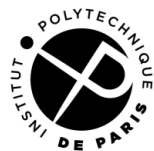


ÉCOLE NATIONALE DES
PONTS
ET **CHAUSSÉES**



IP PARIS

PROJET DE PREMIÈRE ANNÉE 2025

RAPPORT INTERMÉDIAIRE

Informatique Quantique

Réalisé par :

Sahraoui Youssef

Pierre Bressollette

Supervisé par :

Henri Pinsolle Bourtayre

Alicia Negre

Contents

1	Postulats de la Mécanique Quantique	2
1.1	Postulat d'espace d'état :	2
1.2	Postulat de Mesure	3
1.3	Postulat d'évolution temporelle d'un système quantique	3
1.4	Postulat d'opérateur quantique	4
1.5	Exemples	4
1.5.1	Système à <i>1-qubit</i>	4
1.5.2	Système à <i>n-qubits</i>	8
2	Quantum Phase Estimation	10
2.1	Motivation	10
2.2	Contexte	10
2.3	1 ^{ère} Approche : Test de Hadamard	10
2.4	2 ^{ème} Approche : Quantum Fourier Transform QFT	12
2.4.1	Définition	12
2.5	Circuit Quantique de la QFT	14
2.6	Principe de l'Estimation de Phase avec la QFT	14
3	Applications	15
3.1	EDP et Système Linéaire	15
3.2	Équation de Poisson	15
3.2.1	Généralités	15
3.2.2	Discrétisation de l'Équation de Poisson	16
3.3	Équation de la Chaleur	16
3.3.1	Généralités	16
3.3.2	Discrétisation de l'Équation de la Chaleur	17
3.4	Résolution Quantique par l'Algorithme HHL	17
3.4.1	Encodage Unitaire de A	17
3.4.2	Étapes principales de HHL	18
3.4.3	Avantages et Limitations	18
3.5	Conclusion	18
4	Références	18

1 Postulats de la Mécanique Quantique

Remarque

Avant même de commencer, il est important de noter que ces postulats sont adaptés dans leur formulation au formalisme utilisé en informatique quantique.

1.1 Postulat d'espace d'état :

À chaque système quantique est associé un espace de Hilbert $(\mathcal{H}, \langle \cdot | \cdot \rangle)$ hermetien et séparable, où \mathcal{H} est appelé *l'espace des états*, dans le cadre de l'informatique quantique \mathcal{H} est considérée de dimension finie.

→ L'état physique d'un système est défini par un vecteur ψ , noté par un *ket* $|\psi\rangle$.

- $\|\psi\|_{\mathcal{H}} = \langle \psi | \psi \rangle = 1$ (*état normalisé*)
- $\forall \theta \in \mathbf{R}$, $e^{i\theta} |\psi\rangle$ et $|\psi\rangle$ *représentent le même état*

Principe de superposition

Comme \mathcal{H} est un espace vectoriel, la combinaison linéaire complexe d'états acceptable est aussi physiquement acceptable (*à normalisation près*).

Quelques résultats utiles

Pour $\psi \in \mathcal{H}$:

- La transposée complexe est notée avec un *dagger* : ψ^\dagger .
- On introduit une nouvelle notation appelée *bra*, où $\langle \psi | \in \mathcal{H}^*$, qui est une forme linéaire agissant comme ψ^\dagger , cohérente à l'aide *théorème de représentation de Riesz*.
- Comme \mathcal{H} est *séparable*, on prend une base orthonormée $(|\psi_i\rangle)_{i \in \mathcal{I}}$ de \mathcal{H} .

$$|\psi\rangle = \sum_{i \in \mathcal{I}} a_i |\psi_i\rangle \quad ; \quad \langle \psi | = \sum_{i \in \mathcal{I}} a_i^* \langle \psi_i |$$

- La puissance de la notation *bra-ket* réside dans le fait qu'elle simplifie les produits scalaires. Pour $\psi, \phi \in \mathcal{H}$ tels que :

$$|\psi\rangle = \sum_{i \in \mathcal{I}} a_i |\psi_i\rangle \quad \text{et} \quad |\phi\rangle = \sum_{i \in \mathcal{I}} b_i |\psi_i\rangle,$$

On obtient :

$$\begin{aligned} \langle \psi | \phi \rangle &= \langle \sum_{i \in \mathcal{I}} a_i \psi_i | \sum_{i \in \mathcal{I}} b_i \psi_i \rangle = \left(\sum_{i \in \mathcal{I}} a_i^* \langle \psi_i | \right) \left(\sum_{i \in \mathcal{I}} b_i |\psi_i\rangle \right) \\ &= \sum_{i, j \in \mathcal{I}} a_i^* b_j \langle \psi_i | \psi_j \rangle = \sum_{i, j \in \mathcal{I}} a_i^* b_j \langle \psi_i | \psi_j \rangle = \sum_{i \in \mathcal{I}} a_i^* b_i. \end{aligned}$$

1.2 Postulat de Mesure

À toute grandeur physique A associée au système quantique considéré, correspond un opérateur auto-adjoint sur \mathcal{H} , généralement noté \hat{A} , et appelé l'observable A . Ainsi, si l'on mesure la grandeur A , on obtient les résultats suivants :

- Le résultat de la mesure est un élément du *spectre* $\sigma(\hat{A})$, avec $\sigma(\hat{A}) \subset \mathbb{R}$ (*théorème spectral*).

N.B : Le spectre propre $\sigma_{\text{propre}}(\hat{A})$ est inclus dans $\sigma(\hat{A})$, ce qui constitue une notion plus générale, notamment en dimension infinie.

En supposant que le spectre soit dénombrable $\sigma(\hat{A}) = (\lambda_n)_{n \in \mathbb{N}}$

→ La probabilité de mesurer la valeur $a \in \sigma(\hat{A})$, sachant que juste avant la mesure l'état du système était ψ , est donnée par :

$$p(a_n) = \mathbb{E}_\psi(1_{\{a\}}(\hat{A})) = \langle \psi | 1_{\{a\}}(\hat{A}) | \psi \rangle = \sum_{n \in \mathbb{N}} 1_{\{a\}}(\lambda_n) | \langle \psi | \psi_n \rangle |^2.$$

Le nouveau état du système est :

$$|\psi_{\text{après mesure}}\rangle = \frac{1}{\|1_{\{a\}}(\hat{A})\psi\|_{\mathcal{H}}} 1_{\{a\}}(\hat{A}) |\psi\rangle$$

Ici, ψ_n est associé à la valeur du spectre λ_n .

1.3 Postulat d'évolution temporelle d'un système quantique

L'évolution de l'état ψ d'un système quantique isolé est régie par l'équation de Schrödinger.

Elle fait intervenir l'opérateur \hat{H} , associé à l'observable hamiltonien H de l'énergie.

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

La solution de cette équation est donnée par un opérateur Unitaire U , *i.e* ; $U^\dagger U = I$ où $I \equiv I_{\mathcal{H}}$:

$$\begin{cases} |\psi(t)\rangle = U(t) |\psi_0\rangle, & t \in \mathbb{R} \\ |\psi(0)\rangle = |\psi_0\rangle \end{cases}$$

Dans le cas simple où l'Hamiltonien \hat{H} ne dépend pas du temps t :

$$U(t) = e^{-\frac{i}{\hbar} \hat{H} t}$$

1.4 Postulat d'opérateur quantique

Dans le cas général, l'évolution d'un état quantique $|\psi\rangle \rightarrow |\psi'\rangle \in \mathcal{H}$ est toujours réalisée par l'action d'un opérateur unitaire U c'est-à-dire :

$$|\psi'\rangle = U |\psi\rangle, \quad U^\dagger U = I.$$

Dans le contexte de l'informatique quantique, un opérateur unitaire est souvent appelé une *porte quantique* - *Gate*.

Représentation Graphique :

$$|\psi\rangle \text{ --- } \boxed{U} \text{ --- } |\psi'\rangle$$

Remarque :

Une des raisons pour lesquelles on utilise des opérateurs unitaires est qu'ils sont des isométries. Or, les isométries conservent la norme, ce qui permet de garantir la préservation de la normalisation des états quantiques.

1.5 Exemples

1.5.1 Système à 1-qubit

Un *qubit*, comme l'indique son nom, fait référence à un bit quantique, qui est une généralisation des bits classiques $\{0,1\}$ et qui peut être dans une superposition de ces deux états.

- L'espace d'état de ce système est de dimension 2, d'où $\mathcal{H} \cong \mathbb{C}^2$.
- Une base de \mathcal{H} sera $(|0\rangle, |1\rangle)$.

En vue de l'isomorphie, on considérera $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Représentation dans la Sphère de Bloch

L'état d'un *qubit* $|\psi\rangle$ peut être exprimé comme suit, en utilisant les coordonnées sphériques θ et ϕ sur la sphère de Bloch. Notons que, selon le premier postulat de la mécanique quantique, un déphasage global ne modifie pas l'état physique. Par conséquent, on peut ramener tout le déphasage sur un seul côté de la superposition :

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

avec $|a|^2 + |b|^2 = 1$ (la condition de normalisation).

En utilisant cette simplification, l'état $|\psi\rangle$ peut être réécrit sous la forme suivante, où les coefficients a et b sont exprimés en termes des coordonnées sphériques :

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

Ici, θ et ϕ sont les coordonnées sphériques qui paramètrent l'état sur la sphère de Bloch :

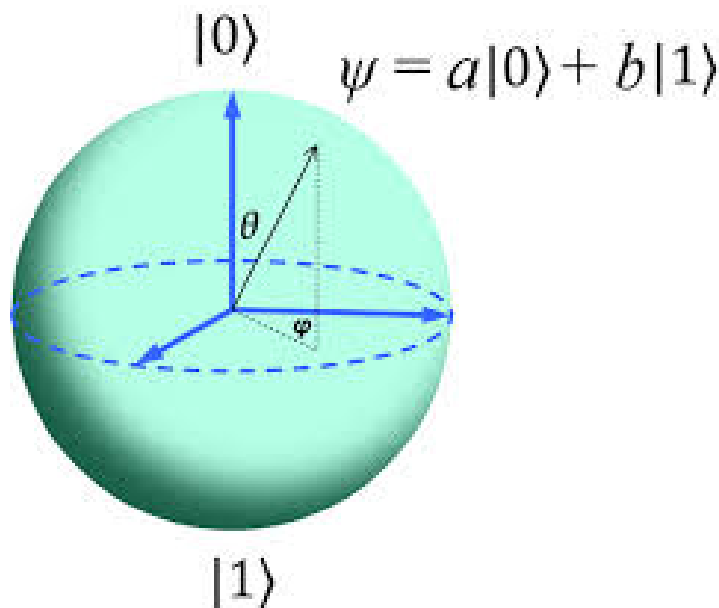


Figure 1: Sphère de Bloch représentant un état $|\psi\rangle$ sur \mathbb{S}^2

Ainsi, chaque état quantique $|\psi\rangle$ correspond à un point sur la sphère de Bloch, et le difféomorphisme entre l'espace de Hilbert \mathcal{H} et la sphère \mathbb{S}^2 est donné par les coordonnées θ et ϕ , qui représentent respectivement l'angle polaire et l'angle azimutal de ce point sur la sphère.

Action des opérateurs et portes quantiques

Les opérateurs agissant sur nos états dans l'espace de Hilbert \mathcal{H} , isomorphe à $\mathbb{C}^{2 \times 2}$, peuvent être interprétés comme des portes quantiques qui modifient l'état d'un *qubit*. Ces opérateurs sont représentés par les matrices de Pauli, qui forment une base naturelle de $\mathbb{C}^{2 \times 2}$, comme suit :

$$\mathbb{C}^{2 \times 2} = \text{Vect}_{\mathbb{C}}(I_2, \sigma_X, \sigma_Y, \sigma_Z)$$

où I_2 est la matrice identité 2×2 , et σ_X , σ_Y , et σ_Z sont les matrices de Pauli :

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ces matrices jouent un rôle crucial dans la manipulation des états quantiques, et leur interprétation en termes de portes quantiques est essentielle pour les circuits quantiques. Voici quelques exemples de portes associées à ces opérateurs :

Porte de SWAP (ou σ_X)

La matrice σ_X , appelée également la porte NOT, agit comme une porte de SWAP dans certains contextes. Plus précisément, elle échange les états $|0\rangle$ et $|1\rangle$. La porte σ_X effectue une opération de **flip** sur le qubit, ce qui peut être vu comme un échange entre les états de base :

$$\sigma_X |0\rangle = |1\rangle, \quad \sigma_X |1\rangle = |0\rangle.$$

Porte de Hadamard

La porte de Hadamard, souvent notée H , est une porte qui applique une superposition . Elle est représentée par la matrice suivante :

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

Cette porte transforme les états de base $|0\rangle$ et $|1\rangle$ de la manière suivante :

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

Ainsi, la porte de Hadamard crée une superposition équivalente entre les états $|0\rangle$ et $|1\rangle$, ce qui est utile pour créer des intrications.

Porte de Rotation

La porte de rotation $R(\theta)$ correspond à une rotation de l'état d'un qubit sur la sphère de Bloch. Elle est représentée par la matrice suivante :

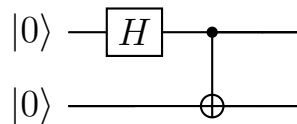
$$R(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

La porte de rotation applique une phase dépendant de θ à l'état $|1\rangle$ tout en laissant $|0\rangle$ inchangé. Plus précisément :

$$R(\theta)|0\rangle = |0\rangle, \quad R(\theta)|1\rangle = e^{i\theta}|1\rangle.$$

Cela correspond à une rotation sur l'axe z de la sphère de Bloch. Les portes de rotation sont très utiles pour appliquer des déphasages dans des circuits quantiques, comme dans les circuits de mesure.

Exemple : Schéma d'un circuit à 2-qubits



Décomposition d'une matrice opérateur

Toute matrice dans $\mathbb{C}^{2 \times 2}$ peut être exprimée comme une combinaison linéaire des matrices de Pauli et de la matrice identité I_2 , ce qui donne une décomposition complète des opérateurs :

$$A = a_0 I_2 + a_1 \sigma_X + a_2 \sigma_Y + a_3 \sigma_Z$$

où a_0, a_1, a_2, a_3 sont des coefficients complexes.

1.5.2 Système à n -qubits

Notant $N = 2^n$

Postulat du produit tensoriel

Lorsqu'un état quantique est composé de n -qubits, chacun ayant un espace d'état $\mathcal{H}_i \cong \mathbb{C}^2$ avec $i = 0, 1, \dots, n-1$, l'espace d'état total est donné par le produit tensoriel de ces espaces d'état. Cet espace est noté :

$$\mathcal{H} = \bigotimes_{i=0}^{n-1} \mathcal{H}_i$$

Si $|\psi_i\rangle$ est un vecteur d'état dans l'espace \mathcal{H}_i , alors l'état global du système est donné par :

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{n-1}\rangle$$

L'espace d'états à n -qubits $\mathcal{H} \cong (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^N$

On pourra donc adopter la notation suivante :

Pour $j \in \{0, 1, \dots, N-1\}$, on écrit la décomposition en base 2 du nombre j sous la forme :

$$j = (\epsilon_{n-1}, \dots, \epsilon_0)^{(2)}$$

où $\epsilon_k \in \{0, 1\}$ pour chaque $k \in \{0, 1, \dots, n-1\}$ est le k -ième chiffre binaire de j dans sa représentation binaire.

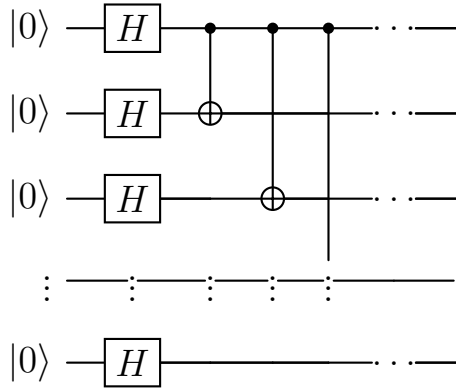
Ainsi, l'état quantique $|j\rangle$, correspondant à la valeur binaire de j , est donné par :

$$|j\rangle = |\epsilon_{n-1}\rangle \otimes |\epsilon_{n-2}\rangle \otimes \dots \otimes |\epsilon_1\rangle \otimes |\epsilon_0\rangle$$

On écrira tout simplement l'état ψ :

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

Exemple : Schéma d'un circuit à n -qubits



Action des opérateurs sur n -qubits

Les opérateurs agissant sur notre nouveau espace \mathcal{H} sont obtenus par tensorisation à partir du cas d'un seul qubit.

Exemple pratique

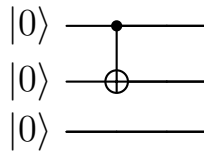
Soit un opérateur U agissant sur un seul qubit, sa version étendue à un système de n qubits est donnée par le produit tensoriel

$$U^{(i)} = I \otimes I \otimes \dots \otimes U \otimes \dots \otimes I$$

où U agit sur le i -ième qubit et I est l'opérateur identité de dimension 2×2 .

Pour un système à trois qubits, si on veut que CNOT agisse sur les deux premiers qubits, on l'étend par tensorisation :

$$\text{CNOT} \otimes I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



Finalement, pour trouver l'état final on agit : $\text{CNOT} \otimes I$ à $|000\rangle$

$$|\psi_{finale}\rangle = \text{CNOT} \otimes I(|000\rangle)$$

2 Quantum Phase Estimation

2.1 Motivation

Après avoir étudié le formalisme mathématique de l'informatique quantique, il est temps de s'intéresser à des algorithmes concrets, comme **l'estimation de phase quantique** (QPE). Cet algorithme est essentiel car il permet d'estimer avec précision la phase d'un opérateur unitaire, c'est-à-dire ses valeurs propres de module 1, ce qui est crucial pour de nombreuses applications en calcul quantique.

Pourquoi s'intéresser à QPE ? Parce que simplement il est au cœur de plusieurs algorithmes importants, comme :

- **L'algorithme de Shor**, qui permet de factoriser des nombres entiers et pourrait remettre en cause la sécurité des systèmes RSA.
- **La résolution des systèmes linéaires quantiques**, notamment avec l'algorithme HHL, qui pourrait accélérer la résolution des EDP et avoir des applications en optimisation.

2.2 Contexte

Soit \mathcal{U} un opérateur unitaire et $|\psi\rangle$ un vecteur propre de \mathcal{U} . Comme les valeurs propres des opérateurs unitaires sont de module 1, l'objectif est de déterminer la phase de cette valeur propre :

$$\mathcal{U}|\psi\rangle = e^{i2\pi\phi}|\psi\rangle, \quad \phi \in [0, 1].$$

2.3 1^{ère} Approche : Test de Hadamard

Connaissant que $\langle\psi|\mathcal{U}|\psi\rangle = e^{i2\pi\phi}$, le test de Hadamard a pour but principal de trouver $\langle\psi|\mathcal{U}|\psi\rangle$.

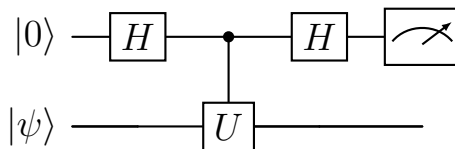


Figure 1. Test de Hadamard pour $\text{Re}(\langle\psi|U|\psi\rangle)$.

Description de ce circuit

Le circuit commence avec l'état initial $|0\rangle |\psi\rangle$. L'application d'une porte Hadamard sur le premier qubit et l'identité sur le second donne :

$$|0\rangle |\psi\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) |\psi\rangle$$

Ensuite, l'opération $c-U$ (porte contrôlée U) est appliquée, ce qui donne :

$$\xrightarrow{c-U} \frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle + |1\rangle U |\psi\rangle)$$

Enfin, une deuxième porte Hadamard est appliquée sur le premier qubit, donnant l'état final :

$$\xrightarrow{H \otimes I} \frac{1}{2} |0\rangle \otimes (1 + e^{i2\pi\phi}) |\psi\rangle + \frac{1}{2} |1\rangle \otimes (1 - e^{i2\pi\phi}) |\psi\rangle$$

Ainsi, la probabilité de mesurer $|0\rangle$ dans le premier qubit est donnée par :

$$p(0) = \frac{1}{2} (1 + \text{Re}(\langle \psi | U | \psi \rangle))$$

Reste à mesurer $\text{Im}(\langle \psi | U | \psi \rangle)$, ce qui peut être fait à l'aide du test suivant, appelé *test de Hadamard imaginaire* :

Notons S la matrice suivante, appelée porte de phase :

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Le circuit correspondant est le suivant :

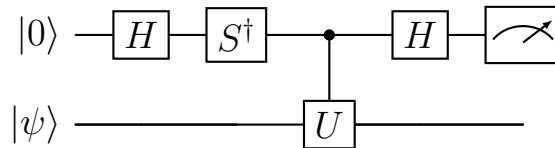


Figure 2. Test de Hadamard pour $\text{Im}(\langle \psi | U | \psi \rangle)$.

Un calcul similaire à celui du *test de Hadamard réel* montre que ce circuit transforme l'état $|0\rangle |\psi\rangle$ en l'état suivant :

$$\frac{1}{2} |0\rangle (|\psi\rangle - iU |\psi\rangle) + \frac{1}{2} |1\rangle (|\psi\rangle + iU |\psi\rangle)$$

Ainsi, la probabilité de mesurer le qubit dans l'état $|0\rangle$ est donnée par :

$$p(0) = \frac{1}{2} (1 + \text{Im}(\langle\psi|U|\psi\rangle))$$

En combinant les résultats des deux circuits, on obtient l'estimation de $\langle\psi|U|\psi\rangle$.

Problème :

À première vue, il semble que cette méthode soit efficace.

Cependant, si l'on souhaite obtenir une grande précision sur la phase ϕ , il est nécessaire d'avoir un grand nombre d'échantillons afin que la loi forte des grands nombres nous fournisse un résultat satisfaisant.

Ordre de Grandeur

L'incertitude sur la mesure est : $\Delta p \sim \frac{1}{\sqrt{N_e}}$, où p est la probabilité que l'on souhaite mesurer.

Pour une précision de l'ordre de ϵ sur ϕ , il nous faut $N_e = \mathcal{O}\left(\frac{1}{\epsilon^4}\right)$.

2.4 2^{ème} Approche : Quantum Fourier Transform QFT

2.4.1 Définition

Pour tout état $|j\rangle$ dans la base de \mathcal{H} , la transformée de Fourier discrète est définie par :

$$U_{\text{FT}} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi \frac{kj}{N}} |k\rangle.$$

L'inverse de la transformée de Fourier discrète est donné par :

$$U_{\text{FT}}^\dagger |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i2\pi \frac{kj}{N}} |k\rangle.$$

L'opérateur de la transformée de Fourier est unitaire

$$U_{\text{FT}}^\dagger U_{\text{FT}} = I$$

Représentation binaire des indices

On peut représenter k et j sous forme binaire :

$$k = (k_{n-1}k_{n-2} \dots k_0)^{(2)}, \quad j = (j_{n-1}j_{n-2} \dots j_0)^{(2)}.$$

On introduit les notations suivantes :

$$(j_{n-1}j_{n-2} \dots j_l \times \dots j_0) = \sum_{k=0}^{n-1} \frac{j_k}{2^{l-k}}$$

$$(\times j_{l-1} \dots j_0) = \sum_{k=0}^{l-1} \frac{j_k}{2^{l-k}}$$

On a ainsi :

$$\begin{aligned} \frac{kj}{N} &= k_0 + k_1 \cdot \frac{j}{2^n} + k_2 \cdot \frac{j}{2^{n-1}} + \dots + k_{n-1} \cdot \frac{j}{2} \\ &= k_0(\times j_{n-1}j_{n-2} \dots j_0) + k_1(j_{n-1} \times j_{n-2} \dots j_0) + \dots + k_{n-1}(j_{n-1}j_{n-2} \dots j_1 \times j_0). \end{aligned}$$

On exprime l'exponentielle comme :

$$e^{i2\pi \frac{kj}{N}} = e^{i2\pi k_0(\times j_{n-1} \dots j_0)} e^{i2\pi k_1(j_{n-1} \times j_{n-2} \dots j_0)} \dots e^{i2\pi k_{n-1}(j_{n-1}j_{n-2} \dots j_1 \times j_0)}$$

L'application de la QFT sur un état $|j\rangle$ donne :

$$U_{\text{FT}} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi \frac{kj}{N}} |k\rangle.$$

Décomposons cette expression sous forme de tenseur :

$$\begin{aligned} |k\rangle &= \bigotimes_{m=0}^{n-1} |k_m\rangle = |k_{n-1}\rangle |k_{n-2}\rangle \dots |k_0\rangle \\ U_{\text{FT}} |j\rangle &= \frac{1}{\sqrt{N}} \bigotimes_{m=0}^{n-1} (|0\rangle + e^{i2\pi(\times j_m j_{m-1} \dots j_0)} |1\rangle). \end{aligned}$$

Cette transformation peut être réalisée par une série de rotations contrôlées de la forme :

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi(\times j_{n-1} \dots j_0)} |1\rangle).$$

2.5 Circuit Quantique de la QFT

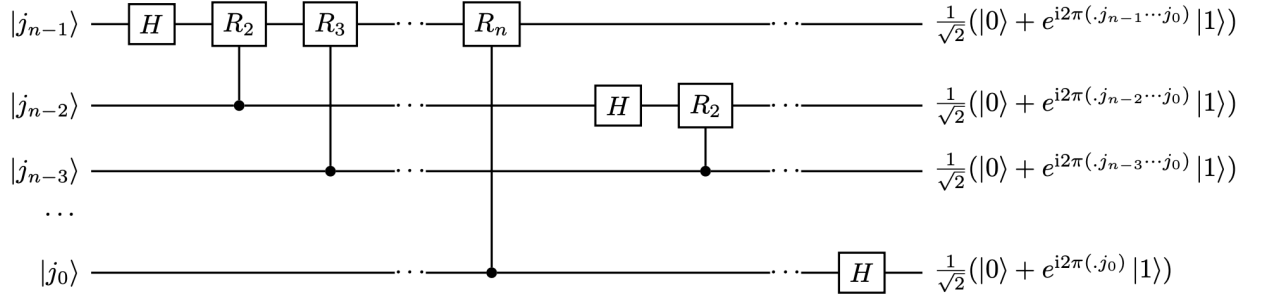


Figure 2: Circuit général pour une QFT sur n qubits

Le circuit général pour une QFT sur n qubits suit le schéma :

1. Appliquer une porte de Hadamard H sur le premier qubit.
2. Appliquer des rotations contrôlées $R_k = R_z(2\pi/2^k)$ sur les autres qubits.
3. Répéter pour chaque qubit avec les rotations adéquates.
4. Appliquer des portes SWAP pour inverser l'ordre des qubits.

avec

$$R_z(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

2.6 Principe de l'Estimation de Phase avec la QFT

Pour estimer notre phase ϕ associée à \mathcal{U} , on suit les étapes suivantes :
Comme $\phi \in [0, 1]$, elle peut être représentée en représentation binaire.
Le nombre de bits choisi reflétera la précision souhaitée pour cette valeur propre.

Étapes Clés de l'algorithme :

1. Préparation de l'état initial :

- Un registre de t qubits initialisés à $|0\rangle$ est utilisé pour stocker l'estimation de ϕ .
- L'état initial est $|0^{\otimes t}\rangle|\psi\rangle$.

2. Application de la QFT inverse :

- La QFT inverse U_{FT}^\dagger est appliquée pour convertir les rotations de phase en une représentation binaire.

3. Mesure du registre :

- La mesure donne une valeur entière $k \approx \phi \cdot 2^t$.
- La phase estimée est $\tilde{\phi} = k/2^t$.

Précision et Nombre d'Échantillonnages

La précision $\epsilon \sim 2^{-d}$ de l'estimation de ϕ et la probabilité de succès $1 - \delta$ déterminent les ressources nécessaires pour l'algorithme :

$$t = d + \lceil \log_2(1/\delta) \rceil \quad (\text{nombre de qubits du registre})$$

3 Applications

3.1 EDP et Système Linéaire

Les équations aux dérivées partielles **EDP** modélisent divers phénomènes physiques, mais leur résolution analytique est souvent impossible.

Une approche numérique consiste à les **discrétiser** pour les transformer en un **système linéaire** de la forme :

$$A\mathbf{u} = \mathbf{f},$$

où A est une **matrice creuse** résultant de la discrétisation de l'opérateur différentiel, et \mathbf{u} est le vecteur des valeurs approximées de la solution $u(x, t)$ sur le maillage discret, tandis que \mathbf{f} est le vecteur des termes sources ou conditions aux bords.

3.2 Équation de Poisson

3.2.1 Généralités

L'équation de Poisson modélise des phénomènes tels que la distribution du potentiel électromagnétique ou la chaleur dans un milieu à température constante. Elle s'écrit généralement sous la forme :

$$-\nabla^2 u(x) = f(x), \quad x \in \Omega,$$

où ∇^2 est l'opérateur laplacien qui représente la somme des dérivées secondes de la fonction u , et $f(x)$ est une fonction donnée représentant une source (charge, par exemple).

3.2.2 Discrétisation de l'Équation de Poisson

Imaginons un problème sur un domaine $[a, b]$ en 1D. En discretisant ce domaine avec un maillage uniforme de pas $h = \frac{b-a}{N+1}$, on remplace les dérivées secondes par des différences finies. L'approximation de la dérivée seconde est donnée par :

$$\frac{u_{i+1} - 2u_i + u_{i-1}}{h^2} \approx \frac{d^2u}{dx^2}.$$

Ainsi, l'équation de Poisson devient :

$$-\frac{u_{i+1} - 2u_i + u_{i-1}}{h^2} = f_i, \quad i = 1, 2, \dots, N.$$

Cela génère un système linéaire :

$$A\mathbf{u} = \mathbf{f},$$

où A est une matrice tridiagonale définie par :

$$A = \frac{1}{h^2} \begin{bmatrix} -2 & 1 & 0 & \dots & 0 \\ 1 & -2 & 1 & \dots & 0 \\ 0 & 1 & -2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & -2 \end{bmatrix},$$

et $\mathbf{u} = [u_1, u_2, \dots, u_N]^T$ est le vecteur des valeurs approximées de $u(x)$ sur le maillage, et $\mathbf{f} = [f_1, f_2, \dots, f_N]^T$ est le vecteur des valeurs de $f(x)$ aux points de discrétisation.

Les conditions aux bords (par exemple $u(0) = 0$ et $u(L) = 0$) imposent des contraintes supplémentaires sur les valeurs aux extrémités du domaine.

3.3 Équation de la Chaleur

3.3.1 Généralités

L'équation de la chaleur modélise l'évolution de la température dans un corps en fonction du temps et de l'espace. Elle s'écrit sous la forme :

$$\frac{\partial u}{\partial t} = \alpha \nabla^2 u(x, t), \quad (x, t) \in \Omega \times (0, T),$$

où α est la diffusivité thermique, et ∇^2 est l'opérateur laplacien spatial.

3.3.2 Discrétisation de l'Équation de la Chaleur

Nous appliquons la méthode des différences finies en temps et en espace pour discrétiser cette équation. Soit $x_i = a + ih$ (discrétisation spatiale) et $t^n = n\Delta t$ (discrétisation temporelle), où h et Δt sont respectivement les pas spatiaux et temporels.

L'approximation de la dérivée temporelle $\frac{\partial u}{\partial t}$ à l'instant t^n est donnée par la méthode d'Euler explicite :

$$\frac{u_i^{n+1} - u_i^n}{\Delta t} \approx \frac{\partial u}{\partial t}.$$

L'approximation du laplacien $\nabla^2 u$ en chaque point spatial est donnée par :

$$\frac{u_{i+1}^n - 2u_i^n + u_{i-1}^n}{h^2} \approx \nabla^2 u.$$

En substituant dans l'équation de la chaleur, on obtient :

$$\frac{u_i^{n+1} - u_i^n}{\Delta t} = \alpha \frac{u_{i+1}^n - 2u_i^n + u_{i-1}^n}{h^2}.$$

Cela peut être réarrangé pour obtenir :

$$u_i^{n+1} = u_i^n + \frac{\alpha \Delta t}{h^2} (u_{i+1}^n - 2u_i^n + u_{i-1}^n).$$

3.4 Résolution Quantique par l'Algorithme HHL

L'algorithme **HHL** (Harrow-Hassidim-Lloyd) permet de résoudre $A\mathbf{x} = \mathbf{b}$ en exploitant l'**estimation de phase quantique QPE**. Cependant, A n'est généralement **pas unitaire**, ce qui empêche une application directe de QPE.

3.4.1 Encodage Unitaire de A

Pour contourner ce problème, on utilise deux méthodes :

- **Exponentielle de matrice** : On utilise la simulation hamiltonienne pour approximer e^{iAt} , qui est unitaire.
- **Block Encoding** : On encode A dans une matrice unitaire plus grande

$$U_A = \begin{bmatrix} A/\alpha & * \\ * & * \end{bmatrix},$$

où α est un facteur d'échelle.

3.4.2 Étapes principales de HHL

1. **Encodage** du vecteur \mathbf{b} en un état quantique $|b\rangle$.
2. **Estimation de phase quantique** : application sur la version unitaire de A .
3. **Application de A^{-1}** via la manipulation des valeurs propres.
4. **Mesure** pour extraire une approximation de \mathbf{x} .

3.4.3 Avantages et Limitations

- **Complexité** : $\mathcal{O}(\log N)$ au lieu de $\mathcal{O}(N^3)$ classiquement à l'aide de l'élimination de Gauss ou de la décomposition LU, où N est la dimension du vecteur \mathbf{b} .
- **Matrice creuse** : bien adapté aux grandes dimensions.
- **Limitations** : nécessité d'un encodage unitaire et extraction de \mathbf{x} par mesure.

3.5 Conclusion

La transformation des **EDP** en systèmes linéaires permet leur résolution efficace par des approches quantiques.

L'algorithme **HHL**, bien que prometteur, nécessite une manipulation astucieuse de A pour être applicable.

4 Références

- 1 L. Lin, *Lecture Notes on Quantum Algorithms for Scientific Computation*, University of California, Berkeley, arXiv:2201.08309, 2022.
- 2 P. Over, S. Bengoechea, P. Brearley, S. Laizet, et T. Rung, *Quantum Algorithm for the Advection-Diffusion Equation by Direct Block Encoding of the Time-Marching Operator*, arXiv preprint, arXiv:2410.07909, 2025.