Masters 2 Systèmes Dynamiques et Signaux

Soutenance de rapport bibliographique

Informatique quantique

23 février 2021

Pierre Engelstein

Membres du jury

Président : Pr. Laurent Hardouin

Examinateurs : Dr. Nicolas Delanoue
Pr. François Chapeau-Blondeau
Pr. Sébastien Lahaye
Dr. Mehdi Lhommeau
Pr. David Rousseau

Encadrants : Dr. Nicolas Delanoue
Pr. François Chapeau-Blondeau

3 Postulats

1. L'état d'un système quantique
2. La dynamique d'un système quantique
3. La mesure d'un système quantique

Références bibliographiques : [1, 2, 3]

Postulat 1 : État d'un système quantique

Définition

Système quantique : vecteur d'état $|\psi\rangle$

- dans un espace de Hilbert complexe $\mathcal{H}$,
- de norme unité : $||\psi||^2 = 1$,
- avec des coordonnées :

$$|\psi\rangle = \sum_i c_i |k_i\rangle \,, \tag{1}$$

- où $\{|k_i\rangle\}_i$ une base orthonormée de $\mathcal{H}$,
- et les coefficients $c_i \in \mathbb{C}$.

Postulat 1 : État d'un système quantique

Système quantique élémentaire : le qubit : $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, dans un espace de Hilbert de dimension 2.

Example

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \,, \tag{1}$$

avec

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ coordonnées de } |0\rangle \text{ et } \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ coordonnées de } |1\rangle \,. \tag{2}$$

Postulat 2 : Dynamique des systèmes quantiques

Définition

La dynamique des systèmes quantiques respecte deux principes :

- Conservation de la norme unité
- Linéarité de l'évolution

Avec un système de coordonnées

Une évolution du système est donnée par une matrice U, telle que : $U^\dagger U = UU^\dagger = I$

Portes quantiques

Exemple

Porte de Pauli X :

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

Soit $|\psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, alors $X|\psi\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

Remarque

La porte de Pauli X est l'équivalent de la porte `NON`

Portes quantiques

Exemple

Porte de Hadamard :

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

Soit $|\psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, alors $H|\psi\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$

Postulat 3 : La mesure projective

Definition

Quand un système quantique est dans un état $|\psi\rangle = \sum_i c_i |k_i\rangle$, on va avoir comme probabilité $|c_i|^2$ de mesurer l'état $|k_i\rangle$.

Remarque

La mesure est ***projective*** *: on pert l'état probabiliste.*

Algorithme de Deutsch-Jozsa [4]

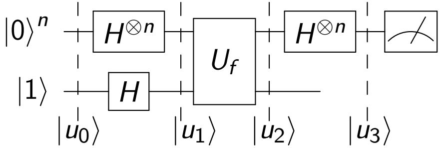
Problème

Déterminer en le moins d'itérations possibles si une fonction f booléenne est constante ou équilibrée

Dans le cas classique : $2^{n-1} + 1$ itérations

Dans le cas quantique : 1 seule itération

Algorithme



1. Initialisation : $|u_0\rangle$
2. $|u_1\rangle$: Mise à l'équilibre : porte de Hadamard
3. $|u_2\rangle$: Application de la fonction U_f
4. $|u_3\rangle$: Préparation pour la mesure

Algorithme de Grover [5]

Problème

On souhaite chercher une entrée spécifique dans une liste non triée à N éléments de façon efficace.

Dans le cas classique : N itération successives.

Dans le cas quantique : $\mathcal{O}(\sqrt{N})$

Opérateur de grover

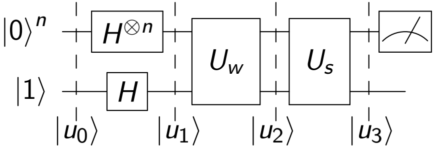
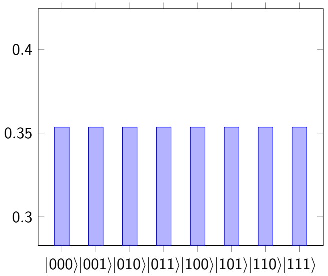


Schéma du circuit de l'algorithme de Grover



$|u_1\rangle$

Opérateur de grover

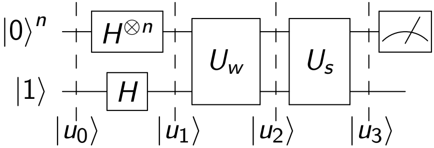
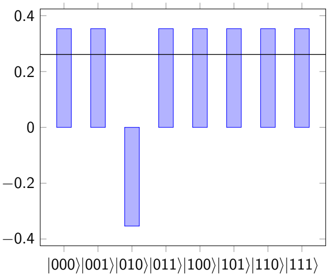


Schéma du circuit de l'algorithme de Grover



$|u_2\rangle$

Opérateur de grover

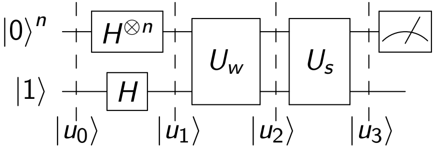
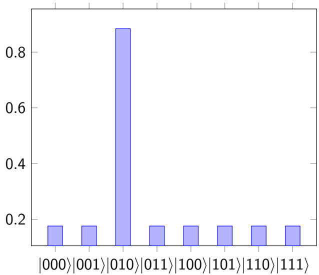


Schéma du circuit de l'algorithme de Grover



$|u_3\rangle$

Opérateur de grover

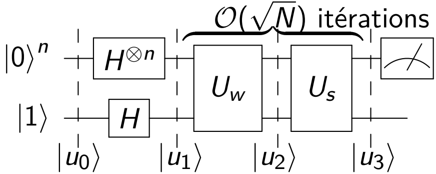


Schéma du circuit de l'algorithme de Grover

Algorithme de Shor [6]

Problème de factorisation de grands entiers en nombres premiers : résoudre $N = p \times q$ avec p et q entiers très grands inconnus.

- Algorithmes classiques : complexité exponentielle

- Algorithmes quantiques : complexité polynomiale

Travail à venir

1. Étendre Deutsch-Jozsa à d'autres problèmes (exemple de Bernstein-Vazirani)
2. Optimalité de la décomposition en portes élémentaires `CNOT`

Conclusion

Domaine de recherche actif, en plein essort.

De nombreuses entreprises se positionnent dessus : IBM, Microsoft, Google, Intel, Atos.

Bibliographie

M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge : Cambridge University Press, 2000.

D. N. Mermin, *Quantum Computer Science : An introduction*. Cambridge : Cambridge University Press, 2007.

C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, pp. 2724–2742, 1998.

D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London A*, vol. 439, pp. 553–558, 1992.

L. K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, p. 212–219. STOC '96, New York, NY, USA : Association for Computing Machinery, 1996.

P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, 1997.