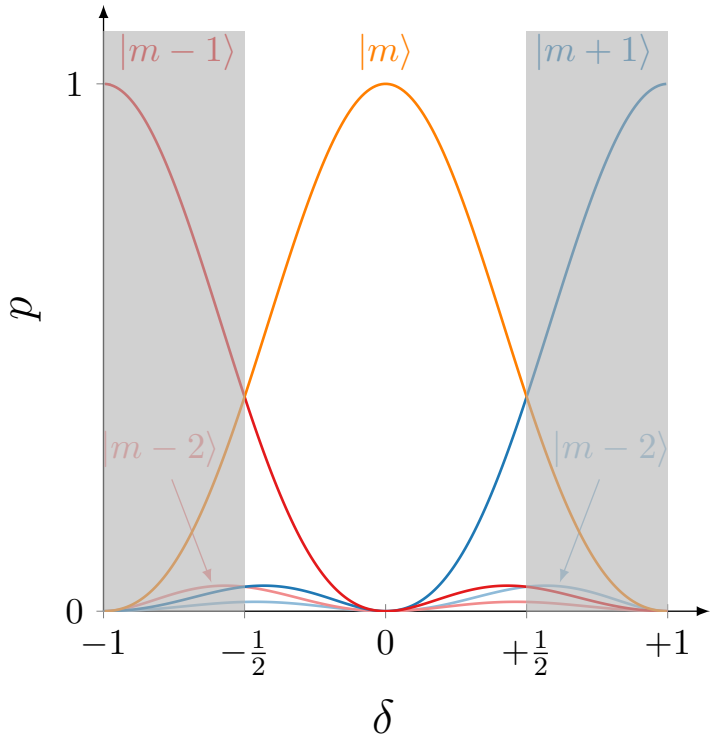
Estimation d'amplitude quantique

Avec la transformée de Fourier quantique
et l'estimation de phase quantique

par

Maxime Dion



Compilé le 10 septembre 2025
Version numérique régulièrement mise à jour.
Pensez-y avant d'imprimer.

AlgoLab Quantique

Institut Quantique

UdS Université de Sherbrooke

Table des matières

Chapitre 1

La transformée de Fourier quantique

La transformée de Fourier quantique ou *Quantum Fourier Transform* (QFT) en anglais est une routine quantique qui trouve des applications dans des algorithmes importants dont l'estimation de phase quantique et la factorisation de grands nombres. Il est donc justifié d'y consacrer du temps et de l'énergie pour bien comprendre cette transformation.

1.1 La transformée de Fourier discrète

La transformée de Fourier peut être formulée et appliquée de plusieurs manières différentes. Dans notre cas, on s'intéressera à sa version discrète. Cette transformée prend un vecteur de N composantes complexes

$$x_0, x_1, \ldots, x_{N-1}$$

et le transforme en un nouveau vecteur comportant autant de nouvelles composantes complexes

$$y_0, y_1, \ldots, y_{N-1}$$

où chacune est obtenue en utilisant la relation

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(2\pi i \frac{kj}{N}\right) x_j. \tag{1.1}$$

Le vecteur des composantes y_k contient alors l'information spectrale contenue dans les composantes x_j.

1.2 La transformée de Fourier comme une transformation unitaire

La QFT implémente une transformée de Fourier discrète (équation 1.1), mais sur un registre quantique, ou plus généralement sur un état quantique. Celle-ci apparait alors comme une transformation unitaire

$$|\tilde{\psi}\rangle = \hat{U}_{\mathrm{QFT}}|\psi\rangle.$$

qui transforme un état $|\psi\rangle$ en un nouvel état $|\tilde{\psi}\rangle$. En particulier, lorsqu'on écrit les états $|\psi\rangle$ et $|\tilde{\psi}\rangle$ sur une base canonique d'états

$$|\tilde{\psi}\rangle = \sum_{k=0}^{N-1} \tilde{\alpha}_k |k\rangle \quad \text{et} \quad |\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle,$$

les composantes $\tilde{\alpha}_k$ de l'état $|\tilde{\psi}\rangle$ sont données par la transformée de Fourier discrète des composantes α_k de l'état $|\psi\rangle$

$$\tilde{\alpha}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(2\pi i \frac{kj}{N}\right) \alpha_j. \tag{1.2}$$

On peut écrire la transformation unitaire de la QFT grâce à la base d'états

$$\hat{U}_{\mathrm{QFT}} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} \exp\left(2\pi i \frac{kj}{N}\right) |k\rangle\langle j|. \tag{1.3}$$

Dans un ordinateur quantique, les états de base $|j\rangle$ (et $|k\rangle$) sont des états à n qubits. Chaque entier représente alors une chaine de bits égale à la forme binaire de l'entier. Le nombre total d'états de bases pour un système de n qubits étant

$$N = 2^n$$

la QFT transforme alors un vecteur avec autant de composantes.

L'objectif des prochaines sections est de mieux comprendre comment la QFT agit pour enfin être capable d'écrire un circuit quantique qui implémente la transformation $\hat{U}_{\mathrm{QFT}}$.

1.3 La QFT d'un état de base

Pour l'état de base $|\psi\rangle = |m\rangle$ la composante à la position m est égale à 1 et toutes les autres sont nulles. Ce qu'on peut écrire comme

$$\alpha_j = \delta_{jm}.$$

Les composantes de l'état résultant de cette transformation sont donc données par,

$$\tilde{\alpha}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(2\pi i \frac{kj}{N}\right) \delta_{jm} = \frac{1}{\sqrt{N}} \exp\left(2\pi i \frac{km}{N}\right).$$

On note $|\tilde{m}\rangle$ l'état résultant de la QFT de l'état $|m\rangle$ et il est donné par

$$|\tilde{m}\rangle = \hat{U}_{\mathrm{QFT}}|m\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{km}{N}\right) |k\rangle.$$

La QFT d'un tel état est donc une superposition de tous les états de base. Cette superposition a la particularité que chacun des états est affecté par une phase donnée par $2\pi\, km/N$.

$$|\tilde{m}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{km}{N}\right) |k\rangle. \tag{1.4}$$

La probabilité de mesurer chacun des états de base $|k\rangle$ est la même

$$\begin{aligned} |\langle j|\tilde{m}\rangle|^2 &= \left| \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{km}{N}\right) \langle j|k\rangle \right|^2 \\ &= \left| \frac{1}{\sqrt{N}} \exp\left(2\pi i \frac{jm}{N}\right) \right|^2 = \frac{1}{N}. \end{aligned}$$

La transformée de Fourier d'un état général sera la superposition des QFT des états de base

$$|\tilde{\psi}\rangle = \hat{U}_{\mathrm{QFT}}|\psi\rangle = \sum_{k=0}^{N-1} \alpha_k \hat{U}_{\mathrm{QFT}}|k\rangle = \sum_{k=0}^{N-1} \alpha_k |\tilde{k}\rangle.$$

1.4 États des qubits

Par construction, les états de base $|k\rangle$ sont des états produits. En effet, on peut écrire chacun d'eux comme le produit tensoriel des états individuels des qubits

$$|k\rangle = |b_{k(n-1)} \dots b_{k1} b_{k0}\rangle = \bigotimes_{q=0}^{n-1} |b_{kq}\rangle \tag{1.5}$$

où chacun des qubits est soit dans l'état $|0\rangle$ ou dans l'état $|1\rangle$. Autrement dit $b_{kq} \in \{0, 1\}$. Par exemple, pour 3 qubits, le tenseur b_{kq} prend les valeurs

$$k \in \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{pmatrix} \qquad \text{et} \qquad b_{kq} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

La valeur de l'entier k et liée aux valeurs des b_{kq} par

$$k = \sum_{q=0}^{n-1} b_{kq} 2^q. \tag{1.6}$$

ou encore

$$\frac{k}{N} = \sum_{q=0}^{n-1} \frac{b_{kq}}{2^{n-q}}. \tag{1.7}$$

car $N = 2^n$.

Ce qui est moins évident est que l'état quantique $|\tilde{m}\rangle$, résultant de la QFT d'un état de base, est également un état produit. Nous allons maintenant démontrer cela. Pour ce faire, on doit remplacer les formes 1.5 et 1.7 dans l'équation 1.4. Avant de pouvoir faire cela, on doit être en mesure de remplacer la somme sur les entiers en sommes sur les qubits. La somme de tous les entiers de 0 jusqu'à $2^n - 1$ peut être remplacée par n sommes sur 0 et 1 imbriquées

$$\sum_{k=0}^{N-1} (\dots) \equiv \sum_{b_{k0}=0}^{1} \sum_{b_{k1}=0}^{1} \dots \sum_{b_{k(n-1)}=0}^{1} (\dots).$$

On peut facilement se convaincre qu'il y a autant de termes des deux côtés de l'équation et que chaque terme k du côté gauche correspond à une des 2^n combinaisons possibles de b_{kq} du côté droit. Il est donc possible d'exprimer la QFT d'un état de base $|m\rangle$ comme étant

$$|\tilde{m}\rangle = \frac{1}{\sqrt{N}} \sum_{b_{k0}=0}^{1} \sum_{b_{k1}=0}^{1} \dots \sum_{b_{k(n-1)}=0}^{1} \exp\left(2\pi i m \sum_{q=0}^{n-1} \frac{b_{kq}}{2^{n-q}}\right) \bigotimes_{q=0}^{n-1} |b_{kq}\rangle.$$

On doit ensuite effectuer quelques manipulations pour montrer que $|\tilde{m}\rangle$ est bien un état produit. D'abord, l'exponentielle d'une somme est un produit d'exponentielles

$$\exp\left(2\pi i m \sum_{q=0}^{n-1} \frac{b_{kq}}{2^{n-q}}\right) = \prod_{q=0}^{n-1} \exp\left(2\pi i \frac{m b_{kq}}{2^{n-q}}\right). \tag{1.8}$$

Pour chaque terme dans ce produit, il y a un terme associé dans le produit tensoriel. On les assemble deux à deux pour écrire

$$\prod_{q=0}^{n-1} \exp\Big(2\pi i \frac{m b_{kq}}{2^{n-q}}\Big) \bigotimes_{q'=0}^{n-1} |b_{kq'}\rangle = \bigotimes_{q=0}^{n-1} \exp\Big(2\pi i \frac{m b_{kq}}{2^{n-q}}\Big) |b_{kq}\rangle$$

que l'on peut remplacer dans l'expression de l'état transformé

$$|\tilde{m}\rangle = \frac{1}{\sqrt{2^n}} \sum_{b_{k0}=0}^{1} \sum_{b_{k1}=0}^{1} \cdots \sum_{b_{k(n-1)}=0}^{1} \bigotimes_{q=0}^{n-1} \exp\Big(2\pi i \frac{m b_{kq}}{2^{n-q}}\Big) |b_{kq}\rangle.$$

Ensuite, comme chacun de termes dans le produit tensoriel ne dépend que d'un seul b_{kq}, chacune des sommes sur les états des qubits peut être incorporée dans le produit tensoriel (voir la section 1.9 pour vous en convaincre). On écrit alors

$$|\tilde{m}\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} \sum_{b_{kq}=0}^{1} \exp\Big(2\pi i \frac{m b_{kq}}{2^{n-q}}\Big) |b_{kq}\rangle$$

Il est alors possible d'effectuer la somme explicitement. Lorsque $b_{kq} = 0$, la phase est nulle. Dans l'autre cas ($b_{kq} = 1$), la phase est proportionnelle à m,

$$|\tilde{m}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}} \Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{n-q}}\Big)|1\rangle\Big) \tag{1.9}$$

On voit alors qu'il est possible d'écrire l'état $|\tilde{m}\rangle$ comme un état produit

$$|\tilde{m}\rangle = \bigotimes_{q=0}^{n-1} |\tilde{b}_{mq}\rangle \tag{1.10}$$

où on identifie l'état du qubit q après la QFT comme étant

$$|\tilde{b}_{mq}\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{n-q}}\Big)|1\rangle\Big). \tag{1.11}$$

En résumé, pour un état de base construit comme un état produit où chaque qubit est soit dans l'état $|0\rangle$ ou l'état $|1\rangle$ (équation 1.5), la QFT est également un état produit (équation 1.10) où chaque qubit est dans l'état donné à l'équation 1.11.

Terminons cette section en combinant les équations 1.4 et 1.9 pour établir la relation suivante

$$|\tilde{m}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\Big(2\pi i \frac{km}{N}\Big)|k\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}} \Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{n-q}}\Big)|1\rangle\Big) \tag{1.12}$$

c'est-à-dire que l'état résultant de la QFT d'un état de base peut être écrit à la fois comme une combinaison linéaire des états base, mais également comme un état produit sur les états des qubits individuels.

1.5 Circuit QFT état de base

Tentons maintenant d'assembler un circuit quantique qui permet de préparer l'état $|\tilde{m}\rangle$. Il semble évident que pour préparer l'état $|\tilde{m}\rangle$ dans un registre quantique initialisé dans l'état $|0\rangle^{\otimes n}$, on pourrait débuter en appliquant une porte Hadamard sur chacun des qubits afin de préparer l'état

$$|+\rangle^{\otimes n} = \hat{H}^{\otimes n}|0\rangle^{\otimes n} = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

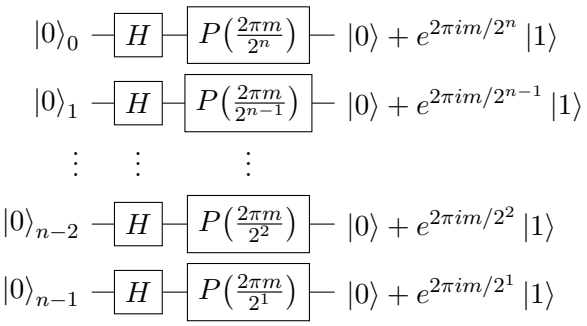


FIGURE 1.1 – Circuit pour préparer l'état $|\tilde{m}\rangle$ avec m connu. L'état final est écrit en omettant le facteur de normalisation.

et ensuite appliquer des phases $2\pi m/2^{n-q}$ sur chacun des ceux-ci tel que

$$\left(\bigotimes_{q=0}^{n-1} \hat{P}(2\pi \frac{m}{2^{n-q}})\right)|+\rangle^{\otimes n} = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{n-q}}\Big)|1\rangle\Big).$$

Le circuit à la figure 1.1 accomplit cela. Le qubit $q = 0$ subit la plus petite phase égale à $2\pi m/2^n$. Les qubits suivants subissent des phases toujours deux fois plus grandes que le qubit précédent, qui culmine avec une phase de $2\pi m/2$ pour le dernier qubit.

Il est intéressant de voir comment ce circuit peut être construit si m est donné sous sa forme binaire b_{mr} tel que

$$m = \sum_{r=0}^{n-1} b_{mr} 2^r. \tag{1.13}$$

Écrivons $|\tilde{m}\rangle$ en fonction des b_{mr} en remplaçant l'équation 1.13 dans l'équation 1.9. On obtient

$$|\tilde{m}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(2\pi i \sum_{r=0}^{n-1} \frac{b_{mr}}{2^{n-q-r}}\right)|1\rangle\right).$$

Écrivons l'exponentielle de la somme comme un produit d'exponentielles

$$|\tilde{m}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\left(|0\rangle + \prod_{r=0}^{n-1} \exp(\frac{2\pi i}{2^{n-q-r}} b_{mr})|1\rangle\right).$$

On constate que pour préparer cet état à partir de l'état $|+\rangle^{\otimes n}$, on peut appliquer une série de phases $\hat{P}(\frac{2\pi}{2^{n-q-r}} b_{mr})$ sur chacun des qubits. Notons que b_{mr} ne peut prendre que les valeurs 0 et 1. Ainsi, une phase non nulle sera appliquée si $b_{mr} = 1$, alors qu'une phase nulle sera appliquée si $b_{mr} = 0$. On constate également que toutes les phases avec $r + q \geq n$ sont multiples entiers de 2π. On peut donc omettre celles-ci ce qui diminue le nombre de termes dans le produit

$$|\tilde{m}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\left(|0\rangle + \prod_{r=0}^{n-q-1} \hat{P}(\frac{2\pi}{2^{n-q-r}} b_{mr})|1\rangle\right).$$

Sous cette forme, on voit que le circuit de la figure 1.1 peut être remplacé par le circuit de la figure 1.2.

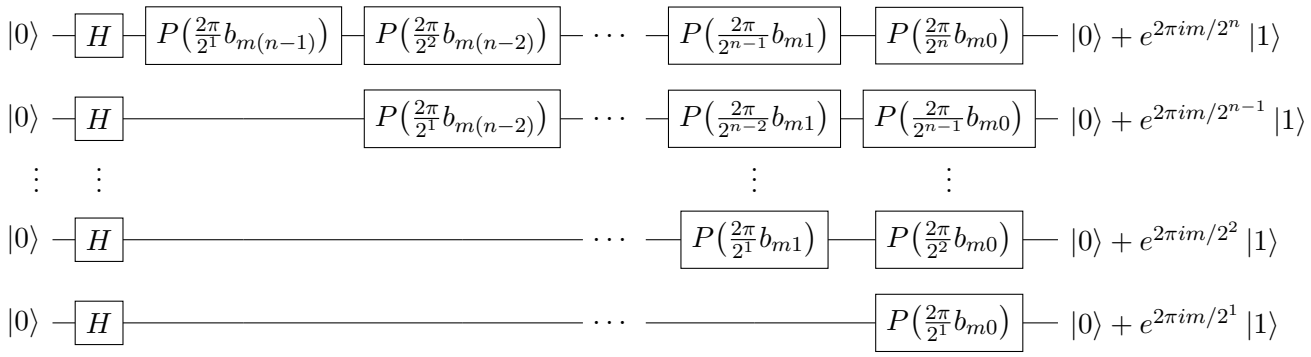


FIGURE 1.2 – Circuit pour préparé l'état $|\tilde{m}\rangle$ avec m connu, phases en puissance de $\frac{1}{2}$.

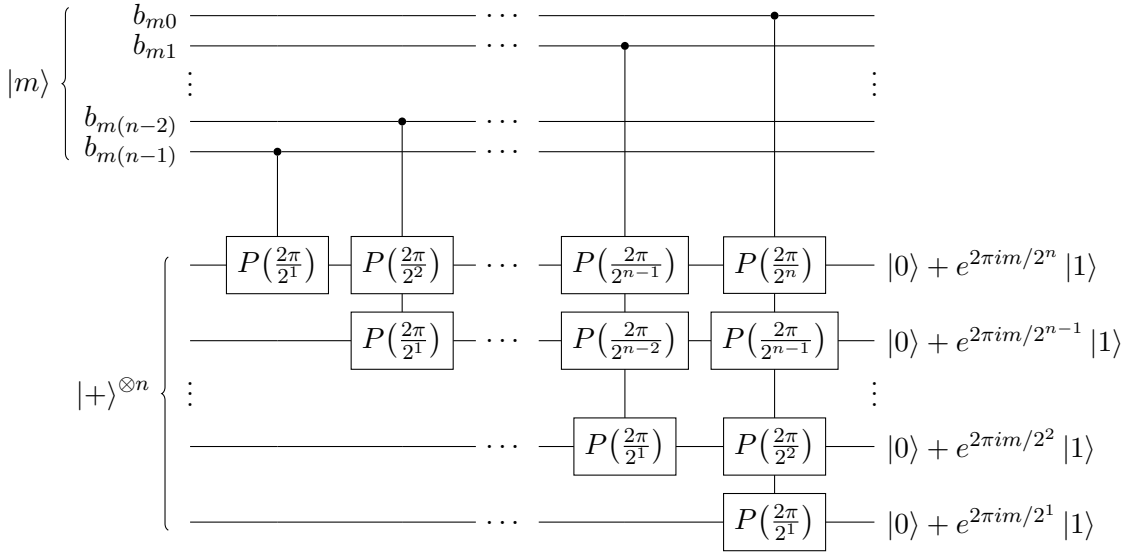


FIGURE 1.3 – Circuit pour préparer l'état $|\tilde{m}\rangle$ avec $|m\rangle$ inconnu, mais dans un autre registre.

1.6 Circuit QFT état de base quelconque

Il est alors intéressant de constater que chacune de porte de phase au circuit de la figure 1.2 est « contrôlée » par la valeur d'un bit classique. Aussi, la manière avec laquelle on a construit le circuit fait en sorte que toutes les portes de phases qui sont dans la même colonne sont contrôlées par le même bit classique.

On peut remplacer ces portes de phases en véritables portes de phase contrôlées en ajoutant un autre registre quantique sur lequel on encode les valeurs de bits classiques sur chacun des qubits qui contrôleront ces phases. Ce faisant, on obtient le circuit présenté à la figure 1.3. Ce circuit permet en fait de préparer $|\tilde{m}\rangle$ dans le second registre pour n'importe quel état $|m\rangle$ dans le premier. Si on écrit la transformation unitaire qu'applique ce circuit, on obtient bien

$$\hat{U}(|+\rangle^{\otimes n} \otimes |m\rangle) = (|\tilde{m}\rangle \otimes |m\rangle). \tag{1.14}$$

Est-il alors possible de préparer la transformée de Fourier à partir d'un état quantique arbitraire (une superposition de plusieurs états de base) qu'on aurait encodé dans le premier registre ? Malheureusement, non. En effet, on constate que si on prépare une combinaison linéaire des $|j\rangle$ dans le premier registre et

on obtient les $|\tilde{j}\rangle$ dans le second registre,

$$\begin{aligned}\hat{U}(|+\rangle^{\otimes n} \otimes \sum_{j=0}^{N-1} \alpha_j |j\rangle) &= \hat{U} \sum_{j=0}^{N-1} \alpha_j (|+\rangle^{\otimes n} \otimes |j\rangle) \\ &= \sum_{j=0}^{N-1} \alpha_j \hat{U}(|+\rangle^{\otimes n} \otimes |j\rangle) \\ &= \sum_{j=0}^{N-1} \alpha_j (|\tilde{j}\rangle \otimes |j\rangle).\end{aligned}$$

Seul problème : chaque $|\tilde{j}\rangle$ est enchevêtré avec le $|j\rangle$ associé, alors qu'on cherche à obtenir l'état

$$\sum_{j=0}^{N-1} \alpha_j |\tilde{j}\rangle$$

directement. Pour résoudre ce problème, on va tenter de se débarrasser du premier registre en modifiant ce circuit.

1.7 Circuit QFT avec un seul registre

Considérons d'abord le dernier qubit du second registre. Ce qubit est d'abord dans l'état $|+\rangle$ et on y applique ensuite une phase de π si $b_{m0} = 1$. La dernière ligne de la figure 1.3 indique plutôt que l'état du qubit est en fait affecté d'une phase $2\pi m/2$. En fait, ces deux expressions sont équivalentes. En effet,

$$\begin{aligned}\frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i m/2}|1\rangle\Big) &= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{\pi i \sum_{q=0}^{n-1} b_{mq} 2^q}|1\rangle\Big) \\ &= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{\pi i (b_{m0} + 2b_{m1} + 4b_{m2} + \ldots)}|1\rangle\Big) \\ &= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{\pi i b_{m0}}|1\rangle\Big).\end{aligned} \tag{1.15}$$

où dernière égalité est vérifiée parce que les autres bits qui forme m génèrent des rotations entières de 2π.

Ce qubit est donc dans l'état $|+\rangle$ si $b_{m0} = 0$ et dans l'état $|-\rangle$ si $b_{m0} = 1$. Or, on peut préparer directement ce même état dans le premier qubit du premier registre en y appliquant une simple porte Hadamard comme cela est illustré à la figure 1.4. En effet, on a l'égalité suivante

$$\hat{P}(b_{0m}\pi)|+\rangle = \hat{H}|b_{0m}\rangle \tag{1.16}$$

qui implique que le premier et le dernier qubit sont exactement dans le même état ! Ce faisant, le dernier qubit devient inutile et on l'élimine pour obtenir le circuit de la figure 1.5.

Peut-on éliminer d'autres qubits ? La réponse est oui ! En effet, on constate que la première phase contrôlée de l'avant-dernier qubit est également une phase de π qui dépend de la valeur de b_{1m}, valeur de l'état du second qubit. On peut donc rediriger l'état préparé sur l'avant-dernier qubit du second registre vers le second qubit du premier registre grâce à

$$\hat{P}(b_{1m}\pi)|+\rangle = \hat{H}|b_{1m}\rangle. \tag{1.17}$$

Ensuite, pour obtenir l'état recherché

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i m/2^2}|1\rangle\Big)$$

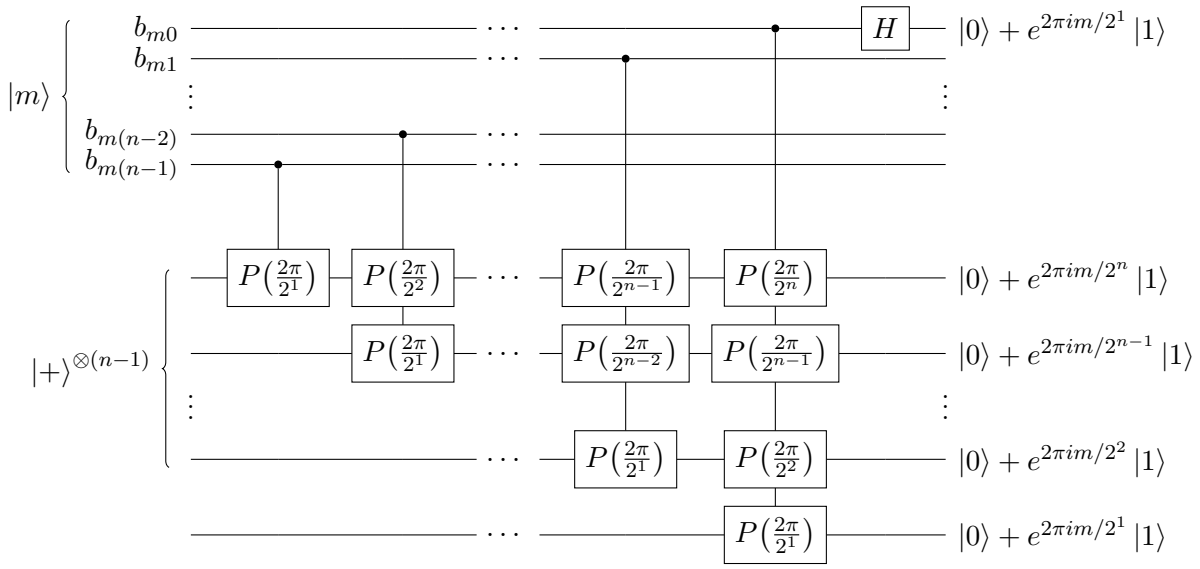


FIGURE 1.4 – Le premier et le dernier qubit sont exactement dans le même état.

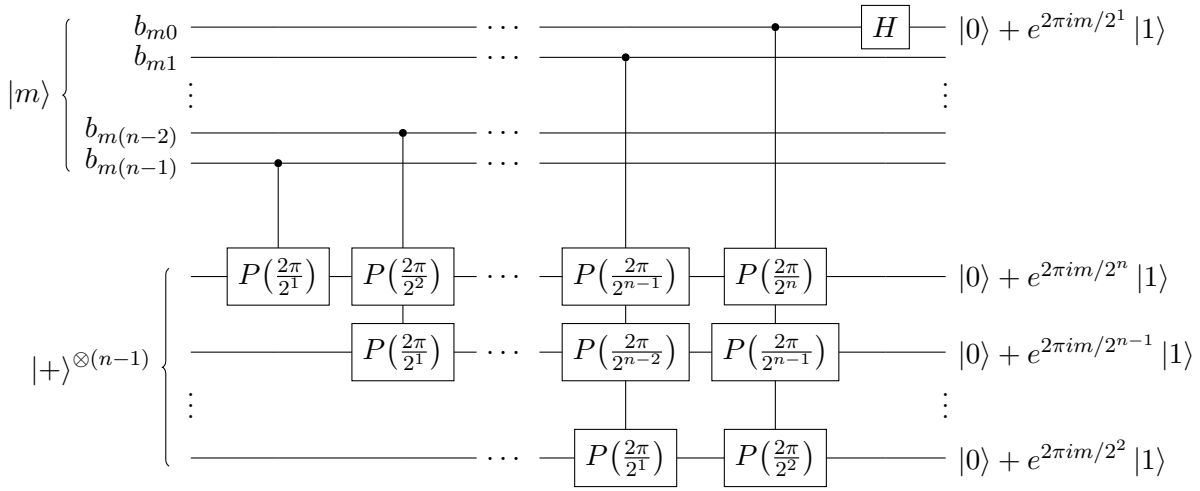


FIGURE 1.5 – Élimination d'un premier qubit.

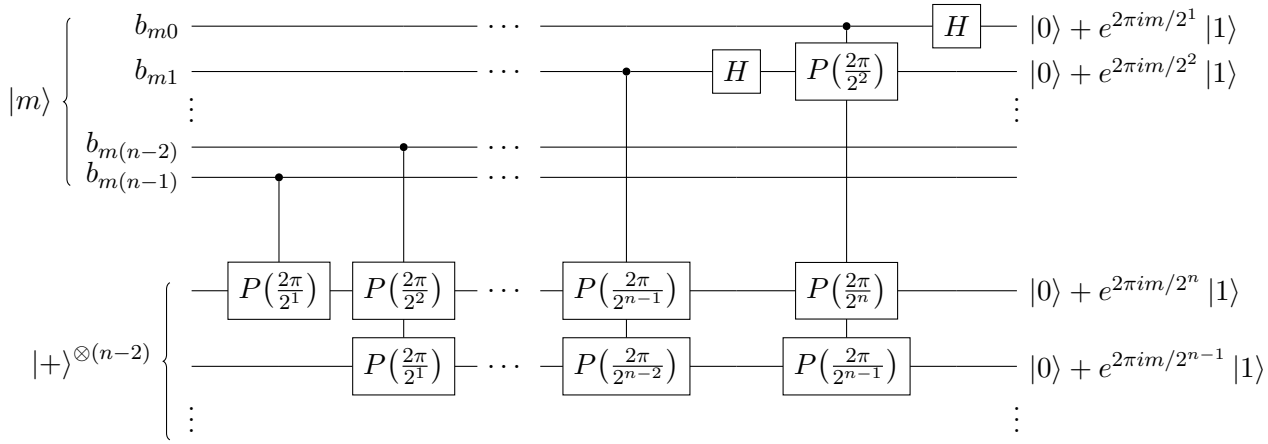


FIGURE 1.6 – Élimination d'un second qubit.

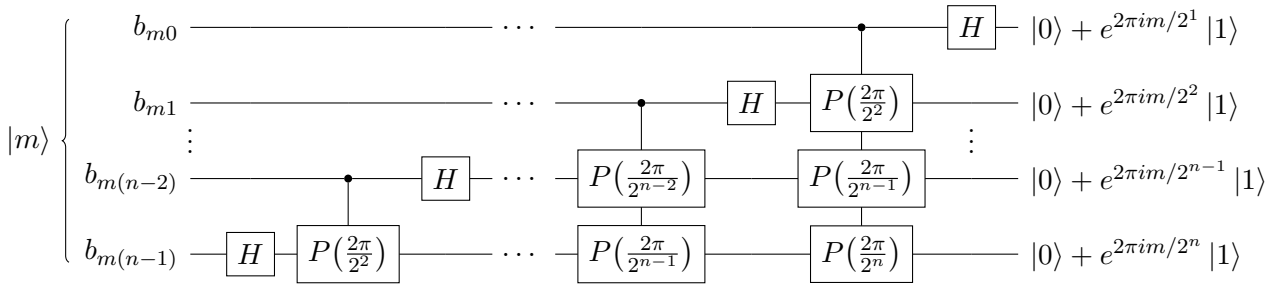


FIGURE 1.7 – Circuit pour préparer l'état $|\tilde{m}\rangle$ à partir $|m\rangle$ inconnu avec un seul registre.

sur le deuxième qubit, on doit également rediriger la phase contrôlée par le premier qubit pour obtenir le circuit de la figure 1.6 sur lequel on a déjà éliminé le qubit redondant.

On peut continuer d'appliquer ce processus sur tous les autres qubits pour obtenir le circuit de la figure 1.7. Ce circuit, à partir de l'état $|m\rangle$, prépare l'état produit

$$\bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{q+1}}\Big)|1\rangle\Big). \tag{1.18}$$

On constate une différence avec le résultat souhaité de l'équation 1.11,

$$|\tilde{b}_{mq}\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\Big(2\pi i \frac{m}{2^{n-q}}\Big)|1\rangle\Big). \tag{1.11}$$

c'est-à-dire que l'ordre des qubits est inversé. En effet, pour l'équation 1.11 la phase du premier qubit est $2\pi m/2^n$ alors que pour l'équation 1.18, c'est le dernier qubit qui possède cette phase.

On pourrait corriger cela en appliquant une série de portes SWAP. En pratique, cela est rarement nécessaire et une simple réindexation des qubits est beaucoup moins couteuse.

Finalement, en se débarrassant d'un registre on élimine le problème d'enchevêtrement et le circuit de la figure 1.7 peut effectuer la QFT d'un état général

$$\begin{aligned}\hat{U}_{\mathrm{QFT}}|\psi\rangle = \hat{U}_{\mathrm{QFT}} \sum_{j=0}^{N-1} \alpha_j |j\rangle &= \sum_{j=0}^{N-1} \alpha_j \hat{U}_{\mathrm{QFT}}|j\rangle \\ &= \sum_{j=0}^{N-1} \alpha_j |\tilde{j}\rangle \\ &= |\tilde{\psi}\rangle.\end{aligned}$$

1.8 Addition quantique avec la QFT

Une application intéressante de la QFT est l'addition d'entiers.

Soit deux entiers x et y, on veut calculer leur somme $z = x + y$ grâce à un ordinateur quantique. On peut utiliser la QFT pour effectuer une telle opération. Supposons que l'état $|x\rangle$ est l'état initial de notre ordinateur quantique. Cet état est facile à préparer en appliquant des portes $\hat{X}$ sur les différents qubits en suivant la représentation binaire de x. On cherche donc à préparer l'état

$$|z\rangle = |x + y\rangle$$

On applique d'abord la QFT pour préparer l'état

$$|\tilde{x}\rangle = \hat{U}_{\mathrm{QFT}}|x\rangle.$$

On utilise la version sans SWAP de sorte que l'état obtenu est

$$|\tilde{x}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\Big(|0\rangle + \exp(2\pi i \frac{x}{2^{q+1}})|1\rangle\Big). \tag{1.19}$$

Si on arrive à obtenir l'état $|\tilde{z}\rangle$, on n'aura qu'à effectuer la QFT inverse pour obtenir $|z\rangle$. Cet état est simplement,

$$|\tilde{z}\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\left(|0\rangle + \exp(2\pi i \frac{x+y}{2^{q+1}})|1\rangle\right) \tag{1.20}$$

$$= \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\Big(|0\rangle + \exp(2\pi i \frac{y}{2^{q+1}})\exp(2\pi i \frac{x}{2^{q+1}})|1\rangle\Big). \tag{1.21}$$

Donc à partir de $|\tilde{x}\rangle$ on doit simplement appliquer une série de phases sur chacun des qubits qui dépendent de y. Autrement dit,

$$\begin{aligned}|\tilde{z}\rangle &= \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}\hat{P}\Big(2\pi\frac{y}{2^{q+1}}\Big)(|0\rangle + \exp(2\pi i \frac{x}{2^{q+1}})|1\rangle) \\ &= \left(\bigotimes_{q=0}^{n-1} \hat{P}\Big(2\pi\frac{y}{2^{q+1}}\Big)\right)|\tilde{x}\rangle.\end{aligned}$$

Il ne reste plus qu'à effectuer la transformée inverse (la version sans SWAP) pour obtenir

$$|z\rangle = \hat{U}_{\text{QFT}}^{\dagger}\left(\bigotimes_{q=0}^{n-1} \hat{P}\Big(2\pi\frac{y}{2^{q+1}}\Big)\right)\hat{U}_{\text{QFT}}|x\rangle.$$

Ainsi le circuit d'addition est

$$\hat{U}_{\text{ADD}}(y) = \hat{U}_{\text{QFT}}^{\dagger}\left(\bigotimes_{q=0}^{n-1} \hat{P}\Big(2\pi\frac{y}{2^{q+1}}\Big)\right)\hat{U}_{\text{QFT}}. \tag{1.22}$$

Si on utilise la QFT avec SWAP, l'ordre des qubits doit simplement être inversé

$$\hat{U}_{\text{ADD}}(y) = \hat{U}_{\text{QFT}}^{\dagger}\left(\bigotimes_{q=0}^{n-1} \hat{P}\Big(2\pi\frac{y}{2^{n-q}}\Big)\right)\hat{U}_{\text{QFT}}.$$

1.9 Exemple de factorisation des états à un qubit pour une QFT sur trois qubits

Nous allons illustrer comment l'état résultant de la transformée de Fourier d'un état quantique de base peut être écrit comme un état produit faisant intervenir les états individuels de chacun des qubits. Nous allons faire cela en considérant un exemple simple à trois qubits. D'abord l'équation 1.4 écrite explicitement pour 3 qubits est

$$\begin{aligned}|\tilde{m}\rangle &= \frac{1}{\sqrt{8}}\sum_{k=0}^{7}\exp\Big(2\pi i\frac{km}{8}\Big)|k\rangle \\ &= \frac{1}{\sqrt{8}}(\exp\Big(2\pi i\frac{0}{8}m\Big)|0\rangle + \exp\Big(2\pi i\frac{1}{8}m\Big)|1\rangle + \ldots + \exp\Big(2\pi i\frac{6}{8}m\Big)|6\rangle + \exp\Big(2\pi i\frac{7}{8}m\Big)|7\rangle).\end{aligned}$$

Il il a $2^3 = 8$ termes dans cette somme. Chaque état $|k\rangle$ est un état de base à 3 qubits. Explicitons cela,

$$|\tilde{m}\rangle = \frac{1}{\sqrt{8}}\left(\exp\left(2\pi i\frac{0}{8}m\right)|000\rangle + \exp\left(2\pi i\frac{1}{8}m\right)|001\rangle + \dots \right.$$
$$\left. + \exp\left(2\pi i\frac{6}{8}m\right)|110\rangle + \exp\left(2\pi i\frac{7}{8}m\right)|111\rangle\right).$$

En même temps, les entiers 0 à 7 peuvent être écrits sous forme binaire également

$$|\tilde{m}\rangle = \frac{1}{\sqrt{8}}\left(\exp\left(2\pi i\frac{0\times 2^2+0\times 2^1+0\times 2^0}{8}m\right)|000\rangle + \exp\left(2\pi i\frac{0\times 2^2+0\times 2^1+1\times 2^0}{8}m\right)|001\rangle + \dots \right.$$
$$\left. + \exp\left(2\pi i\frac{1\times 2^2+1\times 2^1+0\times 2^0}{8}m\right)|110\rangle + \exp\left(2\pi i\frac{1\times 2^2+1\times 2^1+1\times 2^0}{8}m\right)|111\rangle\right). \tag{1.23}$$

Chaque terme dans la somme a alors une forme

$$\exp\left(2\pi i\frac{b_{j2}\times 2^2 + b_{j1}\times 2^1 + b_{j0}\times 2^0}{8}m\right)|b_{j2}b_{j1}b_{j0}\rangle = \exp\left(2\pi i\frac{\sum_{q=0}^{2} b_{jq}2^q}{8}m\right)\bigotimes_{q=0}^{2}|b_{jq}\rangle$$

On peut transformer les exponentielles de sommes et produits d'exponentielles

$$\exp\left(2\pi i\frac{\sum_{q=0}^{2} b_{jq}2^q}{8}m\right)\bigotimes_{q=0}^{2}|b_{jq}\rangle = \left(\prod_{q=0}^{2}\exp\left(2\pi i\frac{b_{jq}2^q}{8}m\right)\right)\left(\bigotimes_{q'=0}^{2}|b_{jq'}\rangle\right)$$

où on prend soin d'utiliser des indices différents pour les deux produits. La phase totale est donc une somme de 3 phases, chacune associée à un qubit ce qui nous permet d'écrire

$$\left(\prod_{q=0}^{2}\exp\left(2\pi i\frac{b_{jq}2^q}{8}m\right)\right)\left(\bigotimes_{q=0}^{2}|b_{jq}\rangle\right) = \bigotimes_{q=0}^{2}\exp\left(2\pi i\frac{b_{jq}2^q}{8}m\right)|b_{jq}\rangle$$

Par exemple pour le terme associé à $|5\rangle$

$$\begin{aligned}\exp\left(2\pi i\frac{5}{8}m\right)|5\rangle &= \exp\left(2\pi i\frac{1\times 2^2+0\times 2^1+1\times 2^0}{8}m\right)|101\rangle \\ &= \left(\exp\left(2\pi i\frac{1\times 2^2}{8}m\right)\exp\left(2\pi i\frac{0\times 2^1}{8}m\right)\exp\left(2\pi i\frac{1\times 2^0}{8}m\right)\right)(|1\rangle\otimes|0\rangle\otimes|1\rangle) \\ &= \left[\exp\left(2\pi i\frac{1\times 2^2}{8}m\right)|1\rangle\right]\otimes\left[\exp\left(2\pi i\frac{0\times 2^1}{8}m\right)|0\rangle\right]\otimes\left[\exp\left(2\pi i\frac{1\times 2^0}{8}m\right)|1\rangle\right].\end{aligned}$$

Cet état est un état produit ; un simple produit tensoriel entre 3 qubits. Le terme associé à $|4\rangle$ diffère uniquement pour le qubit de droite

$$\exp\left(2\pi i\frac{4}{8}m\right)|4\rangle = \left[\exp\left(2\pi i\frac{1\times 2^2}{8}m\right)|1\rangle\right]\otimes\left[\exp\left(2\pi i\frac{0\times 2^1}{8}m\right)|0\rangle\right]\otimes\left[\exp\left(2\pi i\frac{0\times 2^0}{8}m\right)|0\rangle\right].$$

Rappelons-nous qu'on cherche à réécrire la somme de l'équation 1.23 sous la forme d'un état produit. Avant de considérer la somme des huit termes, considérons la somme des termes associés à $|4\rangle$ et $|5\rangle$. On voit que les 2 qubits de gauche sont exactement dans les mêmes états pour ces termes. On peut factoriser les deux premiers qubits pour ces 2 états

$$\exp\left(2\pi i\frac{4}{8}m\right)|4\rangle + \exp\left(2\pi i\frac{5}{8}m\right)|5\rangle = \left[\exp\left(2\pi i\frac{1\times 2^2}{8}m\right)|1\rangle\right]\otimes\left[\exp\left(2\pi i\frac{0\times 2^1}{8}m\right)|0\rangle\right]$$
$$\otimes\left[\exp\left(2\pi i\frac{0\times 2^0}{8}m\right)|0\rangle + \exp\left(2\pi i\frac{1\times 2^0}{8}m\right)|1\rangle\right].$$

On peut faire cela pour les paires d'états $(0,1)$, $(2,3)$, $(4,5)$ et $(6,7)$ et ainsi complètement factoriser le qubit de droite. Si on considère ensuite la somme des termes 4, 5, 6 et 7, on peut alors factoriser le qubit du centre. En effet,

$$\begin{aligned}
&\exp\left(2\pi i\frac{4}{8}m\right)|4\rangle + \exp\left(2\pi i\frac{5}{8}m\right)|5\rangle + \exp\left(2\pi i\frac{6}{8}m\right)|6\rangle + \exp\left(2\pi i\frac{7}{8}m\right)|7\rangle \\
&\quad = [\exp\left(2\pi i\tfrac{1\times 2^2}{8}m\right)|1\rangle] \otimes [\exp\left(2\pi i\tfrac{0\times 2^1}{8}m\right)|0\rangle + \exp\left(2\pi i\tfrac{1\times 2^1}{8}m\right)|1\rangle] \\
&\quad\quad \otimes [\exp\left(2\pi i\tfrac{0\times 2^0}{8}m\right)|0\rangle + \exp\left(2\pi i\tfrac{1\times 2^0}{8}m\right)|1\rangle].
\end{aligned}$$

On peut faire l'équivalent pour les termes 0, 1, 2 et 3. Finalement, pour la somme complète des huit termes, on peut factoriser le qubit de gauche. On peut donc complètement factoriser les 3 qubits

$$\begin{aligned}
|\tilde{m}\rangle &= \frac{1}{\sqrt{8}}\Big(\exp\left(2\pi i\tfrac{0\times 2^2+0\times 2^1+0\times 2^0}{8}m\right)|000\rangle + \exp\left(2\pi i\tfrac{0\times 2^2+0\times 2^1+1\times 2^0}{8}m\right)|001\rangle + \dots \\
&\qquad + \exp\left(2\pi i\tfrac{1\times 2^2+1\times 2^1+0\times 2^0}{8}m\right)|110\rangle + \exp\left(2\pi i\tfrac{1\times 2^2+1\times 2^1+1\times 2^0}{8}m\right)|111\rangle\Big) \\
&= \frac{1}{\sqrt{2}}[\exp\left(2\pi i\tfrac{0\times 2^2}{8}m\right)|0\rangle + \exp\left(2\pi i\tfrac{1\times 2^2}{8}m\right)|1\rangle] \\
&\qquad \otimes [\exp\left(2\pi i\tfrac{0\times 2^1}{8}m\right)|0\rangle + \exp\left(2\pi i\tfrac{1\times 2^1}{8}m\right)|1\rangle] \\
&\qquad \otimes [\exp\left(2\pi i\tfrac{0\times 2^0}{8}m\right)|0\rangle + \exp\left(2\pi i\tfrac{1\times 2^0}{8}m\right)|1\rangle].
\end{aligned}$$

L'état $|\tilde{m}\rangle$ est donc construit en effectuant le produit tensoriel des 3 qubits $\bigotimes|\tilde{b}_{mq}\rangle$. Chaque qubit étant dans l'état de l'équation 1.11

$$|\tilde{b}_{mq}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp\left(2\pi i\frac{2^q}{8}m\right)|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + \exp\left(2\pi i\frac{m}{2^{n-q}}\right)|1\rangle).$$

Chapitre 2

Estimation de phase quantique

Soit un opérateur unitaire $\hat{Q}$ avec un de ses états propres $|q\rangle$ répondant à l'équation aux valeurs propres

$$\hat{Q}|q\rangle = e^{2\pi i\varphi}|q\rangle,$$

l'estimation de phase permet d'estimer la valeur de φ à partir d'un registre Q qui contient l'état $|q\rangle$

$$|\psi_Q\rangle = |q\rangle.$$

Notons que, sous cette forme, la phase φ prendre une valeur entre 0 et 1.

Remarque

Pour introduire plus facilement l'estimation de phase, nous allons nous placer dans des conditions irréalistes, c'est-à-dire que nous allons d'abord supposer que l'état propre $|q\rangle$ est déjà préparé dans un registre quantique. Ensuite, nous supposerons que la phase φ peut être exprimée exactement que le ratio d'un entier m sur une puissance de 2. Notons cette phase

$$\varphi = \frac{m}{2^n}.$$

Plus tard, à la section 2.4 nous lèverons ces contraintes.

2.1 Retour de phase

Pour tenter d'obtenir de l'information sur la phase φ, on pourrait appliquer $\hat{Q}$ sur $|q\rangle$, mais cela ne génère qu'une phase globale impossible à extraire via des mesures du qubit. C'est pour cela qu'on doit utiliser le retour de phase.

Pour introduire le retour de phase, considérons un second registre P (pour phase) contenant un seul qubit dans l'état $|+\rangle$

$$|\psi_P\rangle = |+\rangle$$

et appliquons une version contrôlée par $|\psi_P\rangle$ de l'opérateur $\hat{Q}$ sur $|\psi_Q\rangle$ comme illustré à la figure 2.1. Cette

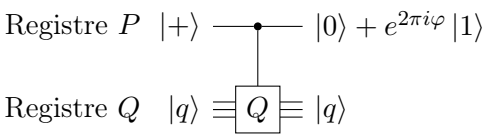


FIGURE 2.1 – Circuit de retour de phase pour un opérateur $\hat{Q}$.

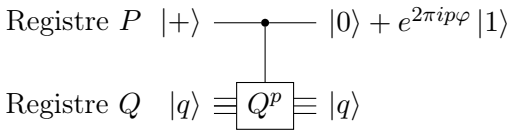


FIGURE 2.2 – Circuit de retour de phase pour une puissance de l'opérateur $\hat{Q}$.

opération produit l'état

$$\begin{aligned} C\hat{Q}|\psi\rangle &= \frac{1}{\sqrt{2}}(C\hat{Q}|q\rangle|0\rangle + C\hat{Q}|q\rangle|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|q\rangle|0\rangle + e^{2\pi i\varphi}|q\rangle|1\rangle) \\ &= |q\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\varphi}|1\rangle). \end{aligned} \tag{2.1}$$

L'état $|q\rangle$ n'est pas affecté par cette opération, alors que le qubit de contrôle accumule une phase relative $2\pi\varphi$. Il est maintenant possible d'obtenir de l'information sur cette phase en effectuant des mesures sur le qubit de contrôle. Ne nous attardons pas tout de suite à comment on pourrait effectuer cela.

Pour l'instant, contentons-nous de constater que si on applique la même porte contrôlée plusieurs fois, on accumule un multiple de la phase

$$(C\hat{Q})^p|\psi\rangle = |q\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi ip\varphi}|1\rangle).$$

Finalement, notons qu'on obtient le même résultat en appliquant une version contrôlée d'une puissance de l'opérateur $\hat{Q}$

$$C\hat{Q}^p|\psi\rangle = |q\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi ip\varphi}|1\rangle) \tag{2.2}$$

comme c'est illustré à la figure 2.2. Cela nous sera utile pour la suite.

2.2 Exploiter la QFT

On sait depuis la section 1.4 que la QFT permet de transformer un état de base à n qubits $|m\rangle$ en un état où chacun des n qubits est affectée d'une phase qui encode la valeur de m. Cet état s'écrit

$$|\tilde{x}_m\rangle = \hat{U}_{\text{QFT}}|m\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i \frac{m}{2^{n-q}})|1\rangle).$$

Comme m se situe entre 0 et 2^n, le ratio $m/2^n$ se situe entre 0 et 1. La phase φ se situe également entre 0 et 1. Cela nous pousse à vouloir écrire la QFT d'un état qui encode la valeur de φ

$$\hat{U}_{\text{QFT}}|2^n\varphi\rangle = \bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 2^q\varphi)|1\rangle).$$

Ainsi, si on arrive a préparer un ensemble de qubits avec des phases $2\pi 2^q\varphi$, on pourra appliquer une QFT inverse pour obtenir l'état $|2^n\varphi\rangle$ et ainsi obtenir la valeur de φ ! Si l'état obtenu après la QFT inverse (et mesuré) est $|m\rangle$, la valeur de cette phase sera donné par

$$\varphi = \frac{m}{2^n}.$$

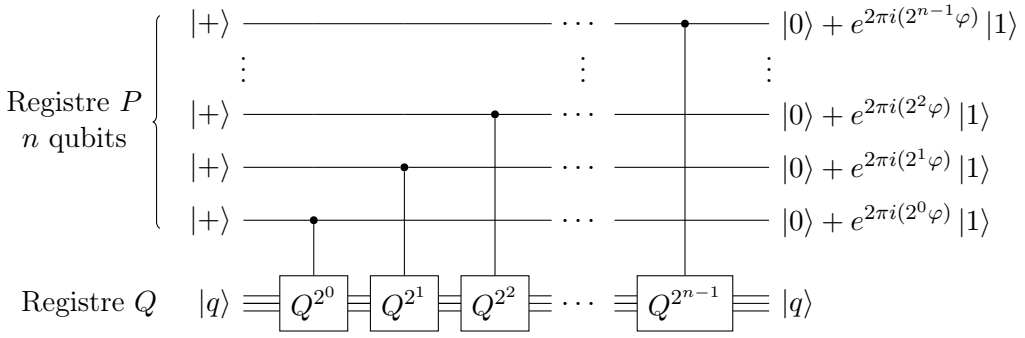


FIGURE 2.3 – Première étape de l'algorithme d'estimation de phase.

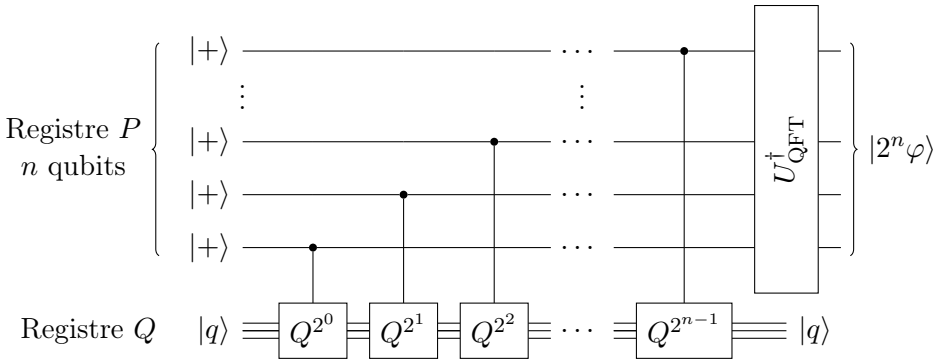


FIGURE 2.4 – Circuit d'estimation de phase $\hat{U}_{\mathrm{PE}}\left(\hat{Q}\right)$.

Remarque

Ici on a supposé que $2^n\varphi$ est un entier. Nous verrons plus loin comment ces idées s'appliquent pour une valeur quelconque de φ.

2.3 Circuit de l'estimation de phase

La première étape du circuit quantique de l'estimation phase consiste à préparé l'état

$$\bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 2^q \varphi)|1\rangle) \tag{2.3}$$

dans un registre (P) de n qubits. Pour pouvoir espérer accomplir cela, on aura besoin d'un registre Q qui contient l'état propre $|q\rangle$. Ensuite, on exploite le retour de phase décrit à la section 2.1, et ce, pour plusieurs qubits et plusieurs puissances de l'opérateur $\hat{Q}$ comme c'est illustré à la figure 2.3. Une fois cet état préparé dans le registre P, il ne reste qu'à effectuer la QFT inverse (figure 2.4) pour obtenir l'état $|m\rangle = |2^n\varphi\rangle$.

On peut résumer l'application du circuit estimation de phase par une opération unitaire telle que

$$\begin{aligned}\hat{U}_{\mathrm{PE}}\left(\hat{Q}\right)(|\psi_P\rangle \otimes |\psi_Q\rangle) &= \hat{U}_{\mathrm{PE}}\left(\hat{Q}\right)(|+\rangle^{\otimes n} \otimes |q\rangle) \\ &= |2^n\varphi\rangle \otimes |q\rangle.\end{aligned} \tag{2.4}$$

Il ne reste alors qu'à mesurer les qubits du registre P pour obtenir l'entier $2^n\varphi$.

2.4 Phase non entière

Comment cet algorithme se comporte-t-il dans le cas où φ ne peut pas être écrit comme un ratio entre un entier et une puissance de 2 ? Pour répondre à cette question, considérons une phase qui peut s'écrire comme

$$\varphi = \frac{m+\delta}{2^n} = \frac{m+\delta}{N}$$

où le désalignement δ se situe entre -0.5 et 0.5 et où m permet la meilleure approximation rationnelle de φ. Utilisons le fait que l'état quantique préparé par la première étape du circuit d'estimation de phase quantique peut également s'écrire comme (revoir équation 1.12)

$$\bigotimes_{q=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 2^q \varphi)|1\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi i \varphi k)|k\rangle.$$

On a donc un état à n qubits dont les composantes devant les états de base à n qubits sont

$$\tilde{\alpha}_k = \frac{1}{\sqrt{N}} \exp(2\pi i \varphi k).$$

En appliquant la QFT inverse sur cet état on obtient un l'état quantique

$$\sum_{j=0}^{N-1} \alpha_j |j\rangle$$

où les composantes sont données par

$$\begin{aligned}
\alpha_j &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(-2\pi i \frac{jk}{N}) \tilde{\alpha}_k \\
&= \frac{1}{N} \sum_{k=0}^{N-1} \exp(-2\pi i \frac{jk}{N}) \exp(2\pi i \varphi k) \\
&= \frac{1}{N} \sum_{k=0}^{N-1} \exp(2\pi i (\varphi - \frac{j}{N}) k) \\
&= \sum_{k=0}^{N-1} (\exp(2\pi i \frac{m-j+\delta}{N}))^k.
\end{aligned}$$

On peut alors utiliser les résultats sur les sommes géométriques

$$\sum_{k=0}^{N-1} r^k = \frac{1-r^N}{1-r}$$

pour réexprimer la somme et obtenir l'amplitude de probabilité devant $|j\rangle$ comme étant une fonction de δ

$$\alpha_j(\delta) = \frac{1}{N} \frac{1-\exp(2\pi i \delta)}{1-\exp(2\pi i \frac{m-j+\delta}{N})}.$$

La probabilité de mesurer l'état $|j\rangle$ est donnée par

$$p_j(\delta) = |\alpha_j(\delta)|^2 = \frac{1}{N^2} \frac{1-\cos(2\pi\delta)}{1-\cos(2\pi \frac{j-m-\delta}{N})}$$

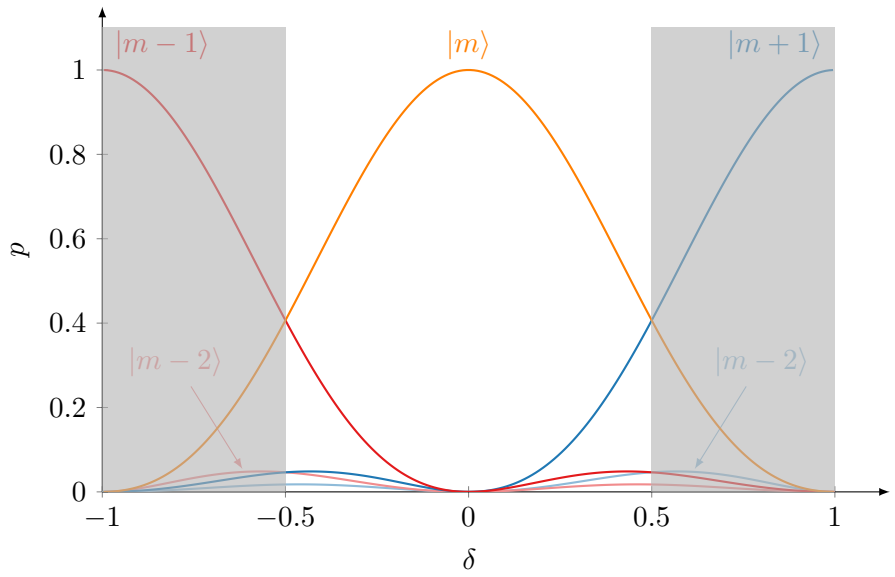


FIGURE 2.5 – Probabilité d'obtenir les résultats $|j\rangle$ lors de la mesure des qubits en fonction de la distance δ qui sépare la vraie valeur de $2^n\phi$ de l'entier le plus proche. Figure obtenue pour un système de 4 qubits.

ou encore (avec un peu de trigonométrie),

$$p_j(\delta) = \left(\frac{\sin(\pi\delta)}{N\sin(\pi\frac{j-m-\delta}{N})}\right)^2. \tag{2.5}$$

Tentons de décrire ce que cette probabilité implique. La courbe du centre à la figure 2.5 trace la probabilité de mesurer l'état $|j\rangle = |m\rangle$ en fonction du désalignement δ.

D'abord, lorsque $\delta \to 0$ (en utilisant $\sin x \sim x$),

$$p_m(\delta = 0) = \left(\frac{\sim \pi\delta}{\sim N\pi\delta/N}\right)^2 = 1.$$

on a 100% des chances de mesurer l'état $|m\rangle$ et 0% des chances de mesurer n'importe quel autre état : c'est le cas qu'on a traité plus haut φ où est donné exactement par la fraction $m/2^n$. Lorsque $\delta \neq 0$ la probabilité d'obtenir la meilleure estimation $|m\rangle$ décroit. Par exemple, si $\delta > 0$ on a de plus en plus de chance de mesurer l'état $|m+1\rangle$ et vice-versa. On voit également qu'on a des probabilités faibles, mais non nulles, d'obtenir d'autres résultats. Dans l'intervalle $\delta \in [-0.5, 0.5]$, ces probabilités décroissent toutes avec $|j-m|$.

La figure 2.5 montre également, en zone ombragée, les courbes pour $|\delta| > 0.5$. Par exemple, on voit que pour $\delta = 1$ on a 100% des chances de mesurer l'état $|m+1\rangle$, ce qui est le résultat attendu étant donné que c'est cet état qui est la meilleure approximation de la phase et non $|x_m\rangle$ si on permet à $|\delta|$ d'être plus grand que 0.5.

Le pire des cas se situe où $\delta = 0.5$, et $2^n\phi$ se trouve exactement entre m et $m+1$. La probabilité d'obtenir m est

$$p_m(\delta = \tfrac{1}{2}) = \left(\frac{1}{N\sin(\pi/2N)}\right)^2.$$

Pour $N \gg \pi/2$,

$$p_m(\delta = \tfrac{1}{2}) \approx \frac{4}{\pi^2} \sim 0.405.$$

2.5 Intervalle de confiance de la phase estimée

La question qu'on se pose maintenant est : quelle est la probabilité d'obtenir un résultat $m/2^n$ qui soit distant de φ au plus d'une erreur $\Delta\varphi$? La probabilité d'obtenir un résultat à l'intérieur de cette zone de confiance est

$$P(|\varphi - m/2^n| \leq \Delta\varphi) = \sum_{m-e \leq j \leq m+e} p_j$$

où on définit l'entier $e = \lfloor 2^n \Delta\varphi \rfloor$ qui caractérise l'erreur. On veut établir une valeur minimale pour cette probabilité. En réalité, il est plus facile d'établir une valeur maximale pour la probabilité d'obtenir un résultat à l'extérieur de la zone de confiance

$$\begin{aligned} P(|\varphi - m/2^n| > \Delta\varphi) &= 1 - P(|\varphi - m/2^n| \leq \Delta\varphi) \\ &= \sum_{\substack{0 \leq j < m-e, \\ m+e < j < N}} \frac{\sin^2(\pi\delta)}{N^2 \sin^2(\pi \frac{j-m-\delta}{N})}. \end{aligned}$$

Pour simplifier la notation, on définit l'ensemble d'indices suivant

$$J_e = \{0, \ldots, m-e-1\} \cup \{m+e+1, \ldots, N-1\}.$$

Pour plafonner $\sum_{j \in J_e} p_j$, on constate d'abord que le numérateur pour chacun des termes de la somme est toujours inférieur ou égal à 1 ($\sin^2(\pi\delta) \leq 1$)

$$\sum_{j \in J_e} p_j = \sum_{j \in J_e} \frac{\sin^2(\pi\delta)}{N^2 \sin^2(\pi \frac{j-m-\delta}{N})} \leq \sum_{j \in J_e} \frac{1}{N^2 \sin^2(\pi \frac{j-m-\delta}{N})}.$$

On effectue ensuite un changement de variable $k = j - m$ pour simplifier l'écriture

$$\sum_{j \in J_e} \frac{1}{N^2 \sin^2(\pi \frac{j-m-\delta}{N})} = \sum_{k \in K_e} \frac{1}{N^2 \sin^2(\pi \frac{k-\delta}{N})}$$

où on a défini un nouvel ensemble d'indices

$$K_e = \{-m, \ldots, -e-1\} \cup \{e+1, \ldots, N-m-1\}.$$

Néanmoins, comme le dénominateur a une période de N, on peut cycler les derniers éléments ($\{N/2, \ldots N-m-1\}$) vers le début de l'ensemble en leur soustrayant la période N (on obtient alors $\{-N/2, \ldots, -m-1\}$). On peut alors utiliser l'ensemble d'indices

$$\begin{aligned} K'_e &= \{-N/2, \ldots, -m-1\} \cup \{-m, \ldots, -e-1\} \cup \{e+1, \ldots, N/2-1\} \\ &= \{-N/2, \ldots, -e-1\} \cup \{e+1, \ldots, N/2-1\}. \end{aligned}$$

pour la somme sur k et obtenir exactement le même résultat, comme cela est illustré à la figure 2.6. La même figure montre également que dans la région d'intérêt, le dénominateur est toujours supérieur à une valeur plancher donnée par une fonction quadratique

$$\sin^2(\pi \frac{k-\delta}{N}) \geq (2 \frac{k-\delta}{N})^2. \tag{2.6}$$

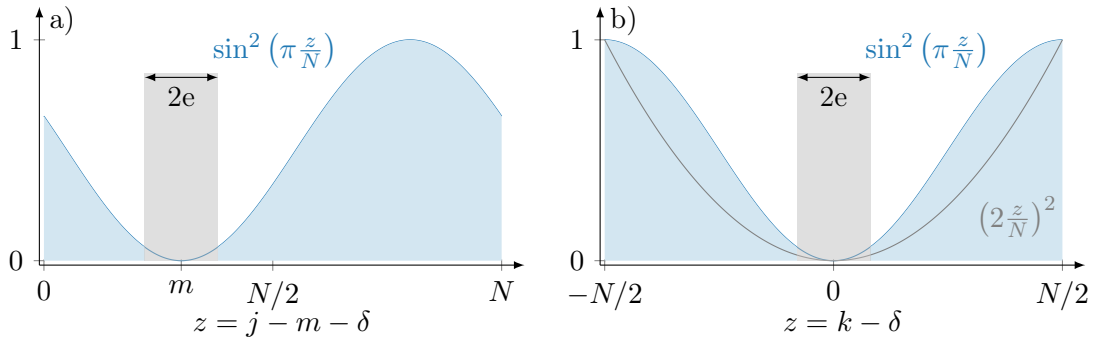


FIGURE 2.6 – Dépendance du dénominateur de la probabilité p_j avec j. a) La somme sur j inclus tous les termes entre 0 et $N-1$ sauf ceux à une distance moindre de e autour de m. b) La somme sur k est équivalente. On peut cependant établir une borne inférieure à la valeur du dénominateur à l'aide d'une fonction quadratique.

Cela nous permet de simplifier davantage la borne supérieure à la probabilité d'obtenir un résultat à l'extérieur de la zone de confiance

$$\sum_{j\in J_e} p_j \leq \frac{1}{4}\sum_{k\in K'_e}\frac{1}{(k-\delta)^2}.$$

L'ensemble K'_e est presque symétrique autour de $k=0$, ce qui nous permet de ressembler les deux côtés en un seule somme

$$\begin{aligned}\sum_{k\in K'_e}\frac{1}{(k-\delta)^2} &= \sum_{-N/2\leq k<-e}\frac{1}{(k-\delta)^2} + \sum_{e<k<N/2}\frac{1}{(k-\delta)^2}\\ &= \sum_{e<k\leq N/2}\frac{1}{(k+\delta)^2} + \sum_{e<k<N/2}\frac{1}{(k-\delta)^2}\\ &\leq \sum_{k\in K''_e}\left(\frac{1}{(k+\delta)^2}+\frac{1}{(k-\delta)^2}\right).\end{aligned}$$

où on ajouté un terme supplémentaire $(N/2)$ à la deuxième somme, ce qui nous a permis d'obtenir deux sommes sur le même ensemble

$$K''_e = \{e+1,\ldots,N/2\}.$$

En combinant les termes, on obtient une expression qui dépend de δ^2. Cette quantité se situe dans l'intervalle $0\leq\delta\leq\frac{1}{2}$. On repousse encore la valeur plafond

$$\sum_{k\in K''_e}\left(\frac{1}{(k+\delta)^2}+\frac{1}{(k-\delta)^2}\right) = 2\sum_{k\in K''_e}\frac{k^2+\delta^2}{(k^2-\delta^2)^2} \leq 2\sum_{k\in K''_e}\frac{k^2}{(k^2-\frac{1}{4})^2}.$$

En effectue ensuite le changement de variables $k = l+1$, ce qui génère le nouvel ensemble

$$L_e = \{e,\ldots,N/2-1\}.$$

Cela nous permet finalement d'obtenir une expression très simple pour la valeur plafond de la somme

$$\sum_{k\in K''_e}\frac{k^2}{(k^2-\frac{1}{4})^2} = \sum_{l\in L_e}\frac{(l+1)^2}{(l^2+2l+\frac{3}{4})^2} \leq \sum_{l\in L_e}\frac{(l+1)^2}{l^2(l+2)^2} \leq \sum_{l\in L_e}\frac{1}{l^2}.$$

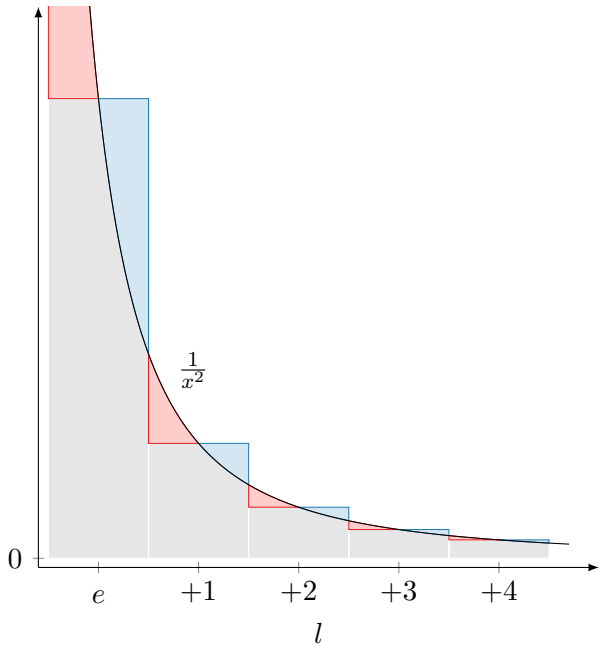


FIGURE 2.7 – Comparaison entre la somme $\sum_l l^{-2}$ et l'intégrale $\int \mathrm{d}x x^{-2}$. En intégrant de $e - \frac{1}{2}$ jusqu'à l'infini, on surévalue la valeur de la somme.

Pour évaluer cette somme, on la transforme en intégrale. On constate que la fonction x^{-2} est décroissante et de courbe positive ce qui implique

$$\frac{1}{l^2} < \int_{l-\frac{1}{2}}^{l+\frac{1}{2}} \frac{1}{x^2} \mathrm{d}x.$$

La figure 2.7 illustre le faire que la somme des l^{-2} est inférieure à l'aire sous la courbe d'une fonction x^{-2}. On peut donc borner la valeur de la somme par une intégrale qui s'évalue rapidement

$$\sum_{l \in L_e} \frac{1}{l^2} \leq \int_{e-\frac{1}{2}}^{\infty} \mathrm{d}x \frac{1}{x^2} = \frac{1}{e - \frac{1}{2}}.$$

On peut finalement combiner les différents coefficients laissés en chemin

$$\sum_{j \in J_e} p_j \leq \frac{1}{4} \sum_{k \in K'_e} \frac{1}{(k-\delta)^2} \leq \frac{2}{4} \sum_{l \in L_e} \frac{1}{l^2} \leq \frac{1}{2} \int_{e-\frac{1}{2}}^{\infty} \mathrm{d}x \frac{1}{x^2}$$

pour obtenir la borne supérieure à la probabilité que l'estimation de phase retourne une valeur à l'extérieure de l'intervalle de confiance

$$P(|\varphi - m/2^n| > \Delta\varphi) \leq \frac{1}{2e-1}. \tag{2.7}$$

Ainsi, supposons que l'on veuille évaluer φ avec une précision exprimée comme une puissance $\Delta\varphi = 2^{-p}$. Dans ce cas, l'entier qui caractérise la zone de confiance est $e = 2^{n-p}$. On vise un taux de succès

$$P(|\varphi - m/2^n| \leq \Delta\varphi) \leq 1 - \epsilon.$$

On doit donc avoir

$$\epsilon = \frac{1}{2e-1}.$$

Pour assurer une précision de $\Delta\varphi = 2^{-p}$ avec un taux de réussite on devra donc employer

$$n = p + \lceil \log(\frac{1}{2\epsilon} + \frac{1}{2}) \rceil \tag{2.8}$$

qubits.

2.6 État quantique quelconque

Au début du chapitre, on a supposé que le registre A contenait $|q\rangle$ un état propre de $\hat{U}$. Qu'en est-il si l'état dans le registre A est un état quelconque $|\psi_Q\rangle$? Dans tous les cas, cet état se décompose sur la base des états propres de $\hat{Q}$. On peut donc écrire

$$|\psi_Q\rangle = \sum_{i=0}^{2_A^n - 1} \beta_i |q_i\rangle$$

où les $|q_i\rangle$ sont les états propres de $\hat{Q}$ répondant à l'équation aux valeurs propres

$$\hat{U}|q_i\rangle = e^{2\pi i \varphi_i}|q_i\rangle.$$

Si on applique l'opération unitaire de l'équation 2.4 dans ce cas, on obtient

$$\begin{aligned}\hat{U}_{\mathrm{PE}}\Big(\hat{Q}\Big)(|\psi_P\rangle \otimes |\psi_Q\rangle) &= \hat{U}_{\mathrm{PE}}\Big(\hat{Q}\Big)(|+\rangle^{\otimes n} \otimes \sum_{i=0}^{2_A^n - 1} \beta_i |q_i\rangle) \\ &= \sum_{i=0}^{2_A^n - 1} \beta_i |2^n \varphi_i\rangle \otimes |q_i\rangle.\end{aligned}$$

La mesure des qubits du registre B va retourner l'entier $2^n\varphi_i$ avec une probabilité $|\beta_i|^2$. Le résultat secondaire de cette mesure est que l'état contenu dans le registre Q est alors exactement l'état propre associé $|q_i\rangle$!

Chapitre 3

Amplification d'amplitude quantique

3.1 Problème classique

Posons le problème suivant. On a un sac de billes avec n_{tot} billes à l'intérieures dont n_{r} billes sont rouges et n_{b} billes sont bleues. Il n'y a que ces deux couleurs de billes dans le sac, de sorte que $n_{\text{tot}} = n_{\text{r}} + n_{\text{b}}$. Notre objectif est de piger une bille bleue. En moyenne, combien de billes doit-on piger avant de piger une bille bleue ?

La probabilité qu'une bille pigée soit bleue est

$$p = \frac{n_{\text{b}}}{n_{\text{tot}}}.$$

Si on pige m billes, la probabilité qu'au moins une d'entre elles soit bleue est mp. Donc, en moyenne, on doit piger

$$m = \frac{1}{p}$$

billes pour en obtenir une bleue.

À l'inverse, le nombre de billes qu'on pige avant d'en obtenir une bleue nous permet d'estimer p et donc la proportion de billes bleues dans le sac.

3.2 Formulation formelle

On suppose une fonction χ qui prend un entier $x \in \mathcal{X} = [0, n_{\text{tot}}[$ en entrée et qui retourne soit 0 ou 1

$$\chi(x_i) = y_i \in \{0, 1\}.$$

On peut séparer l'ensemble $\mathcal{X}$ en deux sous-ensembles $\mathcal{X}_0$ et $\mathcal{X}_1$ tel que

$$\chi(x_i) = \begin{cases} 0 & \text{si } i \in \mathcal{X}_0 \\ 1 & \text{si } i \in \mathcal{X}_1 \end{cases}$$

Il y a $|\mathcal{X}_0|$ éléments dans $\mathcal{X}_0$ et $|\mathcal{X}_1|$ dans $\mathcal{X}_1$. De plus, $|\mathcal{X}_0| + |\mathcal{X}_1| = |\mathcal{X}|$. Si on choisit un x_i au hasard, on a une probabilité $p = |\mathcal{X}_1|/|\mathcal{X}|$ d'obtenir $\chi(x_i) = 1$. Si on appelle m fois la fonction χ avec des instances de x_i on a, en moyenne, une probabilité mp d'obtenir un $\chi(x_i) = 1$. Donc, en moyenne, on doit choisir

$$m = \frac{1}{p}$$

instances de x_i pour trouver un $\chi(x_i) = 1$.

Encore une fois, l'estimation de p nous permet d'estimer les tailles relatives de $|\mathcal{X}_0|$ et $|\mathcal{X}_1|$.

3.3 Algorithme quantique d'estimation d'amplitude

Amplification d'amplitude

Pour traiter le même genre de situation avec un ordinateur quantique, on pose d'abord un opérateur qui prépare l'état quantique suivant à partir de l'état initial

$$\hat{A}|0\rangle^{\otimes n} = \hat{A}|\mathbf{0}\rangle = \sqrt{1-a}|\phi_0\rangle + \sqrt{a}|\phi_1\rangle \tag{3.1}$$

avec $\langle\phi_0|\phi_1\rangle = 0$. Définissons immédiatement

$$a = \sin^2\theta \qquad \text{et} \qquad 1-a = \cos^2\theta$$

de sorte que

$$\hat{A}|\mathbf{0}\rangle = \cos\theta|\phi_0\rangle + \sin\theta|\phi_1\rangle.$$

et plus particulièrement,

$$\left\langle\phi_0\middle|\hat{A}\middle|\mathbf{0}\right\rangle = \cos\theta \qquad \left\langle\phi_1\middle|\hat{A}\middle|\mathbf{0}\right\rangle = \sin\theta.$$

Inspiré par l'algorithme de Grover, on définit l'opérateur

$$\hat{Q} = \hat{A}\hat{S}_{\mathbf{0}}\hat{A}^\dagger\hat{S}_{\phi_0}$$

avec

$$\hat{S}_{\mathbf{0}} = \hat{\mathbb{I}} - 2|\mathbf{0}\rangle\langle\mathbf{0}| \qquad \text{et} \qquad \hat{S}_{\phi_0} = \hat{\mathbb{I}} - 2|\phi_0\rangle\langle\phi_0|.$$

Qu'est-ce que cet opérateur a de particulier en lien avec l'opérateur $\hat{A}$? D'abord, on démontre facilement que,

$$\begin{aligned}\hat{Q}|\phi_0\rangle &= \cos(2\theta)|\phi_0\rangle + \sin(2\theta)|\phi_1\rangle \\ \hat{Q}|\phi_1\rangle &= -\sin(2\theta)|\phi_0\rangle + \cos(2\theta)|\phi_1\rangle.\end{aligned} \tag{3.2}$$

Autrement dit, les états $|\phi_0\rangle$ et $|\phi_1\rangle$ engendrent un sous-espace $\mathcal{E}_\phi$ dont tous les états prennent la forme

$$|\psi\rangle = \alpha_0|\phi_0\rangle + \alpha_1|\phi_1\rangle.$$

Dans ce sous-espace, l'opérateur $\hat{Q}$ prend la forme d'une matrice 2×2.

$$\hat{Q}|\psi\rangle = \begin{pmatrix}\cos(2\theta) & -\sin(2\theta)\\ \sin(2\theta) & \cos(2\theta)\end{pmatrix}\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} = \begin{pmatrix}\alpha_0'\\ \alpha_1'\end{pmatrix} = |\psi'\rangle.$$

Par exemple,

$$\hat{Q}|\phi_0\rangle = \begin{pmatrix}\cos(2\theta) & -\sin(2\theta)\\ \sin(2\theta) & \cos(2\theta)\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}\cos(2\theta)\\ \sin(2\theta)\end{pmatrix}$$

ce qui correspond bien à la première ligne de l'équation 3.2.

L'état $|\psi'\rangle$ s'exprime également comme une combinaison linéaire de $|\phi_0\rangle$ et $|\phi_1\rangle$. Le sous-espace $\mathcal{E}_\phi$ est dit *stable* sous l'action de $\hat{Q}$: l'application de $\hat{Q}$ sur un état de $\mathcal{E}_\phi$ produit un autre état de $\mathcal{E}_\phi$.

Pour ce type d'opérateur, les valeurs propres sont

$$q_\pm = e^{\pm i2\theta}$$

et les états propres sont

$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|\phi_0\rangle \mp i|\phi_1\rangle).$$

Notons que la transformation inverse est

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) \qquad\qquad |\phi_1\rangle = \frac{i}{\sqrt{2}}(|\phi_+\rangle - |\phi_-\rangle)$$

On se rappelle que l'application de $\hat{A}$ sur l'état initial produit l'état

$$\hat{A}|\mathbf{0}\rangle = \cos\theta|\phi_0\rangle + \sin\theta|\phi_1\rangle$$

que l'on peut exprimer cet état sur les états propres de $\hat{Q}$

$$\begin{aligned}\hat{A}|\mathbf{0}\rangle &= \frac{\cos\theta}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) + i\frac{\sin\theta}{\sqrt{2}}(|\phi_+\rangle - |\phi_-\rangle) \\ &= \frac{1}{\sqrt{2}}(e^{i\theta}|\phi_+\rangle + e^{-i\theta}|\phi_-\rangle). \end{aligned} \tag{3.3}$$

Note : Le reste de cette section s'applique uniquement dans le contexte d'amplification d'amplitude. Passez à la section suivante pour voir comment ces concepts sont utilisés dans le contexte de l'estimation d'amplitude.

Dans la base propre de $\hat{Q}$, son application a un effet trivial

$$\hat{Q}|\phi_\pm\rangle = e^{\pm i2\theta}|\phi_\pm\rangle. \tag{3.4}$$

En particulier, une puissance de $\hat{Q}$ produit l'état

$$\hat{Q}^j\hat{A}|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}(e^{i(2j+1)\theta}|\phi_+\rangle + e^{-i(2j+1)\theta}|\phi_-\rangle).$$

En réexprimant cet état dans la base initiale on obtient,

$$\begin{aligned}\hat{Q}^j\hat{A}|\mathbf{0}\rangle &= \frac{1}{2}(e^{i(2j+1)\theta}(|\phi_0\rangle + i|\phi_1\rangle) + e^{-i(2j+1)\theta}(|\phi_0\rangle - i|\phi_1\rangle)) \\ &= \cos((2j+1)\theta)|\phi_0\rangle + \sin((2j+1)\theta)|\phi_1\rangle.\end{aligned}$$

On voit alors qu'en appliquant $\hat{Q}$ un certain nombre de fois, on peut maximiser les probabilités de mesurer $|\phi_1\rangle$. En particulier, on veut que

$$(2j+1)\theta \to \frac{\pi}{2}$$

pour maximiser l'amplitude de l'état $|\phi_1\rangle$.

Estimation d'amplitude

Si on retourne à l'équation 3.3, on voit que l'opérateur $\hat{A}$ permet de préparer un état quantique qui se décompose en une superposition des états propres de $\hat{Q}$. De plus, ces états propres ont comme valeurs propres $e^{\pm i2\theta}$.

On peut donc utiliser le circuit d'estimation en utilisant l'état

$$\hat{A}|\mathbf{0}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta}|\phi_+\rangle + e^{-i\theta}|\phi_-\rangle) \tag{3.5}$$

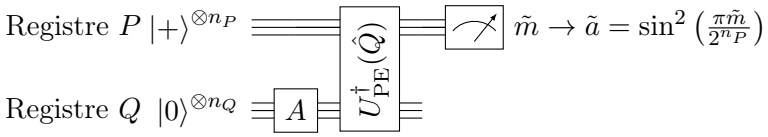


FIGURE 3.1 – Circuit d'estimation d'amplitude $\hat{U}_{\mathrm{AE}}\Big(\hat{A}\Big)$ où $\hat{Q} = \hat{A}\hat{S}_{\mathbf{0}}\hat{A}^{\dagger}\hat{S}_{\phi_0}$.

et $\hat{Q}$ comme opérateur des portes contrôlées. La mesure des qubits après l'application du circuit d'estimation de phase va retourner un entier m qui estime la phase associée à une des deux valeurs propres

$$2\pi\frac{m}{2^n} \sim \pm 2\theta \pmod{2\pi}.$$

Cette phase permet alors d'estimer l'amplitude associée à l'état $|\phi_1\rangle$ grâce à,

$$a = \sin^2\theta$$

On voit que le signe de θ n'a pas d'importance. Finalement, on estime l'amplitude grâce à [1]

$$\tilde{a} = \sin^2(\pi\tilde{m}/2^n).$$

Le circuit de la figure 3.1 résume la construction du circuit qui permet de faire l'estimation d'amplitude pour un opérateur $\hat{A}$.

3.4 Valeur moyenne d'une fonction d'une variable aléatoire

Étant donnée une variable aléatoire X avec une densité de probabilité $\rho(x)$, on cherche a évaluer la valeur moyenne d'une fonction $g(X)$ de cette variable aléatoire. Pour ce faire, on peut prendre $N_{\text{éch}}$ échantillons $x^{(i)}$ et calculer

$$\mathbb{E}[g(X)] \approx \frac{1}{N}\sum_{i=1}^{N_{\text{éch}}} g\Big(x^{(i)}\Big). \tag{3.6}$$

On peut également discrétiser les valeurs possibles de X est une grille x_i. On calcule encore les probabilités d'obtenir une valeur de X dans l'intervalle $[x_i, x_{i+1}[$ de la grille

$$p_i = \int_{x_i}^{x_{i+1}} \mathrm{d}x\rho(x). \tag{3.7}$$

Étant donné ces probabilités, la valeur moyenne peut être estimée grâce à

$$\mathbb{E}[g(X)] \approx \sum_i p_i g(x_i) \tag{3.8}$$

Avec l'estimation d'amplitude

On représente la densité de probabilité $\rho(x)$ d'une variable aléatoire X par une superposition d'états préparée sur un premier registre (1) de n qubits

$$\hat{U}_X|0\rangle_1^{\otimes n} = \sum_i^{2^n-1} \sqrt{p_i}|i\rangle_1 \tag{3.9}$$

1. Ne pas confondre le $\tilde{\cdot}$ avec la transformée de Fourier. Ici, $\tilde{a}$ est la valeur estimée pour a.

avec $\sum p_i = 1$.

On suppose un opérateur qui *calcule* une fonction $g(x)$ à partir de la valeur du premier registre en l'encodant dans les amplitudes de probabilité d'un qubit supplémentaire qui constitue un deuxième registre (2). L'action de cet opérateur lorsque le premier registre dans l'état de base $|i\rangle$ est

$$\hat{G}|i\rangle_1|0\rangle_2 = |i\rangle_1(\sqrt{1-g(x_i)}|0\rangle_2 + \sqrt{g(x_i)}|1\rangle_2). \tag{3.10}$$

Si on agit sur un premier registre qui encode une densité de probabilité comme à l'équation 3.9 l'état du système est plutôt

$$\begin{aligned} |\psi\rangle = \hat{G}\,\hat{U}_X|0\rangle_1^{\otimes n}|0\rangle_2 = \hat{G}(\sum_i^{2^n-1}\sqrt{p_i}|i\rangle_1)|0\rangle_2 &= \sum_i^{2^n-1}\sqrt{p_i}\hat{G}|i\rangle_1|0\rangle_2 \\ &= \sum_i^{2^n-1}\sqrt{p_i}|i\rangle_1(\sqrt{1-g_i}|0\rangle_2 + \sqrt{g_i}|1\rangle_2) \end{aligned} \tag{3.11}$$

où on utilise la notation $g_i = g(x_i)$. On peut à ce stade utiliser les opérateurs $\hat{U}_X$ et $\hat{G}$ dans l'appareillage de l'estimation d'amplitude pour estimer la valeur moyenne $g(X)$ étant donnée la densité de probabilité $\rho(x)$

$$\mathbb{E}[g(X)] \approx \sum_i p_i g(x_i).$$

Pour se convaincre que l'estimation d'amplitude nous retournera bien cette moyenne, tentons d'exprimer la probabilité de mesurer le qubit du deuxième registre dans l'état $|1\rangle_2$. La probabilité de mesurer un qubit dans l'état 1 étant donné un système dans l'état $|\psi\rangle$ est

$$|\langle\psi|1\rangle|^2 = \langle\psi|1\rangle\langle 1|\psi\rangle.$$

Ainsi, cette probabilité peut également être obtenue comme la valeur moyenne de l'opérateur $|1\rangle\langle 1|$, qui dans notre cas peut être exprimée ainsi

$$|1\rangle\langle 1|_2 = \frac{\hat{I}_2 - \hat{Z}_2}{2}.$$

Calculons d'abord la valeur moyenne de $\hat{Z}_2$ pour l'état qu'on a préparé. En se rappelant que les qubits du premier registre sont transparents à $\hat{Z}_2$ et que les états propres de $\hat{Z}_2$ sont $|0\rangle_2$ et $|1\rangle_2$ avec les valeurs propres $+1$ et -1, on obtient

$$\begin{aligned} &(\sum_i^{2^n-1}\sqrt{p_i}\langle i|_1(\sqrt{1-g_i}\langle 0|_2 + \sqrt{g_i}\langle 1|_2))\hat{Z}_2(\sum_j^{2^n-1}\sqrt{p_j}|j\rangle_1(\sqrt{1-g_j}|0\rangle_2 + \sqrt{g_j}|1\rangle_2)) \\ &= \sum_{ij}\sqrt{p_i p_j}\langle i|j\rangle_1(\sqrt{(1-g_i)(1-g_j)}\langle 0|0\rangle_2 - \sqrt{g_i g_j}\langle 1|1\rangle_2) \\ &= \sum_i p_i((1-g_i) - g_i) = 1 - 2\sum_i p_i g_i. \end{aligned}$$

On constante donc que la probabilité de mesurer le qubit du deuxième registre dans l'état $|1\rangle$ est directement donnée par

$$\frac{1}{2}\left\langle\psi\middle|\hat{I}_2 - \hat{Z}_2\middle|\psi\right\rangle = \sum_i p_i g_i \tag{3.12}$$

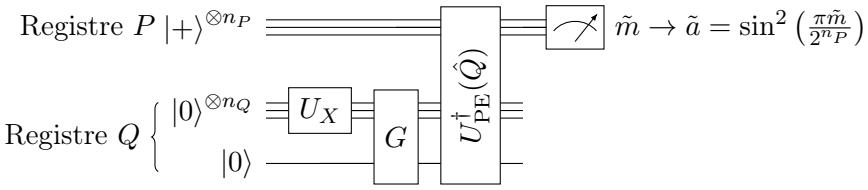


FIGURE 3.2 – Circuit d'estimation d'amplitude pour évaluer la valeur moyenne de $g(X)$ où X est une variable aléatoire avec une densité de probabilité préparée par l'unitaire $\hat{U}_X$. L'estimation de a donne directement la valeur moyenne $\sum_i p_i g_i$.

qui n'est rien d'autre que la valeur moyenne de $g(X)$ étant donnée la densité de probabilité $\rho(x)$!

On peut cependant faire usage de l'estimation d'amplitude pour obtenir cette valeur moyenne. Si on compare l' équation 3.11 avec 3.1 on constante que l'opérateur

$$\hat{G}\,\hat{U}_X|0\rangle_1^{\otimes n}|0\rangle_2 = \sum_i^{2^n-1} \sqrt{p_i(1-g_i)}|i\rangle_1|0\rangle_2 + \sum_i^{2^n-1} \sqrt{p_i g_i}|i\rangle_1|1\rangle_2$$

agit de manière similaire à l'opérateur $\hat{A}$ utilisé dans l'estimation d'amplitude

$$\hat{A}|\mathbf{0}\rangle = \sqrt{1-a}|\phi_0\rangle + \sqrt{a}|\phi_1\rangle.$$

On peut donc exploiter l'algorithme d'estimation d'amplitude en utilisant $\hat{A} = \hat{G}\,\hat{U}_X$. Dans ce cas, on peut immédiatement établir les associations

$$\sqrt{1-a}|\phi_0\rangle = \sum_i^{2^n-1} \sqrt{p_i(1-g_i)}|i\rangle_1|0\rangle_2 \qquad \text{et} \qquad \sqrt{a}|\phi_1\rangle = \sum_i^{2^n-1} \sqrt{p_i g_i}|i\rangle_1|1\rangle_2 \tag{3.13}$$

Les probabilités de mesurer $|\phi_0\rangle$ et $|\phi_1\rangle$ (dans la base $\{|\phi_0\rangle, |\phi_1\rangle\}$) sont alors directement données par

$$1-a = \sum_i^{2^n-1} p_i(1-g_i) \qquad \text{et} \qquad a = \sum_i^{2^n-1} p_i g_i \tag{3.14}$$

L'aspect le plus important ici est que la probabilité de mesurer le qubit du registre 2 dans l'état $|1\rangle$ est directement donnée par a qui est également la valeur moyenne de $g(X)$.

Le choix de $|\phi_1\rangle$ (et donc de $|\phi_0\rangle$) définit l'opérateur $\hat{S}_{\phi_0}$ et donc $\hat{Q}$. La figure 3.2 résume la construction du circuit qui permet d'estimer la valeur moyenne de $g(X)$.

3.5 Valeur moyenne d'un produit de fonctions d'une variable aléatoire

On décrit maintenant comment il est possible d'estimer la valeur moyenne d'un produit de fonctions d'une variable aléatoire

$$\mathbb{E}[g(X)h(X)] \approx \sum_i p_i g(x_i)h(x_i). \tag{3.15}$$

On suppose maintenant 2 opérateurs qui *calculent* les fonctions $g(x)$ et $h(x)$ à partir de la valeur du premier registre en les encodant dans les amplitudes de probabilité de deux qubits supplémentaires qui constituent les registres 2 et 3. Ces opérateurs ont les actions suivantes

$$\hat{G}|i\rangle_1|0\rangle_2|\cdot\rangle_3 = |i\rangle_1(\sqrt{1-g(x_i)}|0\rangle_2 + \sqrt{g(x_i)}|1\rangle_2)|\cdot\rangle_3$$
$$\hat{H}|i\rangle_1|0\rangle_2|\cdot\rangle_3 = |i\rangle_1|\cdot\rangle_2(\sqrt{1-h(x_i)}|0\rangle_3 + \sqrt{h(x_i)}|1\rangle_3).$$

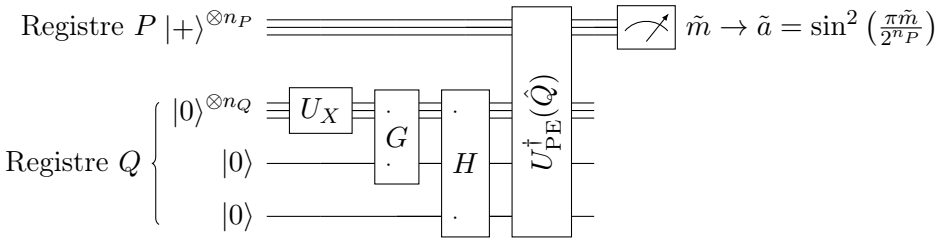


FIGURE 3.3 – Circuit d'estimation d'amplitude pour évaluer la valeur moyenne de $g(X)h(X)$ où X est une variable aléatoire avec une densité de probabilité préparée par l'unitaire $\hat{U}_X$. L'estimation de a donne directement la valeur moyenne $\sum_i p_i g_i h_i$.

De la même manière qu'à la section précédente, l'application de ces opérateurs unitaire produit l'état

$$\begin{aligned}\hat{H}\,\hat{G}\,\hat{U}_X|0\rangle_1^{\otimes n}|0\rangle_2|0\rangle_3 = &\sum_i^{2^n-1}\sqrt{p_i(1-g_i)(1-h_i)}|i\rangle_1|0\rangle_2|0\rangle_3 + \sum_i^{2^n-1}\sqrt{p_i g_i(1-h_i)}|i\rangle_1|1\rangle_2|0\rangle_3 \\ &+ \sum_i^{2^n-1}\sqrt{p_i(1-g_i)h_i}|i\rangle_1|0\rangle_2|1\rangle_3 + \sum_i^{2^n-1}\sqrt{p_i g_i h_i}|i\rangle_1|1\rangle_2|1\rangle_3.\end{aligned}$$

On identifie l'état

$$\sqrt{a}|\phi_1\rangle = \sum_i^{2^n-1}\sqrt{p_i g_i h_i}|i\rangle_1|1\rangle_2|1\rangle_3 \tag{3.16}$$

ce qui définit les opérateurs $\hat{S}_{\phi_0}$ et $\hat{Q}$. L'estimation d'amplitude permet donc d'estimer

$$\tilde{a} \approx \sum_i^{2^n-1} p_i g_i h_i. \tag{3.17}$$

Le circuit de la figure 3.3 résume les étapes de cet algorithme.

3.6 Valeur moyenne d'une fonction de deux variables aléatoires

On s'intéresse ensuite à valeur moyenne d'une fonction de plusieurs variables aléatoires

$$\mathbb{E}[g(X,Y)] \approx \sum_i p_i q_j g(x_i, y_j). \tag{3.18}$$

où les p_i et les q_j sont respectivement les probabilités des valeurs x_i et y_j. Pour estimer cette valeur moyenne, il doit préparer les distributions de ces deux variables dans deux registres à l'aide d'unitaires $\hat{U}_X$ et $\hat{U}_Y$. Ensuite, on doit avoir un opérateur qui, étant donné 2 registres contenant les états $|i\rangle$ et $|j\rangle$, produit l'état suivant

$$\hat{G}|i\rangle_1|j\rangle_2|0\rangle_3 = |i\rangle_1|j\rangle_2(\sqrt{1-g(x_i,y_j)}|0\rangle_3 + \sqrt{g(x_i,y_j)}|1\rangle_3).$$

En combinant ces opérations, on obtient l'état

$$\begin{aligned}|\psi\rangle &= \hat{G}\,(\hat{U}_X|0\rangle_1^{\otimes n_X})(\hat{U}_Y|0\rangle_2^{\otimes n_Y})|0\rangle_3 \\ &= \sum_{i,j}\sqrt{p_i q_j}\hat{G}|i\rangle_1|j\rangle_2|0\rangle_3\end{aligned} \tag{3.19}$$

La suite est identique au cas de la section 3.4. La figure 3.4 illustre le circuit utilisé. À partir d'ici, on peut facilement généraliser pour des fonctions de plusieurs variables.

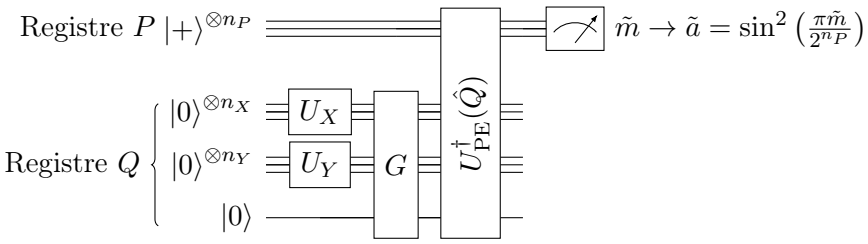


FIGURE 3.4 – Circuit d'estimation d'amplitude pour évaluer la valeur moyenne de $g(X,Y)$ où X et Y sont des variables aléatoires avec des densités de probabilité préparées par les unitaires $\hat{U}_X$ et $\hat{U}_Y$. L'estimation de a donne directement la valeur moyenne $\sum_i p_i q_j g_{ij}$.