Algorithme de Grover

1 Rappels d'algèbre : projection et reflection

Soient deux vecteurs $\overrightarrow{u}$ et $\overrightarrow{u}$, avec $\overrightarrow{v}$ normalisé.

Définition 1 *La matrice de projection P de $\overrightarrow{u}$ sur $\overrightarrow{v}$ est définie par $P = \overrightarrow{v} \cdot \overrightarrow{v^T}$.*

Définition 2 *La matrice de reflection R de $\overrightarrow{u}$ par rapport à $\overrightarrow{v}$ est définie par $R = 2\overrightarrow{v} \cdot \overrightarrow{v^T} - I$.*

Exemple 1 *Prenons $\overrightarrow{u} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ et $\overrightarrow{v} = \begin{bmatrix} 1 \\ -2 \end{bmatrix}$.*

On projete $\overrightarrow{u}$ sur $\overrightarrow{v}$:

$P = \frac{\overrightarrow{v} \cdot \overrightarrow{v^T}}{\|v\|^2} = \begin{bmatrix} \frac{1}{\sqrt{5}} & \frac{-2}{\sqrt{5}} \\ \frac{-2}{\sqrt{5}} & \frac{4}{\sqrt{5}} \end{bmatrix}$

Soit : $\overrightarrow{u_v} = P\overrightarrow{u} = \begin{bmatrix} -0.8 \\ 1.6 \end{bmatrix}$

Exemple 2 *Prenons à nouveau $\overrightarrow{u} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ et $\overrightarrow{v} = \begin{bmatrix} 1 \\ -2 \end{bmatrix}$. On effectue une reflection de $\overrightarrow{u}$*

$R = 2 \times \frac{\overrightarrow{v} \cdot \overrightarrow{v^T}}{\|v\|^2} - I = 2 \times \begin{bmatrix} \frac{1}{\sqrt{5}} & \frac{-2}{\sqrt{5}} \\ \frac{-2}{\sqrt{5}} & \frac{4}{\sqrt{5}} \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

La première étape est la double projection $2 \times P$, ce qui donne le vecteur $\begin{bmatrix} -1.6 \\ 3.2 \end{bmatrix}$.

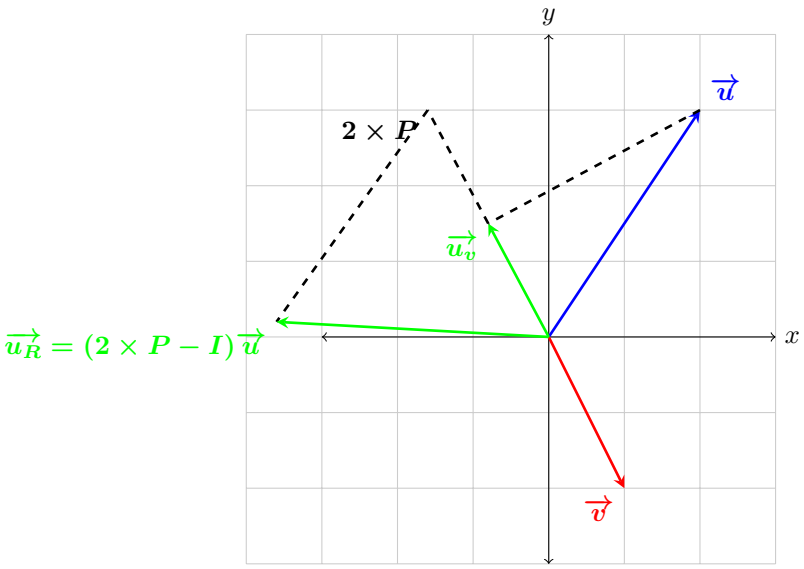
La deuxième étape est d'enlever le vecteur initial, ce qui donne le vecteur $\overrightarrow{u_R} = \begin{bmatrix} -3.6 \\ 0.2 \end{bmatrix}$.

On peut vérifier les angles θ_{UV} et θ_{VU_R} :

$\theta_{UV} = \arccos(\frac{u \cdot v}{\|u\|\|v\|}) = \arccos(\frac{-4}{\sqrt{13} \times \sqrt{5}}) = 119.7°$

$\theta_{VU_R} = \arccos(\frac{v \cdot u_R}{\|v\|\|u_R\|}) = \arccos(\frac{-4}{\sqrt{5} \times \sqrt{13}}) = 119.7°$

Les deux angles sont bien égaux, on a effectué une reflection.



2 Problème à résoudre

Soit une base de données non triée à N entrées. Nous voulons trouver un algorithme permettant de chercher efficacement un enregistrement dans cette base.

2.1 Principe de l'algorithme

L'algorithme de Grover permet de résoudre ce problème en quantique, en disposant de N qubits intriqués pour calculer 2^N état (donc si on a N entrées dans la base, il nous faut $log_2(N)$ qubits intriqués). Dans le cas de cet algorithme, on considère le problème suivant :

On marque $\{0, 1, 2, ..., N-1\}$ les enregistrements de la base de données, et on dénote ω l'état inconnu recherché. On dispose de la fonction suivante :

$$f(x) = \begin{cases} 1, & \text{si x vérifie le critère } \omega \\ 0, & \text{sinon} \end{cases}$$

A la fin, on obtient un set de résultat. Or, lors de la mesure on va avoir au hasard une des solutions suivant les probabilités de chaque état, alors qu'on cherche juste à savoir la (ou les) bonnes solutions. On rajoute donc une amplification d'amplitude permettant d'augmenter les probabilités des bons résultats et de diminuer celles des mauvais.

Initialisation

On commence avec : $|u_0\rangle = (|0\rangle^{\bigotimes n}) \otimes |1\rangle$: n-qubits à $|0\rangle$ et 1-qubit à $|1\rangle$

Etape 1

On applique une porte de Hadamard à $|u_0\rangle$ pour avoir un état équiprobable :
$|u_1\rangle = H|u_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$

On pose alors $|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$

Etape 2 : opérateurs de Grover

On définit les deux opérateurs suivants :

$U_w = I - 2|w\rangle\langle w|$, avec w état cible correspondant à la solution du problème (amplitude de 1 sur l'état visé, amplitude nulle sur le reste)

$U_s = 2|s\rangle\langle s| - I$

Remarque 1 *On reconnait ici que ces deux opérateurs sont semblables à la reflection vue dans la partie 1.*

Inversion d'amplitude L'opérateur U_w effectue l'inversion de l'amplitude de l'état cible, tandis que l'opérateur U_s effectue le miroir des amplitudes par rapport à la moyenne.

On applique U_w puis U_s :

$U_w|s\rangle = (I - 2|w\rangle\langle w|)|s\rangle = |s\rangle - 2|w\rangle\langle w|s\rangle$

Or, $\langle w|s\rangle$ est un produit scalaire. $|w\rangle$ est définit plus haut, et $|s\rangle$ est l'état équiprobable obtenu après la porte de hadamard. Le résultat est donc $\langle w|s\rangle = \frac{1}{\sqrt{2^n}}$. On peut donc réécrire :

$|u_3\rangle = U_w|s\rangle = |s\rangle - \frac{2}{\sqrt{2^n}}|w\rangle$

Miroir à la moyenne On applique ensuite l'opérateur U_s au résultat de U_w. On peut voir qu'en pratique U_s effectue un miroir de $|u_3\rangle$ par rapport à $|s\rangle$.

$$\begin{aligned}
U_s|u_3\rangle &= (2|s\rangle\langle s| - I)(|s\rangle - \frac{2}{\sqrt{2^n}}|w\rangle) \\
&= 2|s\rangle\langle s|s\rangle - |s\rangle - \frac{4}{\sqrt{2^n}}|s\rangle\langle s|w\rangle + \frac{2}{\sqrt{2^n}}|w\rangle \\
&= 2|s\rangle - |s\rangle + \frac{4}{\sqrt{2^n}} \times \frac{1}{\sqrt{2^n}}|s\rangle + \frac{2}{\sqrt{2^n}}|w\rangle \\
&= |s\rangle - \frac{4}{2^n}|s\rangle + \frac{2}{\sqrt{2^n}}|w\rangle \\
|u_4\rangle &= \frac{2^n - 4}{2^n}|s\rangle + \frac{2}{\sqrt{2^n}}|w\rangle \qquad (1)
\end{aligned}$$