

---

# Introduction au Calcul Quantique

---

Algis David et Bois Léo





# Table des matières

<b>1</b>	<b>Principes fondamentaux du calcul quantique</b>	<b>7</b>
1.1	Bit quantique . . . . .	7
1.1.1	État d'un qubit . . . . .	7
1.1.2	Manipulation d'un qubit . . . . .	9
1.1.3	Mesure d'un qubit . . . . .	11
1.2	Systèmes de plusieurs qubits . . . . .	12
1.2.1	État d'un système de plusieurs qubits . . . . .	12
1.2.2	Manipulation d'un système de plusieurs qubits . . . . .	14
1.2.3	Mesure d'un système de plusieurs qubits . . . . .	15
1.2.4	Base de Bell . . . . .	16
1.3	Algorithmique quantique . . . . .	17
1.3.1	Circuit classique et circuit quantique . . . . .	17
1.3.2	Oracle . . . . .	19
1.3.3	Opérateur $H^{\otimes n}$ . . . . .	21
<b>2</b>	<b>Premiers algorithmes</b>	<b>23</b>
2.1	Superdense Coding . . . . .	23
2.2	Téléportation Quantique . . . . .	26
2.3	Algorithme de Deutsch-Josza . . . . .	27
<b>3</b>	<b>Algorithme d'estimation de la phase quantique</b>	<b>31</b>
3.1	Introduction du problème . . . . .	31
3.2	Transformée de Fourier Quantique . . . . .	33
3.3	Résolution du problème et Estimation d'erreurs . . . . .	36
3.4	Pour récapituler . . . . .	37
<b>4</b>	<b>Logiciels pour la simulation d'algorithmes quantiques</b>	<b>39</b>
4.1	GUI . . . . .	39
4.1.1	Q-kit . . . . .	39

4.1.2	Quirk . . . . .	40
4.1.3	IBM Q Composer . . . . .	41
4.2	Langages de programmation . . . . .	42
4.2.1	Qiskit . . . . .	42
4.2.2	Qasm . . . . .	44
4.3	Bilan . . . . .	44
<b>Conclusion</b>		<b>47</b>
<b>Formulaire</b>		<b>49</b>
<b>Bibliographie</b>		<b>51</b>

# Introduction

Depuis leur invention les ordinateurs ont connu un succès croissant, et sont aujourd’hui omniprésents. Grâce à leur puissance de calcul, ils trouvent leur place dans bien des domaines, allant de la cryptanalyse à la simulation physique. Afin de résoudre des problèmes toujours plus sophistiqués, cette puissance n’a cessé d’augmenter. La célèbre loi de Moore — qui prédit la multiplication par deux tous les deux ans du nombre de transistors dans les microprocesseurs [Moo75] — s’est révélée étonnamment exacte, notamment grâce à la miniaturisation desdits transistors.

Malgré tout, les ordinateurs ont leurs limites. La miniaturisation des transistors se heurte à des difficultés physiques : avec une taille de quelques atomes, le phénomène quantique d’*effet tunnel* devient un obstacle à leur bon fonctionnement. Aussi, il existe certains problèmes qui ne peuvent être résolus efficacement avec un ordinateur. On peut par exemple citer la simulation de molécules complexes, qui doit tenir compte des interactions entre de nombreuses particules, ou encore la simulation de systèmes quantiques. Ce que ces problèmes ont en commun est la croissance exponentielle de leur complexité en fonction de leur taille.

Le calcul quantique est la discipline qui vise à tirer profit des concepts de la mécanique quantique pour effectuer des calculs. Il repose sur l’utilisation habile de certains principes comme celui de superposition quantique, pour proposer des algorithmes qui peuvent se révéler autrement plus efficaces que leurs pendants classiques. En particulier, ce sont des algorithmes qui pourraient résoudre ces problèmes qui donnent tant de fil à retordre aux ordinateurs même les plus modernes. Pour pouvoir être utilisés, ces algorithmes nécessitent des machines – des *ordinateurs quantiques* – capables de manipuler des objets dont le comportement est quantique. Différentes technologies sont développées à cet effet, mais elles ne permettent pas encore un usage de ces algorithmes à grande échelle.

L’objectif de ce document est d’introduire les concepts nécessaires à la compréhension des algorithmes quantiques, de manière à pouvoir les mettre en œuvre dans le cadre d’un cours en master de mathématiques appliquées, mais aussi pour poser les bases nécessaires à l’étude d’algorithmes plus complexes. Le premier chapitre met en place le modèle mathématique des bits quantiques et des différentes interactions possibles avec ces derniers. Le second chapitre propose plusieurs algorithmes simples, qui montrent comment on peut tirer avantage des propriétés quantiques des qubits. Le troisième chapitre est consacré à l’explication d’un algorithme plus complexe, qui utilise une opération largement utilisée dans de nombreux algorithmes. Enfin le dernier chapitre présente quelques outils qui ont été développés pour construire et simuler des algorithmes quantiques sur un ordinateur classique.



# Chapitre 1

## Principes fondamentaux du calcul quantique

Dans ce chapitre, nous introduisons le modèle mathématique utilisé en calcul quantique. Nous commençons par introduire le modèle du bit quantique, puis nous décrivons le fonctionnement des systèmes de plusieurs bits quantiques. Nous énonçons à cet effet des postulats tirés des axiomes de la mécanique quantique, sous une forme adaptée au calcul quantique. Les axiomes en question peuvent être trouvés dans [Pre16] ; la formulation que nous avons retenue provient de [PK07]. Pour finir, nous introduisons la notion de circuit quantique, qui nous permettra de réaliser les algorithmes du chapitre suivant.

### 1.1 Bit quantique

Le bit quantique, ou *qubit*, constitue le support d'information élémentaire d'un ordinateur quantique. Il peut s'agir d'un électron, d'un photon, d'un dispositif supraconducteur, ou autre ; l'essentiel étant que ce soit un objet physique qui puisse être mis dans une superposition quantique de deux états. Nous n'entrons pas dans l'interprétation physique de cette notion<sup>1</sup>, mais nous décrivons dans cette partie le modèle mathématique qui décrit un tel objet et la manière dont nous pouvons interagir avec lui.

#### 1.1.1 État d'un qubit

On appelle système quantique un objet ou un ensemble d'objets dont le comportement n'est pas décrit par les lois de la physique classique, mais par celles de la physique quantique. En particulier, un ou plusieurs qubits constituent un système quantique. Le modèle proposé ici s'applique à des systèmes fermés, c'est-à-dire qui n'interagissent pas avec leur environnement. Il ne tient donc pas compte des interactions qui peuvent avoir lieu dans un système réel entre les qubits et leur environnement, mais il est suffisant pour introduire les principaux concepts du calcul quantique.

C'est à travers le formalisme de l'algèbre linéaire que nous allons décrire un système quantique. Rappelons qu'un espace de Hilbert est un espace vectoriel muni d'un produit scalaire, qui est complet pour la norme associée. Dans la suite, nous ne considérerons que des espaces de Hilbert complexes et de dimension finie. Aussi nous utiliserons les notations de Dirac pour les vecteurs, car ce sont les notations standard dans le domaine du calcul quantique. Ainsi, un vecteur nommé  $\psi$  sera noté  $|\psi\rangle$  (lire « ket psi »). Notre premier postulat est le suivant.

**Postulat 1** (Espace des états). *L'état d'un système quantique peut être décrit par une droite dans un espace de Hilbert.*

Autrement dit, un état peut être décrit par un ensemble de vecteurs qui diffèrent d'un coefficient complexe.

---

1. une approche par l'intermédiaire d'une expérience avec des photons peut être trouvée dans [PK07]

Dans la pratique, nous décrivons l'état d'un système par un représentant de norme 1 de cet ensemble. Un tel représentant est unique à un coefficient  $e^{i\varphi}$  près, où  $\varphi \in \mathbb{R}$  est appelé phase globale.

Dans le cas d'un système réduit à un qubit, l'espace de Hilbert correspondant est un espace de dimension 2. Étant donnée une base orthonormée de cet espace notée  $(|0\rangle, |1\rangle)$  et qu'on désignera dans la suite de base canonique, on peut décrire l'état d'un qubit quelconque par une combinaison linéaire normalisée :

$$a|0\rangle + b|1\rangle \quad , \quad a, b \in \mathbb{C} \text{ tels que } |a|^2 + |b|^2 = 1$$

Dans cette superposition :

- la phase globale n'est pas physiquement significative : on identifie  $a|0\rangle + b|1\rangle$  et  $e^{i\varphi}(a|0\rangle + b|1\rangle)$ .
- la phase relative entre les coefficients  $a$  et  $b$  est physiquement significative : on n'identifie pas  $a|0\rangle + b|1\rangle$  et  $a|0\rangle + e^{i\varphi}b|1\rangle$ .

Dans la pratique, on utilise assez peu les notations matricielles car leur taille augmente exponentiellement avec le nombre de qubits. Nous les donnons tout de même ici, pour que lecteur puisse se familiariser progressivement avec les notations de Dirac. Ainsi, dans la base  $(|0\rangle, |1\rangle)$ , les vecteurs  $|0\rangle$  et  $|1\rangle$  ont pour coordonnées respectives

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

et un qubit dans l'état  $a|0\rangle + b|1\rangle$  a pour coordonnées

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

La sphère de Bloch (prononcer « Bloc ») permet de représenter simplement l'ensemble des états possible d'un qubit. Intuitivement, si  $a$  et  $b$  étaient des coefficients réels, l'ensemble des vecteurs  $a|0\rangle + b|1\rangle$  de norme 1 serait en bijection avec le cercle unité.  $a$  et  $b$  sont complexes, mais seule la phase relative  $\varphi \in ]-\pi; \pi]$  entre ces coefficients est physiquement significative, si bien que l'ensemble des états possibles d'un qubit se trouve en bijection avec la surface de révolution obtenue en faisant tourner le cercle unité, à savoir la sphère unité.

Plus rigoureusement, notons  $a = Ae^{i\varphi_a}$  et  $b = Be^{i\varphi_b}$ , où  $A$  et  $B$  sont des réels positifs, et  $\varphi_a$  et  $\varphi_b$  des coefficients réels dans l'intervalle  $]-\pi; \pi]$ .

- Puisque  $|a|^2 + |b|^2 = 1$  on a  $A^2 + B^2 = 1$ , et comme  $A$  et  $B$  sont positifs, il existe  $\theta \in [0; \frac{\pi}{2}]$  tel que  $A = \cos \theta$  et  $B = \sin \theta$ . Pour des raisons géométriques, prenons plutôt  $\theta \in [0; \pi]$  tel que

$$A = \cos \frac{\theta}{2} \quad \text{et} \quad B = \sin \frac{\theta}{2}$$

- Comme la phase globale n'est pas physiquement significative, on peut multiplier  $a$  et  $b$  par  $e^{-i\varphi_a}$ , et poser

$$\varphi = \varphi_b - \varphi_a$$

Ainsi une superposition quelconque des états  $|0\rangle$  et  $|1\rangle$  peut s'écrire :

$$\cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle \quad , \quad \theta \in [0; \pi], \varphi \in ]-\pi; \pi]$$

Les angles  $\theta$  et  $\varphi$  nous permettent alors d'identifier l'ensemble des états possibles d'un qubit avec l'ensemble des points de la sphère unité, repérée avec les coordonnées sphériques, montrée figure 1.1.

Faisons quelques observations sur cette sphère :

- Les états orthogonaux  $|0\rangle$  et  $|1\rangle$  sont situés aux pôles de la sphère. Plus généralement, on peut montrer que les états orthogonaux sont exactement les états diamétralement opposés.
- Le coefficient  $\theta$  correspond au rapport des amplitudes entre les coefficients  $a$  et  $b$  dans la superposition  $|\psi\rangle = a|0\rangle + b|1\rangle$ . En particulier, si  $\theta = 0$  alors  $|\psi\rangle = |0\rangle$ , si  $\theta = \pi$  alors  $|\psi\rangle = |1\rangle$ , et si  $\theta = \frac{\pi}{2}$ , alors  $|\psi\rangle$  est situé sur l'équateur et  $|a| = |b| = \frac{1}{\sqrt{2}}$ .
- Le coefficient  $\varphi$  correspond à la phase relative entre les coefficients  $a$  et  $b$ . En particulier, si  $\varphi = 0$  alors  $a$  et  $b$  sont « alignés » et peuvent tous deux être considérés réels et positifs, et si  $\varphi = \pi$  alors  $a$  et  $b$  sont opposés.



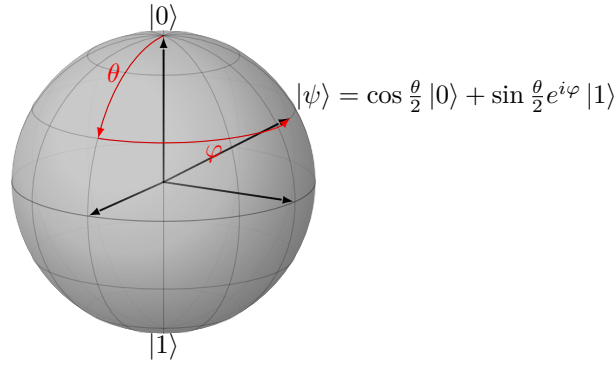


FIGURE 1.1 – Sphère de Bloch

### 1.1.2 Manipulation d'un qubit

Afin d'effectuer des calculs à l'aide d'un système quantique, on doit être en mesure de modifier son état. On utilise à cet effet ce qu'on appelle des portes quantiques, qui sont l'équivalent quantique des portes logiques classiques comme NOT, AND, OR, XOR, etc. L'action de ces portes quantiques satisfait alors le postulat suivant.

**Postulat 2** (Évolution). *L'évolution entre deux instants d'un système quantique isolé est décrit par un opérateur unitaire.*

Ainsi les portes quantiques que nous allons appliquer aux qubits agissent comme des opérateurs unitaires. Dans la suite, nous considérerons donc comme synonymes les termes « porte quantique » et « opérateur unitaire ». Rappelons qu'un opérateur unitaire est un opérateur linéaire  $U$  tel que  $UU^* = U^*U = Id$ , où  $U^*$  désigne l'adjoint de  $U$ . Il est équivalent de dire que  $U$  est un opérateur qui préserve le produit scalaire.

Voyons quelques exemples de portes quantiques qui agissent sur un seul qubit et peuvent être implémentées dans un ordinateur quantique. Un tel opérateur peut être décrit de plusieurs manières. Comme il s'agit d'un opérateur linéaire, on peut se contenter de décrire son action sur une base : son action sur une superposition d'états s'en déduit par linéarité. On peut aussi facilement décrire un tel opérateur par sa matrice, qui n'est dans ce cas qu'une matrice carrée complexe de taille 2. Enfin nous pouvons décrire son action sur la sphère de Bloch qui, comme nous allons le voir, y est tout à fait adaptée.

#### La porte $H$

Une porte incontournable est la porte d'Hadamard, notée  $H$ , qui permet notamment d'introduire une superposition d'états à partir de l'état initial  $|0\rangle$ . Cette porte est définie par

$$H : \begin{cases} |0\rangle & \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \text{ parfois noté } |+\rangle \\ |1\rangle & \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \text{ parfois noté } |-\rangle \end{cases}$$

Dans la base  $(|0\rangle, |1\rangle)$ , sa matrice est la suivante :

$$H : \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Sur la sphère de Bloch, l'action de la porte d'Hadamard se traduit par une rotation d'angle  $\pi$  autour de la première bissectrice de l'axe des  $x$  et de l'axe des  $z$ , montrée figure 1.2.

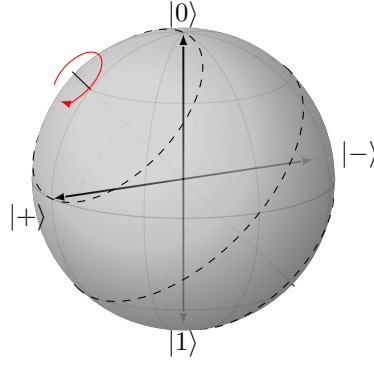
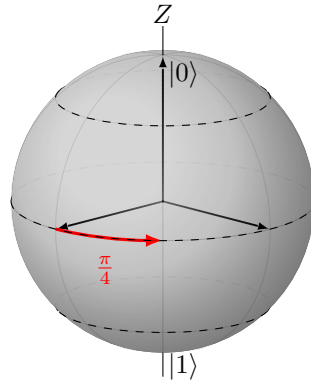


FIGURE 1.2 – Action de la porte d'Hadamard sur la sphère de Bloch

FIGURE 1.3 – Action de la porte  $T$  sur la sphère de Bloch

### La porte $T$

Une autre porte intéressante est la porte  $T$ , qui permet d'introduire une phase à partir d'un état superposé. Dans la base  $(|0\rangle, |1\rangle)$ , sa matrice est la suivante :

$$T : \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

Son action sur les états  $|+\rangle$  et  $|-\rangle$  est donc :

$$T : \begin{cases} |+\rangle & \mapsto \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle) \\ |-\rangle & \mapsto \frac{1}{\sqrt{2}}(|0\rangle - e^{i\frac{\pi}{4}}|1\rangle) \end{cases}$$

Tant qu'on ne considère qu'un système avec un seul qubit,  $T$  agit sur la base canonique comme l'identité. En effet, la phase introduite est, dans ce cas particulier, une phase globale :

$$T : \begin{cases} |0\rangle & \mapsto |0\rangle \\ |1\rangle & \mapsto e^{i\frac{\pi}{4}}|1\rangle \equiv |1\rangle \end{cases}$$

On fera attention au fait que ce n'est plus le cas dès qu'on considère un système de plusieurs qubits.

Sur la sphère de Bloch, l'action de la porte  $T$  se traduit par une rotation d'angle  $\frac{\pi}{4}$  autour de l'axe des  $z$ , montrée figure 1.3.

### Les portes de Pauli

Le fait que les deux portes précédentes agissent sur la sphère de Bloch par des rotations n'est pas un hasard. En fait, on peut montrer que tout opérateur unitaire qui agit sur un qubit se traduit par une

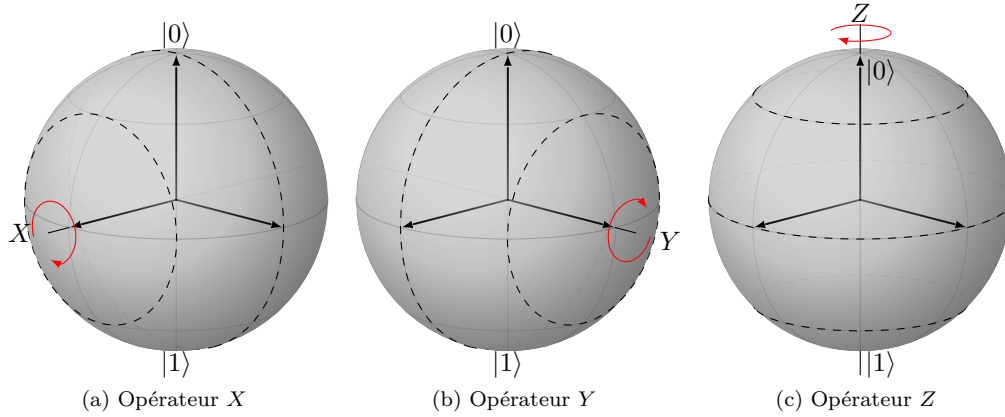


FIGURE 1.4 – Action des portes de Pauli sur la sphère de Bloch

certaine rotation de la sphère<sup>2</sup>. Les portes notées  $X$ ,  $Y$  et  $Z$  correspondent en particulier aux rotations d'angle  $\pi$  et d'axes respectifs l'axe des  $x$ , des  $y$  et des  $z$ . Avec la porte identité  $I$ , ces quatre opérateurs sont appelés « portes de Pauli ». Leurs matrices dans la base canonique sont les suivantes :

$$I : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y : \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad Z : \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

L'opérateur  $X$  est souvent considéré comme l'équivalent quantique de la porte logique « NOT » en informatique classique : il transforme l'état  $|0\rangle$  en l'état  $|1\rangle$ , et l'état  $|1\rangle$  en l'état  $|0\rangle$ .

La démarche permettant d'exprimer tout opérateur unitaire comme une rotation peut par exemple être trouvée dans [PK07]. Ce résultat passe notamment par l'utilisation des portes suivantes.

### Les portes de rotation

Les portes de Pauli permettent de définir les « portes de rotation » suivantes :

$$R_x(\theta) = e^{-i\theta X/2}, \quad R_y(\theta) = e^{-i\theta Y/2}, \quad R_z(\theta) = e^{-i\theta Z/2},$$

Ces portes correspondent aux rotations d'angle  $\theta$  quelconque autour des axes des  $x$ , des  $y$  et des  $z$  respectivement. En particulier<sup>3</sup>,  $X = e^{i\pi/2}R_x(\pi)$ ,  $Y = e^{i\pi/2}R_y(\pi)$  et  $Z = e^{i\pi/2}R_z(\pi)$ .

Dans le chapitre 3, nous utilisons par exemple les portes de rotation autour de l'axe des  $z$  définies par

$$R_k = e^{i\pi/2^k} R_z\left(\frac{2\pi}{2^k}\right), \quad \text{de matrice} \quad R_k : \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^k}} \end{pmatrix}$$

### 1.1.3 Mesure d'un qubit

Il est donc possible de manipuler un qubit à l'aide de portes quantiques. Mais ces manipulations ne sont possibles que si le système est isolé, ce qui en mécanique quantique signifie en particulier qu'il ne faut pas observer l'état du système. Pour tirer une information d'un qubit, il faut effectuer ce qu'on appelle une mesure. Cette mesure est très contraignante car pleine de défauts : non seulement elle modifie le système de manière irréversible — le système n'étant plus isolé, son action n'est pas décrite par un opérateur unitaire —, mais en plus le résultat de cette mesure ne donne qu'une information partielle, et pour finir ce résultat est aléatoire. Plus précisément, une mesure satisfait le postulat suivant.

2. À un coefficient  $e^{i\varphi}$  près, qui a son importance dans un système de plusieurs qubits, mais que l'on peut ignorer lorsqu'on considère un système d'un seul qubit, puisque ce coefficient introduit une phase alors globale.

3. Là encore, le coefficient  $e^{i\pi/2}$  n'a son importance que dans un système de plusieurs qubits ; sur un seul qubit, ce coefficient ne fait qu'introduire une phase globale et peut donc être ignoré.

**Postulat 3** (Mesure - première version). *Étant donnée une base orthonormée  $(|e_i\rangle)_{i \in I}$  d'un espace de Hilbert, il est possible d'effectuer une mesure relativement à cette base qui, pour un système dans l'état*

$$|\psi\rangle = \sum_i a_i |e_i\rangle$$

*va renvoyer le résultat  $i$  avec probabilité  $|a_i|^2$  et laisser alors le système dans l'état  $|e_i\rangle$ .*

Dans un ordinateur quantique, un dispositif permet d'effectuer une telle mesure pour chaque qubit, relativement à la base  $(|0\rangle, |1\rangle)$ .

**Exemple.** *Considérons un qubit dans l'état*

$$\sqrt{\frac{1}{3}} |0\rangle + \sqrt{\frac{2}{3}} i |1\rangle$$

*La mesure relativement à la base  $(|0\rangle, |1\rangle)$  de ce qubit va :*

- *renvoyer 0 et laisser le qubit dans l'état  $|0\rangle$  avec probabilité  $\left|\sqrt{\frac{1}{3}}\right|^2 = \frac{1}{3}$ , ou bien*
- *renvoyer 1 et laisser le qubit dans l'état  $|1\rangle$  avec probabilité  $\left|\sqrt{\frac{2}{3}}i\right|^2 = \frac{2}{3}$*

On observe ici un phénomène qui n'a aucun équivalent dans un ordinateur classique, puisque le résultat obtenu est purement aléatoire ; non pas par défaillance du système, mais par son essence même. Autrement dit, tandis qu'un qubit peut bien être décrit par un vecteur donné, le résultat de la mesure de ce qubit ne peut être décrit que par une variable aléatoire. Par exemple, la mesure d'un qubit dans la superposition  $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$  simule exactement une variable aléatoire qui suit la loi de Bernoulli de paramètre  $\frac{1}{2}$ .

Notons que ce dispositif de mesure permet tout à fait d'effectuer une mesure relativement à une autre base : il suffit pour cela d'effectuer au préalable le changement de base adéquat. Rappelons en effet qu'un changement de base d'une base orthonormée à une autre correspond à l'action d'un opérateur unitaire, qui peut donc être implémenté par une (ou plusieurs) porte quantique. Par exemple, la porte d'Hadamard permet d'effectuer une mesure relativement à la base  $(|+\rangle, |-\rangle)$ .

Même si le phénomène de superposition quantique offre une infinité d'états possibles à un qubit et lui permet donc théoriquement d'encoder une infinité d'informations, un qubit seul ne permet pas d'effectuer des calculs complexes. En effet, nous avons vu que nous ne pouvions le modifier qu'au travers d'opérateurs unitaires, ce qui limite les calculs que l'on peut effectuer avec un qubit. Mais surtout nous avons vu que seule une mesure permet de tirer des renseignements d'un qubit, et le résultat de cette mesure n'a que deux issues possibles. Si les concepts de mécanique quantique peuvent être utilisés à notre avantage, c'est donc à travers des systèmes de plusieurs qubits. De tels systèmes héritent cependant des défauts d'un qubit seul, comme l'aléatoire inhérent à leur mesure. Ce hasard constitue une véritable difficulté lors de la création d'algorithmes, dont un des enjeux est de préparer un état final exploitable.

## 1.2 Systèmes de plusieurs qubits

Nous allons voir dans cette partie comment les postulats de la partie 1.1 s'appliquent aux systèmes de plusieurs qubits, et introduire les nouvelles notions propres à ces systèmes.

### 1.2.1 État d'un système de plusieurs qubits

Dans la partie 1.1.1, nous avons vu que l'état d'un système quantique est modélisé mathématiquement par une droite dans un espace de Hilbert complexe. Ce premier postulat s'applique non seulement à un qubit seul, mais aussi à un système composite de plusieurs qubits. Le postulat suivant décrit cet espace.

**Postulat 4** (Composition de systèmes). *Lorsque deux systèmes quantiques ayant respectivement comme espace d'états  $\mathcal{H}_1$  et  $\mathcal{H}_2$  sont regardés comme un seul système quantique, ce dernier a pour espace d'états l'espace  $\mathcal{H}_1 \otimes \mathcal{H}_2$ . Si le premier système est dans l'état  $|\psi_1\rangle$  et le deuxième dans l'état  $|\psi_2\rangle$ , alors le système composite est dans l'état  $|\psi_1\rangle \otimes |\psi_2\rangle$ .*

Notons que ce postulat permet de construire par récurrence l'espace des états de systèmes de  $n$  qubits, comme produit tensoriel de  $n$  espaces d'états.

Pour bien comprendre ce modèle de système composite, donnons quelques résultats sur les produits tensoriels donnés ci-dessus. Supposons données une base  $(|e_1^{(1)}\rangle, \dots, |e_1^{(n)}\rangle)$  de  $\mathcal{H}_1$  et une base  $(|e_2^{(1)}\rangle, \dots, |e_2^{(m)}\rangle)$  de  $\mathcal{H}_2$ . Alors il existe des coefficients  $a_1^{(1)}, \dots, a_1^{(n)}, a_2^{(1)}, \dots, a_2^{(m)}$  tels que

$$|\psi_1\rangle = \sum_{i=1}^n a_1^{(i)} |e_1^{(i)}\rangle \quad \text{et} \quad |\psi_2\rangle = \sum_{j=1}^m a_2^{(j)} |e_2^{(j)}\rangle$$

Le produit tensoriel de  $|\psi_1\rangle$  et  $|\psi_2\rangle$  s'écrit alors :

$$|\psi_1\rangle \otimes |\psi_2\rangle = \sum_{i,j} a_1^{(i)} a_2^{(j)} |e_1^{(i)}\rangle \otimes |e_2^{(j)}\rangle$$

L'espace produit  $\mathcal{H}_1 \otimes \mathcal{H}_2$  est l'espace de Hilbert engendré par les vecteurs de la forme  $|\psi_1\rangle \otimes |\psi_2\rangle$ . En particulier, la famille  $(|e_1^{(i)}\rangle \otimes |e_2^{(j)}\rangle)_{i,j}$  forme une base de  $\mathcal{H}_1 \otimes \mathcal{H}_2$ . On en déduit notamment que  $\dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = nm = \dim(\mathcal{H}_1) \dim(\mathcal{H}_2)$ .

Matriciellement, dans les bases introduites ci-dessus, le produit tensoriel s'écrit

$$\begin{pmatrix} a_1^{(1)} \\ \vdots \\ a_1^{(n)} \end{pmatrix} \otimes \begin{pmatrix} a_2^{(1)} \\ \vdots \\ a_2^{(m)} \end{pmatrix} = \begin{pmatrix} a_1^{(1)} a_2^{(1)} \\ \vdots \\ a_1^{(1)} a_2^{(m)} \\ \vdots \\ a_1^{(n)} a_2^{(1)} \\ \vdots \\ a_1^{(n)} a_2^{(m)} \end{pmatrix}$$

Pour en revenir au cadre du calcul quantique, l'espace d'états d'un système de deux qubits est donc le produit tensoriel de deux espaces de Hilbert de dimension 2, de bases respectives  $(|0\rangle_1, |1\rangle_1)$  et  $(|0\rangle_2, |1\rangle_2)$ . C'est donc un espace de Hilbert de dimension 4 dont une base est constituée des vecteurs

$$|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2$$

Pour alléger les notations, nous pouvons omettre les indices car ils se déduisent simplement de la position du vecteur dans le produit tensoriel. Nous omettrons également le symbole  $\otimes$  la plupart du temps. Les vecteurs de la base s'écrivent alors :

$$|0\rangle |0\rangle, |0\rangle |1\rangle, |1\rangle |0\rangle, |1\rangle |1\rangle$$

ou encore, comme nous le ferons souvent dans la suite :

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Un système de deux qubits peut donc être décrit par un vecteur de la forme

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad , \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

**Exemple.** Considérons deux qubits exprimés dans la base  $(|0\rangle, |1\rangle)$  par :

$$|\psi_1\rangle = a_1|0\rangle + b_1|1\rangle \quad \text{et} \quad |\psi_2\rangle = a_2|0\rangle + b_2|1\rangle$$

alors le système composé de ces deux qubits est dans l'état

$$\begin{aligned} |\psi\rangle &= (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \\ &= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle \end{aligned}$$

ce qui peut s'écrire matriciellement

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{pmatrix}$$

Mais un vecteur de la forme  $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$  n'est pas forcément le produit tensoriel de deux vecteurs. Par exemple, on vérifie facilement que le vecteur

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

ne peut s'écrire sous la forme  $a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$ . Lorsqu'un système composite est dans un tel état, on dit que les qubits sont intriqués. Il n'est alors pas possible de décrire chaque qubit séparément, par des vecteurs  $|\psi_1\rangle$  et  $|\psi_2\rangle$  dans leurs espaces respectifs  $\mathcal{H}_1$  et  $\mathcal{H}_2$ . Autrement dit, dans un système de plusieurs qubits, parler de l'état d'un qubit en particulier n'a *a priori* pas de sens.

Pour autant, il est toujours possible d'interagir avec les qubits un à un, comme décrit dans les parties 1.1.2 et 1.1.3.

### 1.2.2 Manipulation d'un système de plusieurs qubits

Rappelons que le postulat 2 affirme que l'évolution d'un système isolé est décrite par un opérateur unitaire. Ce postulat s'applique à un système de plusieurs qubits. En particulier, lorsqu'on applique un opérateur  $U_1$  à un premier qubit et un opérateur  $U_2$  à un second qubit, on applique l'opérateur unitaire  $U_1 \otimes U_2$  au système composé des deux qubits. Sur un système dans l'état

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

cet opérateur est défini par :

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1 |\psi_1\rangle) \otimes (U_2 |\psi_2\rangle)$$

Sur un système de qubits intriqués, l'action de cet opérateur se déduit par linéarité. Ainsi, on a en toute généralité :

$$(U_1 \otimes U_2)(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) = a(U_1 \otimes U_2)|00\rangle + b(U_1 \otimes U_2)|01\rangle + c(U_1 \otimes U_2)|10\rangle + d(U_1 \otimes U_2)|11\rangle$$

Aussi, lorsqu'on applique seulement un opérateur  $U$  à un premier qubit, on applique l'opérateur  $U \otimes I$  au système, où  $I$  désigne l'identité.

Mais de la même manière qu'il existe des vecteurs de  $\mathcal{H}_1 \otimes \mathcal{H}_2$  qui ne s'écrivent pas comme produit tensoriel de vecteurs, il existe des opérateurs de  $\mathcal{H}_1 \otimes \mathcal{H}_2$  qui ne s'écrivent pas comme produit tensoriel d'un opérateur de  $\mathcal{H}_1$  avec un opérateur de  $\mathcal{H}_2$ . Contrairement aux opérateurs de la forme  $U_1 \otimes U_2$ , un tel opérateur permet d'intriquer un système de qubits non intriqués.

Un exemple incontournable de tel opérateur est la porte CNOT, définie par :

$$\text{CNOT} \begin{cases} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{cases}$$

ou encore, par linéarité :

$$\text{CNOT}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$$

Cette porte permet par exemple d'obtenir l'état intriqué vu précédemment :

$$\begin{aligned} \text{CNOT} \left( \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes |0\rangle \right) &= \text{CNOT} \left( \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |10\rangle \right) \\ &= \frac{1}{\sqrt{2}} \text{CNOT} |00\rangle + \frac{1}{\sqrt{2}} \text{CNOT} |10\rangle \\ &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \end{aligned}$$

Cet opérateur tire son nom de la porte logique classique définie de la même manière, c'est-à-dire qui applique la porte NOT au deuxième bit lorsque le premier bit vaut 1, et ne fait rien sinon. On dit que le premier bit est un bit de contrôle, d'où le nom *controlled*-NOT. Par analogie, on dit que le premier qubit est un qubit de contrôle pour la porte CNOT quantique, pour signifier que lorsque ce qubit est dans l'état  $|1\rangle$ , la porte  $X$  (NOT) est appliquée au deuxième qubit, et lorsqu'il est dans l'état  $|0\rangle$ , c'est la porte  $I$  (identité) qui est appliquée. Mais le premier qubit pouvant se trouver dans une superposition d'états, ce vocabulaire peut parfois s'avérer trompeur. Par exemple, dans la base  $(|+\rangle, |-\rangle) = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle)$ , on peut vérifier que la porte CNOT agit plutôt sur le premier qubit sous contrôle du deuxième :

$$\text{CNOT} \begin{cases} |++\rangle \mapsto |++\rangle \\ |+-\rangle \mapsto |--\rangle \\ |-+\rangle \mapsto |-+\rangle \\ |--\rangle \mapsto |+-\rangle \end{cases}$$

### 1.2.3 Mesure d'un système de plusieurs qubits

Dans un système de plusieurs qubits comme pour un système d'un seul qubit, la seule manière d'obtenir des informations sur le système est d'effectuer une mesure. Nous avons vu dans la partie 1.1.3 qu'il était possible d'effectuer une mesure de chaque qubit relativement à la base canonique  $(|0\rangle, |1\rangle)$ . Dans un système de plusieurs qubits, la mesure d'un seul qubit correspond à une « mesure partielle » du système. Une telle mesure est décrite par le postulat suivant, qui généralise celui de la première partie.

**Postulat 5** (Mesure). *Soit  $|e_1\rangle, \dots, |e_n\rangle$  est une base orthonormée d'un espace  $\mathcal{H}_1$ , et soit  $|\psi_1\rangle, \dots, |\psi_n\rangle$  une famille de vecteurs normés (pas forcément orthogonaux) d'un espace  $\mathcal{H}_2$ . Alors la mesure relativement à la base  $(|e_i\rangle)_i$  d'un système dans l'état*

$$|\psi\rangle = \sum_i a_i |e_i\rangle |\psi_i\rangle, \quad \text{avec} \quad \sum_i |a_i|^2 = 1$$

*va renvoyer  $i$  avec probabilité  $|a_i|^2$  et laisser alors le système dans l'état  $|e_i\rangle |\psi_i\rangle$ .*

**Exemple.** *Considérons un système de deux qubits dans l'état*

$$|\psi\rangle = \sqrt{\frac{1}{12}} |00\rangle + \sqrt{\frac{1}{6}} |01\rangle + \sqrt{\frac{3}{10}} |10\rangle + \sqrt{\frac{9}{20}} |11\rangle$$

*et illustrons comment se comporte une mesure du premier qubit de ce système, relativement à la base  $(|0\rangle, |1\rangle)$ . Pour ce faire, on factorise l'expression ci-dessus pour obtenir :*

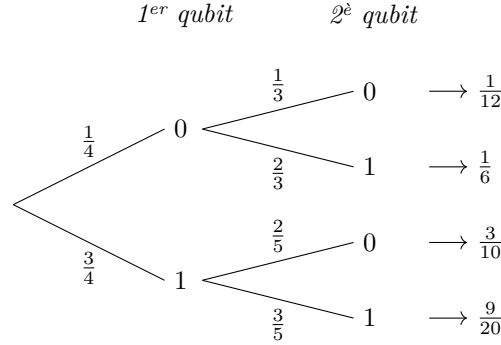
$$|\psi\rangle = |0\rangle \left( \sqrt{\frac{1}{12}} |0\rangle + \sqrt{\frac{1}{6}} |1\rangle \right) + |1\rangle \left( \sqrt{\frac{3}{10}} |0\rangle + \sqrt{\frac{9}{20}} |1\rangle \right)$$

*puis, après normalisation :*

$$|\psi\rangle = \sqrt{\frac{1}{4}} |0\rangle \left( \sqrt{\frac{1}{3}} |0\rangle + \sqrt{\frac{2}{3}} |1\rangle \right) + \sqrt{\frac{3}{4}} |1\rangle \left( \sqrt{\frac{2}{5}} |0\rangle + \sqrt{\frac{3}{5}} |1\rangle \right)$$

*On a ainsi exprimé l'état du système sous la forme donnée dans le postulat. Il en découle que la mesure du premier qubit relativement à la base  $|0\rangle, |1\rangle$  va*

— renvoyer 0 et laisser le système dans l'état  $|0\rangle \left( \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right)$  avec probabilité  $\frac{1}{4}$ , ou bien  
 — renvoyer 1 et laisser le système dans l'état  $|1\rangle \left( \sqrt{\frac{2}{5}}|0\rangle + \sqrt{\frac{3}{5}}|1\rangle \right)$  avec probabilité  $\frac{3}{4}$   
 Si on effectue ensuite la mesure du deuxième qubit, on obtient alors l'arbre de probabilités suivant :



On remarque notamment que la mesure successive des qubits relativement à la base  $(|0\rangle, |1\rangle)$  aboutit exactement à une mesure du système complet relativement à la base  $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ , comme décrit par le postulat 3.

Ainsi, le postulat 5 nous permet de décrire le résultat de la mesure d'un seul qubit à l'aide d'une variable aléatoire. Notons  $X_1$  et  $X_2$  les variables aléatoires associées à chacun des qubits d'un système de deux qubits. Dans l'exemple ci-dessus,  $X_1$  et  $X_2$  ne sont pas indépendantes, puisque la loi de  $X_2$  conditionnée par l'évènement  $\{X_1 = 0\}$  n'est pas la même que celle de  $X_2$  conditionnée par l'évènement  $\{X_1 = 1\}$ . Dans le cas de qubits non intriqués, et seulement dans ce cas, les variables aléatoires  $X_1$  et  $X_2$  sont indépendantes. En effet, l'état du système peut alors s'écrire  $(a|0\rangle + b|1\rangle)|\psi\rangle = a|0\rangle|\psi\rangle + b|1\rangle|\psi\rangle$ , si bien que la mesure du premier qubit va laisser le système ou bien dans l'état  $|0\rangle|\psi\rangle$ , ou bien dans l'état  $|1\rangle|\psi\rangle$ ; dans tous les cas, le deuxième qubit reste dans l'état  $|\psi\rangle$  et le résultat  $X_2$  de sa mesure ne dépend donc aucunement de  $X_1$ .

Autrement dit, on peut voir les systèmes intriqués comme les systèmes dont la mesure d'un qubit a une influence sur le résultat de la mesure des autres qubits. Des qubits intriqués pouvant théoriquement être séparés par une distance arbitrairement grande, notons qu'on entrevoit ici un concept pour le moins contre-intuitif.

#### 1.2.4 Base de Bell

Nous terminons cette partie par l'introduction d'une base d'états incontournable des systèmes de deux qubits. Il s'agit de la base de Bell, constituée des états suivants :

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

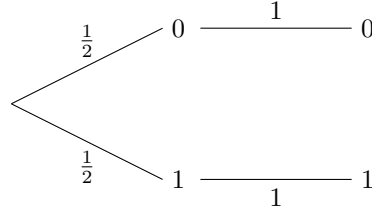
et dont on vérifie aisément qu'elle est orthonormée. On peut retrouver cette définition dans [PK07].

Une grande différence de cette base avec la base canonique est qu'elle est constituée d'états intriqués, et même « d'intrication maximale » : contrairement à des qubits non intriqués pour lesquels la mesure du premier qubit n'a aucune influence sur la mesure du deuxième, ici le résultat de la première mesure



détermine entièrement le résultat de la deuxième mesure. En effet, la mesure d'un seul des deux qubits laisse toujours le système dans l'un des états  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  ou  $|11\rangle$ , si bien que le résultat de la mesure de l'autre qubit est alors complètement déterministe.

Par exemple, les mesures successives des qubits d'un système dans l'état  $|\beta_{00}\rangle$  aboutit à l'arbre de probabilités suivant :



Si nous reprenons les notations introduites dans la partie précédente et désignons par  $X_1$  et  $X_2$  les variables aléatoires associées aux deux qubits, alors  $X_1$  et  $X_2$  suivent toutes les deux la loi de Bernoulli de paramètre  $\frac{1}{2}$ , mais elles sont loin d'être indépendantes puisque, d'après l'arbre ci-dessus, elles sont liées par la relation  $X_1 = X_2$ .

Par ailleurs, les portes quantiques vues précédemment (sections 1.1.2 et 1.2.2) permettent simplement d'obtenir ces états à partir de l'état initial  $|00\rangle$ . Par exemple, pour obtenir  $|\beta_{00}\rangle$ , il suffit d'appliquer la porte  $H$  au premier qubit, puis la porte CNOT avec le premier qubit comme bit de contrôle :

$$|0\rangle \otimes |0\rangle \xrightarrow{H \otimes I} \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes |0\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

Une manière d'obtenir les autres états de cette base est présentée dans la section 2.1.

## 1.3 Algorithmique quantique

Dans cette partie nous précisons notre modèle de circuit quantique, qui nous permettra de représenter les algorithmes décrits dans le chapitre suivant, et nous présentons quelques opérations utiles.

### 1.3.1 Circuit classique et circuit quantique

Commençons par décrire le modèle du circuit classique. Nous nous appuyons pour ce faire sur le chapitre 5 de [Pre16], où figure une description plus détaillée. Un circuit classique comporte un certain nombre  $n$  de bits en entrée, et un certain nombre  $m$  de bits en sortie. À une valeur donnée de chacun des  $n$  bits en entrée, il associe de manière déterministe une valeur à chacun des  $m$  bits en sortie. Autrement dit, un circuit classique implémente l'évaluation d'une fonction  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ . Puisqu'une telle fonction est équivalente à  $m$  fonctions ayant  $n$  bits en entrée et un seul bit en sortie, on peut considérer que la tâche élémentaire d'un circuit classique est l'évaluation d'une fonction

$$f : \{0, 1\}^n \rightarrow \{0, 1\}$$

Une telle fonction peut se décomposer en opérations très simples sur un ou deux bits<sup>4</sup>, appelées portes logiques ; si bien qu'un nombre très réduit d'opérations différentes est nécessaire pour implémenter un circuit (classique) quelconque. Par exemple, les portes logiques NOT, OR et AND permettent à elle seules d'implémenter n'importe quel circuit classique. Autrement dit, un ordinateur classique est potentiellement capable d'effectuer n'importe quel calcul dès lors qu'il peut effectuer ces trois seules opérations. On dit pour cette raison que les portes NOT, OR et AND sont universelles.

Passons au modèle du circuit quantique. Un circuit quantique comporte un certain nombre  $n$  de qubits, aussi bien en entrée qu'en sortie, dont on note  $\mathcal{H}$  l'espace des états. Comme nous l'avons vu dans la

---

4. voir [Pre16] pour plus de détails

section 1.2.1, il s'agit d'un espace de Hilbert complexe de dimension  $2^n$ . Par convention, les  $n$  qubits sont initialement dans l'état  $|0 \cdots 0\rangle$ . Le circuit se compose ensuite de portes quantiques, dont nous avons vu dans les sections 1.1.2 et 1.2.2 qu'il s'agit d'opérateurs unitaires. Ainsi, ces portes quantiques implémentent ensemble un opérateur unitaire

$$U : \mathcal{H} \rightarrow \mathcal{H}$$

Enfin, le circuit quantique se termine par une mesure de chacun des qubits, dont le résultat est *a priori* aléatoire, comme nous l'avons vu dans les sections 1.1.3 et 1.2.3.

On représente un circuit quantique à l'aide d'un diagramme comme celui montré figure 1.5. À chaque qubit correspond une ligne horizontale, sur laquelle sont placées les portes logiques appliquées à ce qubit. On retrouve tout à gauche du circuit l'état initial  $|0 \cdots 0\rangle$ , et tout à droite la mesure de chaque qubit. Notons la représentation un peu particulière de la porte CNOT, qui est la deuxième porte appliquée au système dans notre exemple. Cette représentation vient de son interprétation classique : le point sur la ligne du haut relié par un segment vertical à la ligne du bas signifie que le premier qubit (en haut) agit comme qubit de contrôle pour l'opération sur le deuxième qubit (en bas), au sens vu dans la section 1.2.2.

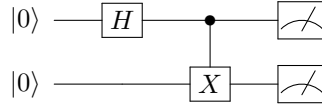


FIGURE 1.5 – Exemple de représentation d'un circuit quantique à deux qubits. Le système est d'abord dans l'état  $|00\rangle$ . La porte  $H$  est appliquée au premier qubit, puis la porte CNOT avec le premier qubit en contrôle. Le système est alors dans l'état  $|\beta_{00}\rangle$ , et les mesures finales vont renvoyer aléatoirement 00 ou 11.

Comme expliqué dans [Pre16], la convention de choisir comme état initial l'état  $|0 \cdots 0\rangle$  vient du fait qu'il n'est pas trivial de mettre un système quantique dans une superposition arbitraire d'états. Cette convention empêche donc de masquer une partie de la complexité d'un algorithme en partant d'un état initial qui nécessiterait de nombreux calculs.

On peut se demander si, comme pour les ordinateurs classiques, disposer d'un petit nombre de portes quantiques différentes est suffisant pour effectuer tous les calculs possibles. Si on souhaite pouvoir implémenter tous les opérateurs unitaires  $U : \mathcal{H} \rightarrow \mathcal{H}$  de manière exacte, la réponse est non : l'ensemble de ces opérateurs est un ensemble non dénombrable, qui ne saurait être recouvert par l'ensemble des circuits possibles avec un nombre fini de portes différentes. Cependant, on peut en réalité se contenter d'approcher n'importe quel opérateur avec une erreur arbitrairement petite, et il s'avère qu'un nombre très réduit d'opérations différentes est requis pour cette tâche. Par exemple, les portes quantiques  $H$ ,  $T$  et CNOT en sont capables ; on dit pour cette raison que ce sont des portes quantiques universelles. Dans ce document, nous n'aurons pas recours à de telles approximations et supposons que les portes utilisées implémentent de manière exacte l'opérateur considéré. Ceci étant dit, le lecteur intéressé pourra consulter [PK07] pour plus de détails et de références à ce sujet.

Une propriété intéressante des circuits quantiques est leur réversibilité. En effet, avant les mesures finales, un circuit quantique implémente un opérateur unitaire  $U$ , qui est par définition une fonction inversible. Ainsi, tout circuit quantique possède un « inverse » qui implémente l'opérateur  $U^{-1}$ . Ceci s'avère très utile en pratique. Par exemple, si un circuit effectue un changement de base d'une base  $\mathcal{B}_1$  vers une base  $\mathcal{B}_2$ , son inverse effectue le changement de base de  $\mathcal{B}_2$  vers  $\mathcal{B}_1$  ; mieux encore, si un circuit permet d'encoder une information, son inverse permet de la décoder. Nous aurons l'occasion d'illustrer cela dans les chapitres suivants.

Qui plus est, ce circuit inverse s'obtient très facilement. Comme le produit (au sens de la composition) d'opérateurs  $U_1$  et  $U_2$  a pour inverse  $(U_1 U_2)^{-1} = U_2^{-1} U_1^{-1}$ , il suffit de remplacer chaque porte par son inverse, et de renverser leur ordre. Un exemple est donné figure 1.6.

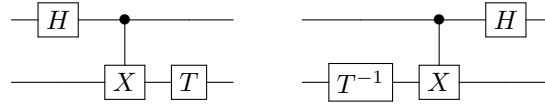


FIGURE 1.6 – Un circuit et son inverse. Le circuit initial est exécuté « à l'envers », en remplaçant chaque porte par son inverse. Noter que les portes  $H$  et CNOT sont leur propre inverse.

### 1.3.2 Oracle

Nous avons vu qu'un circuit classique implémente une fonction  $f : \{0,1\}^n \rightarrow \{0,1\}$ . Une telle fonction encode la solution d'un *problème de décision* : selon son argument, elle renvoie « oui » ou « non ». Par exemple, un tel circuit peut vérifier si oui ou non un nombre est premier. De nombreux problèmes peuvent se mettre sous cette forme, et il peut donc être utile de disposer d'un circuit quantique qui implémente une telle fonction. Par ailleurs, certains problèmes ont pour donnée un tel circuit, et cherche à déterminer des propriétés de la fonction  $f$  associée. Pour pouvoir comparer l'algorithme quantique à l'algorithme classique sur ce type de problème, il est donc important d'avoir un équivalent quantique de ce circuit. Dans ce contexte, un tel circuit est traité comme une « boîte noire », ou un « oracle ». Comme c'est dans ce contexte que nous utiliserons un tel circuit, nous le désignerons par le terme d'« oracle ». Dans cette partie, nous introduisons conceptuellement cet opérateur ; nous n'essayons pas de le construire à partir de portes quantiques élémentaires, puisque nous considérerons qu'il s'agit d'une donnée du problème.

Un circuit quantique étant réversible, il faut transformer  $f$  de manière à la rendre inversible. Ceci peut s'obtenir en posant

$$\tilde{f} : \begin{cases} \{0,1\}^n \times \{0,1\} & \longrightarrow & \{0,1\}^n \times \{0,1\} \\ (x, y) & \longmapsto & (x, y \oplus f(x)) \end{cases}$$

où  $\oplus$  désigne l'addition modulo 2. Cette fonction prend  $n + 1$  bits en entrée, et se contente de modifier le dernier bit si, et seulement si, l'image par  $f$  des  $n$  premiers bits est 1. On vérifie facilement que cette fonction est son propre inverse. On peut définir son équivalent quantique  $U_f$ , qui agit sur la base canonique de la manière suivante : si  $x \in \{0,1\}^n$  et  $y \in \{0,1\}$ ,

$$U_f : |x\rangle |y\rangle \longmapsto |x\rangle |y \oplus f(x)\rangle$$

Comme d'habitude, son action sur une superposition quelconque d'états se déduit par linéarité. Cet opérateur est bien un opérateur unitaire, puisqu'il se contente de permuter certains vecteurs de la base canonique.

**Exemple.** *Considérons la fonction*

$$f : \begin{cases} \{0,1\}^2 & \longrightarrow & \{0,1\} \\ (x_1, x_2) & \longmapsto & x_1 x_2 \end{cases}$$

Cette fonction n'est autre que la fonction implémentée par la porte classique AND : elle renvoie 1 si ses deux arguments sont égaux à 1, et renvoie 0 sinon. Sa version inversible prend trois arguments et sa table de valeurs est la suivante :

$(x_1, x_2, y)$	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 0)	(1, 1, 1)
$\tilde{f}(x_1, x_2, y)$	(0, 0, 0)	(0, 0, 1)	(0, 1, 0)	(0, 1, 1)	(1, 0, 0)	(1, 0, 1)	(1, 1, 1)	(1, 1, 0)

Par conséquent, l'opérateur équivalent  $U_f$  permute les deux derniers vecteurs de la base canonique :

$ x_1 x_2 y\rangle$	$ 000\rangle$	$ 001\rangle$	$ 010\rangle$	$ 011\rangle$	$ 100\rangle$	$ 101\rangle$	$ 110\rangle$	$ 111\rangle$
$U_f  x_1 x_2 y\rangle$	$ 000\rangle$	$ 001\rangle$	$ 010\rangle$	$ 011\rangle$	$ 100\rangle$	$ 101\rangle$	$ 111\rangle$	$ 110\rangle$

Allons plus loin et voyons comment nous pouvons utiliser un tel opérateur. L'utilisation classique serait de l'appliquer à un système mis préalablement dans l'état  $|x\rangle |0\rangle$ . La mesure du dernier qubit donne

alors — exactement comme pour un circuit classique — la valeur de  $f(x)$ . On peut aussi utiliser à notre avantage le principe de superposition. En mettant au préalable les  $n$  premiers qubits dans une superposition uniforme de tous les vecteurs de la base canonique, on peut calculer « en parallèle » l'image par  $f$  de tous les  $x \in \{0,1\}^n$ , avec une seule utilisation de la porte  $U_f$  :

$$\begin{aligned} U_f \left( \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle \right) &= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} U_f |x\rangle |0\rangle \\ &= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \end{aligned}$$

Ainsi, la fonction  $f$  est d'une certaine manière encodée dans le dernier qubit du système.

**Exemple.** Avec l'opérateur  $U_f$  introduit dans l'exemple précédent :

$$\begin{aligned} &\frac{1}{2} (|000\rangle + |010\rangle + |100\rangle + |110\rangle) \\ &\quad \downarrow U_f \\ &\frac{1}{2} (|000\rangle + |010\rangle + |100\rangle + |111\rangle) \end{aligned}$$

Le résultat peut se lire comme suit : l'image par  $f$  de  $(0,0)$  est 0, celle de  $(0,1)$  est 0, celle de  $(1,0)$  est 0, et celle  $(1,1)$  est 1.

Mais afin d'exploiter la fonction  $f$ , nous verrons qu'il est plus utile de l'encoder dans les phases des coefficients de cette superposition. C'est un principe qu'on retrouve dans plusieurs algorithmes, et dont nous discutons plus largement dans le chapitre 3. Ici, nous souhaitons avoir un opérateur qui agit comme suit :

$$\begin{aligned} \tilde{U}_f |x\rangle &= \begin{cases} |x\rangle & \text{si } f(x) = 0 \\ -|x\rangle & \text{si } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)} |x\rangle \end{aligned}$$

**Exemple.** Avec la fonction  $f$  introduite dans l'exemple ci-dessus, nous souhaitons avoir :

$$\begin{aligned} &|00\rangle + |01\rangle + |10\rangle + |11\rangle \\ &\quad \downarrow \tilde{U}_f \\ &|00\rangle + |01\rangle + |10\rangle - |11\rangle \end{aligned}$$

Autrement dit, nous voulons introduire une phase de  $\pi$  (puisque  $-1 = e^{i\pi}$ ) dans les coefficients des vecteurs  $|x\rangle$  tels que  $f(x) = 1$ . Et c'est justement ce que nous obtenons lorsque nous appliquons  $U_f$  non pas à  $|x\rangle |0\rangle$ , mais  $|x\rangle |-\rangle$ , où  $|-\rangle$  désigne la superposition  $\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$  : si  $f(x) = 0$ , alors

$$\begin{aligned} U_f |x\rangle |-\rangle &= \frac{1}{\sqrt{2}} U_f |x\rangle |0\rangle - \frac{1}{\sqrt{2}} U_f |x\rangle |1\rangle \\ &= \frac{1}{\sqrt{2}} |x\rangle |0\rangle - \frac{1}{\sqrt{2}} |x\rangle |1\rangle \\ &= |x\rangle |-\rangle \end{aligned}$$

tandis que si  $f(x) = 1$ , alors

$$\begin{aligned} U_f |x\rangle |-\rangle &= \frac{1}{\sqrt{2}} U_f |x\rangle |0\rangle - \frac{1}{\sqrt{2}} U_f |x\rangle |1\rangle \\ &= \frac{1}{\sqrt{2}} |x\rangle |1\rangle - \frac{1}{\sqrt{2}} |x\rangle |0\rangle \\ &= -|x\rangle |-\rangle \end{aligned}$$

Dans tous les cas, on a bien  $U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$ . On peut alors ignorer le dernier qubit qui sera de toute manière dans l'état  $|-\rangle$ , et obtenir exactement un opérateur qui encode  $f$  dans les phases d'une superposition uniforme. C'est souvent de cette manière qu'est utilisé l'opérateur  $U_f$ , si bien qu'on peut parfois (mais rarement) trouver dans la littérature un oracle défini simplement par  $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$

### 1.3.3 Opérateur $H^{\otimes n}$

Dans la section précédente, nous avons vu que le principe de superposition peut permettre d'effectuer de nombreux calculs en parallèle en appliquant un opérateur à des qubits dans une superposition uniforme d'états, mais nous n'avons pas dit comment obtenir une telle superposition à partir de l'état initial  $|0 \cdots 0\rangle$ . Il s'avère que c'est très simple : il suffit d'appliquer la porte  $H$  à chaque qubit, c'est-à-dire d'appliquer l'opérateur  $H \otimes \cdots \otimes H = H^{\otimes n}$  à l'ensemble du système. Puisqu'il s'agit d'un opérateur courant, détaillons son action sur un état quelconque.

Rappelons que la porte  $H$  agit sur un seul qubit de la manière suivante :

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ H|1\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

ce que l'on peut aussi noter, pour  $x_1 \in \{0, 1\}$  :

$$H|x_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1} \frac{1}{\sqrt{2}}|1\rangle$$

Ainsi, pour  $x = (x_1, \dots, x_n) \in \{0, 1\}^n$ , on a :

$$\begin{aligned} H^{\otimes n}|x\rangle &= (H|x_1\rangle) \otimes \cdots \otimes (H|x_n\rangle) \\ &= \left( \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1} \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \cdots \otimes \left( \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_n} \frac{1}{\sqrt{2}}|1\rangle \right) \end{aligned}$$

Notons comme suit la décomposition de ce produit dans la base canonique :

$$\sum_{y \in \{0,1\}^n} a_y |y\rangle$$

Soit  $y = (y_1, \dots, y_n) \in \{0, 1\}^n$ . Déterminons le coefficient  $a_y$  du vecteur  $|y\rangle = |y_1 \cdots y_n\rangle$ . Pour obtenir ce vecteur à partir du produit ci-dessus, il faut prendre le terme en  $|y_1\rangle$  dans la première parenthèse, le terme en  $|y_2\rangle$  dans la deuxième, etc. jusqu'au terme en  $|y_n\rangle$  dans la dernière parenthèse. Si  $y_i = 0$ , le terme  $|y_i\rangle = |0\rangle$  de la  $i$ -ème parenthèse vient avec le coefficient  $\frac{1}{\sqrt{2}}$ . Si  $y_i = 1$ , le terme  $|y_i\rangle = |1\rangle$  de la  $i$ -ème parenthèse vient avec le coefficient  $(-1)^{x_i} \frac{1}{\sqrt{2}}$ . Dans tous les cas, on remarque que ce coefficient peut s'écrire  $(-1)^{x_i y_i} \frac{1}{\sqrt{2}}$ . Ainsi,

$$\begin{aligned} a_y &= (-1)^{x_1 y_1} \frac{1}{\sqrt{2}} \times \cdots \times (-1)^{x_n y_n} \frac{1}{\sqrt{2}} \\ &= \frac{1}{2^{n/2}} (-1)^{x_1 y_1 + \cdots + x_n y_n} \\ &= \frac{1}{2^{n/2}} (-1)^{x_1 y_1 \oplus \cdots \oplus x_n y_n} \end{aligned}$$

En notant  $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$ , on obtient donc  $a_y = \frac{1}{2^{n/2}} (-1)^{x \cdot y}$ , et finalement :

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

En particulier, puisque  $(-1)^{0 \cdot y} = 1$  pour tout  $y \in \{0, 1\}^n$ , on a :

$$H^{\otimes n}|0 \cdots 0\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} |y\rangle$$

Nous avons ainsi exprimé l'action de l'opérateur  $H^{\otimes n}$  sur les vecteurs de la base canonique. Comme toujours, son action sur une superposition quelconque se déduit par linéarité.



## Chapitre 2

# Premiers algorithmes

Dans ce chapitre, nous allons étudier trois algorithmes basiques de calcul quantique.

Dans les deux prochaines sections, nous débuterons par deux algorithmes de communication quantique. Tous deux ont de larges applications dans la communication quantique, mais nous les décrivons ici pour leur intérêt pédagogique. En effet, ce sont deux algorithmes qui illustrent de manière simple l'utilisation de l'intrication et de la superposition.

Enfin nous terminerons ce chapitre sur l'algorithme de Deutsch-Josza dans la dernière section.

Le lecteur qui souhaitera avoir un condensé des informations du premier chapitre pourra se référer au formulaire à la fin du document.

### 2.1 Superdense Coding

Le superdense coding est un algorithme de communication quantique, qui vise à échanger des données classiques (des bits), en utilisant uniquement des qubits. Il a été imaginé par deux chercheurs Charles H. Bennett et Stephen J. Wiesner dans leur article [CHB92].

Considérons deux personnes, nommées Alice et Bob. Alice souhaite envoyer deux bits classiques à Bob, mais ils n'ont en leur possession que deux qubits. Pour résoudre leur problème nous allons procéder en 3 étapes :

1. Le système va être *préparé*, puis distribué entre Bob et Alice ;
2. Alice va *encoder* l'information qu'elle souhaite envoyer à Bob dans le système, puis lui envoyer ;
3. Bob va *décoder* l'information que lui a transmise Alice.

Détaillons chacune de ces étapes.

#### Préparation

On dispose de deux qubits dans l'état  $|00\rangle$ , qu'on souhaite mettre dans l'état intriqué  $|\beta_{00}\rangle$ . Pour ce faire, on procède comme expliqué dans la section 1.2.4 . On commence par appliquer la porte d'Hadamard  $H$  sur le premier qubit, puis on applique la porte CNOT sur le deuxième qubit avec le premier qubit en contrôle.

On obtient ainsi deux qubits intriqués dans l'état de Bell

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

On en donne un à Alice et un à Bob.

Cette préparation est illustrée figure 2.1.

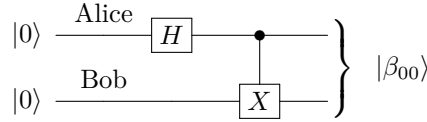


FIGURE 2.1 – Préparation pour le superdense coding

**Remarque.** Algébriquement, ce circuit effectue un changement de base : de la base canonique à la base de Bell.

### Encodage

Pour transmettre l'information qu'elle souhaite, Alice va d'abord appliquer des portes de Pauli à son qubit selon la table suivante, avant de l'envoyer à Bob.

Couple de bits à envoyer	Porte quantique à appliquer	Résultat dans la base de Bell
(0,0)	$I$	$ \beta_{00}\rangle = \frac{1}{\sqrt{2}}( 00\rangle +  11\rangle)$
(0,1)	$X$	$ \beta_{01}\rangle = \frac{1}{\sqrt{2}}( 10\rangle +  01\rangle)$
(1,0)	$Z$	$ \beta_{10}\rangle = \frac{1}{\sqrt{2}}( 00\rangle -  11\rangle)$
(1,1)	$Z \circ X$	$ \beta_{11}\rangle = \frac{1}{\sqrt{2}}(- 10\rangle +  01\rangle)$

### Décodage

Bob a donc reçu le qubit modifié d'Alice, cependant s'il fait une mesure sur les deux qubits maintenant il y aura deux résultats possibles avec une probabilité  $\frac{1}{2}$  d'apparaître chacun. On est encore loin du résultat escompté.

Les qubits sont dans la base de Bell, Bob souhaite donc faire un changement de base de la base Bell à la base canonique. Afin de retrouver ce que Alice voulait lui envoyer. De plus pour que notre problème soit résolu efficacement, il faut qu'une fois mesuré le système ne puisse qu'être projeté dans un unique espace, celui qu'Alice souhaite transmettre à Bob.

Pour arriver à un tel état, Bob va appliquer deux portes quantiques à ses qubits. D'abord la porte CNOT à son qubit, avec le qubit d'Alice comme qubit de contrôle. Et ainsi on met le qubit de Bob en facteur. Enfin on applique la porte d'Hadamard au qubit d'Alice ce qui permet à Bob de découvrir les bits envoyés par Alice.

**Remarque.** On remarque que Bob a procédé à l'inverse des opérations faites dans l'étape préparation.

Ici on a illustré un principe plus général que l'on retrouvera tout au long de ce chapitre et du suivant. En effet si on récapitule :

- On a d'abord procédé à un changement de base, de la base canonique à la base de Bell.
- Une fois dans la nouvelle base, on a appliqué des portes quantiques spécifiques au problème que l'on souhaite traiter. Par exemple, ici si on veut envoyer 10, on a appliqué la porte  $Z$ .
- Enfin on retourne dans la base canonique, en procédant au changement de base inverse de l'étape 1.

On a un processus quasi symétrique que l'on distingue mieux sur la figure 2.2!

**Exemple.** Faisons un exemple Alice souhaite envoyer 11 à Bob.<sup>1</sup> Supposons que les 2 qubits intriqués sont déjà répartis entre Alice et Bob.

Afin de distinguer le qubit de Bob et celui d'Alice, on a indexé les kets de la base d'Alice (resp. Bob) par un "A" (resp. "B").

1. voir figure 2.2



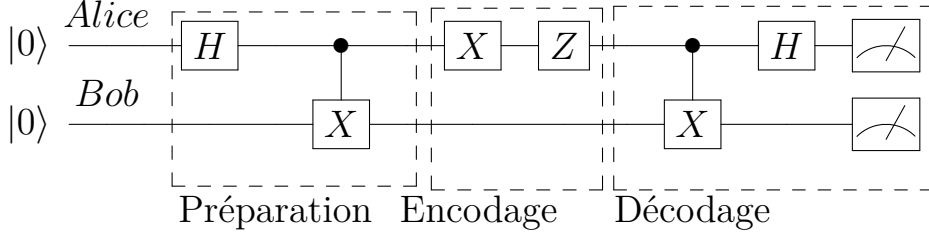


FIGURE 2.2 – Exemple circuit superdense coding

Le système est dans l'état :

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle).$$

Alice va donc appliquer la porte  $Z \circ X$  à son qubit<sup>2</sup> :

$$\begin{aligned} ((Z \circ X) \circ I) |\beta_{00}\rangle &= ((Z \circ X) \circ I) \left( \frac{1}{\sqrt{2}} (|0_A 0_B\rangle + |1_A 1_B\rangle) \right) \\ &= \frac{1}{\sqrt{2}} (((Z \circ X)(|0_A\rangle) \otimes |0_B\rangle + (Z \circ X)(|1_A\rangle) \otimes |1_B\rangle)) \\ &= \frac{1}{\sqrt{2}} (Z(|1_A\rangle) \otimes |0_B\rangle + Z(|0_A\rangle) \otimes |1_B\rangle) \\ ((Z \circ X) \circ I) |\beta_{00}\rangle &= \frac{1}{\sqrt{2}} (-|1_A 0_B\rangle + |0_A 1_B\rangle) \end{aligned}$$

De ce fait les qubits intriqués dans la base de Bell correspondent exactement à la forme :

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(-|1_A 0_B\rangle + |0_A 1_B\rangle)$$

Alice a envoyé son qubit à Bob il va donc appliquer les portes quantiques :

— D'abord CNOT sur le qubit B avec le qubit A comme qubit de contrôle.

$$\begin{aligned} CNOT |\beta_{11}\rangle &= CNOT \left( \frac{1}{\sqrt{2}} (-|1_A 0_B\rangle + |0_A 1_B\rangle) \right) \\ &= \frac{1}{\sqrt{2}} (-|1_A 1_B\rangle + |0_A 1_B\rangle) \\ CNOT |\beta_{11}\rangle &= \frac{1}{\sqrt{2}} ((-|1_A\rangle + |0_A\rangle) \otimes |1_B\rangle) \end{aligned}$$

On remarque la porte CNOT permet de mettre en facteur le qubit de Bob.

— Ensuite Hadamard sur le qubit de Alice On a :

$$\begin{aligned} \frac{1}{\sqrt{2}} (H(-|1_A\rangle + |0_A\rangle) \otimes |1_B\rangle) &= \frac{1}{\sqrt{2}} (H(|1_A\rangle) + H(|0_A\rangle)) \otimes |1_B\rangle \\ &= \frac{1}{\sqrt{2}} \left( \frac{1}{\sqrt{2}} (-|0_A\rangle + |1_A\rangle + |0_A\rangle + |1_A\rangle) \otimes |1_B\rangle \right) \\ &= \frac{1}{2} ((|1_A\rangle + |1_A\rangle) \otimes |1_B\rangle) \\ \frac{1}{\sqrt{2}} (H(-|1_A\rangle + |0_A\rangle) \otimes |1_B\rangle) &= |1_A 1_B\rangle \end{aligned}$$

Ainsi, après mesure, Bob obtient dans tout les cas l'information qu'Alice voulait lui transmettre, c'est à dire le couple 1,1.

2. c'est à dire elle va appliquer  $(Z \circ X) \otimes I$  à  $|\beta_{00}\rangle$

## 2.2 Téléportation Quantique

**Question.** *Comment échanger l'état d'un qubit par le biais d'un canal de communication classique ?*

Tout d'abord précisons que par canal de communication classique, on entend un transfert physique de bits.

De même que précédemment, prenons le cas d'Alice et Bob. Alice souhaite échanger l'état d'un qubit à Bob, mais ils n'ont en leur possession que deux qubits intriqués, en plus du qubit dont Alice souhaite échanger l'état avec Bob.

On a donc un premier qubit

$$|\psi\rangle = a|0\rangle + \beta|1\rangle \text{ avec } |a|^2 + |\beta|^2 = 1$$

et deux autres qubits à l'état  $|0\rangle$ .

Comme pour le superdense coding dans la phase de préparation<sup>3</sup> on va mettre nos deux qubits dans la base de Bell.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle).$$

De ce fait le système est dans un état

$$|\Psi\rangle = |\psi\rangle \otimes |\beta_{00}\rangle$$

**Remarque.** *Ici échanger l'état d'un qubit ne correspond pas à un échange physique, en effet l'échange physique se fait par le biais du canal de communication classique. Alice souhaite uniquement envoyer a et b à Bob. Avec ces informations Bob sera en mesure de reconstituer l'état dans lequel était le qubit  $\psi$ .*

Remarquons les identités suivantes :

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

On va donc appliquer dans l'expression de  $|\Psi\rangle$  les identités.

$$\begin{aligned} |\psi\rangle \otimes |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle) \otimes (|0_A 0_B\rangle + |1_A 1_B\rangle) \\ &= \frac{1}{\sqrt{2}}(a|0\rangle|0_A 0_B\rangle + a|0\rangle|1_A 1_B\rangle + b|1\rangle|0_A 0_B\rangle + b|1\rangle|1_A 1_B\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}(|\beta_{00}\rangle + |\beta_{10}\rangle)\right)a|0_B\rangle + \left(\frac{1}{\sqrt{2}}(|\beta_{01}\rangle + |\beta_{11}\rangle)\right)a|1_B\rangle + \right. \\ &\quad \left. \left(\frac{1}{\sqrt{2}}(|\beta_{01}\rangle - |\beta_{11}\rangle)\right)\beta|0_B\rangle + \left(\frac{1}{\sqrt{2}}(|\beta_{00}\rangle - |\beta_{10}\rangle)\right)\beta|1_B\rangle\right) \\ |\psi\rangle \otimes |\beta_{00}\rangle &= \frac{1}{2}(|\beta_{00}\rangle(a|0_B\rangle + \beta|1_B\rangle) + |\beta_{10}\rangle(a|0_B\rangle - \beta|1_B\rangle) + \\ &\quad |\beta_{01}\rangle(a|1_B\rangle + \beta|0_B\rangle) + |\beta_{11}\rangle(a|1_B\rangle - \beta|0_B\rangle)) \end{aligned}$$

---

3. paragraphe 2.1

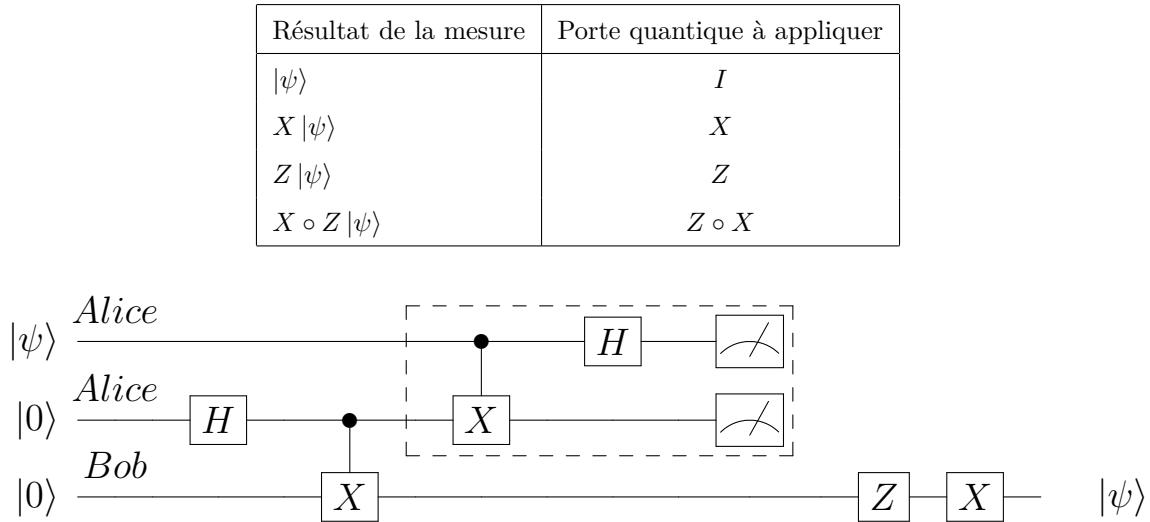


FIGURE 2.3 – Exemple de circuit illustrant la téléportation quantique avec un résultat de mesure (1,1)

Ici on a uniquement donné une réécriture de l'état initial, plus précisément on a effectué un changement de base, pour écrire l'état initial dans la base de Bell.

Maintenant, Alice fait une mesure de ses 2 qubits dans la base de Bell. C'est à dire elle procède à un changement de base, de la base de Bell vers la base canonique en appliquant la porte CNOT puis la porte d'Hadamard. Et enfin elle fait une mesure relative à la base canonique. Elle obtient l'un de ses 4 états de façon équiprobable :

- $|\beta_{00}\rangle (a|0_B\rangle + b|1_B\rangle) = |\beta_{00}\rangle |\psi\rangle$ .
- $|\beta_{10}\rangle (a|0_B\rangle - b|1_B\rangle) = |\beta_{10}\rangle Z(|\psi\rangle)$ .
- $|\beta_{01}\rangle (a|1_B\rangle + b|0_B\rangle) = |\beta_{01}\rangle X(|\psi\rangle)$ .
- $|\beta_{11}\rangle (a|1_B\rangle - b|0_B\rangle) = |\beta_{11}\rangle (X \circ Z)(|\psi\rangle)$ .

Ensuite, en fonction de l'état qu'elle obtient elle va envoyer différents couples de bits à Bob. Le résultat est aléatoire, cependant il permet à Bob de savoir dans quel état est laissé le 3ème qubit.

Après réception, en fonction du couple de bits reçu Bob va appliquer différentes portes quantiques, afin de retrouver les valeurs de  $a$  et  $b$ , et donc de  $|\psi\rangle$ .

**Exemple.** *Le circuit associé à cet exemple est représenté sur la figure 2.3*

*Alice mesure ses deux qubits supposons qu'elle obtienne l'état :*

$$|\beta_{11}\rangle (a|0_B\rangle - b|1_B\rangle) = |\beta_{11}\rangle (X \circ Z)(|\psi\rangle).$$

*Elle envoie donc les bits 1,1 à Bob.*

*Bob en déduit qu'il lui suffit d'appliquer l'inverse de la porte  $(X \circ Z)$  (ie.  $Z \circ X$ ) à son qubit pour retomber exactement sur le qubit  $\psi$ .*

$$\text{En effet } |\beta_{11}\rangle (Z \circ X)(X \circ Z)|\psi\rangle = |\beta_{11}\rangle |\psi\rangle$$

**Remarque.** *Les protocoles de Superdense Coding, et de téléportation quantique, sont des protocoles de communication, qui permettraient à plus long terme d'envisager un réseau quantique. Des expériences de communication quantique ont d'ores et déjà lieu, notamment entre la Chine et l'Autriche. Pour plus d'informations le lecteur se dirigera vers [SKL18].*

## 2.3 Algorithme de Deutsch-Josza

Dans cette section, nous allons étudier l'algorithme de Deutsch-Josza, qui bien qu'il ne soit pas très intéressant dans la pratique, fait partis des premiers algorithmes quantiques plus performants que les

algorithmes classiques. Il a été découvert par David Deutsch et Richard Josza dans [DD92]. De plus cette section est en partie inspiré [PK07].

**Remarque.** L'algorithme de Deutsch-Josza est une généralisation pour  $n$  qubits d'un algorithme appelé l'algorithme de Deutsch imaginé en 1985 par David Deutsch dans [Deu85].

Dans cette section, nous nous sommes largement inspirés du didacticiel de l'IBM Q Experience [https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=004-Quantum\\_Algorithms~2F080-Deutsch-Jozsa\\_Algorithm](https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=004-Quantum_Algorithms~2F080-Deutsch-Jozsa_Algorithm)

**Question.** On a un circuit réversible qui calcule  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . On suppose que la fonction est : soit constante, soit équilibrée, c'est à dire elle prend comme valeur 0 dans la moitié des cas et 1 dans l'autre.

On veut déterminer si la fonction est constante ou équilibrée en faisant le moins possible d'évaluations de  $f$ ?

**Remarque.** Le circuit quantique qui implémente  $f$ , correspond à l'oracle  $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$ <sup>4</sup>

## Classique

Classiquement, dans le pire des cas on peut évaluer la fonction  $f$  sur la moitié des valeurs ( $2^{n-1}$ ) possibles en étant toujours tombé sur 0 ou 1, sans avoir de réponse. Il faut donc faire une évaluation en plus c'est à dire  $2^{n-1} + 1$  évaluation dans le pire des cas pour résoudre le problème.

## Quantique

On va procéder par étape, sur un registre de  $n$  qubits (cf. figure 2.4).

1. On part de  $n$  qubits dans l'état  $|0\rangle$ . Donc le système est dans l'état :

$$|\psi_1\rangle = |0\rangle^n$$

2. On met le système dans une superposition uniforme en appliquant la porte d'Hadamard sur chaque qubits (cf. section 1.3.3). D'où le système est :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

3. On applique l'oracle sur chacun des qubits.

Après application, on obtient un système dans l'état :

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

4. On ré-applique une porte d'Hadamard (cf. section 1.3.3) sur chaque qubit. On a donc :

$$|\psi_4\rangle = \frac{1}{2^n} \sum_y \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} |y\rangle$$

5. On mesure chaque qubit.

Ainsi la probabilité de trouver  $y$  dans une mesure est donné par

$$\left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} \right|^2$$

. En particulier, on en déduit que la probabilité d'obtenir  $y = 00\dots 0$  est  $\left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|^2$ .

Maintenant procédons par disjonctions des cas :

---

4. Définit section 1.3.2

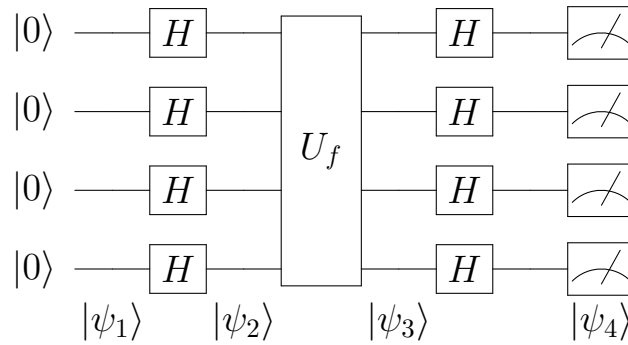


FIGURE 2.4 – Circuit Deutsch-Josza pour 4 qubits, si on obtient 00...0 la fonction est constante, et si on a autre chose la fonction est équilibrée

- Soit  $f$  est constante c'est à dire  $f(x) = c$  pour tout  $x \in \{0, 1\}^n$ , dans ce cas la probabilité d'obtenir  $y = 00...0$  est

$$\left| \frac{1}{2^n} \sum_{x \in \{0, 1\}^n} (-1)^c \right|^2 = 1$$

- Soit  $f$  est équilibré, dans ce cas la probabilité d'obtenir  $y = 00...0$  est :

$$\left| \frac{1}{2^n} \sum_{x \in \{0, 1\}^n} (-1)^{f(x)} \right|^2 = 0 \text{ les termes s'annulent un à un}$$

Ainsi après la mesure, on a soit 00...0 et la fonction est constante, soit autre chose et la fonction est équilibrée.

On a donc résolu notre problème en une seule évaluation de  $f$ .



## Chapitre 3

# Algorithme d'estimation de la phase quantique

Dans ce chapitre, nous allons construire un algorithme plus complexe que ceux du chapitre précédent.

Cette algorithme nécessite un opérateur très utile en calcul quantique la transformée de Fourier quantique. Avec cette opérateur nous serons en mesure de résoudre le problème, cependant contrairement aux autres algorithmes montrés jusqu'ici, nous n'aurons qu'une estimation de la solution du problème.

Cette section a de multiples inspiration, d'abord la section 7.1 de [Pre16], mais aussi la section II.5 de [MAN00], et enfin les deux lectures de John Watrous sur le sujet [Wat06a] et [Wat06b].

### 3.1 Introduction du problème

Supposons que l'on ait un circuit avec  $n$  qubits en entrées. On lui associe un opérateur unitaire  $U$  quelconque qui sera donc de taille  $2^n \times 2^n$ . Ainsi, dès lors que  $n$  dépasse quelques dizaines, il devient très compliqué voire impossible de stocker la matrice associée à  $U$ . Par exemple pour  $n = 20$ , la matrice aurait plus de  $2^{20} > 10^{24}$  coefficients...

Toutefois, le fait que la matrice soit unitaire nous donne deux informations. D'abord  $U$  est diagonalisable et de plus il préserve la distance euclidienne.

D'où si on pose  $N = 2^n$ , il existe  $|\psi_1\rangle, \dots, |\psi_N\rangle$  une base orthonormée de vecteurs propres associés à  $N$  valeurs propres  $e^{2\pi i \theta_1}, \dots, e^{2\pi i \theta_N}$  Où  $\theta_i \in [0, 1]$  pour tout  $i \in 1, \dots, N$ .

Autrement dit, on a l'existence de  $N$   $|\psi_j\rangle$  et de  $N$   $\theta_j$  tels que :

$$U |\psi_j\rangle = e^{2\pi i \theta_j} |\psi_j\rangle \quad (3.1)$$

**Question.** Soit un circuit à  $n$  qubits, on lui associe un opérateur unitaire  $U$ . On se donne un vecteur propre  $|\psi\rangle$  de  $U$ . Comment trouver  $\theta$  tel que :

$$U |\psi\rangle = e^{2\pi i \theta} |\psi\rangle \quad (3.2)$$

On a donc un premier registre<sup>1</sup> de  $n$  qubits dans un état initial  $|\psi\rangle$ .

Comme dans les algorithmes vus ci-dessus, afin de résoudre le problème nous allons devoir introduire un second registre avec des qubits « en contrôle » du premier registre. Notons  $m$  le nombre de qubits du second registre chacun dans état initial  $|0\rangle$ . On a donc :

$$|\chi_0\rangle = |0\rangle^{\otimes m} |\psi\rangle \quad (3.3)$$

---

1. un ensemble de qubits

Afin de créer un état de superposition on applique une porte d'Hadamard à chacun des qubits du second registre. On en déduit :

$$|\chi_1\rangle = H^{\otimes m}(|0\rangle^{\otimes m})|\psi\rangle \quad (3.4)$$

$$= \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle |\psi\rangle \quad (3.5)$$

On définit la porte  $c-U$  (*controlled-U*) comme suit :

$$c-U : \begin{cases} |0\rangle & \mapsto |0\rangle |x\rangle \\ |1\rangle & \mapsto |1\rangle U|x\rangle \end{cases},$$

et  $U^i$  comme la composition de  $i$  portes  $U$ .

Ensuite afin de faire apparaître  $\theta$ , on applique  $m$  fois la porte de contrôle- $U^{2^i}$  pour  $i$  allant de 0 à  $m-1$  au premier registre avec le  $i$ -ème qubit du second registre comme cible.

**Remarque.** Pour déterminer l'application des puissances de  $U$  sur  $|\psi\rangle$ , on utilise l'équation 3.2 :

$$U^{2^l} |\psi\rangle = U^{2^l-1} U |\psi\rangle \quad (3.6)$$

$$= U^{2^l-1} e^{2\pi i \theta} |\psi\rangle \quad (3.7)$$

$$= U^{2^l-2} e^{2\pi i \theta 2} |\psi\rangle \quad (3.8)$$

$$= \dots \quad (3.9)$$

$$U^{2^l} |\psi\rangle = e^{2\pi i \theta 2^l} |\psi\rangle \quad (3.10)$$

A l'aide de cette remarque appliquons  $U^{2^l}$  à  $|\psi\rangle$  avec le  $l$ -ième qubit du deuxième registre. On a donc :

$$\begin{aligned} U^{2^l} \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |\psi\rangle \right) &= \frac{1}{\sqrt{2}} (U^{2^l} (|0\rangle |\psi\rangle) + U^{2^l} (|1\rangle |\psi\rangle)) \\ &= \frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle) + U^{2^l} (|1\rangle |\psi\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle) + |1\rangle e^{2\pi i \theta 2^l} |\psi\rangle \\ U^{2^l} \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |\psi\rangle \right) &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle e^{2\pi i \theta 2^l}) |\psi\rangle \end{aligned}$$

Ainsi si on décrit l'état des  $m$  qubits du second registre on a :

$$\frac{1}{\sqrt{2^m}} (|0\rangle + e^{2\pi i \theta 2^0} |1\rangle) \otimes (|0\rangle + e^{2\pi i \theta 2^1} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i \theta 2^{m-1}} |1\rangle) \quad (3.11)$$

Finalement on peut réécrire l'équation 3.11 comme :

$$|\chi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{2\pi i \theta k} |k\rangle \quad (3.12)$$

Le premier registre de qubits, ne nous sera plus utile, de ce fait on ne considère plus que le second, c'est à dire uniquement l'équation 3.12.

Rappelons que l'objectif du problème est de déterminer  $\theta$ , ou du moins d'en trouver une bonne approximation. On cherche donc un opérateur unitaire  $Q$  tel que  $Q(|\chi_2\rangle) = \theta$ . Cette opérateur est d'une importance capitale en calcul quantique et il revient souvent dans de nombreux algorithmes dont le fameux algorithme de décomposition en nombre premiers de Shor. De ce fait la section suivante lui est entièrement dédié.



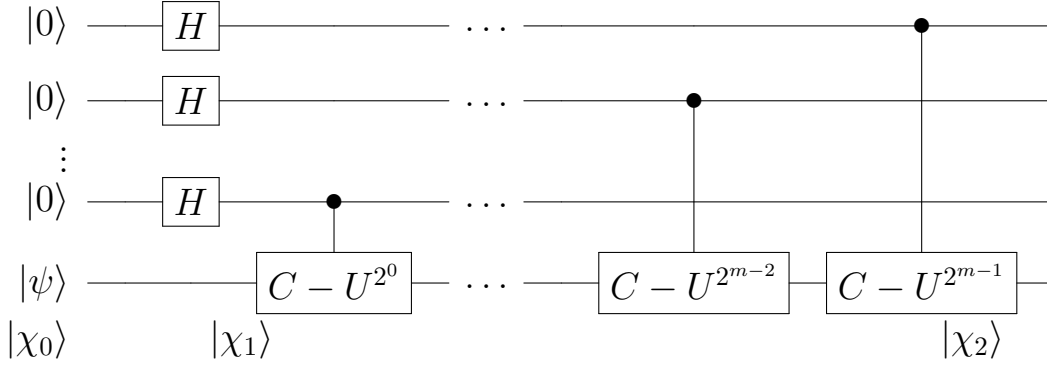


FIGURE 3.1 – Les 2 premières opérations de l'estimation de phase quantique

## 3.2 Transformée de Fourier Quantique

Avant de commencer à introduire cet opérateur nous allons parler d'encodage et décodage. Pour cela revenons sur un opérateur qui nous est bien plus familier l'opérateur d'Hadamard.

Soit  $n$  qubits, on applique  $H^{\oplus n}$  sur un état  $|x\rangle$ , on obtient :

$$H^{\oplus n}(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

On peut dire qu'on a *encodé*  $|x\rangle$  dans la base  $|y\rangle$  avec une *phase*  $(-1)^{x \cdot y}$ .

Pour *décoder* l'information, il suffit de ré-appliquer  $H^{\oplus n}$ .

Cependant  $(-1)^{x \cdot y}$  correspond à des phases très particulières, donc si on utilise un autre type d'encodage avec une phase quelconque de la forme  $e^{2\pi i \omega}$  où  $\omega \in [0, 1]$ , on ne pourra pas la décoder avec la transformation  $H^{\oplus n}$ . On cherche donc une généralisation de l'opérateur d'Hadamard, capable de décoder un plus grands nombre de phases.

L'objet de cette section est la définition de cet opérateur qu'on appelle transformée de Fourier de quantique :

**Définition 1.** On note  $QFT$  l'opérateur de la transformée de Fourier quantique et il est défini pour l'état d'une base orthogonale  $(|0\rangle, \dots, |N-1\rangle)$  par la formule suivante :

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle$$

De façon équivalente l'opérateur QFT peut être vu comme la matrice :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \omega_n^3 & \dots & \omega_n^{N-1} \\ 1 & \omega_n^2 & \omega_n^4 & \omega_n^6 & \dots & \omega_n^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega_n^{N-1} & \omega_n^{2(N-1)} & \omega_n^{3(N-1)} & \dots & \omega_n^{(N-1)(N-1)} \end{pmatrix}$$

**Remarque.** On comprend directement son nom en remarquant les similitudes avec la transformée de Fourier discrète.

**Remarque.** Dans la suite il sera utile d'écrire les données dans leurs représentation binaire.

On note  $j = j_1 j_2 \dots j_n$  pour dire que  $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$ .

Dans la suite on adopte la notation  $0.j_l j_{l+1} \dots j_m$  pour représenter la fraction binaire  $\frac{j_l}{2} + \frac{j_{l+1}}{2^2} + \dots + \frac{j_m}{2^{m-l+1}}$

On va donner une autre réécriture de la transformée de Fourier quantique pour  $N = 2^n$ , qui sera bien plus pratique dans notre cas.

**Proposition.** Soit  $|j\rangle$  un état de la base orthogonale  $(|0\rangle, \dots, |2^n - 1\rangle)$ , et son écriture binaire donnée par  $j = j_1 j_2 \dots j_n$ . Alors on a :

$$QFT(|j\rangle) = \frac{1}{\sqrt{2^n}} ( (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 \dots j_n} |1\rangle) ) \quad (3.13)$$

*Démonstration.* En effet, cela résulte de :

$$\begin{aligned} QFT(|j\rangle) &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j \frac{k}{2^n}} |k\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n \frac{k_l}{2^l})} |k_1 \dots k_n\rangle \\ &= \frac{1}{\sqrt{2^n}} ( (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 \dots j_n} |1\rangle) ) \end{aligned}$$

□

**Remarque.** On remarque directement une similitude entre l'équation 3.13 et l'équation 3.11.

L'équation 3.13 nous donne une construction de la QFT en fonction d'opérateurs plus élémentaires. En effet, raisonnons pour différentes valeurs de  $n$  :

— Pour  $n = 1$ , on a

$$QFT(|j\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle)$$

procédons par disjonction des cas sur la valeurs de  $j = j_1 \times 2^{-1}$ , soit  $j = 0 \times 2^{-1}$  et dans ce cas on a

$$QFT(|j\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

, soit  $j = 1$  ou en écriture binaire  $j = 1 \times 2^{-1}$  et on a

$$QFT(|j\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 1 \times 2^{-1}} |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Finalement on en déduit que pour  $n = 1$

$$QFT = H$$

— Pour  $n = 2$ , on a

$$QFT(|j\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0 \cdot j_2} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2} |1\rangle)$$

Nous remarquons de prime abord que le premier terme correspond, comme précédemment à  $H$ . Pour le second terme procédons par disjonction de cas sur la valeur de  $j_2$ .

—  $j_2 = 0$ , d'où le second terme est dans l'état

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle)$$

On retombe exactement sur le premier terme, et il s'agit uniquement à nouveau de  $H$ .

—  $j_2 = 1$ , d'où le second terme est dans l'état

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0 \cdot j_1 1} |1\rangle)$$

Dans ce cas l'opérateur  $H$  ne suffit pas, il faut légèrement modifier la phase. Plus précisément, il faut effectuer une rotation  $0.01$  (en binaire) c'est à dire de  $1/4$ . Pour cela on utilise l'opérateur de rotation  $R_2$  introduit dans la section 1.1.2.

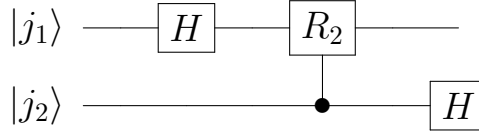


FIGURE 3.2 – Circuit QFT pour 2 qubits

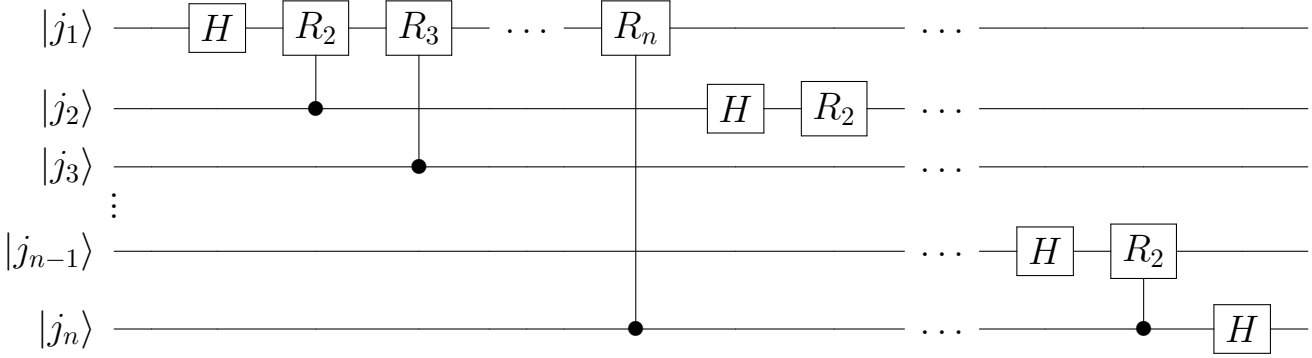


FIGURE 3.3 – Circuit QFT pour n qubits

Donc pour récapituler dans le cas  $n = 2$ , la QFT de  $j_1$  et  $j_2$  correspond à une porte d'Hadamard sur  $j_1$ , puis la porte  $R_2$  en contrôle par rapport à  $j_2$ , et enfin on applique une porte d'Hadamard sur  $j_2$ . On a le circuit 3.2.

- Pour  $n$  quelconque, la généralisation n'est pas compliquée. En effet, le  $i$ -ème terme qui sera de la forme

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_i} |1\rangle)$$

De ce fait, il faudra effectuer  $i-1$  rotation (toujours en contrôle des  $j_i$ ) d'angle  $1/2^k$  (c'est à dire applique  $R_k$ ) pour  $k$  allant de 2 à  $i$ .

La QFT est défini comme le circuit représenté figure 3.3.

De ce fait, l'opérateur QFT peut être défini par la composition d'opérateurs unitaires. Or l'ensemble des opérateurs unitaires forment un groupe par la composition, on en déduit le théorème suivant :

**Théorème.** *L'opérateur QFT est un opérateur unitaire.*

Dans notre problème (cf. équation 3.12), nous avons un état déjà encodé dans une phase particulière, on cherche donc plutôt à décoder.

De ce fait, on va non pas utiliser la transformée de Fourier quantique, mais son inverse :

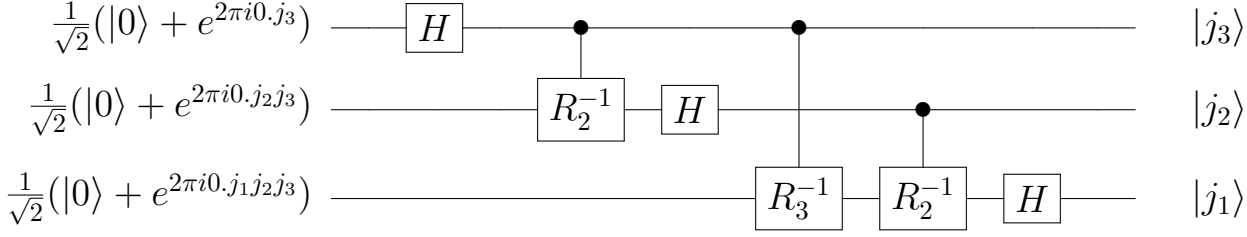
**Définition 2.** *On note  $QFT^{-1}$  l'inverse de la transformée de Fourier quantique et il est défini pour l'état d'une base orthogonale  $(|0\rangle, \dots, |N-1\rangle)$  par la formule suivante :*

$$QFT^{-1}(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j \frac{k}{N}} |k\rangle$$

ou bien de façon équivalente :

$$QFT^{-1}\left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle\right) = |j\rangle$$

**Remarque.** *Des propositions et constructions analogues à celles qui s'appliquaient à la transformée de Fourier quantique s'applique bien sûr à son inverse. Par exemple sa construction en portes élémentaires pour trois qubits est donnée par la figure 3.4*

FIGURE 3.4 – Circuit  $\text{QFT}^{-1}$  pour 3 qubits

Avec la transformée de Fourier inverse, on a trouvé un opérateur capable d'approximativement décoder la phase de l'équation 3.12. Revenons en au problème initial.

### 3.3 Résolution du problème et Estimation d'erreurs

Rappelons que le système se trouve dans l'état :

$$|\chi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{2\pi i \theta k} |k\rangle \quad (3.14)$$

On veut décoder l'information, en utilisant l'inverse de la transformée de Fourier quantique.

Cependant on remarque que l'inverse de la transformée de Fourier quantique dans un cas, décode parfaitement l'information du système. De ce fait raisonnons par disjonction des cas, sur ce cas favorable puis les autres.

Traitions d'abord le cas favorable  $\theta = \frac{j}{2^m}$  pour un entier  $j \in \{0, \dots, 2^m - 1\}$

Dans ce cas par définition de l'inverse de la transformée de Fourier quantique<sup>3</sup>, on obtient directement après mesure du second registre tout les  $j_i$  qui définissent  $j = 0.j_1 \dots j_m$  et donc on peut en déduire  $\theta$  uniquement en divisant par  $2^m$ .

Maintenant les cas plus défavorable  $\theta \neq \frac{j}{2^m}$ .

Appliquons d'abord l'inverse de la transformée de Fourier quantique

$$\begin{aligned} \text{QFT}^{-1} |\chi_2\rangle &= \text{QFT}^{-1} \left( \frac{1}{2^m} \sum_{k=0}^{2^m-1} e^{2\pi i \theta k} |k\rangle \right) \\ &= \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{k=0}^{2^m-1} e^{2\pi i \theta k} e^{-2\pi i k \frac{x}{2^m}} |x\rangle \\ &= \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{k=0}^{2^m-1} e^{-2\pi i \frac{k}{2^m} (x - 2^n \theta)} |x\rangle \end{aligned}$$

Le système est donc dans l'état :

$$|\chi_3\rangle = \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{k=0}^{2^m-1} e^{-2\pi i \frac{k}{2^m} (x - 2^n \theta)} |x\rangle \quad (3.15)$$

2. On remarque que la porte  $R_2$  sera appliqué en contrôle, car elle dépend de  $j_2$ .

3. définition 2

La valeur de  $\theta 2^n$ , n'étant pas entière par hypothèse on va donner son approximation à l'entier le plus proche.

C'est à dire on a  $2^n \theta = j + 2^n \delta$  où  $j$  est l'entier le plus proche de  $2^n \theta$  et  $2^n \delta$  satisfait l'inéquation suivante  $0 \leq |2^n \delta| \leq \frac{1}{2}$ .

On peut donc réécrire l'équation 3.15 comme :

$$|\chi_3\rangle = \frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{k=0}^{2^m-1} e^{-2\pi i \frac{k}{2^m}(x-j)} e^{2\pi i \delta k} |x\rangle \quad (3.16)$$

Comme ci-dessus on effectue une mesure sur tout le second registre. On obtient la probabilité de mesuré  $j$  est :

$$p_j = \frac{1}{2^{2m}} \left| \sum_{k=0}^{2^m-1} e^{2\pi i \delta k} \right|^2$$

En utilisant la formule d'une somme géométrique (comme  $\delta \neq 0$  par hypothèse on obtient :

$$p_j = \frac{1}{2^{2m}} \left| \frac{1 - e^{2\pi i 2^m \delta}}{1 - e^{2\pi i \delta}} \right|^2 \quad (3.17)$$

Plus précisément on a le résultat suivant :

**Théorème.** Soit  $j$  l'entier le plus proche de  $\theta 2^m$ . Alors l'estimation de phase quantique retourne  $j$  avec une probabilité d'au moins  $\frac{4}{\pi^2} \approx 0.4$

*Démonstration.* Ce résultat se déduit des équations suivantes :

$$\begin{aligned} p_j &= \frac{1}{2^{2m}} \left| \frac{1 - e^{2\pi i 2^m \delta}}{1 - e^{2\pi i \delta}} \right|^2 \\ &= \frac{1}{2^{2m}} \left| \frac{2\sin(\pi 2^m \delta)}{2\sin(\pi \delta)} \right|^2 \text{ en effet } |1 - e^{2ix}|^2 = 4|\sin(x)|^2 \\ &\geq \frac{1}{2^{2m}} \frac{|\sin(\pi 2^m \delta)|^2}{|\pi \delta|^2} \text{ car } \delta \text{ est suffisamment petit} \\ &\geq \frac{1}{2^{2m}} \frac{|2 \cdot 2^m \delta|^2}{|\pi \delta|^2} \\ &= \frac{4}{\pi^2} \end{aligned}$$

□

**Remarque.** En d'autres termes ce théorème nous dit que l'estimation de phase quantique détermine un  $j$  avec une probabilité d'au moins  $\frac{4}{\pi^2}$  tel que  $|\frac{j}{2^m} - \theta| \leq \frac{1}{2^{m+1}}$ .

De plus, l'algorithme d'estimation de phase quantique nous donne un des  $2k$  entiers les plus proches de  $2^m \theta$  avec une probabilité d'au moins  $1 - \frac{1}{2^{(k-1)}}$ . Enfin, on en déduit que l'estimation de phase quantique nous donne un  $\tilde{\theta}$  avec une probabilité d'au moins  $1 - \frac{1}{2^n}$  tel que  $|\tilde{\theta} - \theta| \leq \frac{1}{2^r}$  où  $m = n + r + 1$ .

### 3.4 Pour récapituler

On cherche à résoudre le problème suivant :

**Question.** Soit un circuit à  $n$  qubit, on lui associe un opérateur unitaire  $U$ . On se donne un vecteur propre  $|\psi\rangle$  de  $U$ . Comment trouver  $\theta$  tel que :

$$U |\psi\rangle = e^{2\pi i \theta} |\psi\rangle \quad (3.18)$$

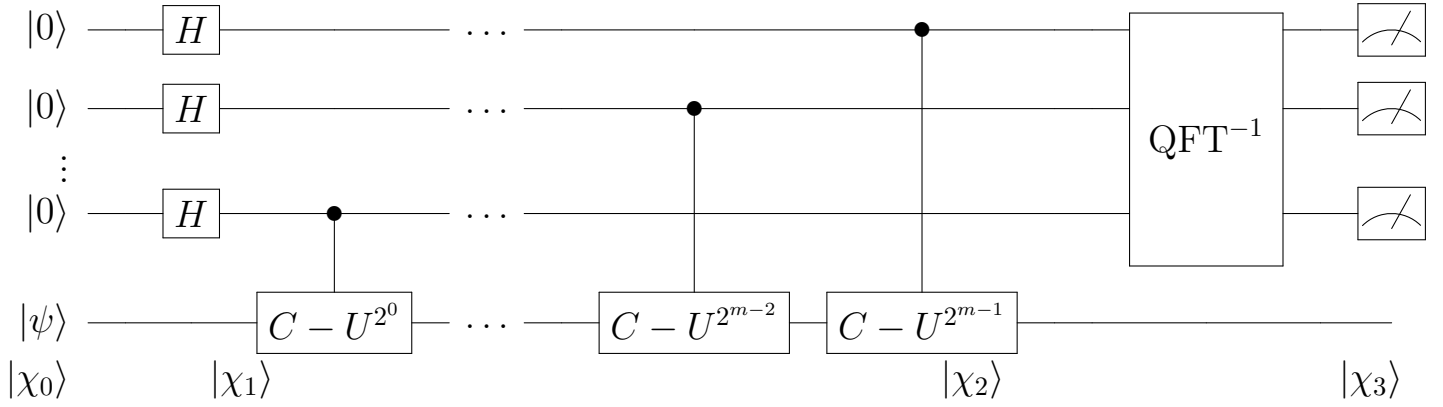


FIGURE 3.5 – Circuit de l'estimation de phase quantique

Pour cela on prends un second registre de  $m$  qubits chacun dans l'état  $|0\rangle$ . On a deux registres sur lesquels on applique l'algorithme suivant (résumé sur la figure 3.5) :

1. On applique  $H^{\oplus m}$  au second registre.
2. On applique  $m$  fois la porte de contrôle- $U^{2^i}$  pour  $i$  allant de 0 à  $m-1$  au premier registre avec le  $i$ -ème qubit du second registre comme cible.
3. On applique l'opérateur  $\text{QFT}^{-1}$  au second registre.
4. Enfin on mesure les qubits du second registre. Et on obtient un  $\tilde{\theta}$  avec une probabilité d'au moins  $1 - \frac{1}{2^n}$  tel que  $|\tilde{\theta} - \theta| \leq \frac{1}{2^r}$  où  $m = n + r + 1$ .

## Chapitre 4

# Logiciels pour la simulation d'algorithmes quantiques

Au cours de la rédaction des deux chapitres précédents, nous avons eu l'occasion de voir la nécessité d'expérimenter les différents algorithmes. Dans cette tâche, nous avons utilisé *des simulateurs quantiques*. Un simulateur quantique est un programme sur un ordinateur classique qui simule le fonctionnement d'un ordinateur quantique. De fait, un simulateur quantique sera rapidement limité par la puissance d'un ordinateur classique. A partir de 50 qubits on parle du seuil de la *suprématie quantique*<sup>1</sup> au delà duquel le meilleur superordinateur classique n'est plus capable de simuler un ordinateur quantique.

Dans ce chapitre, nous allons décrire les différents simulateurs que nous avons utilisés. Précisons qu'en aucun cas, la liste des simulateurs que nous évoquons dans la suite est exhaustive. Pour avoir un aperçu plus large on redirigera le lecteur vers la liste suivante <https://quantiki.org/wiki/list-qc-simulators>.

Nous avons eu affaire au cours de nos pérégrinations à deux types de simulateurs :

- Les premiers plus accessibles, des *GUI* pour *graphical user interface*
- Les seconds pouvant réaliser des tâches plus complexes, des *langages de programmation* ou des bibliothèques associées à des langages existants.

Chacun de ces types ayant des avantages et des inconvénients que nous détaillerons par la suite.

### 4.1 GUI

Les GUI se basent uniquement sur de la programmation visuelle, c'est à dire que les seules actions que le développeur doit faire sont glisser/déposer/cliquer avec sa souris.

Le but ici sera uniquement de reproduire le diagramme de circuit associé à l'algorithme que l'on souhaite implémenter dans le simulateur. Cela rend l'expérience très intuitive. On oublie toute la difficulté technique, et on se focalise uniquement sur le problème qu'on souhaite résoudre.

Le principal inconvénient de ce type de simulateur vient du fait que dès lors que l'on souhaite implémenter un algorithme comme la QFT sur une dizaine de qubits, il faudra ajouter une dizaine de fois la porte H et la porte  $R_k$ . Cela devient très vite redondant et pour donner une analogie, cela revient au même que d'implémenter un algorithme itératif sans boucle *for*.

#### 4.1.1 Q-kit

Q-kit est un logiciel en développement disponible à l'adresse suivante <https://sites.google.com/view/quantum-kit/download?authuser=0>.

---

1. Pour plus d'information sur ce sujet on dirigera le lecteur vers [Pre11]

Le logiciel est on ne peut plus simple à installer, de plus même si l'interface semble au premier abord un peu aride (cf. figure 4.1), on comprend très rapidement le fonctionnement finalement simple du logiciel.

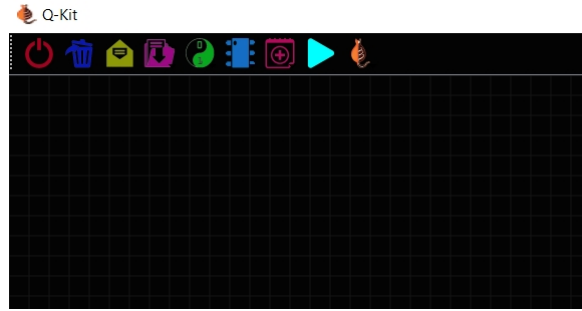


FIGURE 4.1 – Q-kit au démarrage

Mais surtout Q-kit a un atout majeur : il permet de voir l'évolution du système à chaque étape, ce qui donne un intérêt pédagogique au logiciel (cf. figure 4.2).

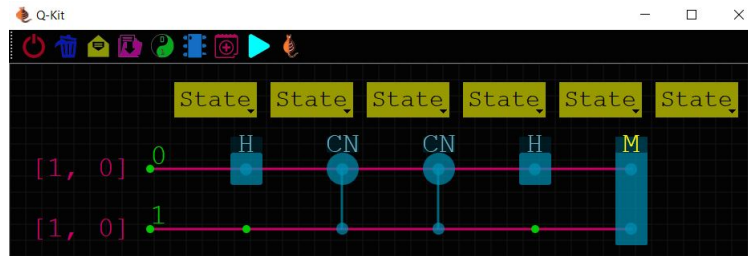


FIGURE 4.2 – Superdense Coding sur Q-kit

### 4.1.2 Quirk

Quirk est un éditeur de circuit quantique complètement disponible en ligne à l'adresse <https://algassert.com/quirk>.



FIGURE 4.3 – Quirk au démarrage

Quirk dispose d'un tutoriel intégré dans l'interface, ce qui facilite la compréhension et l'accessibilité de l'expérience. De plus il donne accès à des exemples basiques d'algorithmes. Quirk peut aussi être utilisé à



un niveau plus avancé, avec notamment des portes un peu plus complexes, comme des portes dépendant du temps, etc...

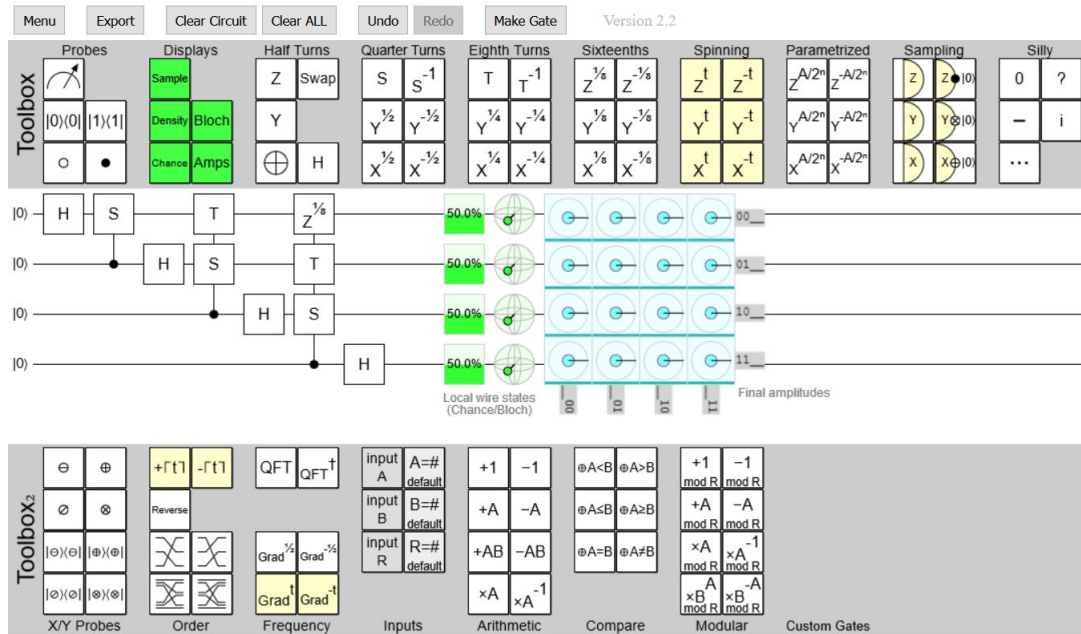


FIGURE 4.4 – QFT avec Quirk

### 4.1.3 IBM Q Composer

En 2016 la société IBM lance la plateforme en ligne *IBM Q Experience*. Cette plateforme donne accès à d'innombrables ressources comme des didacticiels, un forum dédié au calcul quantique. Mais surtout, elle rend accessible par le biais du cloud à un véritable ordinateur quantique de 5 qubits.

Cette ordinateur quantique permet à quiconque de lancer un programme quantique, implémenter à l'aide d'une GUI que nous allons décrire ici, ou du langage Qasm que nous décrirons dans la section 4.2.2.

Pour être utilisé IBM Q Experience nécessite uniquement une inscription sur le site <https://quantumexperience.ng.bluemix.net/qx/community>. Une fois l'inscription effectuée, on peut accéder au *IBM Q composer* et créer un nouveau programme. A cette étapes là, deux choix s'offrent à nous :

- Soit on se restreint à des circuits de 5 qubits ou moins qui seront exécutables en ligne sur l'ordinateur quantique de IBM (figure 4.6).
- Soit on choisit un nombre plus important de qubits et dans ce cas on pourra uniquement simuler les programmes (figure 4.5).

Au niveau interface et accessibilité, *l'IBM Q composer* propose une interface simple, épurée et dispose uniquement des fonctionnalités les plus rudimentaires. De plus, les didacticiels de *l'IBM Q experience* proposent pour chaque algorithme présenté, un lien directement dans *l'IBM Q composer* avec l'algorithme implémenté.

De plus un bouton permet de passer du programme en GUI au fichier écrit en QASM 4.2.2.

Enfin, nous avons eu l'occasion d'essayer nos programmes sur les ordinateurs quantiques de IBM, de même rien de plus simple, il suffit de cliquer sur le bouton *run*, puis IBM nous informe que notre programme sera exécuté sous peu. Quelques heures plus tard, on a le résultat envoyé par mail (cf. figure 4.7)

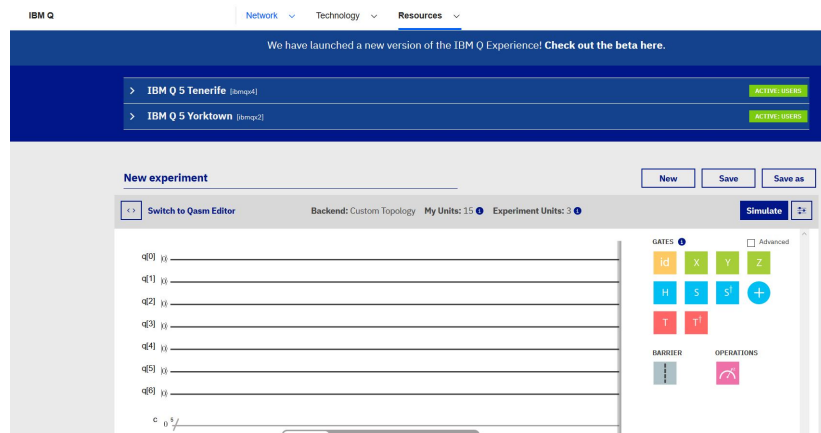


FIGURE 4.5 – IBM Q decomposer - un circuit vierge avec 7 qubits

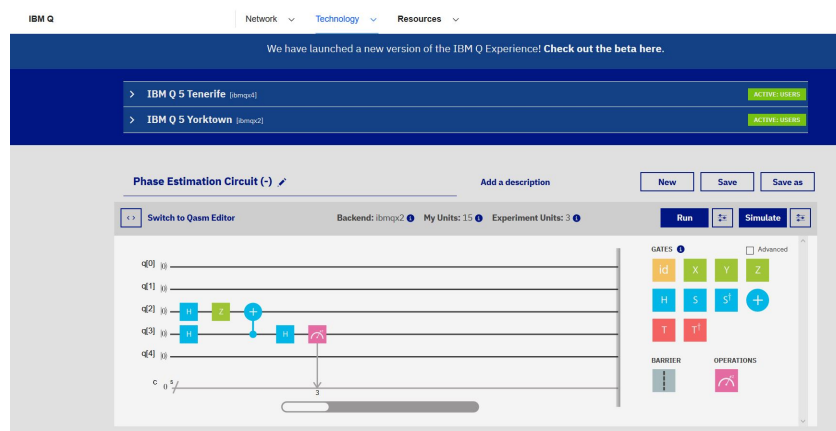


FIGURE 4.6 – IBM Q decomposer - l'estimation de phase exécutable sur l'ordinateur quantique

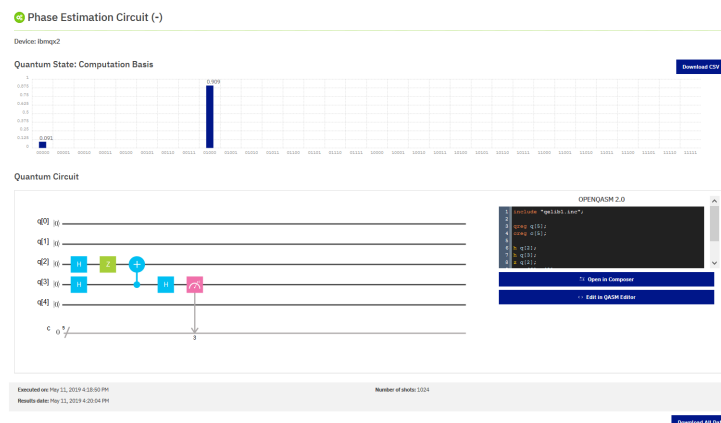


FIGURE 4.7 – Résultat - l'estimation de phase

## 4.2 Langages de programmation

### 4.2.1 Qiskit

Qiskit est un module python créé par IBM.

Une documentation et un didacticiel plutôt complets sont disponibles sur <https://qiskit.org/>.

Qiskit, est un module python très simple à comprendre et à appréhender. De plus il possède l'avantage

et la profondeur qu'offre un langage de programmation. C'est à dire par rapport au GUI de pouvoir faire toutes ces choses rudimentaires qu'offre le python : des boucles, des instructions conditionnelles, des fonctions, etc...

Par exemple, le code ci-dessous permet d'appliquer la porte quantique H à  $n$  qubits avec une boucle for et d'effectuer une mesure sur chacun de ces qubits. Cet exemple aurait été très redondant à faire sur les GUI vus précédemment.

```

1  n=5
2  q = QuantumRegister(n, 'q')
3  circ = QuantumCircuit(q)
4  for i in range(n):
5      circ.h(q[i])
6  c = ClassicalRegister(n, 'c')
7  meas = QuantumCircuit(q, c)
8  meas.barrier(q)
9  meas.measure(q, c)
10 qc = circ+meas
11 qc.draw(output='mpl')

```

Encore un autre avantage vient du fait, que l'on peut rajouter une module de visualisation des circuits en latex. Par exemple le code retourne la figure 4.8.

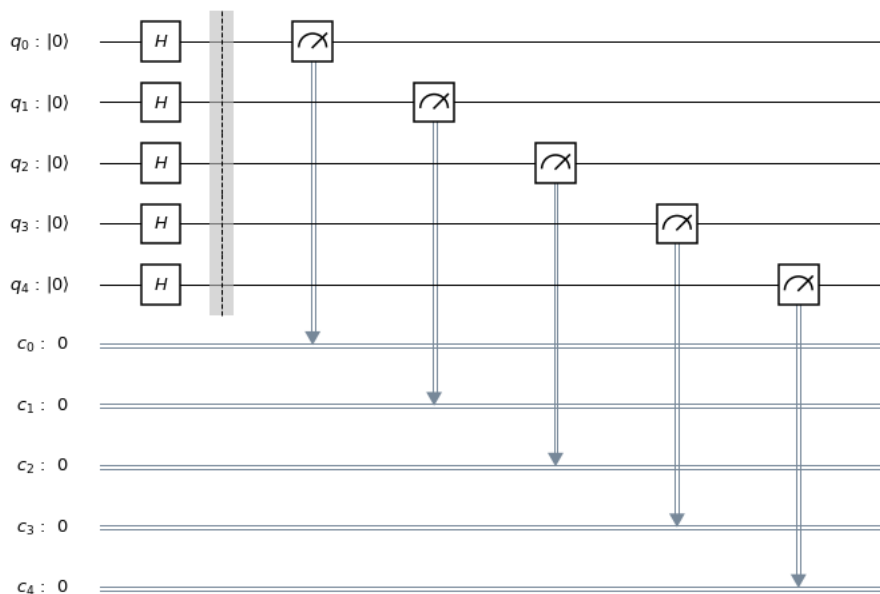


FIGURE 4.8 – Qiskit - Visualisation Latex circuit

Mais on peut aussi visualiser le résultat sous forme d'histogramme pour 100000 simulations avec les commandes suivantes :

```

1  backend_sim = Aer.get_backend('qasm_simulator')
2  job_sim = execute(circ, backend_sim, shots=100000)
3  result_sim = job_sim.result()
4  counts = result_sim.get_counts(circ)
5  plot_histogram(counts)

```

Ce qui retourne la figure 4.9 ci-dessous :

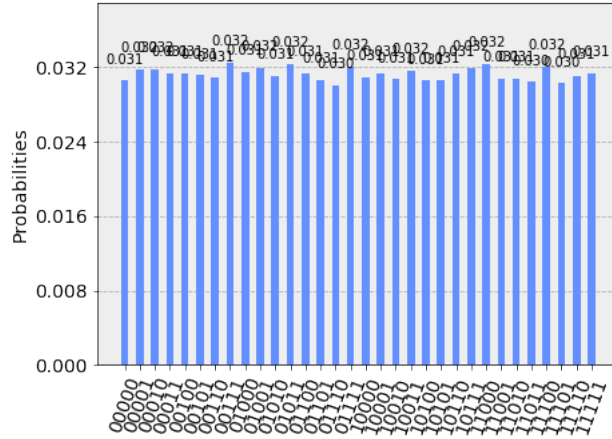


FIGURE 4.9 – Qiskit - Visualisation des résultats

### 4.2.2 Qasm

QASM ou OpenQASM pour *Open Quantum Assembly Language* est le langage lié au IBM Decomposer (cf. section 4.1.3), en effet en un clique on peut passer de l'un à l'autre. Le QASM ne possède pas, de fonctions classiques de programmation comme des boucles ou des instructions conditionnelles. De ce fait, tout comme les GUI, faire un circuit compliqué en QASM peut devenir très redondant. Voici par exemple un programme en QASM ainsi que sa visualisation en latex figure 4.10 :

```

1  def c-Z,1,'Z'
2  qubit    q0,\psi
3  qubit    q1,0
4  qubit    q2,0
5  H    q1
6  cnot   q0,q1
7  cnot   q1,q2
8  cnot   q0,q1
9  cnot   q1,q2
10 H    q0
11 c-Z  q2,q0
12 H    q0
13 H    q0

```

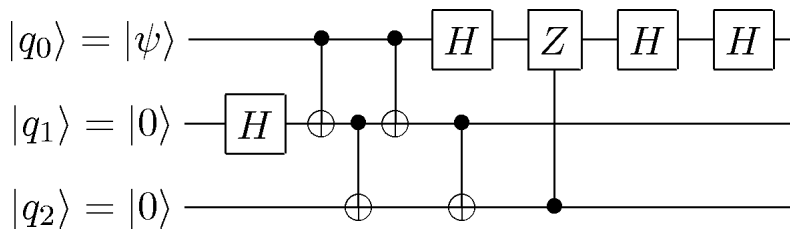


FIGURE 4.10 – QASM - Visualisation latex du circuit

## 4.3 Bilan

En conclusion de ce chapitre, si le lecteur doit utiliser un simulateur quantique<sup>2</sup> au cours de sa lecture du présent document.

On lui conseillera de débiter sur *l'IBM Decomposer* décrit à la section 4.1.3, en effet celui-ci est le plus

<sup>2</sup>. ce que nous conseillons vivement afin d'expérimenter les algorithmes des chapitres 4 et 2

simple pour une première utilisation. Enfin pour une utilisation plus avancée nous recommandons le lecteur d'utiliser Qiskit (pour plus de détail cf. section 4.2.1), qui donne une plus large souplesse que les GUI.



# Conclusion

Avant d’attaquer la conclusion, nous allons tenter de faire un rapide état de l’art du calcul quantique, ainsi que brièvement et humblement évoquer les évolutions possibles.

Pour cela nous nous sommes en grande partie inspirés des deux papiers [MM19] et [Pre16]. A l’heure où se document a été rédigé en mai 2019, Google<sup>3</sup> et IBM<sup>4</sup> font une courses au nombre de qubits de leurs ordinateurs quantiques. Tout deux proclament qu’ils ont dépassé les 50 qubits du seuil de suprématie quantique dont nous avons parlé dans l’introduction du chapitre 4.

Une question demeure : que pouvons-nous faire avec ces ordinateurs quantiques ?

Pour y répondre, introduisons la notion de *bruit quantique* qui donne un obstacle supplémentaire à l’utilisation d’ordinateur quantique. Dans la section 1.1.1 nous avons précisé que nous ne tenions pas compte de l’interaction entre les systèmes et de leur environnement respectif. Or dans la réalité, l’interaction avec l’environnement peut être minimisée, mais pas annulée. Mais cette interaction même faible provoque des erreurs dans l’exécution d’un programme sur une machine quantique. Par exemple, le pourcentage d’erreur par porte quantique pour 2 qubits est de 1%<sup>5</sup> ! Il a aussi été développé ce qu’on appelle de la correction d’erreur pour pallier aux erreurs de bruit quantique, cependant ces techniques nécessite un grand nombre de qubits.

Donc non seulement nous sommes limités par le nombre de qubits disponibles, mais en plus nous sommes limités par le nombre de portes quantiques, qui risquerait de provoquer des trop gros taux d’erreurs. À cela il faut ajouter que les algorithmes les plus « révolutionnaires », comme par exemple l’algorithme de décomposition des nombres premiers de Shor, nécessitent non pas une centaine de qubits mais plusieurs milliers voire millions de qubits.

Nous nous trouvons donc dans une période où le nombre de qubits disponibles sur nos machines sera entre une cinquantaine et une petite centaine, et où le bruit quantique rend compliqué l’exécution d’algorithmes quantiques complexes. John Preskill a donné un nom à cette période : le *NISQ*, pour *Noisy Intermediate-Scale Quantum*. *Noisy*, car nous avons un contrôle imparfait sur nos qubits dû au bruit quantique, et *Intermediate-Scale* par rapport au nombre restreint de qubits de nos ordinateurs quantiques.

L’objectif à court terme pendant le NISQ est donc de déterminer des algorithmes quantiques exécutables sur nos machines actuelles. Deux exemples de tels algorithmes peuvent être trouvés dans les articles [JRM15] et [EF14]. Un autre objectif serait de développer des langages et des techniques de compilation pour offrir aux programmeurs une plus grande souplesse.

À un certain degré, les ordinateurs quantiques ressemblent aux ordinateurs des années 50. Des ordinateurs ayant très peu d’applications concrètes et avant tout développés dans le monde de la recherche. Ainsi, et pour conclure cet état de l’art, en continuant la comparaison des ordinateurs des années 50, il nous semble que nous sommes à l’aube d’un domaine fascinant, sur lequel nous avons encore peu d’applications, mais où tout reste encore à faire !

En conclusion, au cours de ce document, nous avons donné des bases théoriques dans le chapitre 1 et pratiques dans les chapitres 2 et 3 suffisantes pour appréhender le monde en plein essor qu’est le calcul quantique. Ainsi, le lecteur avide de connaissances sur ce domaine sera tout à fait à même de comprendre d’autres algorithmes. Ce même lecteur pourra être intéressé par l’algorithme quantique de résolution de

---

3. <https://www.technologyreview.com/s/612381/google-has-enlisted-nasa-to-help-it-prove-quantum-supremacy-within-months/>

4. <https://www.hpcwire.com/2019/01/10/ibm-quantum-update-q-system-one-launch-new-collaborators-and-qc-center-plans/>

5. [Pre16]

systèmes linéaires détaillé dans l'article [AWH09], mais aussi par l'algorithme de Shor et Grover analysés dans [PK07], ou encore par la méthode des éléments finis quantique découverte dans l'article [AM15].



# Formulaire

## Analyse Hilbertienne

**Définition** (Espace de Hilbert). On appelle espace de Hilbert complexe un espace vectoriel complexe muni d'un produit hermitien  $\langle \cdot | \cdot \rangle$ , qui est complet pour la norme associée  $x \mapsto \|x\| = \sqrt{\langle x | x \rangle}$ .

**Notation** (de Dirac). Les notations de Dirac consistent, entre autres, à représenter les vecteurs d'un espace de Hilbert sous forme de ket :  $|x\rangle$ .

**Définition** (Base orthonormée). Soit  $\mathcal{H}$  un espace de Hilbert complexe de dimension  $N$ . Une famille de vecteurs de  $\mathcal{H}$   $(|x_i\rangle)_{i \in \{1, \dots, N\}}$  est une base orthonormée de  $\mathcal{H}$  lorsque :

- ces vecteurs sont deux à deux orthogonaux :  $\forall i \neq j, \langle x_i | x_j \rangle = 0$  ;
- ces vecteurs sont normés :  $\forall i \in \{1, \dots, N\}, \langle x_i | x_i \rangle = 1$ .

**Proposition** (Opérateur adjoint). Soient  $\mathcal{H}$  un espace de Hilbert et  $U : \mathcal{H} \rightarrow \mathcal{H}$  un opérateur linéaire. Il existe un unique opérateur  $U^*$ , appelé adjoint de  $U$ , tel que  $\langle Ux | y \rangle = \langle x | U^*y \rangle$  pour tous  $x, y \in \mathcal{H}$ .

**Définition** (Opérateur unitaire). Soit  $\mathcal{H}$  un espace de Hilbert. Un opérateur linéaire  $U : \mathcal{H} \rightarrow \mathcal{H}$  est dit unitaire lorsqu'il vérifie  $UU^* = U^*U = I$ , où  $I$  désigne l'identité. Il est équivalent de dire que  $U$  conserve le produit scalaire, ou bien la norme :  $\forall x, y \in \mathcal{H}, \langle Ux | Uy \rangle = \langle x | y \rangle$  et  $\|Ux\| = \|x\|$ .

---

## Postulats

**Postulat 1** (Espace des états). L'état d'un système quantique peut être décrit par une droite dans un espace de Hilbert.











**Postulat 2** (Évolution). L'évolution entre deux instants d'un système quantique isolé est décrit par un opérateur unitaire.

**Postulat 3** (Mesure - première version). Étant donnée une base orthonormée  $(|e_i\rangle)_{i \in I}$  d'un espace de Hilbert, il est possible d'effectuer une mesure relativement à cette base qui, pour un système dans l'état  $|\psi\rangle = \sum_i a_i |e_i\rangle$  va renvoyer le résultat  $i$  avec probabilité  $|a_i|^2$  et laisser le système dans l'état  $|e_i\rangle$ .

**Postulat 4** (Composition de systèmes). Lorsque deux systèmes quantiques ayant respectivement comme espace d'états  $\mathcal{H}_1$  et  $\mathcal{H}_2$  sont regardés comme un seul système quantique, ce dernier a pour espace d'états l'espace  $\mathcal{H}_1 \otimes \mathcal{H}_2$ . Si le premier système est dans l'état  $|\psi_1\rangle$  et le deuxième dans l'état  $|\psi_2\rangle$ , alors le système composite est dans l'état  $|\psi_1\rangle \otimes |\psi_2\rangle$ .

**Postulat 5** (Mesure). Soit  $|e_1\rangle, \dots, |e_n\rangle$  est une base orthonormée d'un espace  $\mathcal{H}_1$ , et soit  $|\psi_1\rangle, \dots, |\psi_n\rangle$  une famille de vecteurs normés (pas forcément orthogonaux) d'un espace  $\mathcal{H}_2$ . Alors la mesure relativement à la base  $(|e_i\rangle)_i$  d'un système dans l'état  $|\psi\rangle = \sum_i a_i |e_i\rangle |\psi_i\rangle$ , avec  $\sum_i |a_i|^2 = 1$  va renvoyer  $i$  avec probabilité  $|a_i|^2$  et laisser alors le système dans l'état  $|e_i\rangle |\psi_i\rangle$ .

## Portes quantiques

Opérateur	Notation dans un circuit
$I : \begin{cases}  0\rangle \mapsto  0\rangle \\  1\rangle \mapsto  1\rangle \end{cases}$	
$X : \begin{cases}  0\rangle \mapsto  1\rangle \\  1\rangle \mapsto  0\rangle \end{cases}$	
$Z : \begin{cases}  0\rangle \mapsto  0\rangle \\  1\rangle \mapsto - 1\rangle \end{cases}$	
$Y : \begin{cases}  0\rangle \mapsto i 1\rangle \\  1\rangle \mapsto -i 0\rangle \end{cases}$	
$H : \begin{cases}  0\rangle \mapsto \frac{1}{\sqrt{2}}( 0\rangle +  1\rangle) \\  1\rangle \mapsto \frac{1}{\sqrt{2}}( 0\rangle -  1\rangle) \end{cases}$	
$T : \begin{cases}  0\rangle \mapsto  0\rangle \\  1\rangle \mapsto e^{i\pi/4} 1\rangle \end{cases}$	
$R_k : \begin{cases}  0\rangle \mapsto  0\rangle \\  1\rangle \mapsto e^{i\frac{2\pi}{2^k}} 1\rangle \end{cases}$	
$\text{CNOT} : \begin{cases}  0\rangle x\rangle \mapsto  0\rangle x\rangle \\  1\rangle x\rangle \mapsto  1\rangle X x\rangle \end{cases}$	
$\text{c-}U : \begin{cases}  0\rangle x\rangle \mapsto  0\rangle x\rangle \\  1\rangle x\rangle \mapsto  1\rangle U x\rangle \end{cases}$	
$\text{QFT} :  j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}}  k\rangle$	

# Bibliographie

- [AM15] Sam Pallister Ashley Montanaro. Quantum algorithms and the finite element method. *Arxiv*, 2015.
- [AWH09] Seth Lloyd Aram W. Harrow, Avinatan Hassidim. Quantum algorithm for linear systems of equations. *Arxiv*, 2009.
- [CHB92] Stephen J. Wiesner Charles H. Bennett. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Arxiv*, 1992.
- [DD92] Richard Jozsa David Deutsch. Rapid solution of problems by quantum computation. 1992.
- [Deu85] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. 1985.
- [EF14] Sam Gutmann Edward Farhi, Jeffrey Goldstone. A quantum approximate optimization algorithm. *Arxiv*, 2014. Available online at <https://arxiv.org/abs/1411.4028>.
- [JRM15] Ryan Babbush Alán Aspuru-Guzik Jarrod R. McClean, Jonathan Romero. The theory of variational hybrid quantum-classical algorithms. *Arxiv*, 2015. Available online at <https://arxiv.org/abs/1509.04279>.
- [MAN00] Isaac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge, 2000.
- [MM19] Martin Roetteler Margaret Martonosi. Next steps in quantum computing : Computer science's role. *Arxiv*, 2019. Available online at <https://arxiv.org/ftp/arxiv/papers/1903/1903.10541.pdf>.
- [Moo75] Gordon E. Moore. Progress in digital integrated electronics. *IEEE Text Speech*, 1975.
- [PK07] Michele Mosca Phillip Kaye, Raymon Laflamme. *An Introduction to Quantum Computing*. Oxford University Press Inc., New York, 2007.
- [Pre11] John Preskill. Quantum computing and the entanglement frontier. *Arxiv*, 2011. Available online at <https://arxiv.org/abs/1203.5813>.
- [Pre16] John Preskill. Lecture notes for his course on quantum computation (California Institute of Technology). Available online at <http://theory.caltech.edu/people/preskill/ph229/>, 1997-2016.
- [SKL18] Johannes Handsteiner ... Sheng-Kai Liao, Wen-Qi Cai. Satellite-relayed intercontinental quantum network. Available online at <https://arxiv.org/abs/1801.04418>, 2018.
- [Wat06a] John Watrous. Lecture 8 - phase estimation. Available online at <https://cs.uwaterloo.ca/watrous/LectureNotes/CPSC519.Winter2006/08.pdf>, 2006.
- [Wat06b] John Watrous. Lecture 9 - phase estimation and quantum fourier transform. Available online at <https://cs.uwaterloo.ca/watrous/CPSC519/LectureNotes/09.pdf>, 2006.