Notes de cours
Semaine 3

Cours Turing+

1 Axiomes de base de la physique quantique

Nous listons ci-dessous brièvement les principes de base de la physique quantique (restreints au cadre des circuits quantiques).

Etat d'un système quantique

En général, l'état d'un système quantique est représenté par un *vecteur unité* dans un espace vectoriel muni d'un produit scalaire $\langle\cdot|\cdot\rangle$. Et comme nous l'avons déjà vu, l'état d'un système de n qubits est représenté en particulier par un vecteur unité dans $\mathbb{R}^{2^n}$.

Evolution d'un système quantique

En général, l'évolution d'un système quantique (isolé) au cours du temps est décrite une *transformation unitaire* $|\varphi_0\rangle \to |\varphi_t\rangle = U_t\,|\varphi_0\rangle$ [1]. En particulier, le passage de n qubits à travers un circuit quantique peut toujours être décrit par une transformation unitaire U, représentée par une matrice de dimensions $2^n \times 2^n$.

Le postulat de la mesure

Aussi étrange que cela puisse paraître, lorsqu'on observe un système quantique, on perturbe (presque) toujours l'état du système ! Plus précisément, toute observation s'effectue dans une certaine base de l'espace vectoriel. Pour ce cours, nous supposerons toujours que l'observation s'effectue dans la base computationnelle de $\mathbb{R}^{2^n}$: $\big\{\,|x_1,\ldots,x_n\rangle\,,\text{avec } x_1,\ldots,x_n \in \{0,1\}\big\}$.

Si le système est dans un état superposé $|\psi\rangle \in \mathbb{R}^{2^n}$ avant la mesure, il se retrouve après celle-ci dans l'état $|x_1,\ldots,x_n\rangle$ avec probabilité

$$\text{prob}(x_1,\ldots,x_n) = \langle x_1,\ldots,x_n|\psi\rangle^2$$

[1] Plus précisément, l'évolution d'un système quantique est décrite par l'*équation de Schrödinger*, mais continuer sur cette piste nous emmènerait un peu loin...

Exemple : Si un qubit est avant la mesure dans l'état $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ (avec $\alpha_0^2 + \alpha_1^2 = 1$), alors après la mesure, le qubit se retrouve dans l'état $|0\rangle$ avec probabilité α_0^2 ou dans l'état $|1\rangle$ avec probabilité α_1^2 (et donc il est vrai que dans le cas exceptionnel où $|\psi\rangle = |0\rangle$ ou $|\psi\rangle = |1\rangle$ avant la mesure, celle-ci ne perturbe pas le système).

Dans le cas encore plus particulier où $|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, l'état après la mesure est $|0\rangle$ ou $|1\rangle$ avec probabilité $1/2$ pour chaque état.

Autre exemple : Si deux qubits sont dans l'état de Bell $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$ avant la mesure, alors ceux-ci se retrouvent dans l'état $|0,0\rangle = |0\rangle \otimes |0\rangle$ ou l'état $|1,1\rangle = |1\rangle \otimes |1\rangle$ après la mesure, avec de nouveau une probabilité $1/2$ pour chaque état. Notez que chaque sortie possible est un état produit, mais que quelle que soit la sortie, la valeur d'un des deux qubits détermine de façon certaine la valeur de l'autre qubit (d'où le qualificatif d'*état intriqué* pour l'état $|\psi\rangle$ de départ).

Remarques : - Comment définir quand a précisément lieu une observation d'un système quantique ? Une façon un peu "simpliste" de voir la chose est de dire qu'une observation a lieu lorsque le système quantique (microscopique) interagit avec un appareil de mesure (macroscopique). Mais c'est OK si cette réponse ne vous satisfait pas...

- De manière plus générale, si tout ce qui précède vous perturbe, rassurez-vous, c'est normal ! (et ceci vous place du reste dans le même groupe de gens qu'Albert Einstein !) Voilà maintenant bientôt 100 ans que la physique quantique est née, et on en est toujours à vouloir essayer de comprendre la magie derrière...

Composition de systèmes quantiques

Si n_1 qubits sont dans un état $|\varphi_1\rangle \in \mathbb{R}^{2^{n_1}}$ et n_2 autres qubits sont dans un état $|\varphi_2\rangle \in \mathbb{R}^{2^{n_2}}$, alors les $n_1 + n_2$ qubits ensemble sont dans l'état produit

$$|\varphi_1\rangle \otimes |\varphi_2\rangle \in \mathbb{R}^{2^{n_1}} \otimes \mathbb{R}^{2^{n_2}} = \mathbb{R}^{2^{n_1} \cdot 2^{n_2}} = \mathbb{R}^{2^{n_1+n_2}}$$

mais notez que ceux-ci ne sont que les états produits, et qu'il existe aussi des états plus généraux intriqués entre tous ces qubits (comme nous l'avons déjà vu dans le cas particulier $n_1 = n_2 = 1$).

2 Modèle de Deutsch pour les circuits quantiques

La construction d'un circuit quantique peut servir deux buts :

- la simulation d'un système physique, afin de mieux comprendre le fonctionnement de celui-ci (mais ce n'est pas ce que nous ferons dans ce cours) ;

- la résolution efficace d'un problème d'algorithmique classique, impliquant typiquement une fonction booléenne $f : \{0,1\}^n \to \{0,1\}^m$. C'est sur ce second point que nous allons nous concentrer.

Trois étapes principales

1. Préparation d'un état de superposition

Par défaut, l'entrée d'un circuit quantique est toujours un ensemble de *qubits* dans l'état produit $|0,0,\ldots,0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$. Ce nombre de qubits est toujours supérieur à n : les n premiers qubits sont utilisés pour les entrées de la fonction f et les qubits suivants sont des qubits auxiliaires qui servent pour le calcul.

La première étape consiste à préparer l'état du système dans un état de superposition $|\varphi\rangle$ en faisant passer généralement chaque qubit à travers une porte de Hadamard (pour rappel, une porte de Hadamard transforme l'état $|0\rangle$ en l'état $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$).

2. Opération unitaire U (= circuit proprement dit)

Cette étape constitue le coeur de l'algorithme quantique. Elle est composée notamment d'un ou plusieurs appels à la porte oracle U_f qui permet d'évaluer la fonction f (simultanément en plusieurs points $(x_1,\ldots,x_n)$ grâce à l'état de superposition $|\varphi\rangle$ décrit ci-dessus). La sortie de ce circuit est donnée par

$$|\psi\rangle = U\,|\varphi\rangle$$

3. Mesure dans la base computationnelle

L'état de sortie $|\psi\rangle$ du circuit est finalement mesuré dans la base computationnelle $\big\{\,|x_1,\ldots,x_n\rangle\,,$ avec $x_1,\ldots,x_n \in \{0,1\}\big\}$ (pour être plus précis, ce sont les n premiers qubits de l'état de sortie $|\psi\rangle$ qui sont mesurés), et donc le résulat de la mesure vaut $|x_1,\ldots,x_n\rangle$ avec probabilité

$$\text{prob}(x_1,\ldots,x_n) = \langle x_1,\ldots,x_n|\psi\rangle^2 = (\langle x_1,\ldots,x_n|\,U\,|\varphi\rangle)^2$$

Pour finir

Le but de la construction d'un circuit quantique est que l'état de sortie qui nous intéresse (par exemple le point $(x_1,\ldots,x_n)$ où la fonction f est minimum, si on recherche celui-ci) sorte du circuit avec une grande probabilité.

Remarques - Il est intéressant de noter ici qu'il n'y a pas nécessairement besoin que cette probabilité soit égale à 1 : une probabilité simplement plus grande que les autres peut être satisfaisante dans certains cas.

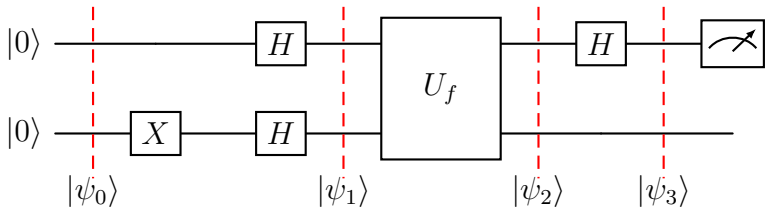
- A noter aussi que les circuits quantiques sont bruités en réalité, et qu'à cause de cela, les promesses théoriques de ces circuits ne sont parfois pas réalisées en pratique. Ceci constitue d'ailleurs un des grands problèmes de ces circuits, encore en 2'024. Une des pistes envisagées pour remédier à ce problème consiste à ajouter des mécanismes de *correction d'erreurs* sur les portes du circuit, mais ceci amène son autre lot de challenges...

3 Problème de Deutsch (et résolution de celui-ci)

Voici l'énoncé de ce problème : étant donné une fonction booléenne $f : \{0,1\} \to \{0,1\}$, on aimerait savoir si $f(0) = f(1)$ ou $f(0) \neq f(1)$. Classiquement, il n'y a qu'une seule façon de répondre à cette question : il faut évaluer $f(0)$ et $f(1)$ (ce qui correspond à deux appels à l'"oracle" f), puis comparer ces deux valeurs. Avec un circuit quantique cependant, il est possible de répondre à la question avec une seule évaluation de la fonction f !

Circuit de Deutsch

Ce circuit quantique est le suivant :



avec donc deux qubits en entrée et en sortie, mais seule la valeur du premier est mesurée à la sortie (ce qui est symbolisé ci-dessus par un appareil mesure standard type voltmètre, mais vous vous imaginez bien que la mesure d'un système quantique, c'est tout autre chose en réalité !).

Analysons pas à pas les états successifs des deux qubits dans ce circuit :

- Au départ, ceux-ci sont dans l'état de base $|\psi_0\rangle = |0\rangle \otimes |0\rangle = |0,0\rangle$.

- Nous faisons ensuite passer le premier qubit à travers une porte H et le second qubit à travers deux portes successives X et H, obtenant ainsi l'état superposé :

$$|\psi_1\rangle = H|0\rangle \otimes HX|0\rangle = H|0\rangle \otimes H|1\rangle = |+\rangle \otimes |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle = \frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} |x\rangle \otimes |-\rangle$$

Notez que c'est voulu de décrire ici un peu différemment l'action de la porte H sur chacun des deux qubits.

- Vient maintenant l'action de la porte oracle U_f vue la semaine dernière. Pour rappel, nous avons par définition :

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

Nous allons voir que

$$U_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

ce qui ressemble à l'effet étrange déjà observé la semaine dernière à propos de la porte CNOT : même si la porte U_f n'est censée agir que sur le second qubit, ceci n'est plus vrai lorsque l'on considère des états superposés. Voyons pourquoi à la page suivante.

$$U_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}} \left(U_f(|x\rangle \otimes |0\rangle) - U_f(|x\rangle \otimes |1\rangle)\right) = \frac{1}{\sqrt{2}} \left(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\right)$$
$$= \frac{1}{\sqrt{2}} \left(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes \left|\overline{f(x)}\right\rangle\right)$$

Donc si $f(x) = 0$, nous obtenons

$$U_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}} \left(|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle\right) = |x\rangle \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right)\right) = |x\rangle \otimes |-\rangle$$

tandis que si $f(x) = 1$:

$$U_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}} \left(|x\rangle \otimes |1\rangle - |x\rangle \otimes |0\rangle\right) = |x\rangle \otimes \left(\frac{1}{\sqrt{2}} \left(|1\rangle - |0\rangle\right)\right) = - |x\rangle \otimes |-\rangle$$

En conclusion, nous avons bien $U_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)} |x\rangle \otimes |-\rangle$ comme annoncé ; ne sont multipliés par un facteur -1 que les états $|x\rangle$ pour lesquels $f(x) = 1$. Ceci nous permet de calculer facilement l'état $|\psi_2\rangle$ des deux qubits à la sortie de la porte U_f, par linéarité :

$$\psi_2 = U_f |\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} U_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

- Il manque une dernière étape : celle qui consiste à appliquer encore une fois une porte H sur le premier qubit (à partir de là, on peut en effet oublier en quelque sorte le second qubit auxiliaire, qui a déjà joué son rôle au passage de la porte U_f). Ceci donne l'état de sortie

$$|\psi_3\rangle = (H \otimes I) |\psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{f(x)} H |x\rangle \otimes |-\rangle$$

Pour calculer l'action de la porte H sur un état $|x\rangle$, remarquez que

$$H |0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) \quad \text{et} \quad H |1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right)$$

ce qui peut se résumer en $H |x\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^x |1\rangle\right)$. Et donc

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{f(x)} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^x |1\rangle\right)\right) \otimes |-\rangle$$
$$= \left(\underbrace{\frac{1}{2} \sum_{x \in \{0,1\}} (-1)^{f(x)}}_{A} |0\rangle + \underbrace{\frac{1}{2} \sum_{x \in \{0,1\}} (-1)^{f(x)+x}}_{B} |1\rangle\right) \otimes |-\rangle$$

Remarquez maintenant que si $f(0) = f(1)$, alors

$$A = \frac{1}{2} \left((-1)^{f(0)} + (-1)^{f(1)}\right) = (-1)^{f(0)} \quad \text{et} \quad B = \frac{1}{2} \left((-1)^{f(0)} + (-1)^{f(1)+1}\right) = 0$$

tandis que si $f(0) \neq f(1)$, alors c'est l'inverse qui se produit :

$$A = \frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right) = 0 \quad \text{et} \quad B = \frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)+1}\right) = (-1)^{f(0)}$$

et donc :

dans le premier cas, $|\psi_3\rangle = (-1)^{f(0)}\,|0\rangle\otimes|-\rangle$, tandis que dans le second, $|\psi_3\rangle = (-1)^{f(0)}\,|1\rangle\otimes|-\rangle$.

Finalement, en mesurant l'état du premier qubit, nous trouvons soit $|0\rangle$ avec probabilité 1, ce qui correspond au cas où $f(0) = f(1)$, soit $|1\rangle$ avec probabilité 1, ce qui correspond au cas où $f(0) \neq f(1)$ (à noter que le signe $(-1)^{f(0)}$ n'influence en rien le résultat de la mesure). Ainsi donc, il est possible de répondre à la question de départ avec un seul appel à l'oracle U_f, c'est-à-dire une seule évaluation de la fonction f.

Question : Si vous avez été attentif à tout ce qui a été dit jusqu'à maintenant, vous aurez remarqué un problème dans tout cet argument : quel est-il ?

Réponse : Le problème est que pour construire la porte U_f, il faut déjà connaître la fonction f, donc la réponse à la question ! (sauf si on maintient la version stricte de l'existence d'un oracle qui nous donne U_f, en quelque sorte. Nous verrons à la fin du cours une application d'un algorithme à un cas plus intéressant.