

TP IQ01/AI29 Algorithmes quantiques

* Comprendre l'Oracle :

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7515329/#:~:text=In%20the%20quantum%20case%20we,rather%20than%20on%20classical%20bits.>

Exercice 1 : l'algorithme de Deutsch-Jozsa

A. Le problème

Nous avons une fonction mathématique $f : \{0,1\}^n \rightarrow \{0,1\}$. Cette fonction est une boîte noire mais nous savons que cette fonction est soit constante (la sortie est 0 ou 1 pour toutes les entrées) soit équilibrée (la sortie est 0 dans la moitié des cas, 1 dans les autres).

Si un algorithme classique et déterministe est utilisé alors il faut $2^{n-1}+1$ évaluation de la fonction F pour déterminer si elle est constante ou équilibrée.

B. L'algorithme Deutsch-Jozsa

Est un algorithme quantique qui permet de trouver une réponse toujours correcte avec une seule évaluation de la fonction F . C'est le premier algorithme quantique qui montre l'efficacité d'un programme quantique sur un programme classique.

Dans cet algorithme, nous utilisons

Voici l'explication détaillée de cet algorithme : <https://qiskit.org/textbook/ch-algorithms/deutsch-jozsa.html#1.3-Quantum-Solution-->

Questions :

1. Implémenter les circuits qui représentent l'oracle de votre fonction :
 - Version équilibrée,
 - Version constante.
2. Existe-t-il d'autres implémentations ?
3. Implémenter l'algorithme Deutsch-jozsa généralisé à n qubits (voir la documentation du lien précédent).
4. Modifier votre code pour utiliser l'oracle `dj_problem_oracle` de la librairie `qiskit_textbook.problems` :

```
from qiskit_textbook.problems import dj_problem_oracle  
  
oracle = dj_problem_oracle(1)
```

5. Expliquer le fonctionnement de « `dj_problem_oracle` ».
6. Finaliser votre rapport en expliquant les différentes étapes et le résultat de votre implémentation sur le simulateur (`aer_simulator`) et le vrai ordinateur quantique IBM.

Exercice 2 : l'algorithme de Simon

A. Le problème

Le problème classique de Simon est un problème avec oracle* dont il est prouvé que ce problème ne peut pas être résolu par un algorithme classique aléatoire non-exponentiel.

On a une fonction F inconnue (boîte noire), elle a une des deux formes possibles :

1. $F(x)=y=x$.
2. $F(x)=y$, et y a deux valeurs possibles. Nous savons que dans cette forme, on a b une chaîne de bits où :
 - a. Soit x_1 et x_2 : $f(x_1) = f(x_2)$ alors il est sûr : $x_1 \oplus x_2 = b$

B. La solution

Étant donné cette fonction inconnue, comment pouvons-nous déterminer efficacement si F est forme 1 ou 2 ? Et à quelle vitesse on peut déterminer b si on est dans la deuxième forme ? On peut définir le problème comme la recherche de b chaîne de bits et la chaîne 000... correspond à la forme 1. C'est l'algorithme de SIMON qui implémente la solution quantique et qui répond à cette question : <https://github.com/qiskit-community/qiskit-textbook/blob/main/content/ch-algorithms/simon.ipynb>

Questions

Les mêmes questions que l'exercice 1.