – Circuit appliqué par Bob pour décoder

$$
\begin{array}{llllll}
|\omega_1\rangle & \xrightarrow{c-NOT} & \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) & \xrightarrow{H} & \frac{1}{2}[\ (|0\rangle + |1\rangle)|0\rangle + (|0\rangle - |1\rangle)|0\rangle\ ] & = |\mathbf{00}\rangle \\
|\omega_2\rangle & \longrightarrow & \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) & \longrightarrow & \frac{1}{2}[\ (|0\rangle + |1\rangle)|1\rangle + (|0\rangle - |1\rangle)|1\rangle\ ] & = |\mathbf{01}\rangle \\
|\omega_3\rangle & \longrightarrow & \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) & \longrightarrow & \frac{1}{2}[\ (|0\rangle + |1\rangle)|0\rangle - (|0\rangle - |1\rangle)|0\rangle\ ] & = |\mathbf{10}\rangle \\
|\omega_4\rangle & \longrightarrow & \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) & \longrightarrow & \frac{1}{2}[\ (|0\rangle + |1\rangle)|1\rangle - (|0\rangle - |1\rangle)|1\rangle\ ] & = |\mathbf{11}\rangle
\end{array}
$$

Ainsi, Alice peut en effet transmettre deux bits d'information qu'elle doit avoir préalablement choisi, en n'envoyant qu'un seul qubit au destinataire Bob.

3.3 Cryptographie quantique

La cryptographie se défini comme la conception de mécanismes cryptologiques destinés à garantir les notions de sécurité à des fins de confidentialité, d'authenticité et d'intégrité de l'information, mais aussi pour d'autres notions comme l'anonymat. Le problème de la transmission de messages secrets remonte à très loin dans le temps, et l'Homme n'a cessé de se surpasser dans le cryptage et la sécurisation des communications sensibles. Ce problème peut être considéré comme résolu à partir du moment où l'on sait coder un message de façon à ce que tout espion ne connaisssant pas la clé de décodage ne puisse pas le déchiffrer, tout en permettant au destinataire initial de facilement déchiffrer le code, en possèdant la clé de décodage préalablement.

Il existe aujourd'hui deux principaux types de codages : ceux à clé privée et ceux à clé publique.

Dans un codage à clé privée l'emmeteur et recepteur (Alice et Bob) possèdent tous deux la clé servant à la fois au codage et au décodage. La subtilité de ces protocoles réside dans la capacité pour Alice et Bob de se transmettre la clé de codage de façon fiable.

Dans un codage à clé publique, seulement Alice possède les deux clés de codage et de décodage, tandis que Bob ne reçoit que la clé de codage. Bob ne pourra ici que coder, et c'est Alice qui pourra décoder le message de Bob lors de sa réception.

L'application de la théorie de l'information quantique au cryptage de données permet de sécuriser de manière encore plus fiable et maniable la transmission d'informations. En effet, l'utilisation ici du postulat de mesure et de l'état d'un système quantique, ainsi que l'intrication quantique permet un contrôle et des possibilités beaucoup plus vastes que ce que permet l'informatique classique.

Le but de cette section est de donner un aperçu des différents protocoles de cryptographie quantique déjà mis en place, et d'évaluer le risque d'espionnage pour chacun.

3.3.1 Protocole BB84

Afin d'étudier la protocole BB84 [2], nous nous plaçons ici dans le cadre d'un codage à clé privée.

L'information transmise par Alice vers Bob prendra la forme de photons, dont la polarisation sert de support au codage de l'information. On introduit donc les états de base de polarisation d'un photon, en leur associant chacun la valeur d'un qubit :

$$|\rightarrow\rangle \equiv |0\rangle$$
$$|\uparrow\rangle \equiv |1\rangle$$

Alice dispose en fait d'un emmeteur, "un par un", de photons, muni d'un polariseur lui permettant de polariser horizontalement ou verticalement ce photon, codant ainsi le $|0\rangle$ ou le $|1\rangle$. Bennett et Brassard proposent alors d'introduire une nouvelle base de polarisation dans laquelle les polariseurs sont inclinés de -45° par rapport à la base précédente. Les états possibles du photons seront donc :

$$|\searrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \equiv |0\rangle$$
$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle) \equiv |1\rangle$$

De ce fait, le qubit $|1\rangle$ pourra être codé de 2 manières différentes : soit par la polarisation $|\uparrow\rangle$, soit par la polarisation $|\nearrow\rangle$. Pour savoir dans quelle base de polarisation on travaille, on introduit la notation $\oplus$ pour la base de polarisation horizontale/verticale, et $\otimes$ pour la base de polarisation à 45°.

Ainsi, un photon polarisé $|\nearrow\rangle$ aura une probabilité de 1 d'être le résultat de la mesure du photon dans la base $\otimes$, mais une probabilité de $\frac{1}{2}$ dans la base $\oplus$, car $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$.

Exemple de transmission d'un seul qubit

Supposons qu'Alice veuille transmettre un qubit $|0\rangle$ en polarisant un photon avec un polariseur orienté au hasard $\oplus$ ou $\otimes$. Ce même photon est intercepté par un espion, que l'on nommera Eve, qui en mesure la polarisation dans la base $\oplus$. On cherche à savoir qu'elle est la probabilité pour qu'il mesure bien $|0\rangle$.

Eve utilise donc la base $\oplus$ pour la mesure.

— Si Alice utilise la base $\oplus$ pour polariser son photon, alors Eve mesurera $|0\rangle$ avec une probabilité de 1.

— Si Alice utilise la base $\otimes$ pour polariser son photon, elle enverra donc le photon polarisé $|\searrow\rangle$. Comme $|\searrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle)$, le qubit a une chance sur deux d'être projeté sur l'un des vecteurs de base de la base de mesure $\oplus$. Eve mesurera alors $|0\rangle$ avec une probabilité de $\frac{1}{2}$.

En supposant qu'Alice ait autant de chance de choisir l'une ou l'autre des deux bases de polarisation, c'est à dire une chance sur deux de choisir $\oplus$ ou $\otimes$, on peut calculer la probabilité qu'Eve mesure $|0\rangle$ sur le photon intercepté.

Soient les évènements A : "Eve mesure $|0\rangle$", B : "Alice choisit la base $\oplus$" et C : "Alice choisit la base $\otimes$". Comme les évènements B et C forment un système complet d'évènements, d'après la formule des probabilité totales, nous avons donc :

2. C. H. Bennett et G. Brassard en 1984

$$\mathrm{p}(A) = \mathrm{p}(A \cap B) + \mathrm{p}(A \cap C)$$

D'où d'après les formule des probabilités conditionnelles :

$$\mathrm{p}(A) = \mathrm{p}(B) \times \mathrm{p}_B(A) + \mathrm{p}(C) \times \mathrm{p}_C(A)$$

Or on sait que $\mathrm{p}(B) = \mathrm{p}(C) = \mathrm{p}_C(A) = \frac{1}{2}$ et que $\mathrm{p}_B(A) = 1$. On obtient alors le résultat suivant :

$$\mathrm{p}(A) = \frac{1}{2} \times \frac{1}{2} + 1 \times \frac{1}{2} = \frac{3}{4}$$

L'espion Eve a donc 75% de chances de mesurer $|0\rangle$ pour un photon codé initialement $|0\rangle$ par Alice dans une base choisie au hasard.

Introduisons maintenant, encore un fois, une nouvelle base de polarisation. Au lieu cette fois ci de tourner la base $\oplus$ d'un angle de 45°, nous effectuerons une rotation de cette même base $\oplus$ mais d'un angle θ. On défini ainsi les deux vecteurs de base, $|\theta\rangle$ et $|\theta_\perp\rangle$ de cette nouvelle base vérifient :

$$|\theta\rangle = \cos(\theta)|\rightarrow\rangle + \sin(\theta)|\uparrow\rangle \equiv |0\rangle$$
$$|\theta_\perp\rangle = \sin(\theta)|\rightarrow\rangle - \cos(\theta)|\uparrow\rangle \equiv |1\rangle$$

Il sera utile pour la suite de relier dès à présent les vecteurs de cette nouvelle base que l'on appellera Θ. En utilisant les relations déjà établies entre les 2 bases $\oplus$ et $\otimes$ on obtient :

$$|\rightarrow\rangle = \cos(\theta)|\theta\rangle + \sin(\theta)|\theta_\perp\rangle$$
$$|\uparrow\rangle = \sin(\theta)|\theta\rangle - \cos(\theta)|\theta_\perp\rangle$$
$$|\searrow\rangle = \frac{\cos(\theta) - \sin(\theta)}{\sqrt{2}}|\theta\rangle + \frac{\cos(\theta) + \sin(\theta)}{\sqrt{2}}|\theta_\perp\rangle$$
$$|\nearrow\rangle = \frac{\sin(\theta) + \cos(\theta)}{\sqrt{2}}|\theta\rangle + \frac{\sin(\theta) - \cos(\theta)}{\sqrt{2}}|\theta_\perp\rangle$$

On sait qu'à présent Eve utilise donc la base Θ pour la mesure.

— Si Alice utilise la base $\oplus$ pour polariser son photon, alors Eve mesurera $|0\rangle$ avec une probabilité de $\cos^2(\theta)$.
— Si Alice utilise la base $\otimes$ pour polariser son photon, alors Eve mesurera $|0\rangle$ avec une probabilité de $(\frac{\cos(\theta)-\sin(\theta)}{\sqrt{2}})^2 = \frac{1}{2} - \sin(\theta)\cos(\theta)$.

En supposant qu'Alice ait toujours autant de chance de choisir l'une ou l'autre des deux bases de polarisation $\oplus$ ou $\otimes$, on peut calculer la probabilité $\mathrm{p}(\theta)$ qu'Eve mesure $|0\rangle$ sur le photon intercepté :

$$\mathrm{p}(\theta) = \frac{1}{2} \times \cos^2(\theta) + \frac{1}{2} \times (\frac{1}{2} - \sin(\theta)\cos(\theta))$$

On linéarise cette expression à l'aide des formules de trigonométrie usuelles :

$$\mathrm{p}(\theta) = \frac{1}{4} \times (\cos(2\theta) + 1) + \frac{1}{2} \times (\frac{1}{2} - \frac{1}{2}\sin(2\theta))$$

Après simplification, on trouve :

$$\mathrm{p}(\theta) = \frac{1}{4}(2 + \cos(2\theta) - \sin(2\theta))$$

Il serait maintenant intéressant de chercher pour quel angle optimal θ tel que la probabilité pour Eve de mesurer $|0\rangle$ est la plus élevée. Il suffit en effet de trouver pour quelle valeur de θ on atteint la maximum de la fonction $\mathrm{p}(\theta)$. Après étude de la fonction, on trouve que pour un angle $\theta = \frac{7\pi}{8}$ la fonction atteint son maximum $\mathrm{p}(\frac{7\pi}{8}) = \frac{2+\sqrt{2}}{4} \simeq 85\%$.

L'espion Eve a donc 85% de chance au maximum de mesurer $|0\rangle$ dans la base Θ pour un photon codé initialement $|0\rangle$ par Alice dans une base choisie au hasard parmi $\oplus$ et $\otimes$.

Supposons maintenant qu'Alice et Bob aient leur polariseurs orientés dans la même direction, mais que le photon, émis initialement par Alice dans l'état $|0\rangle$ soit intercepté par l'espion Eve. Celui-ci mesure la polarisation avec un choix aléatoire d'orientation entre $\oplus$ et $\otimes$: quelle la probabilité qu'Eve altère l'information de départ, c'est à dire, **quelle est la probabilité que Bob reçoive le photon dans l'état $|1\rangle$?**

Pour répondre à cette question, dans le fond promordiale en cryptographie quantique, il apparait important dans un premier temps de lister toutes les combinaisons de choix de base pour Alice, Bob et Eve :

	Alice	Eve	Bob
1.	$\oplus$	$\oplus$	$\oplus$
2.	$\oplus$	$\otimes$	$\oplus$
3.	$\otimes$	$\otimes$	$\otimes$
4.	$\otimes$	$\oplus$	$\otimes$

Soit l'évènement D : "Bob reçoit la photon dans l'état $|1\rangle$". On se propose de calculer la probabilité de l'évènement D en fonction de chaque cas de figure figurants ci-dessus.

— Si la base utilisée par Alice et Bob et la même que celle utilisée par Eve, alors la polarisation du photon ne sera pas altérée. Ceci se manifeste dans les cas 1 et 3, d'où :

$$\mathrm{p}_1(D) = \mathrm{p}_3(D) = 0$$

— Si la base utilisée par Alice et Bob diffère de celle utilisée par Eve, il y a une probabilité d'$\frac{1}{2}$ qu'Eve mesure et modifie l'état du qubit $|0\rangle$ en $|1\rangle$, du fait de la différence de base entre Alice et Eve. Ensuite, Bob a lui aussi une probabilité d'$\frac{1}{2}$ de modifier le qubit, du fait de la différence entre sa base et celle d'Eve. On retrouve ce cas de figure dans les cas 2 et 4, d'où :

$$\mathrm{p}_2(D) = \mathrm{p}_4(D) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$$

Au final, en supposant que chacun de ces 4 cas ait la même probabilité de se réaliser, on trouve :

$$\mathrm{p}(D) = \frac{1}{4}(\mathrm{p}_1(D) + \mathrm{p}_2(D) + \mathrm{p}_3(D) + \mathrm{p}_4(D))$$

D'où

$$\mathrm{p}(D) = \frac{1}{4}$$

Bob a donc 1 chance sur 4 de mesurer le mauvais qubit transmit, sachant qu'un espion à antérieurement intercepté ce dernier.

Exemple de transmission de plusieurs qubits

On s'intéresse maintenant au cas où Alice tente de transmettre plus qu'un seul qubit d'information à Bob. Pour transmettre plusieurs qubits à Bob on supposera qu'Alice les transmet un par un. De plus, pour chaque qubit, Alice choisit aléatoirement la base de polarisation, toujours entre $\oplus$ et $\otimes$. Alice transmet alors les photons polarisés en fonction du message binaire, et de la base choisie pour chaque bit.

Lorsque Bob reçoit les photons, il procède de son côté à la même opération qu'Alice : il choisit aléatoirement, pour chaque qubit, la base de mesure entre $\oplus$ et $\otimes$. Une fois les différents choix effectués, il communique publiquement la liste de ses choix à Alice. Alice compare alors les deux listes de choix de bases de polarisation.

Alice transmet alors, toujours publiquement, quelles sont les positions des qubits de la séquence pour lesquels la base de polarisation est la même. Pour ces positions là, Alice et Bob auront bien les même valeurs de qubits, puisque pour ces qubits là, ils auront utilisés le même choix de codage.

Ainsi Alice et Bob peuvent utiliser ces qubits "sûrs" pour constituer une clé privée de codage.

La théorie étant éconcée, voyons un exemple pratique de transmission de 6 qubits entre Alice et Bob :

Alice	Bits à transmettre	1	0	0	1	1	0
	Choix de base	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
	Polarisation envoyée	$\lvert\uparrow\rangle$	$\lvert\searrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$
Bob	Choix de base	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
	Polarisation mesurée	$\lvert\uparrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\searrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\rightarrow\rangle$
	Bits lus	1	1	0	1	0	0
Alice et Bob	Bits acceptés ?	✓	×	×	✓	×	✓
	Message secret	1			1		0

La clé de codage secrète ainsi générée et partagée par Alice et Bob sera donc : **110**. Ainsi, dans cet exemple, Alice et Bob ont engendré 3 bits. Ils peuvent en fait engendrer autant qu'ils veulent en utilisant ce système. En moyenne, Bob devinera le bon positionnement de la base dans 50% des cas. Alice devra donc envoyer en moyenne $2n$ photons pour générer un code à n bits.

Mais, à présent, comment s'assurer que ce message n'a pas été intercepté par un espion ?

Si un espion intercepte un photon, et que Bob a choisi la même base qu'Alice : l'espion a donc 25% de chance de modifier la valeur du qubit, et donc 75% de chances de ne pas modifier cette valeur [3].

On prélève alors 700 bits pour être comparés entre Alice et Bob. Attardons-nous sur 2 questions intéressantes

3. voir *Exemple de transmission d'un seul qubit*

Quelle est la probabilité que, si un espion mesure tous les qubits transmis, aucun des 700 bits ne soit modifié par cette interception ?

Pour un qubit, la probabilité que l'espion ne le modifie pas après interception est de $\frac{3}{4}$. Ainsi, si on transmet 700 qubits, la probabilité d'en modifier aucun tout en espionnant est de $(\frac{3}{4})^{700} \simeq 3,5.10^{-88}$.

La ligne a un taux d'erreur physique de 3%. Quel pourcentage de qubit l'espion peut-il intercepter pour le taux d'erreurs dû à l'interception ne soit pas supérieur au taux physique ?

S'il y a un taux d'erreur physique sur la ligne, Alice et Bob peuvent accepter que $700 \times 3\% = 21$ qubits soient mal transmis. Sachant que l'espion a 25% (1 chance sur 4) de modifier un qubit intercepté, si il ne veut pas créer plus de 21 erreurs, il doit se limiter à observer $21 \times 4 = 84$ qubits. Donc Eve ne pourra regarder que $\frac{84}{700} = 12\%$ du message.

Ainsi, pour s'assurer que le canal de transmission n'est pas "écouté", il suffit à Alice et Bob de prendre un échantillon de bits acceptés par Bob et Alice, et donc pour lesquels Alice et Bob possèdent exactement les bases de polarisation. Alice et Bob se communiquent cet échantillon là, et ils comparent chacuns le résultat de la transmission par rapport à la l'échantillon initial : *tous les bits doivent être identiques.* Une seule différence signe la présence d'un intrus ou d'une erreur physique sur la ligne. L'intrusion n'est avérée que si le taux de bits qui diffèrent dans le processus de reconnassance est supérieur au taux d'erreur physique. Si le nombre de bits échangés est suffisamment grand, le fait qu'ils soient tous indentiques correspond à la quasi-certitude de n'avoir pas été écouté.

Si une erreur est détectée sur cette transmission de vérification, Alice et Bob devront recommencer un nouveau processus et retester la sécurité de la ligne.

3.3.2 Protocole B92

Ce protocole mis en place, cette fois-ci par Bennett seul, en 1992, ressemble assez au protocole BB84. Cependant, la majeure différence entre eux est le nombre d'états utilisés pour le codage : 4 pour BB84 contre 2 pour B92 [4]. Les états utilisés pour le protocole B92 sont choisi de telle sorte qu'il ne soient pas orthogonaux.

Afin de transmettre un bit x à Bob, Alice adopte le codage suivant :

$$|\uparrow\rangle \rightarrow x = 0$$
$$|\nearrow\rangle \rightarrow x = 1$$

De son côté, Bob associe au tirage aléatoire de la base de mesure un bit y tel que :

$$\text{Base } \oplus \rightarrow y = 0$$
$$\text{Base } \otimes \rightarrow y = 1$$

Enfin, Bob associé également un bit b au résultat de la mesure de la façon suivante :

$$\text{Bob mesure } |\uparrow\rangle \text{ ou } |\nearrow\rangle \rightarrow b = 0$$
$$\text{Bob mesure } |\rightarrow\rangle \text{ ou } |\searrow\rangle \rightarrow b = 1$$

4. C. H. Bennett en 1992

Similairement au protocole BB84, Alice envoie son photon polarisé. Alice ne choisit plus ici aléatoirement la base de codage, mais son choix de polarisation du photon imposera forcément la base. En effet, si elle décide d'envoyer $|\uparrow\rangle$, elle devra obligatoirement passer par la base $\oplus$, et si elle décide d'envoyer $|\nearrow\rangle$, elle devra obligatoirement passer par la base $\otimes$. Bob, quant à lui, continue de choisir aléatoirement sa base de mesure.

Intéressons nous à présent, après cette introduction, sur les différents cas de figures, en fonction du photon envoyé par Alice et de la base choisie par Bob. Le tableau, ci-après, résume tous les cas possibles de transmission :

x	y	b
0	0	0
0	1	0 ou 1
1	0	0 ou 1
1	1	0

De ce tableau on en déduit les implications suivantes :

$$x = y \implies b = 0$$
$$b = 1 \implies x \neq y$$

Ainsi, le résultat $b = 1$ ne peut être obtenu que si les bits x et y sont différents. Par contre le fait que $b = 0$ n'implique rien sur x et y.

Alice envoie alors son photon polarisé. Bob le mesure dans sa base choisie, et en déduit la valeur du bit b. On répète alors cela tant qu'Alice n'a pas transmit son message en entier. Il suffira ensuite à Bob de d'informer à Alice pour quels bits x la valeur de b a été 1. Enfin, l'un d'entre Alice ou Bob inversera ses bits correspondant à b=1, et ils auront alors généré un clé secrète connue d'eux seuls.

Voici un exemple de transmission de 8 bits selon le protocole B92 :

Alice	Bit à transmettre (x)	1	0	1	1	0	0	0	1
	Polarisation envoyée	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$
Bob	Bit de la base (y)	1	0	0	0	1	1	0	1
	Choix de base	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
	Polarisation mesurée	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\searrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$
	Bit résultat (b)	0	0	1	0	1	0	0	0
Alice et Bob	Bit accepté ?	×	×	✓	×	✓	×	×	×

Dans cet exemple, pour 8 bits transmis on génère une clé secrète de 2 bits. Cette clé secrète dépendera de qui doit inverser ses qubits entre Alice et Bob : s'ils se mettent d'accord pour que ce soit Bob qui inverse ses bits, la clé sera **10**, dans le cas contraire la clé sera **01**.

On montre que si Alice et Bob veulent générer un clé secrète de taille n bits, Alice doit en moyenne envoyer $4 \times n$ bits.

En effet, le nombre de bits qu'Alice doit envoyer pour générer une clé de n bits dépendera de la probabilité d'obtenir $b = 1$, car c'est seulement dans ce cas là que l'on ajoute un bit à la

clé secrète. D'après le tableau résumant tous les cas de figures pour x et y, on voit qu'il y a une probabilité de 50% pour que x soit différent de y. Néanmoins, $x \neq y \nRightarrow b = 1$. Il y a en réalité une probabilité de 50% pour que $b = 1$ sachant que $x \neq y$. Ainsi la probabilité pour que $b = 1$ est de $50\% \times 50\% = 25\%$.

De ce fait, Alice doit envoyer en moyenne 4 fois plus de bits qu'il ne faut pour générer la clé secrète de taille n. On remarque que ce protocole s'avère moins efficace que le protocole BB84, car l'on perd plus de données lors de la création de la clé secrète.

Enfin, on peut également vérifier que la probabilité qu'un espion intercepte un photon sans le modifier, dans le cas où $b = 1$, est toujours de $\frac{3}{4}$.

Chapitre 4

Algorithmes quantiques

Même si les ordinateurs quantiques n'ont pas encore été conçus, ces derniers laissent cependant de grands espoirs aux scientifiques pour le développement de nouvelles technologies. En effet, même si nous n'en sommes qu'à la théorie, l'informatique quantique pourrait révolutionner notre monde, de par sa rapidité d'exécution et ses nouvelles possibilités d'action. Cette nouvelle manière de "penser" nous amène à de nouvelles performances, grâce notamment à de nouveaux algorithmes.

Par conséquent, nous allons, dans cette partie, nous pencher sur l'étude d'algorithmes quantiques qui, pour des raisons de concision, sont les plus connus : l'algorithme de Deutsch-Joza, Grover et enfin l'algorithme de Shor ; qui nous le verrons permettent d'effectuer des tâches que les ordinateurs classiques ne pourraient réaliser. Même si c'était le cas, ces derniers ne pourraient rivaliser au niveau de la rapidité d'exécution : les algorithmes quantiques sont en effet d'une ordre de complexité moins élevé.

4.1 Algorithme de Deutsch-Jozsa

Soit f une fonction de $Z_2 \rightarrow Z_2$. La fonction f est mise en oeuvre par la porte logique $U_f : |x\rangle|y\rangle Uf \rightarrow |x\rangle, |y \oplus f(x)\rangle$. Une telle fonction est soit constante, c'est-à-dire $f_0(x) = 0$; pour x=0 ou 1 ; ou $f_1(x) = 1$; pour x=0 ou 1, ou soit au contraire équilibrée (c'est-à-dire qu'elle prend autant de fois la valeur 0 que 1). L'algorithme de Deustch [1] permet de déterminer la nature de la fonction, c'est-à-dire savoir si f est constante ou si f est équilibrée, grâce à uniquement une seule et unique évaluation de la fonction f. Comparé à l'informatique classique, qui elle nécessite au moins 2 évaluations de la fonction f , on pourrait croire que cet algorithme n'est pas très performant puisqu'il divise seulement par 2 le nombre d'évaluations de la fonction. Cependant si nous réeffectuons ce schéma pour un registre à n qubits, on peut alors montrer qu'il suffit, encore une fois, d'une seule évaluation de la fonction f pour déterminer la nature de la fonction (soit équilibrée ou soit constante) alors qu'il faut en moyenne $2^{n-1} + 1$ évaluations en utilisant l'informatique classique. Ceci est l'objet de l'algorithme de Deutsch-Jozsa.
Ainsi, nous allons tout d'abord voir comment établir qu'une fonction est soit constante ou soit équilibrée à l'aide d'une seule évaluation de la fonction f (Algorithme de Deutsch). Et ensuite, nous allons généraliser cette méthode pour une fonction qui a, en entrée, un registre à n qubits (Algorithme Deutsch-Jozsa).

1. David Deutsch de l'Université d'Oxford (UK) proposa cet algorithme en 1985 à l'appui de sa thèse sur la version quantique de la machine de Turing

4.1.1 Deustch

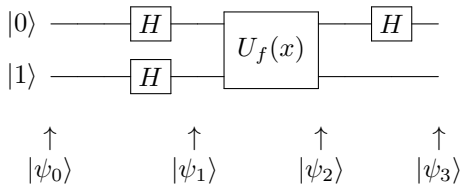


FIGURE 4.1 – Circuit de Deutsch

Tout d'abord, nous allons définir un système à 2 qubits en entrée. On va utiliser un registre de donnée $|x\rangle$ et un registre de résultat à un qubit $|y\rangle$. Nous les initialisons tels que :

$$|\psi_0\rangle = |01\rangle$$

Ensuite, nous "préparons" les deux qubits d'entrée. En effet, sur le premier qubit $|0\rangle$ nous appliquons la porte de Hadamard et nous obtenons, par conséquent, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. De même, le deuxième qubit $|1\rangle$ devient $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

On obtient donc l'état du système :

$$|\psi_1\rangle = (\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \frac{1}{2}(\sum_{x=0,1} |x\rangle)(|0\rangle - |1\rangle)$$

La troisième étape consiste à évaluer ce système à 2 qubits par la fonction f (qui ne modifie que le second terme du système à 2 qubits) et on obtient :

$$|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1} |x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) = \frac{1}{2}\sum_{x=0,1} |x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle$$

Pour pouvoir simplifier cette expression, il nous faut remarquer que :

$$\text{si f(x)=0 alors } y \oplus f(x) = y$$

$$\text{si f(x)=1 alors } y \oplus f(x) = \bar{y}$$

De fait,

$$\text{si f(x)=0 alors } |x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = |x, 0\rangle - |x, 1\rangle$$

$$\text{si f(x)=1 alors } |x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = |x, 1\rangle - |x, 0\rangle$$

Par conséquent , on a :

$$|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1} (-1)^{f(x)}(|x, 0\rangle - |x, 1\rangle)$$

Enfin, nous appliquons la porte de Hadamard sur le premier qubit et nous obtenons :

$$|x'\rangle = \frac{1}{2}(-1)^{f(0)}\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{1}{2}(-1)^{f(1)}\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{2\sqrt{2}}[(-1)^{f(0)} + (-1)^{f(1)}]|0\rangle + \frac{1}{2\sqrt{2}}[(-1)^{f(0)} - (-1)^{f(1)}]|1\rangle$$

Conclusion : Ainsi, il nous suffit de mesurer l'état du premier qubit $|x'\rangle$ de l'état final du système à 2 qubits $|\psi_3\rangle$ pour déterminer la nature de la fonction f. En effet,

— Si, après mesure, nous trouvons $|x'\rangle = |0\rangle$ alors $f(0) = f(1)$ donc f est constante.

— Si, après mesure, nous trouvons $|x'\rangle = |1\rangle$ alors $f(0) \neq f(1)$ donc f est équilibrée.

Ainsi, en une seule évaluation, nous avons pu déterminer la nature d'une fonction qui a, en entrée, un "registre" à un qubit. Qu'en est-il pour un registre à n qubits ?

Remarque 4.1 *Cette algorithme pourrait permettre de savoir en un seul lancer d'une pièce de monnaie si celle-ci à 2 faces "pile" ou si c'est une vraie pièce.*

4.1.2 Algorithme Deutsch-Jozsa

Il s'agit de l'extension de l'algorithme de Deutsch au cas de fonctions de $(0,1)^n \to (0,1)$ qui sont soit constantes soit équilibrées. En effet, l'algorithme de Deustch fut amélioré par Deustch et Jozsa (1992) et finalement par Cleve-Ekert-Macchiavello-Mosca (1998).

La structure de l'algorithme reste le même que celui de Deustch, mais les entrées sont différentes. En effet, on prend un registre de données à n qubits et un registre de résultat à un qubit. De fait, on prend $|\psi\rangle = |xy\rangle$. Ensuite, on initialise le registre de données à $|0\rangle^{\otimes n}$ et on obtient comme système à n+1 qubits :

$$|\psi_0\rangle = |00...0\rangle|1\rangle = |0\rangle^{\otimes n}|1\rangle$$

Ensuite, on réalise la porte de Hadamard sur chacun des n qubits du registre de données et sur le qubit $|1\rangle$ du registre à résultat et on a :

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}[\sum_{x\in(0,1)^n} |x\rangle][\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

Après, nous envoyons l'état $|\psi_1\rangle$ sur la porte de la fonction notée $U_{f(x)}$ et on obtient donc (avec les mêmes simplifications que dans l'algorithme de Deustch) :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}[\sum_{x\in(0,1)^n} (-1)^{f(x)}|x\rangle][\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

On fait de nouveau subir à l'état $|\psi_2\rangle$ une transformation de Hadamard (porte de Hadamard sur chaque qubit sauf sur le qubit de résultat) et on obtient :

$$|\psi_3\rangle = [\sum_{z=0}^{2^n-1} A(z)|z\rangle][\frac{|0\rangle - |1\rangle}{\sqrt{2}}] = \sum_z \sum_x \frac{(-1)^{x.z+f(x)}|z\rangle}{2^n}[\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

avec

$$A(z) = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x.z+f(x)}$$

Avec $x.z = x_1z_1 + x_2z_2 + ... + x_Nz_N \mod 2$.

car

$$H^{\otimes n}|x\rangle = H^{\otimes n}|i_1i_2i_3...i_n\rangle$$

$$= \frac{1}{\sqrt{2^n}}(|0\rangle \pm |1\rangle)(|0\rangle \pm |1\rangle)...(|0\rangle \pm |1\rangle)$$

$$= \frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{x.z}|z\rangle$$

Ainsi, Alice observe maintenant l'état du registre de données.En conclusion : après le processus de mesure si $|0\rangle = |0....0\rangle$ est observé on peut conclure "f constante" et si autre chose est observé on peut conclure " f balancée". Remarquablement il suffit de faire l'expérience et d'utiliser l'oracle quantique qu'une seule fois !

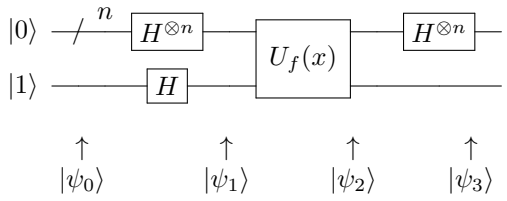


FIGURE 4.2 – Circuit de Deutsch-Jozsa

4.2 Algorithme de Grover

Dans cette partie, nous allons étudier l'algorithme de Grover [2] élaboré en 1996 par l'informaticien du même nom. Celui-ci permet de rechercher un (ou plusieurs) élément(s) spécifiques dans une base de donnée non structurée. Par exemple, cet algorithme pourrait être utilisé pour rechercher quel serait le plus court chemin pour aller d'un point A vers un point B. Dans ce cas bien précis, la base de donnée serait composée de tous les chemins possibles (supposons qu'il y en ait N) pour effectuer ce trajet et l'élément spécifique recherché serait le chemin le plus court. Grâce à un ordianteur classique, on pourrait remédier à ce problème en calculant, pour chaque chemin, la distance parcourue et puis comparer toutes ces distances pour en enfin établir le chemin le plus court. En utilisant ce procédé, il nous faut évidemment de l'ordre de N (O(N)) opérations afin de déterminer le chemin le plus court. Cependant, nous allons voir ensemble qu'en utilisant un ordinateur quantique et particulèrement l'algorithme de Grover, nous pourrons réduire ce coût et par conséquent accélerer la maniputlation et ainsi nécessiter que de $O(\sqrt{N})$ opérations

Remarque 4.2 *A première vue, on pourrait croire que cet algorithme nous permet de savoir quel élément est spécifique dans une base de donnée (par rapport à des critères établis). Cependant, il faut bien comprendre que dans toute cette partie nous allons voir comment optimiser la méthode de recherche (ou de reconnaissance) de l'élément spécifique, en ayant bien à l'esprit que l'on connaît, dès le départ de la manipulation, les caractéristiques qui rendent cet élément spécifique, ainsi le problème ici est que nous ne savons pas où est placé cet élément dans la base de donnée. Ainsi, il est facile de reconnaitre la solution mais difficile de la trouver.*

2. Lov Kumar Grover (né en 1961) est un informaticien indo-américain. Il a obtenu son diplôme de premier cycle à l'Institut indien de technologie de Delhi. Il a travaillé un court moment comme professeur adjoint à l'Université Cornell, puis a rejoint les Laboratoires Bell dans le New Jersey, où il est actuellement un membre du personnel technique dans la recherche en sciences physiques.

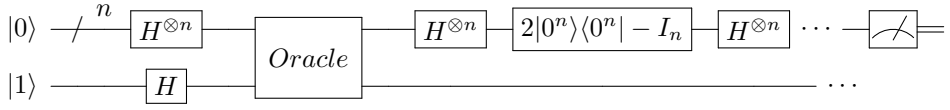


FIGURE 4.3 – Circuit de Grover

4.2.1 Explication

Le principe de l'algorithme de Grover est représenté par le circuit de la figure 4.3. Nous allons voir quels sont les éléments qui composent ce circuit et étudier les étapes de l'algorithme.

Soit une base de donnée composée de N éléments. Tout d'abord, pour plus de commodité, on va affecter à chaque élément un indice compris entre 0 et N-1 et par conséquent nous allons tout simplement rechercher un nombre et non pas l'élément directement. De plus, nous prendrons $N = 2^n$ pour pouvoir stocker les indices dans n qubits. On prend un registre de donnée initialisé à $|0\rangle^{\otimes n}$ et un qubit auxilliaire (registre de résultats) initialisé à l'état $|1\rangle$ et on pose $|\psi_0\rangle = |00..0\rangle|1\rangle$.

A présent, nous allons appliquer la porte d'Hadamard sur chacun des qubits, on applique exactement n+1 fois la porte d'Hadamard. On obtient :

$$H|1\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

et

$$\begin{aligned} H^{\otimes n}|0\rangle^{\otimes n} &= \overbrace{(\frac{(|0\rangle + |1\rangle)}{\sqrt{2}})(\frac{(|0\rangle + |1\rangle)}{\sqrt{2}})...(\frac{(|0\rangle + |1\rangle)}{\sqrt{2}})}^{nfois} \\ &= \frac{1}{\sqrt{2^n}}(|00...0\rangle + |00...1\rangle + ... + |11...1\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle \end{aligned}$$

Ainsi

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Pour pouvoir continuer à expliquer cet algorithme, nous allons introduire une fonction de reconnaissance qui va de $Z_2^n \to Z_2$. Cette dernière a la particularité de savoir reconnaitre un élément spécifique. En effet, f(x)=0 si x$\neq x_0$ et f(x)=1 si $x = x_0$. Cette fonction va être mise en oeuvre par l'intermédiaire d'un opérateur unitaire appellé Oracle qui a en entrée un registre de n qubits et un qubit auxilliaire tel que :

$$|x\rangle|q\rangle \overset{Oracle}{\to} |x\rangle|q \oplus f(x)\rangle$$

De plus, si l'état $|q\rangle = H|1\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ alors on obtient

$$|x\rangle|q\rangle \overset{Oracle}{\to} (-1)^{f(x)}|x\rangle|q\rangle$$

Remarque 4.3 *On voit que le qubit auxilliaire n'a pas été changé et par conséquent on s'interessera plus particuliement à l'état de superposition* $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle$.

La deuxième étape consiste donc à effectuer l'oracle sur l'état

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

et on obtient alors :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle \frac{(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle + ... - |x_0\rangle + |x_0 + 1\rangle + ... + |N-1\rangle) \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Ici, on voit que l'état spécifique que l'on cherche a été "taggé" par un signe moins.

Remarque 4.4 *Le problème, maintenant, est que nous ne pouvons pas lire le résultat obtenu sans le détruire. Par conséquent, nous allons augmenter l'amplitude de l'élément recherché et diminuer l'amplitude des autres éléments.*

De plus, on peut noter que cette opération quantique est l'analogue de celle qu'on fait classiquement, c'est-à-dire répéter pour chaque élément le test de spécificité. En effet, la différence fondamentale est que nous avons fait le test simultanément sur tous les éléments, ceci est due à une particularité quantique : la superposition. On évite ainsi de faire N/2 fois (en moyenne) l'étape pour obtenir l'élément recherché. Cependant l'étape qui va suivre n'est pas aussi triviale que cette dernière. En effet, nous allons maintenant appliquer répétitivement la porte de Grover définie par :

$$G = OS_\psi$$

Où O est l'oracle vu précédemment et S_ψ un opérateur unitaire que nous allons maintenant étudier. On définit tout d'abord l'operation qui change tous les états sauf l'état $|0\rangle$ tel que :

$$S_0 : |0\rangle \to |0\rangle$$

$$|x\rangle \to -|x\rangle \text{Pour } x \neq |0\rangle$$

On peut écrire S_0 sous la forme $(2|0\rangle\langle 0| - I_N)$. En effet, $2|0\rangle\langle 0|$ peut être représenté par la matrice :

$$2 \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & . & . & . & . & 0 \end{pmatrix} \text{ dans la base } \{|0\rangle, |1\rangle, ..., |N-1\rangle\}.$$

Et par conséquent, $(2|0\rangle\langle 0| - I_N)$ est représenté par la matrice (dans la même base que précédemment) :

$$\begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 0 & -1 & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & . & . & . & . & -1 \end{pmatrix}$$

Ainsi, cette matrice effectue bien l'opération qui change tous les états sauf l'état $|0\rangle$.

On définit, ensuite, l'opérateur de diffusion tel que :

$$S_\psi = H^{\otimes n} S_0 H^{\otimes n} = H^{\otimes n}(2|0\rangle\langle 0| + I_N)H^{\otimes n}$$

$$= 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - H^{\otimes n}H^{\otimes n}$$

Or :

$$H^{\otimes n}H^{\otimes n} = I_N$$

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

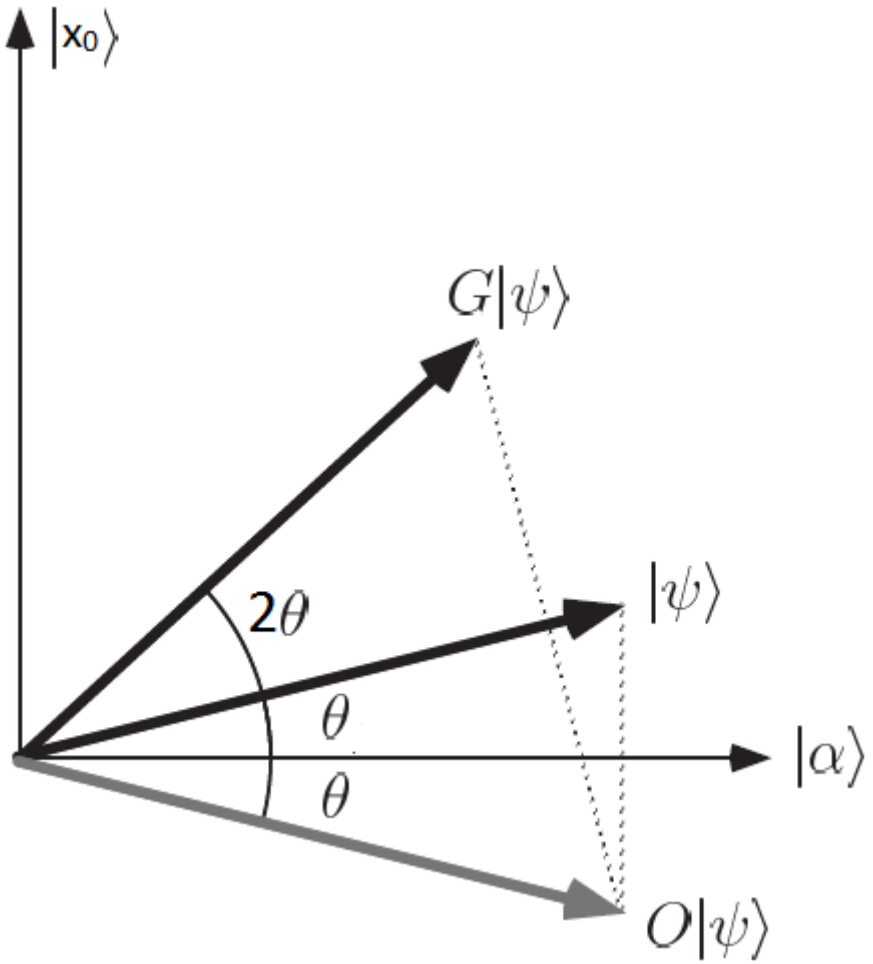
$$H^{\otimes n}\langle 0| = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\langle y|$$

D'où :

$$S_\psi = H^{\otimes n} S_0 H^{\otimes n} = \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle\langle y| - I_N$$

La porte de Grover consistuée de l'opérateur Oracle et S_ψ, opérateur de diffusion, doit être appliquée un nombre suffisant de fois (cette opération ne nécessite, en moyenne, que $\sqrt{N}$ réalisations).

4.2.2 Interprétation géométrique



Tout d'abord, prenons $|\psi\rangle$ tel que $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N}-1}{\sqrt{N}}|\alpha\rangle$ avec $|\alpha\rangle = \frac{1}{\sqrt{N}} \sum_{x=0, x\neq x_0}^{N-1} |x\rangle$. Lorsque nous appliquons l'oracle à $|\psi\rangle$, nous obtenons

$$O|\psi\rangle = -\frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N}-1}{\sqrt{N}}|\alpha\rangle$$

Cette opération est tout simplement la symètrie de $|\psi\rangle$ par rapport à $|\alpha\rangle$ représentée par la figure ci-dessus. Ensuite, nous effectuons l'opérateur S_ψ sur $O|\psi\rangle$ qui effectue la symètrie de $|O\psi\rangle$ par rapport à $|\psi\rangle$ et nous obtenons :

$$S_\psi(O|\psi\rangle) = (2|\psi\rangle\langle\psi| - Id)(-\frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N}-1}{\sqrt{N}}|\alpha\rangle)$$

Par ailleurs :

$$|\psi\rangle = sin(\theta)|x_0\rangle + cos(\theta)|\alpha\rangle$$

Lorsque l'on applique l'oracle et la diffusion sur cet état, on obtient

$$|S_\psi(O\psi\rangle) = sin(\theta + 2\theta)|x_0\rangle + cos(\theta + 2\theta)|\alpha\rangle$$

Et enfin, on réitère cette opération (porte de Grover) k fois et on obtient :

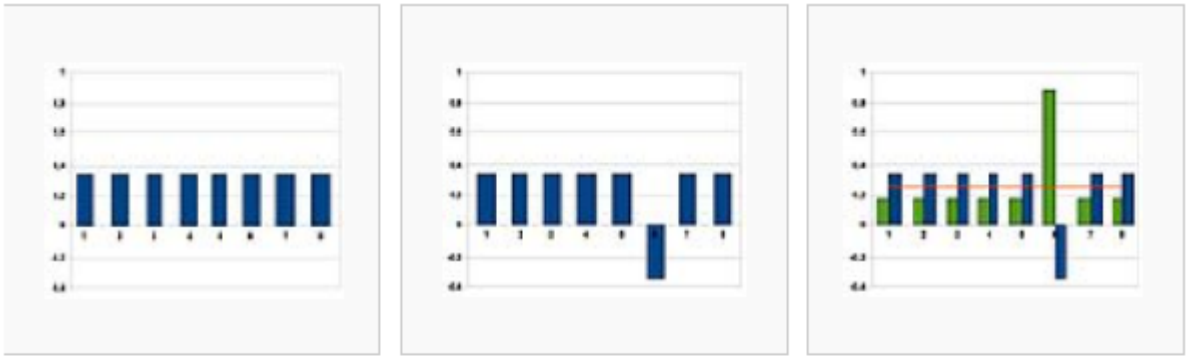
$$(G(|\psi\rangle))^k = sin(\theta + 2k\theta)|x_0\rangle + cos(\theta + 2k\theta)|\alpha\rangle$$

Or, on veut que $|\psi\rangle$ arrive jusqu'à $|x_0\rangle$, c'est-à-dire que $\theta + 2k\theta$ doit être égal à $\pi/2$. Ce qui équivaut à :

$$2k\theta = \pi/2$$

De plus, l'angle θ est supposé petit, d'où $sin(\theta) \simeq \theta$. Or $sin(\theta) = \frac{1}{\sqrt{N}}$. Ainsi, le nombre minimum de fois qu'il faut répeter cette itération est d'environ $k \simeq \frac{\pi}{4}\sqrt{N}$.

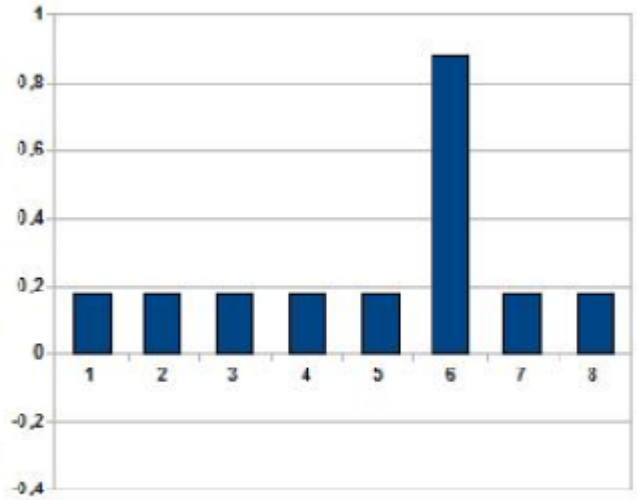
4.2.3 Interprétation grâce à un diagramme



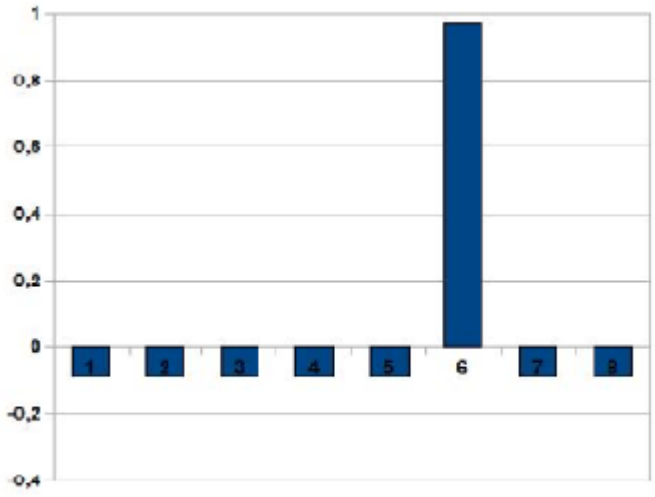
1 : État initial

2 : Application de l'oracle

3 : Application de l'opérateur « miroir autour de la moyenne »



3 : État amplifié



4 : État final, après une itératon supplémentaire

Le diagramme précédent montre l'évolution du qubit signé par l'oracle et des autres éléments par l'opération de diffusion.

On peut voir que l'élément marqué a une probabilité de plus en plus proche de 1. De plus, si nous étudions l'opérateur de diffusion de plus près, on pourra dire qu'il effectue la symètrie des amplitudes par rapport à la moyenne de ces dernière (Diagramme 3). En effet,

$$\begin{aligned}
S_\psi(\sum_{k=0}^{N-1} c_k|k\rangle) &= \frac{2}{N}\sum_{x,y=0}^{N-1}|x\rangle\langle y|(\sum_{k=0}^{N-1} c_k|k\rangle) - \sum_{k=0}^{N-1} c_k|k\rangle \\
&= \frac{2}{N}\sum_{x,y=0}^{N-1}|x\rangle c_y - \sum_{k=0}^{N-1} c_k|k\rangle \\
&= \frac{2}{N}\sum_{y=0}^{N-1} c_y * \sum_{x=0}^{N-1}|x\rangle - \sum_{k=0}^{N-1} c_k|k\rangle \\
&= 2\bar{c}\sum_{x=0}^{N-1}|x\rangle - \sum_{k=0}^{N-1} c_k|k\rangle \\
&= \sum_{k=0}^{N-1}(2\bar{c} - c_k)|k\rangle
\end{aligned}$$

4.3 Algorithme de Shor

L'algorithme de Shor [3], établit par le mathématicien du même nom [4], connu en grand succès grâce à l'avancée considérable qu'il proposait : passer d'une complexité exponentielle, pour un algorithme classique, à une complexité polynomiale, pour un même problème de factorisation arithméique.

4.3.1 Transformée de Fourier quantique

La Transformée de Fourier Quantique est un opérateur unitaire qui agit sur un système à n-qubits. On pose $N = 2^n$. On notera alors TFQ_N la transformée de Fourier quantique appliquée sur un système à n-qubits.

Soit $|x\rangle$ un système quelconque à n-qubits. On peut ainsi l'écrire sous notation décimale de cette manière :

$$|x\rangle = \sum_{j=0}^{N-1} x_j|j\rangle \text{ , avec } x_j \in \mathbb{C}^2 \text{ et } \sum |x_j|^2 = 1$$

Ainsi :

$$TFQ_N|x\rangle = \sum_{k=0}^{N-1} y_k|k\rangle \tag{4.1}$$

$$\text{avec } y_k = \sum_{j=0}^{N-1} \omega^{jk} x_j \text{ , où } \omega = e^{\frac{2i\pi}{N}} \text{est une racine N-ième de l'unité}$$

3. Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, 1994

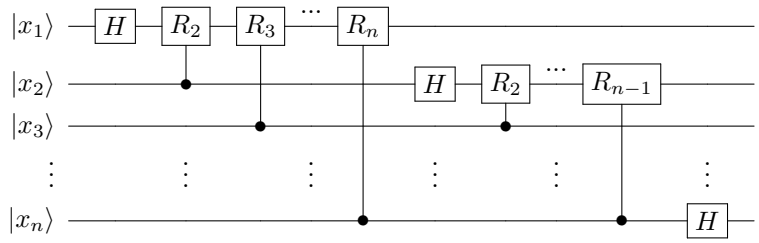
4. Peter Williston Shor, né le 14 août 1959, est un mathématicien américain. Connu pour son travail dans le calcul quantique, il est professeur au MIT et membre du CSAIL

D'autre part, on représente aussi sous forme matricielle, comme suit, l'opérateur Transformée de Fourier quantique, dans la base $|0\rangle, |1\rangle, |2\rangle, ..., |N-1\rangle$:

$$TFQ_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^1 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix} \tag{4.2}$$

où $\omega = e^{\frac{2i\pi}{N}}$ est une racine N-ième de l'unité

Enfin, en ce qui concerne la représentation de la TFQ, elle peut encore prendre la forme d'un circuit quantique à n entrées :



avec $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$

FIGURE 4.4 – Circuit de la Transformée de Fourier quantique

Propriétés fondamentales de TFQ :

1) Unitaire

2) $TFQ_N|0\rangle = \sum_{j=0}^{N-1} |j\rangle$ **: état parallélisé**

3) Transforme un signal périodique en un autre signal périodique, sans prendre en compte le "point de départ" : linear shift invariant

Preuves :

1) La TFQ, comme sont circuit quantique l'indique, n'est formée que par des opération unitaires (porte de Hadamard, R_k). Ainsi, la TFQ est elle même unitaire.

2) Pour chacun des qubits $|0\rangle$ du système $|0\rangle = |0...00\rangle$ on a $R_k|0\rangle = |0\rangle$. Ainsi $TFQ_N|0\rangle$ n'est en réalité qu'une succession de porte de Hadamard sur chacun des qubits du système, soit $H^{\otimes n}|0\rangle$. On obtient donc bien un état parallélisé.

3) Soit $|x\rangle$ un état périodique de période r. On a $N = 2^n$ et K qui est le nombre d'éléments non nuls de $|x\rangle$ (le nombre de vecteurs de base dans l'écriture sous forme de somme de $|x\rangle$). On note alors $|x\rangle$ comme suit :

$$|x\rangle = \sum_{j=0}^{N-1} \varphi(j)|j\rangle$$

$$\text{avec } \varphi(j) = \begin{cases} \frac{1}{\sqrt{K}} \text{ si } j = x_0 + kr \\ 0 \text{ sinon} \end{cases}$$

On peut alors ré-écrire le système $|x\rangle$ sous cette forme :

$$|x\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle$$

On suppose que r divise exactement N, c'est à dire que $K = \frac{N}{r}$. Si ce n'est pas le cas, on montre qu'avec quelques traitement suplémentaires (ne changeant pas la complexité du problème) on peut se replacer dans ce cas de figure.

Appliquons à présent l'opérateur TFQ_N à notre état périodique $|x\rangle$:

$$TFQ_N|x\rangle = \sum_{s=0}^{N-1} y_s|s\rangle$$

$$\text{avec } y_s = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega^{js} = \frac{1}{\sqrt{NK}} \sum_{k=0}^{K-1} \omega^{(x_0+kr)s}$$

On simplifie la forme de y_s par un travail sur les puissance de ω :

$$y_s = \frac{\omega^{x_0 s}}{\sqrt{NK}} \sum_{k=0}^{K-1} \omega^{(kr)s}$$

On peut encore simplifier l'expression de y_s en fonction de la valeur de s. Pour cela on distingue le cas où s est un multiple de K, et le cas contraire. Dans le cas contraire, on utilise le fait que la somme des racines n-ièmes de l'unité est égale à 0. Alors, $\exists q \in \mathbb{Z}$ tel que :

$$y_s = \begin{cases} \frac{K}{\sqrt{NK}} \omega^{x_0 s} \text{ si } s = qK \\ 0 \text{ sinon} \end{cases} = \begin{cases} \frac{1}{\sqrt{r}} \omega^{x_0 s} \text{ si } s = qK \\ 0 \text{ sinon} \end{cases}$$

Ainsi en prenant $s = qK$, avec $q \in [\![0, r-1]\!]$, on aura :

$$TFQ_N|x\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} e^{\frac{2i\pi}{r} q x_0} \left| q\frac{N}{r} \right\rangle$$

TFQ_N transforme donc un état périodique de période r débutant à x_0, en un état période de période $\frac{N}{r}$ débutant à 0.

Pour terminer ce paragraphe introductif sur la Transformée de Fourier quantique, il semble intéressant de parler de la complexité de cette opération. Utilisons simplement le circuit quantique, représenté précedemment, pour cela.

Sur la première ligne du circuit, on effectue une porte de Hadamard, puis $(n-1)$ fois la porte R_k. Sur la seconde ligne du circuit, on effectue un porte de Hadamard, puis $(n-2)$ fois la porte R_k. En général, sur la i-ème ligne du circuit, on effectue une porte de Hadamrd, puis $(n-i)$ portes R_k. Ainsi, il en résulte un nombre $(n-i)+1$ d'opérations sur la i-ème ligne.

Etant donné qu'il y a n lignes dans le circuit, le nombre total β d'opérations effectuées par le circuit quantique est égal à :

$$\beta = \sum_{i=1}^{n} n - i + 1 = \sum_{i=1}^{n} i = \frac{n(n+2)}{2}$$

Ainsi la Transformée de Fourier quantique réalise $\beta = \frac{n(n+2)}{2} = O(n^2)$ opérations. Cette opération a donc un coût polynomial en n.

Exemple : TFQ_8

On se propose ici d'étudier l'exemple pour N = 8, c'est à dire pour un système à 3 qubits. La matrice représentative de TFQ_8 donne donc :

$$TFQ_N = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

$$\text{avec } \omega = e^{\frac{2i\pi}{8}} \text{ d'où } \omega^8 = (e^{\frac{2i\pi}{8}})^8 = 1$$

On vérifie la première propriété fondamentale, c'est à dire que TFQ_8 est bien unitaire en calculant $TFQ_8.{}^{\mathrm{t}}\overline{TFQ_8}$ ce qui donne I_8. On utilisera pour cela la simplification suivante :

$$\sum_{k=0}^{7} \omega^k = 0$$

Par ailleurs, on peut également vérifier la seconde propriété fondamentale :

$$TQF_8|0\rangle = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{8}} \sum_{k=0}^{7} |k\rangle \text{ : état parallélisé}$$

En outre, la troisième propriété fondamentale peut également être vérifiée en pratique. Prenons, par exemple, un état $|psi\rangle$ périodique de période 2, exprimé comme suit dans la base $|0\rangle, ..., |7\rangle$:

$$|\psi\rangle = \frac{1}{2}\begin{pmatrix}0\\1\\0\\1\\0\\1\\0\\1\end{pmatrix} \Rightarrow TFQ_8|\psi\rangle = \frac{1}{4\sqrt{2}}\begin{pmatrix}4\\ \omega+\omega^3+\omega^5+\omega^7\\ 2\omega^2+2\omega^6\\ \omega^3+\omega+\omega^7+\omega^5\\ 4\omega^4\\ \omega^5+\omega^7+\omega+\omega^3\\ 2\omega^2+2\omega^6\\ \omega^7+\omega^5+\omega^3+\omega\end{pmatrix}$$

En utilisant le fait que les racines 8-ièmes de l'unité 1, ω, ω^2 et ω^3 soient respectivement symétriques par rapport à l'origine à ω^4,ω^5, ω^6 et ω^7, on obtient :

$$TFQ_8|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\\-1\\0\\0\\0\end{pmatrix}$$

Cet état est bien périodique de période $4 = \frac{N}{r} = \frac{8}{2}$ débutant à l'origine.

4.3.2 Mise en place du problème

Bien avant même l'époque d'Euclide, on savait que chaque entier naturel n était décomposable, de manière unique, en produit de facteurs premiers. Les mathématiciens se sont pendant long-temps intéressés à la question de savoir comment factoriser un certain nombre en un produit de nombres premiers. Si un grand nombre à n-bit est le produit de deux nombres premiers qui sont probablement de la même taille, alors aucun algorithme classique n'est actuellement connu pour pouvoir le factoriser en temps polynomial. Ce qui veut dire qu'il n'existe pas d'algorithme connu pouvant le factoriser en temps $O(n^k)$ quelle que soit la constante k. Il existe des algorithmes classiques, néanmoins, qui sont aussi "rapides" que $O(e^n)$. En d'autres termes, les meilleurs algorithmes connus sont sous-exponentiels, mais super-polynômiaux. En particulier, le meilleur algorithme connu s'exécutant en temps asymptotique est le crible général de corps de nombres (GNFS).

Par ailleurs, en utilisant un calculateur quantique, on pourrait arriver à surpasser les résultats actuels sur les ordinateurs classiques. Comme aucun calculateur quantique n'a encore été officiellement mise en place, on ne peut utiliser les nombreux avantages du calcul quantique. Néanmoins, les algorithmes quantiques qui pourraient y être implémentés ont déjà été établis, notamment un qui résoud le problème de factorisation d'un entier en nombres premiers en un temps polynomial : l'algorithme de Shor.

Principe de l'algorithme

Soit $N \in \mathbb{N}$ un grand nombre. On cherche à trouver un diviseur de N.
Pour cela on utilise tout d'abord un théorème d'arithmétique :

Théorème 4 (Euler-Fermat) *Soit N un entier strictement positif et a un entier premier avec N, alors on a*

$$a^{\varphi(n)} \equiv 1 \text{ [N]}$$

, avec $\varphi(n)$ la fonction indicatrice d'Euler

Si on choisit un entier a premier avec N, il existe donc un entier r tel que :

$$a^r \equiv 1 \text{ [N]} \iff a^r - 1 \equiv 0 \text{ [N]}$$

Si r est pair, alors on aura :

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} - 1) \equiv 0 \text{ [N]} \iff \exists k \in \mathbb{Z} \ / \ (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} - 1) = k\text{N}$$

Ceci revient à dire que soit $a^{r/2} - 1$ ou $a^{r/2} + 1$ divise N. Pour vérifier lequel est diviseur, il suffit de calculer PGCD(N,$a^{r/2} - 1$) et PGCD(N,$a^{r/2} + 1$).

Pour trouver un diviseur de N, il faudra donc trouver un nombre premier avec N, puis son ordre, pair, associé pour que le reste dans la division euclidienne de ce nombre par N soit 1. Trouver un nombre premier n'est pas l'étape plus difficile : c'est trouver l'ordre r qui consititue le cœur du problème.

4.3.3 Recherche de la période

Cette section fait le lien entre le problème d'arithmétique énoncé précedemment et l'utilisation de la Transformée de Fourier quantique. En effet, l'idée ici est de ramener le problème de recherche de l'ordre r, à un problème de recherche de période d'un système périodique.

Théorie

Soit une fonction $f : Z_N \to Z_N$ avec $Z_N = \{x \in \mathbb{N} \ / \ x < N\}$. On dit que f est périodique de période $r < N$, lorsque :

$$\forall x \in [\![0, N - r - 1]\!],\ f(|x + r\rangle) = f(|x\rangle)$$

On suppose par ailleurs que f ne prend jamais deux fois la même valeur dans une même période.

On pose alors $f(|x\rangle) = |a^x[N]\rangle$ qui prend un état $|x\rangle$ en praramètre et renvoie l'état $|a^x \text{ modulo } N\rangle$.

On définit également une porte $U_f : (x, y) \to (x, y \oplus f(x))$, avec x appelé le registre de données, dont le résultat sera contenu dans le registre de résultats $y \oplus f(x)$

On pose alors :

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|0\rangle$$

On applique alors la porte U_f au qubit $|\psi_0\rangle$:

$$|\psi_1\rangle = U_f|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\big|a^k[N]\big\rangle$$

On fait ensuite une mesure sur le second registre, et on mesure $\big|a^{k_0}\big\rangle$ une valeur particulière de $\big|a^k[N]\big\rangle$. Or $\big|a^{k_0}\big\rangle$ n'est pas atteinte seulement pour $k = k_0$ mais pour toutes les valeurs périodiques associées à k_0, c'est à dire pour tous les $k = k_0 + jr$, avec j un entier.

Comme $a^{k_0+jr} = a^{k_0}(a^r)^j = a^{k_0}$, car $f : k \mapsto a^k[N]$ est périodique de période r, on obtient après mesure du second registre :

$$|\psi_2\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |k_0 + jr\rangle \left|a^{k_0}\right\rangle$$

Une mesure sur le premier registre ne nous permettra pas de déterminer la période r, car l'origine k_0 est inconnue. A la place, on applique la Transformée de Fourier quantique à l'état $|\psi_2\rangle$:

$$|\psi_3\rangle = TFQ_N|\psi_2\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} e^{\frac{2i\pi}{r}qk_0} \left|q\frac{N}{r}\right\rangle \left|a^{k_0}\right\rangle$$

A présent on mesure le premier registre de données, afin de déterminer la période r. Comme la norme de l'exponentielle complexe est 1, après la mesure on obtient :

$$|\psi_4\rangle = \left|q_0\frac{N}{r}\right\rangle$$

On récupère donc grâce à la Transformée de Fourier quantique et à une mesure la valeur de $z = q_0\frac{N}{r}$. D'où $\frac{z}{N} = \frac{q_0}{r}$. On connait z et N, mais l'on ne connait ni q_0 ni r. A première vu, on ne peut pas en déduire r, car q_0 nous est inconnu, mais si on tente de réduire la fraction $\frac{z}{N}$, on peut arriver à trouver la période r.

En effet, si l'on réduit la fraction $\frac{z}{N}$ en une fraction irréductible, on en déduira la fraction $\frac{q_0}{r}$. Si q_0 et r sont premiers entre eux, on en déduira les valeurs de q_0 et de la période r. S'ils ne sont pas premiers entre eux, on peut répéter la mesure faire pour obtenir $|\psi_4\rangle$.

On appliquera alors cette méthode pour obtenir la période r de la fonction f, et donc trouver r tel que $a^r \equiv 1[N]$.

4.3.4 Algorithme de Shor

Cette section aura pour principal but de regrouper les différentes parties de l'algorithme traitées séparement ci-dessus, et d'énoncer les étapes, et relations entre ces dernières, de l'algorithme.

Etape 1

Il convient tout d'abord, bien entendu, de choisir un entier $N \in \mathbb{N}$ à factoriser. L'entier ne doit pas être premier, sinon il ne sera pas possible de la factoriser. On passe ensuite à la seconde étape.

Etape 2

On vérifie, avant tout calcul, que l'entier N choisi n'est pas pair, auquel cas l'algorithme est terminé et 2 sera le candidat sûr comme diviseur de N.

L'algorithme prend alors fin immédiatement, renvoyant ainsi l'entier 2.

Si 2 ne divise pas N, on passe dans ce cas à l'étape 3.

Etape 3

On choisit ensuite, au hasard, un entier $a \in [1, N-1]$.

Si PGCD$(a, N) = d > 1$, alors on retourne l'entier d, diviseur certain de N.

Sinon, c'est à dire si a et N sont premiers entre eux, on passe à l'étape 4.

Etape 4

On utilise l'algorithme de recherche de la période pour trouver l'ordre r de a^x modulo N, c'est à dire r tel que $a^r \equiv 1[N]$.

Une fois r trouvé, on continue avec l'étape 5.

Etape 5

On opère alors à une vérification sur r :

Si r est impair, on retourne à l'étape 3.

Si r est pair, on calcule PGCD$(a^{r/2}+1, N)$ et PGCD$(a^{r/2}-1, N)$. L'un de ces deux nombres sera forcément un diviseur de N. On renvoie alors le bon diviseur de N

Complexité de l'algorithme

L'une des plus importantes propriétés de cet Algorithme de Shor est bien entendu sa complexité, dont l'ordre révolutionna le monde de l'informatique classique comme quantique. En pratique, l'informatique classique doit déployer des algorithmes aux coûts exponentiels pour résoudre ce problème de factorisation en produit de nombres premiers, alors que l'algorithme de Shor suit un coût polynomial.

En effet, l'algorithme de Shor fait appel à la Transformée de Fourier quantique qui a une complexité d'ordre polynomiale. En outre, la fonction périodique f a également un coût polynomial en n. Une succession d'opérations à coûts polynomiaux reste à coût polynomial.

Pour donner un ordre d'idée de l'efficacité de l'algorithme, voici quelques estimations temporelles de calcul pour factoriser un nombre de 1024 bits :

— Temps de factorisation pour un ordinateur classique (en 2006) : 100 000 ans

— Temps de factorisation pour une ordinateur quantique (avec un registre de 5100 qubits et environ 10^9 de portes quantiques) : 5 minutes.

Ainsi Shor a permi, grâce à son algorithme à résoudre, dans le monde quantique, un problème crucial de sécurité du monde de l'informatique classique. Le plus grand obstacle entre ces deux mondes demeure toujours l'établissement d'un ordinateur/calculateur quantique.

Première application pratique

En 2001, le centre de recherche d'IBM a implémenté cet algorithme sur un ordinateur quantique à 7 qubits. Cette expérience leur a permis de factoriser le nombre 15 en 5 fois 3. En prenant $a = 7$, il ont trouvé une période de $r = 4$. Ils en ont déduits que $a^{r/2} \equiv 4[15]$. Ainsi, soit 3 ou soit 5 divise 15 : dans ce cas là, les deux divisent 15.

Annexes

Produit tensoriel

Définition

Le produit tensoriel est une technique permettant de construire une représentation d'un groupe fini à partir de deux autres.

Soient E et F deux espaces vectoriels sur un corps commutatif K. Il existe alors un espace vectoriel noté $E \otimes F$ et une application linéaire ayant la propriété suivante :

Pour tout espace vectoriel G, et pour toute application bilinéaire g de E dans G, il existe une, et une seule, application linéaire $\tilde{g}$ de $E \otimes F$ dans G telle que :

Pour tout $x \in E, y \in F, g(x, y) = \tilde{g}(x \otimes y)$

Ainsi l'espace $E \otimes F$ est le produit tensoriel de E et F et $x \otimes y$ le produit tensoriel de x et y.

De plus, $dim(E \otimes F) = dim(E) \times dim(F)$

Groupes et matrices unitaires

Groupes unitaires

Théorème 5 *Soit E un espace vectoriel préhilbertien complexe. Pour tout automorphisme $u \in \mathcal{GL}(E)$ les assertions suivantes sont équivalentes :*

- *(i) $\forall x \in E$, $||u(x)|| = ||x||$ (on dit que u conserve la norme).*
- *(ii) $\forall (x, y) \in E^2$, $\langle u(x), u(y) \rangle = \langle x, y \rangle$ (on dit que u conserve le produit scalaire).*
- *(iii) L'automorphisme u a un adjoint u^* et $u^* = u^{-1}$.*

Si u vérifie l'une de ces assertions, on dit que u est un automorphisme *unitaire* de E. On note $\mathcal{U}(E)$ l'ensemble des automorphismes unitaires de E.

Proposition 1 *Soit u un endomorphisme de l'espace hermitien E, les assertions suivantes sont équivalentes :*

- *(i) $u \in \mathcal{U}(E)$.*
- *(ii) l'image de u de toute base orthonormée de E est une base orthonormée.*
- *(iii) il existe une bse orthonormée de E dont l'image par u est une base orthonormée.*

Matrices unitaires

Proposition 2 *Soit $P \in M_n(\mathbb{C})$, les conditions suivantes sont équivalentes :*

- *(i) la matrice P est unitaire.*
- *(ii) $PP^* = P\,{}^t\overline{P} = I_n$.*
- *(iii) $P^*P = {}^t\overline{P}P = I_n$.*
- *(iv) les vecteurs colonnes de P forment une base de $\mathbb{C}^n$.*
- *(v) les vecteurs lignes de P forment une base de $\mathbb{C}^n$.*

Espace hermitien

Définition 2 *Un espace hermitien est un espace vectoriel complexe de dimension finie. Il dispose d'un produit scalaire $\langle , \rangle$ de $E \times E$ dans $\mathbb{C}$. Le **produit scalaire hermitien** sur E est une application de $E \times E$ dans $\mathbb{C}$. Cette application est :*

- *(i) hermitienne : $\forall (x, y) \in E^2$, $\langle x, y\rangle = \overline{\langle y, x\rangle}$.*
- *(ii) définie positive : $\forall x \in E$, $\langle x, x\rangle \in R^+$ et $\langle x, x\rangle = 0$ si et seulement si $x = 0$.*
- *(iii) linéaire à droite : $\forall (x, y, z) \in E^3$, $\langle x, \alpha y + z\rangle = \alpha\langle x, y\rangle + \langle x, z\rangle$.*

En outre, $\forall x \in E$, on note la norme $||x|| = \sqrt{\langle x, x\rangle}$.

Principe des tiroirs

Si E et F sont deux ensembles finis, tels que $card(E) > card(F)$ et si $f : E$ est une application de E dans F, alors il existe un élément de F qui admet au moins deux antécédents par f ; autrement dit il n'existe pas d'application injective de E dans F.

Bibliographie

[1] Y Leroyer, Introduction à l'information quantique. Notes de cours ENSEIRB-MATMECA, 2012-2013

[2] Daniel Baye, Techniques de résolution numérique de l'équation de Schrödinger dépendant du temps. Université Libre de Bruxelles, Faculté des Sciences Appliquées

[3] Michael A.Nielsen and Isaac L.Chuang, Quantum Computation and Quantum Information. CAMBRIDGE UNIVERSITY PRESS 10th Anniversary edition published 2010

[4] Anton Zeilinger, La téléportation quantique. Pour la science- Numéro 272 : juin 2000

[5] Jordan David, Introduction à l'information quantique. February 11, 2002

[6] J D Cresser Quantum Physics Notes, 2009

[7] Remy MOSSERI and Rossen DANDOLOFF Geometry of entangled states, Bloch Spheres ans Hopf Fibrations, 2001

[8] Remy MOSSERI Two and Three qubits geometry and Hopf Fibrations, 2003

[9] Peter W. Shor Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, janvier 1996

[10] http ://www.toutestquantique.fr

[11] http ://www.if.ufrgs.br/ betz/quantum/SGPeng.htm

[12] http ://fr.wikipedia.org/wiki/Principe_des_tiroirs

[13] http ://fr.wikipedia.org/wiki/Equation_de_Schrödinger

[14] http ://fr.wikipedia.org/wiki/Sphère_de_Bloch