Cours 3 — 25 janvier

Enseignant : Frédéric Magniez *Rédacteur : Alexis Fluteaux*

3.1 Notion de qubit

On appelle qubit un état quantique qui représente la plus petite unité de stockage d'information quantique.

Définition 3.1. *Un bit quantique est une superposition linéaire de deux états de base notés* $|0\rangle$ *et* $|1\rangle$*, ce qui constitue la différence majeure avec un bit classique, qui vaut 0 ou 1 de façon certaine. On l'écrit sous forme d'un vecteur complexe de dimension 2 normé.*

On parle d'état quantique pur lorsque que l'état du système peut s'écrire comme somme d'états propres.

Plusieurs types de système peuvent être décrits par un qubit, notamment l'état de polarisation d'un photon ou le spin d'un électron.

3.2 Mesure d'un qubit

Les fonctions d'onde, c'est-à-dire les distributions de probabilité de présence, à la base de la théorie quantique, sont issues de calculs totalement déterministes. La source d'aléa est dans l'acte d'observation lui-même, c'est-à-dire la mesure. En effet, suite à une mesure, le système quantique se fixe dans un état avec une certaine probabilité, liée au carré de l'amplitude de l'état.

La notion de base de mesure est également importante : les états que l'on peut mesurer sont non seulement des états propres, mais aussi des états de base. Si on essaie de mesurer la polarisation d'un photon avec un analyseur horizontal, le résultat est incertain et lié à l'angle de polarisation. En revanche, le résultat est déterministe si on se place dans une base contenant la polarisation (rectiligne) de ce photon. Une mesure dans une base quelconque donne des résultats avec une probabilité égale au carré du produit scalaire entre l'état du qubit et le vecteur de base, ce qui revient à changer de base, faire la mesure dans la base classique ($|0\rangle$, $|1\rangle$), puis revenir à la base initiale.

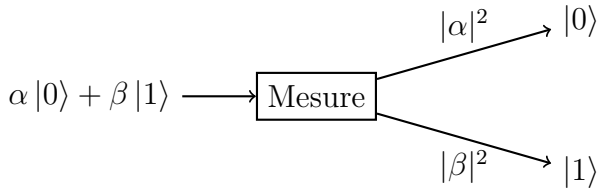

Figure 3.1: Résultats possibles d'une mesure dans la base classique ($|0\rangle$, $|1\rangle$)

En optique, changer de base revient à tourner un analyseur.

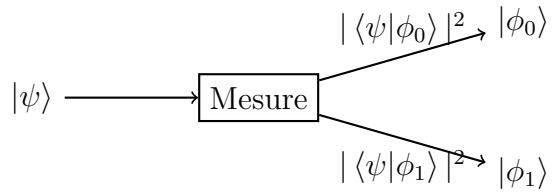

Figure 3.2: Résultats possibles d'une mesure dans une base quelconque

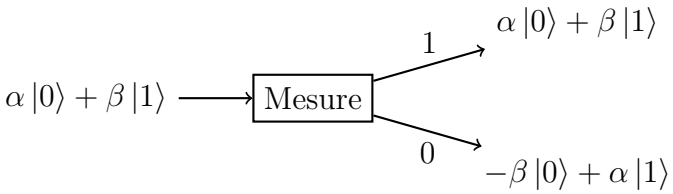

Figure 3.3: Mesure certaine

Figure 3.4: Mesure avec changement de base

3.3 Systèmes à n qubits

Dans le cas d'un système classique, on peut décrire l'ensemble par l'état de chaque composant. En revanche, un système de n qubits ne peut pas toujours être décrit par l'état de chacun des qubits. Des qubits séparés contiennent donc moins d'information que s'ils sont **intriqués** dans un système quantique. L'espace vectoriel décrivant n bits classiques est de dimension 2n (il s'agit de $\left(\mathbb{C}^{\{0,1\}}\right)^n$), alors que celui décrivant n qubits est de dimension 2^n ($\bigotimes_n \mathbb{C}^{\{0,1\}}$). C'est cette augmentation exponentielle du nombre d'états avec le nombre de particules qui suggère la puissance des potentiels ordinateurs quantiques. Certains états peuvent être *factorisés* comme des produits tensoriels d'états propres, comme $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$, mais d'autres ne le sont pas (notamment $|00\rangle + |11\rangle$). La mesure d'un état $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ conduit à un état $|x\rangle$ avec une probabilité $|\alpha_x|^2$.

3.4 Transformations sur les qubits

Des dispositifs physiques permettent de modifier l'état d'un qubit. Certains correspondent à une transformation classique, réversible, alors que d'autres ne peuvent être expliqués en accord avec la mécanique classique. Il est toujours possible de conserver suffisamment d'information de sorte à ce qu'une porte quantique soit réversible (il suffit d'une bijection entre les états d'entrée et les états de sortie).

Négation

La négation d'un bit quantique peut être réalisée en faisant passer un photon au travers d'une lame demi-onde à 45 °, le système considéré étant la polarisation du photon.
On peut mesurer l'état du système sans perturber le fonctionnement d'une porte NOT, dans la mesure où l'image d'un état de base est un état de base.

Transformation de Hadamard

On réalise la transformation de Hadamard $H = \frac{1}{\sqrt{2}} \times \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ à l'aide d'une lame demi-onde à 22,5 °
$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ et $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
Cette transformation correspond à une symétrie, elle est sa propre inverse.

Application 3.2. *On peut réaliser un générateur de nombres aléatoires avec cette transformation : comme l'image du qubit $|0\rangle$ est $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, la probabilité de mesurer le qubit dans l'état $|0\rangle$ ou $|1\rangle$ est de $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.*

Avec une lame demi-onde dans un autre angle, on obtient un générateur biaisé (par exemple avec 30 °, il vient $G = \frac{1}{2} \times \begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$, soit des probabilités de 3/4 et 1/4). Il est possible d'équilibrer ce type de générateur en modifiant la base de mesure (avec 30 °, on peut mesurer dans la base $\frac{|1\rangle\pm|0\rangle}{\sqrt{2}}$)

C-Not

Une porte $C-G$ est une transformation linéaire conditionnelle sur l'un des qubits, en préservant l'autre (qubit de contrôle). Elle est représentée par $C\text{–}G\,|0a\rangle = |0\rangle\,|a\rangle\,;\, C\text{–}G\,|1a\rangle = |1\rangle\,G\,|a\rangle$.

La porte quantique Controlled-NOT correspond au XOR logique : $C-\text{NOT}\,|a\rangle\,|b\rangle = |a\rangle\,|a\oplus b\rangle$. Elle peut être réalisée dans un système consistant en les transitions entre deux états d'ions piégés dans un champ magnétique, en utilisant des lasers pour déclencher des interactions quantiques. (cf http ://arxiv.org/abs/quant-ph/0212079)

Porte quelconque

Les portes C-NOT et H sont très utiles pour la conception d'un calculateur quantique. Elles permettent de réaliser aisément :

– une porte SWAP qui échange deux qubits :

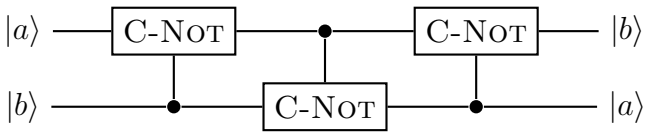

Figure 3.5: Porte SWAP

– une porte C-NOT inversée (cela présente surtout un intérêt théorique !) :

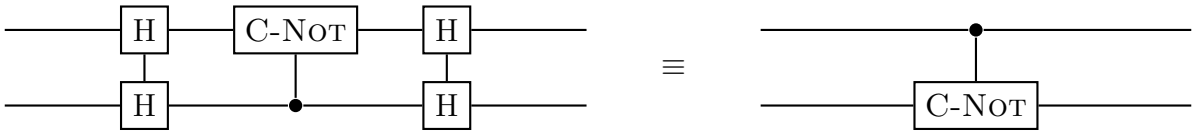

Figure 3.6: Porte C-NOT inversée

– une porte AND et une porte OR. La difficulté vient du fait que les portes d'Hadamard et Controlled-NOT ne permettent de réaliser que des transformations réversibles (des bijections entre les ensembles des états de départ et d'arrivée). Une porte ne renverrait que $aANDb$ et un autre qubit constituant une perte d'information, on doit réaliser une porte qui renvoie a, $a\ AND\ b$ et $a\ OR\ b$:

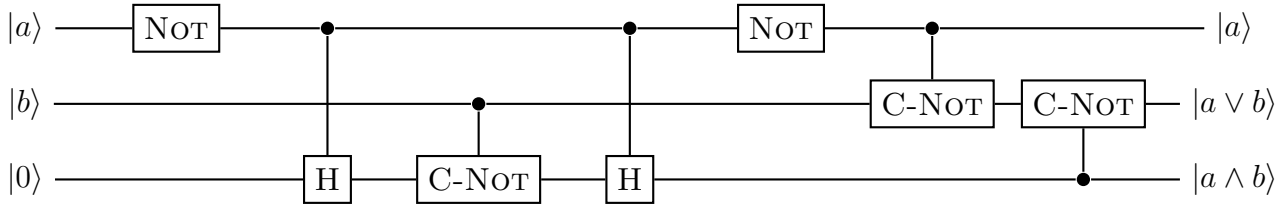

Figure 3.7: Portes AND et OR

3.5 Matrices densité

L'écriture formelle de la mesure d'un seul qubit du système s'écrit à l'aide de projecteurs ($P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes I_2$ et $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes I_2$).

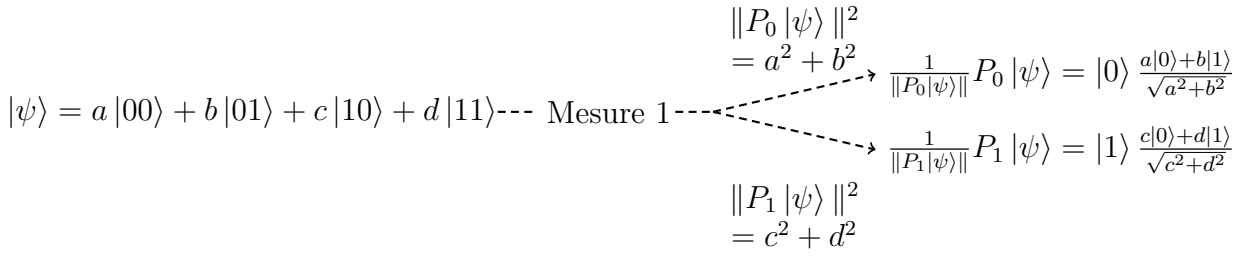

Figure 3.8: Mesure du premier de deux qubits

Dans le cas d'un système de deux qubits, la mesure d'un seul bit quantique introduit un mélange statistique provenant de deux phénomènes. D'une part l'incertitude quantique liée au fait que le deuxième qubit est encore dans une superposition cohérente d'états propres ; d'autre part le résultat de la mesure du premier bit est donné par une distribution statistique des différents kets possibles.

Le mathématicien et physicien John Von Neumann a introduit, pour simplifier ce formalisme, la notion de **matrice densité**, qui résume à un instant donné l'ensemble de tous les états quantiques possibles d'un système. Dans le cas d'un état pur $|\psi\rangle = a|0\rangle + b|1\rangle$, la matrice densité s'écrit simplement $\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |a|^2 & ab* \\ a*b & |b|^2 \end{pmatrix}$. Pour un mélange statistique d'états quantiques $(|\psi_i\rangle, p_i)_{i\in I}$, elle devient $\sum_{i\in I} p_i |\psi_i\rangle\langle\psi_i|$

La matrice densité est hermitienne, et peut donc être diagonalisée en base orthonormée, avec des valeurs propres positives. De par sa forme, la trace de toute matrice densité vaut 1 (car $\sum_{i\in I} p_i = 1$ et $Tr(|\psi_i\rangle\langle\psi_i|) = 1$ pour tout $i \in I$).

Pour une matrice de densité ρ, l'état obtenu après mesure correspond à la matrice densité diagonale $\langle 0|\rho|0\rangle |0\rangle\langle 0| + \langle 1|\rho|1\rangle |1\rangle\langle 1|$. On ne peut donc pas distinguer deux systèmes de même matrice densité.

Théorème 3.3. *Les statistiques d'observation d'un qubit dans une base quelconque ne sont liées qu'à sa matrice densité.*

Preuve: Soit M la matrice de changement de base $(|0\rangle, |1\rangle) \Rightarrow (|\psi_0\rangle, |\psi_1\rangle)$, et ρ l'état mélangé $\sum p_i |\phi_i\rangle\langle\phi_i|$.

En mesurant après changement de base, on obtient la matrice densité

$$\langle 0|M^*\rho M|0\rangle |0\rangle\langle 0| + \langle 1|M^*\rho M|1\rangle |1\rangle\langle 1| = \langle\psi_0|\rho|\psi_0\rangle |0\rangle\langle 0| + \langle\psi_1|\rho|\psi_1\rangle |1\rangle\langle 1|$$

. En revenant à la base initiale, on obtient

$$\langle\psi_0|\rho|\psi_0\rangle |\psi_0\rangle\langle\psi_0| + \langle\psi_1|\rho|\psi_1\rangle |\psi_1\rangle\langle\psi_1|$$

. □