Notes de cours
Semaine 5

Cours Turing+

1 Problème de la recherche d'un élément

Soient $n \geq 1$ et $f : \{0,1\}^n \to \{0,1\}$ une fonction booléenne. On définit l'ensemble

$$A = \{(x_1, \ldots, x_n) \in \{0,1\}^n \ : \ f(x_1, \ldots, x_n) = 1\}$$

Le problème qu'on cherche à résoudre ici est de trouver efficacement un élément $(x_1, \ldots, x_n) \in A$ (c'est-à-dire un élément $(x_1, \ldots, x_n) \in \{0,1\}^n$ tel que $f(x_1, \ldots, x_n) = 1$).

On définit encore : $\begin{cases} N = |\{0,1\}^n| = 2^n \text{ (la taille de l'ensemble } \{0,1\}^n) \\ M = |A| \text{ (la taille de l'ensemble } A) \end{cases}$

Exemple avec $n = 2$ et $f(x_1, x_2) = \begin{cases} 1 & \text{si } x_1 = x_2 = 0 \\ 0 & \text{sinon} \end{cases}$:

Dans ce cas, $A = \{(0,0)\}$ et $M = 1$, tandis que $N = 2^2 = 4$.

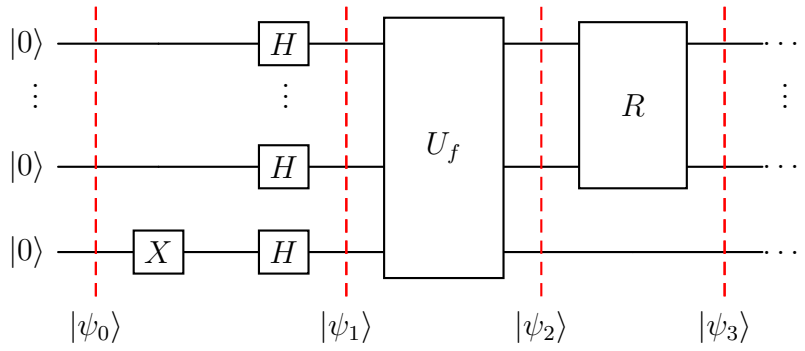
En général, si le rapport M/N est grand, il est relativement facile de trouver un élément de l'ensemble A par des méthodes classiques (si par exemple $M = N/2$, alors en tirant un élément uniformément au hasard dans l'ensemble $\{0,1\}^n$, on a une chance sur deux de trouver un élément de A ; en tirant 10 éléments indépendamment et uniformément au hasard, on a environ 999 chances sur 1'000 de trouver un élément de A). A l'autre extrême, si $M = 1$ et N est grand, on se retrouve alors dans la situation de chercher une aiguille dans une botte de foin : de l'ordre de N évaluations de la fonction f en moyenne sont nécessaires pour trouver l'unique élément de A (et exactement N dans le pire des cas).

L'algorithme quantique de Grover décrit dans les pages suivantes permet de chercher plus efficacement l'aiguille dans la botte de foin, avec seulement de l'ordre de $\sqrt{N}$ évaluations de f.

2 Algorithme de Grover

L'idée de base de l'algorithme de Grover est simple : partant d'un état quantique initial $|0,\dots,0\rangle$, effectuer une série de transformations pour se retrouver le plus proche possible d'un état $|x_1,\dots,x_n\rangle$ avec $(x_1,\dots,x_n) \in A$ (la mesure finale donnant alors le bon résultat avec grande probabilité).

Aussi surprenant que cela puisse paraître, la première partie du circuit qui permet d'arriver là ressemble très fortement au circuit de Deutsch-Josza ! Voici donc la première partie de ce **circuit de Grover** :



Comme vous le voyez, les deux premières étapes de ce circuit sont totalement identiques au circuit de Deutsch-Josza... Seule change la troisième partie composée de la transformation R (pour "réflexion"), que nous détaillerons plus loin.

Pour l'instant, passons en revue les deux premières étapes de ce circuit, tout en apportant un nouvel éclairage sur celles-ci :

- $|\psi_0\rangle = |0,\cdots,0\rangle$ rien de spécial à dire là-dessus... (si ce n'est qu'il y a toujours $n+1$ qubits ici : n pour les variables $x_1,\dots,x_n$ et 1 qubit auxiliaire)

- $|\psi_1\rangle = \dfrac{1}{2^{n/2}} \displaystyle\sum_{(x_1,\dots,x_n)\in\{0,1\}^n} |x_1,\dots,x_n\rangle \otimes |-\rangle$, qu'on peut réécrire sous la forme :

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \left(\underbrace{\sum_{(x_1,\dots,x_n)\in A^c} |x_1,\dots,x_n\rangle}_{N-M \text{ termes}} + \underbrace{\sum_{(x_1,\dots,x_n)\in A} |x_1,\dots,x_n\rangle}_{M \text{ termes}} \right) \otimes |-\rangle$$

Nous avons séparé ici la somme en deux parties pour distinguer les états $|x_1,\dots,x_n\rangle$ avec $(x_1,\dots,x_n)$ appartenant au complémentaire de l'ensemble A, qui ne nous intéressent pas, et ceux avec $(x_1,\dots,x_n)$ appartenant à l'ensemble A, qui sont donc les états qui nous intéressent. Définissons encore

$$|P\rangle = \frac{1}{\sqrt{N-M}} \sum_{(x_1,\dots,x_n)\in A^c} |x_1,\dots,x_n\rangle \quad \text{et} \quad |S\rangle = \frac{1}{\sqrt{M}} \sum_{(x_1,\dots,x_n)\in A} |x_1,\dots,x_n\rangle$$

Il y a plusieurs choses à dire à ce stade :

- Premièrement, $|P\rangle$ et $|S\rangle$ définissent chacun un nouvel état quantique. En effet, les états de base $|x_1, \ldots, x_n\rangle$ sont orthogonaux entre eux (et de norme 1), donc

$$\begin{aligned}\langle P|P\rangle &= \left(\frac{1}{\sqrt{N-M}} \sum_{x_1,\ldots,x_n \in A^c} \langle x_1, \ldots, x_n|\right) \cdot \left(\frac{1}{\sqrt{N-M}} \sum_{y_1,\ldots,y_n \in A^c} |y_1, \ldots, y_n\rangle\right) \\ &= \frac{1}{N-M} \sum_{x_1,\ldots,x_n \in A^c} \sum_{y_1,\ldots,y_n \in A^c} \langle x_1, \ldots, x_n | y_1, \ldots, y_n\rangle \\ &= \frac{1}{N-M} \sum_{x_1,\ldots,x_n \in A^c} \langle x_1, \ldots, x_n | x_1, \ldots, x_n\rangle = \frac{|A^c|}{N-M} = 1\end{aligned}$$

et il en va de même pour $\langle S|S\rangle$.

- Deuxièmement, $|P\rangle$ et $|S\rangle$ sont orthogonaux, encore à cause du fait que les les états de base $|x_1, \ldots, x_n\rangle$ sont orthogonaux entre eux :

$$\langle P|S\rangle = \frac{1}{\sqrt{N-M}\sqrt{M}} \sum_{x_1,\ldots,x_n \in A^c} \sum_{y_1,\ldots,y_n \in A} \langle x_1, \ldots, x_n | y_1, \ldots, y_n\rangle = 0$$

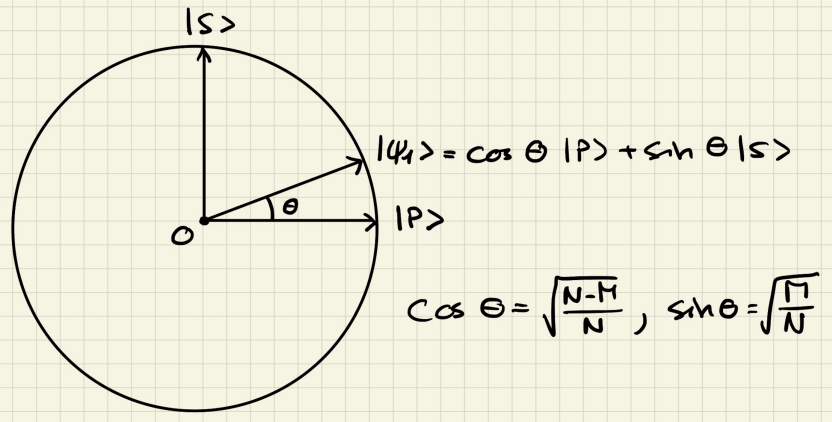
- Et finalement, l'état $|\psi_1\rangle$ peut être réécrit ainsi :

$$|\psi_1\rangle = \left(\sqrt{\frac{N-M}{N}}\ |P\rangle + \sqrt{\frac{M}{N}}\ |S\rangle\right) \otimes |-\rangle$$

et comme $\frac{N-M}{N} + \frac{M}{N} = 1$, il existe un angle $\theta \in [0, \pi/2]$ tel que

$$\sqrt{\frac{N-M}{N}} = \cos(\theta) \quad \text{et} \quad \sqrt{\frac{M}{N}} = \sin(\theta)$$

Voici ce que ça donne graphiquement (notez bien qu'on oublie volontairement de représenter le qubit auxiliaire dans l'état $|-\rangle$ ici) :



A ce stade, rappelons notre but ; amener le système dans un état proche d'un vecteur de base $|x_1, \ldots, x_n\rangle$ avec $(x_1, \ldots, x_n) \in A$, ce qui peut se traduire par : amener le système dans un état proche de l'état $|S\rangle$.

L'état de superposition $|\psi_1\rangle$ est en quelque sorte déjà "partiellement proche" de $|S\rangle$, en ce sens qu'il fait un angle θ avec l'état $|P\rangle$ (qui est l'état à éviter, puisque tous les $(x_1, \ldots, x_n)$ représentés dans cet état ne font pas partie de l'ensemble A), mais nous aimerions trouver un moyen de nous rapprocher plus de $|S\rangle$.

Remarque : Même si cette interprétation géométrique du problème peut laisser croire que celui-ci a une solution simple, à savoir faire pivoter l'état $|\psi_1\rangle$ du bon angle et dans la bonne direction pour arriver à $|S\rangle$, il faut se rappeler que les états $|P\rangle$ et $|S\rangle$ ne sont pas connus a priori (c'est en fait ce qu'on cherche à trouver) et aussi que tous ces états "vivent" dans un espace vectoriel de dimension 2^n dans lequel il n'est pas facile de s'orienter (ce que vous voyez sur le dessin de la page précédente n'est qu'une projection bidimensionelle sur le plan engendré par $|P\rangle$ et $|S\rangle$, qui encore une fois n'est pas connu).

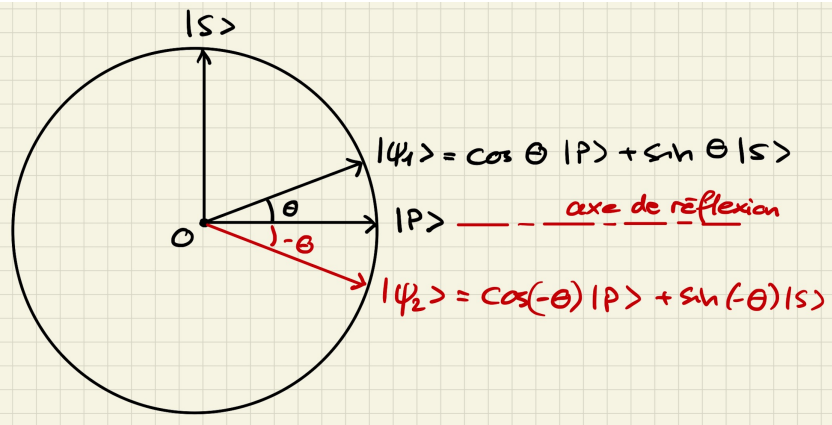
- Revenons maintenant au circuit et analysons plus en détail l'état $|\psi_2\rangle$ après le passage de la porte U_f. Pour rappel, nous avons vu la semaine dernière que

$$|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{(x_1,\ldots,x_n)\in\{0,1\}^n} (-1)^{f(x_1,\ldots,x_n)} |x_1, \ldots, x_n\rangle \otimes |-\rangle$$

Donc tous les états $|x_1, \ldots, x_n\rangle$ tels que $f(x_1, \ldots, x_n) = 1$ (i.e., $(x_1, \ldots, x_n) \in A$) sont multipliés par -1, tandis que les autres sont laissés tels quels. Ceci se traduit avec nos nouvelles notations :

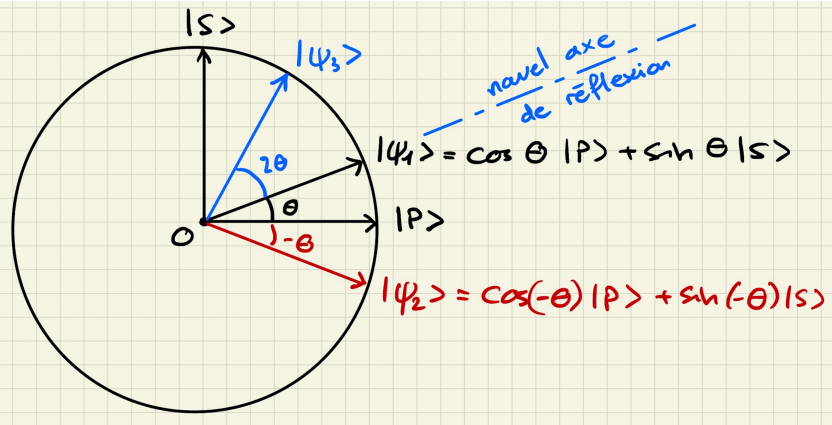
$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{N}} \left(\sum_{(x_1,\ldots,x_n)\in A^c} |x_1, \ldots, x_n\rangle - \sum_{(x_1,\ldots,x_n)\in A} |x_1, \ldots, x_n\rangle \right) \otimes |-\rangle \\
&= \left(\sqrt{\frac{N-M}{N}}\ |P\rangle - \sqrt{\frac{M}{N}}\ |S\rangle \right) \otimes |-\rangle = (\cos(\theta)\ |P\rangle - \sin(\theta)\ |S\rangle) \otimes |-\rangle \\
&= (\cos(-\theta)\ |P\rangle + \sin(-\theta)\ |S\rangle) \otimes |-\rangle
\end{aligned}$$

L'action de la porte U_f peut ainsi être vue comme une *réflexion autour de l'axe* $|P\rangle$ (on oublie à nouveau volontairement ici de représenter le qubit auxiliaire dans l'état $|-\rangle$, mais notez que celui-ci jour un rôle crucial dans l'action de la porte U_f) :



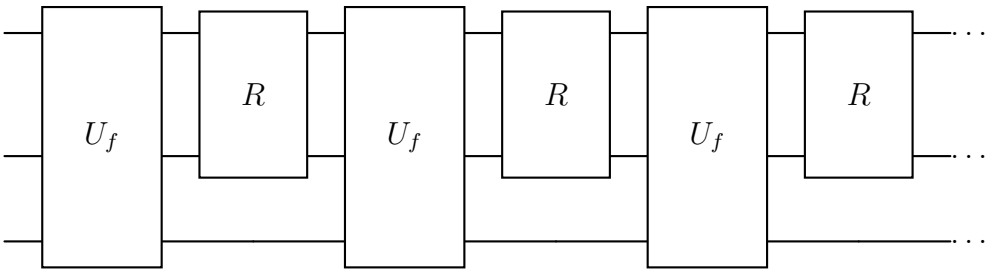
Notez que cette opération de réflexion autour de l'axe $|P\rangle$ n'est possible que grâce à l'évaluation de la fonction f, qui est en quelque sorte encodée dans le vecteur $|P\rangle$. Mais elle ne semble malheureusement pas nous rapprocher de l'axe $|S\rangle$ (et même plutôt nous en éloigner...).

Ceci dit, sans la connaissance de la fonction f, il est maintenant possible d'effectuer une autre opération de réflexion autour de l'axe $|\psi_1\rangle$, qui lui nous est connu. C'est cette opération qui est symbolisée par une porte R dans le circuit plus haut, et que vous réaliserez concrètement lors de la séance d'exercices. Cette opération fait passer l'état $|\psi_2\rangle$ à l'état $|\psi_3\rangle$ représenté ci-dessous :



Vous pouvez maintenant vérifier que la succession des deux réflexions autour de l'axe $|P\rangle$, puis autour de l'axe $|\psi_1\rangle$, équivaut au total à une *rotation d'angle* 2θ *en direction de l'axe* $|S\rangle$. Nous nous sommes ainsi bien rapprochés de l'axe $|S\rangle$ au terme de cette opération.

Reste maintenant encore une idée-clé : répéter l'opération jusqu'à arriver au plus proche de l'état $|S\rangle$, afin de maximiser les chances d'observer un état $|x_1, \ldots, x_n\rangle$ avec $(x_1, \ldots, x_n) \in A$ lors de la mesure finale. Ceci implique de répliquer le sous-circuit composé des portes U_f et R autant de fois que nécessaire :



Et la dernière question qui se pose est : combien de fois fait-il répliquer le sous-circuit composé des portes U_f et R pour approcher au mieux l'état $|S\rangle$? Cette réponse dépend clairement de l'angle initial θ que fait l'état $|\psi_1\rangle$ avec l'état $|P\rangle$, et donc du rapport entre M et N, vu que

$$\sin(\theta) = \sqrt{\frac{M}{N}}$$

Sur la page suivante, nous analysons en détail deux cas particuliers.

Cas particulier $M = N/4$

Dans ce cas, $\sqrt{\frac{M}{N}} = \sqrt{\frac{1}{4}} = \frac{1}{2}$, donc $\theta = \pi/6$. En appliquant une seule fois la rotation de Grover d'angle $2\theta = \pi/3$ (donc en appliquant une fois la porte U_f et une fois la porte R), l'état de sortie $|\psi_3\rangle$ fait un angle de $\pi/6 + \pi/3 = \pi/2$ avec l'axe $|P\rangle$. Autrement dit, l'état $|\psi_3\rangle$ est exactement l'état $|S\rangle$! Dans ce cas particulier, une seule évaluation de f suffit donc à trouver un état $|x_1, \ldots, x_n\rangle$ tel que $(x_1, \ldots, x_n) \in A$ (car la mesure finale donnera un de ces états avec probabilité 1).

Cas particulier $M = 1$

Dans ce cas, $\sqrt{\frac{M}{N}} = \frac{1}{\sqrt{N}} = \sin(\theta)$. Si on suppose de plus que N est grand, alors $\frac{1}{\sqrt{N}} = \sin(\theta)$ est petit. Mais lorsque $\sin(\theta)$ (et θ) sont petits, il est raisonnable de faire l'approximation $\sin(\theta) \simeq \theta$. Ceci veut dire que

$$\theta \simeq \frac{1}{\sqrt{N}}$$

En appliquant k fois la rotation de Grover d'angle 2θ à l'état initial $|\psi_1\rangle$, l'angle que fait l'état final avec l'axe $|P\rangle$ vaut

$$\theta + k \cdot 2\theta \simeq \frac{2k+1}{\sqrt{N}}$$

Pour que cet angle atteigne une valeur proche de $\pi/2$, il faut donc que $2k + 1 \simeq (\pi/2)\sqrt{N}$, autrement dit que de l'ordre de $\sqrt{N}$ rotations de Grover soient effectuées. Ainsi seules de l'ordre de $\sqrt{N}$ évaluations de f sont nécessaires pour trouver l'unique élément $(x_1, \ldots, x_n)$ tel que $f(x_1, \ldots, x_n) = 1$, contrairement au cas classique, où de l'ordre de N évaluations sont nécessaires.

Remarque finale : La même remarque qui s'appliquait au problème de Deutsch-Josza semble s'appliquer ici aussi : c'est bien joli tout ça, mais pour pouvoir construire la porte U_f, il faut a priori connaître entièrement la fonction f, et donc forcément aussi sa valeur en tout point $(x_1, \ldots, x_n) \in \{0,1\}^n$? Ce qui voudrait dire qu'au-delà de l'hypothèse de l'existence d'un réel oracle qui nous fournit le circuit U_f, la question étudiée n'a pas beaucoup d'intérêt en pratique.

La réponse est pourtant différente ici : en effet, il existe beaucoup de fonctions booléennes f qui sont en fait *définies* par le circuit qui permet de les calculer, comme par exemple la fonction f suivante (pour n=4) :

$f(x_1, x_2, x_3, x_4) = (x_1$ OR x_2 OR $\overline{x_3})$ AND $(\overline{x_2}$ OR x_3 OR $x_4)$ AND $(x_1$ OR $\overline{x_2}$ OR $x_4)$ AND (etc.)

Lorsque n est grand et que le nombre de clauses (= expressions faisant intervenir trois litérals ci-dessus) est également grand, trouver un point $(x_1, \ldots, x_n)$ satisfaisant $f(x_1, \ldots, x_n) = 1$ est un problème NP-difficile, ce qui veut dire que la seule "solution" que l'on connaît à ce problème à l'heure actuelle est de tester toutes les solutions $(x_1, \ldots, x_n)$ possibles, donc de l'ordre de $2^n = N$ essais. L'algorithme de Grover permet, du moins en théorie, de réduire considérablement ce nombre d'essais à $\sqrt{N}$. Ceci dit, il reste encore en pratique le problème du bruit présent dans les ordinateurs quantiques...