

# Algorithme de Grover

## 1 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.

### 1.1 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  $\{0, 1, 2, \dots, N - 1\}$  les enregistrements de la base de données, et on dénote  $\omega$  l'état inconnu recherché. On dispose de la fonction suivante:

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

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.

Les étapes sont les suivantes:

- Préparation des qubits dans un état équiprobable (porte de Hadamard)
- La boîte noire inverse la phase de(s) état(s) vérifiant le critère  $\omega$ . Puisque la probabilité vaut le carré, l'état est toujours valide.
- L'amplificateur d'amplitude vient faire un miroir des amplitudes autour de la moyenne, permettant de favoriser le ou les états correct au profit des autres états.

On répète les deux dernières étapes un certain nombre de fois de façon à obtenir un état qui, quand mesuré, donnera avec quasi-certitude l'état cherché. Entre autres, il faut répéter  $\frac{\pi}{4}\sqrt{N}$  fois ces étapes.