Notes de cours d'Informatique Quantique

Yann Miguel

26 janvier 2021

Table des matières

1 Introduction

Dans l'informatique classique, l'unité de base est le bit. Dans l'informatique quantique, elle est nomée qubit, aussi noté qbit.

1.1 Espace d'Hilbert

Un espace vectoriel normé sur $\mathbb{C}$, complet pour la distance issue de sa norme, dont la norme est un vecteur x, ||x|| découle d'un produit scalaire, ou Hermitien, par la formule:

$$||x|| = \sqrt{< x, x >}$$

On utilise des espaces d'Hilbert de dimension 2 car on possède un système à deux niveaux. Les vecteurs de ce système sont nommés **ket**.
Chaque espace d'Hilbert est noté sur une base orthonormée.
Comme tout vecteur de tout espace vectoriel, un vecteur générique $|\phi >$ admet une décomposition en fonction de |0> et de |1>.

1.2 Projecteurs

Pour une base orthonormée arbitraire, on peut définir les projecteurs suivants: |0><0| et |1><1|.
Les projecteurs sont idempotents, c'est à dire, (|0><0|)^2 = |0><0|.

1.3 Calcul de produit de Kronecker

|0><0| = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\otimes$ (1 0) = 1.(1 0) et 0.(1 0) = $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

1.4 Notations

- <v|w>: produit scalaire
- |w><v|: produit externe de Kronecker

2 Cours 1

En informatique quantique, il n'existe pas d'opération qui n'est pas inversable.

2.1 Espace produit tenseur

Soient H_1 et H_2, deux espaces d'Hilbert. On peux définir un nouvel espace H, du espace produit tenseur.
Le produit tenseur est associatif et distributif.
Soit $|\phi_i>$ une base de H_1 et $|\psi_i>$ une base de H_2. Le produit tenseur $|\phi_i> \otimes |\psi_i>$ est une base de $H = H_1 \otimes H_2$.
Pour les espaces fini, le produit tenseur est réalisé par le produit de Kronecker.

3 Cours 2

Il y a deux type de portes logiques:
- les portes non-réversibles, comme la porte et
- les portes réversibles, comme la porte non

Une porte est dite réversible lorsqu'à partir de la sortie on peux reconstruire l'entrée sans ambigüité.

La porte de Toffoli est une porte logique contenant deux bits de contrôle. Elle est dit universelle, car, en faisant varier les bits de contrôle, on peux avoir une très grande variété de portes logiques.

La porte de Fredkin est une porte à trois bits universelle. Elle comporte un bit de contrôle. Ses sorties sont:
- Si x=0, la sortie de y est y, et la sortie de z est z.
- Si x=1, la sortie de y est z, et la sortie de z est y.

Une porte quantique est un opérateur unitaire agissant sur un ou plusieurs qubits.

Des exemples de portes quantiques sont:
- la porte CNOT(Controlled NOT)
- la porte de Toffoli
- la porte de Fredkin

La linéarité rend la copie d'information impossible en informatique quantique.

4 Cours 3

On ne peux pas calculer un état bien défini, juste la probabilité de l'avoir en partant d'un état donné.

4.1 Algorithme de Deutsch

Cet algorithme définit la nature de la fonction f, c'est à dire si elle est constante ou pas.

4.2 Algorithme de Grover

Il s'agit d'un algorithme de recherche. Cet algorithme consiste à trouver l'élément x_0 dans un tableau de N éléments non triés en faisant en moyenne moins de $\frac{n}{2}$ tirages. Pour cet algorithme, l'état initial doit être une superposition uniforme d'états. Pour faire cela, on crée une combinaison d'état avec des matrices d'Hadamard. Cet algorithme va "signer" l'élément voulu, et on va ensuite l'extraire avec une porte inversant le signe des éléments non nuls. Ensuite, on applique $H^{\otimes N}$ à l'entrée et à la sortie de chaque porte.

5 Cours 4

H^2=Identité.

5.1 Algorithme de Shor

Soit N un nombre composite tel que N=$p_1p_2...p_n$, où $p_i \in \mathbb{P}$.
Trouver un non-trivial de N, c'est à dire un nombre dont les diviseurs sont compris entre 1 et N.

5.1.1 Partie classique

Choisir un nombre aléatoire a tel que 1<a<N.
Calculer le GCD entre a et N. On peux utiliser l'algorithme d'Euclide, qui fait ça en temps polynomial.
Si GCD est différent de 1, cela veut dire que a est un facteur non-triviale de N.
Si GCD est égal à un, cela veut dire que N et a sont co-premiers.
Dans ce cas, il faudra utiliser l'algorithme de Shor.

On veut donc calculer la fonction $f_{a/N}$(x)=a^*ModN.
Pour une grande majorité de "a", la période de $f_{a/N}$ sera un nombre pair. Si jamais la période de a n'est pas paire, il faut choisir un autre a.
Si la période de a est paire, il faut soustraire 1 de chaque côté de l'égalité.

6 Cours 5

6.1 Transformation de Fouriel quantique

Changement de base entre la base canonique et la base de Fouriel.

6.2 Protocole pour Shor

On choisit aléatoirement un nombre a compris entre 1 et N. Si le GCD(a,N) est différent de 1, on applique Euclide. Sinon, on applique Shor.
Avec Shor, on calcule la période de a, nommée r. Si elle est paire, on continue, sinon, on choisit un autre a aléatoire.
On a donc x=a$^{n/2}$ModN, et donc, en ajoutant un +1 et un -1 à gauche et à droite, on peux donc calculer les GCD entre les deux, c'est à dire x+1 et x-1, avec N, et on obtiendra les valeurs de p et de q.

7 Informations importantes

Plutôt qu'un schéma traditionnel CM puis TD, ce cours se fera avec un système de CM et TD en parallèle.

7.1 Évaluation

2 devoirs maisons sur 3 points chacuns, et une présentation sur le projet sur 14 points, le tout faisant une note sur 20.