Traitement quantique de l'information I (automne 2009)
Série 20: Algorithme de Grover à 2 qu-bits

Considérer le circuit quantique décrit dans la Figure 1. Ici, la porte quantique "oracle" nous dit si la valeur d'un régistre à 2 qu-bits x est égale ou non à une valeur donnée x_0. Plus précisement elle prend en entrée le régistre $|x_1 x_2 0\rangle$, avec $x = x_1 + 2x_2$ et donne à la sortie $|x_1 x_2 y\rangle$, où $y = 1$ si $x = x_0$ et $y = 0$ autrement. Pour $x_0 = 0, 1, 2, 3$ les circuits correspondant à l'oracle sont indiqués en Figure 2.

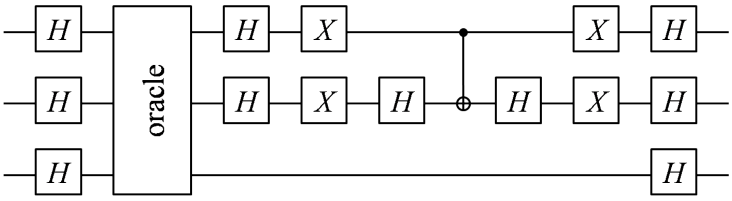

Figure 1: Circuit quantique de Grover à 2 qu-bits

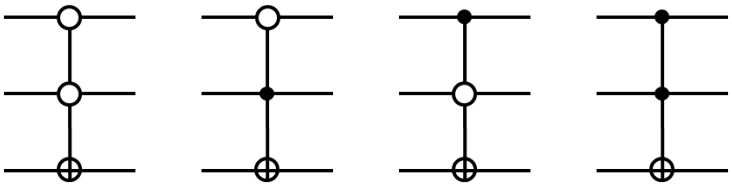

Figure 2: Possibles circuits oracle

Supposer de ne pas savoir lequel parmi les quatre valeurs de x_0 on a choisi pour l'oracle. Appliquer en entrée du circuit $|001\rangle$ (premiers deux qu-bits en haut à zéro, qu-bit en bas à 1). Quel est l'état à la sortie? En combien d'applications de l'oracle on arrive à établir la valeur de x_0? Combien il en faudrait (en moyenne) si l'oracle était un circuit classique?

Ceci est un exemple élémentaire d'algorithme de recherche de Grover. Cette classe d'algorithmes est très importante puisque – en plus de permettre une recherche dans une base de données non structurée avec complexité $\sqrt{N}$ – elle permet en général d'accélérer la solution de tous les problèmes NP-complets (avec une complexité qui est la racine carrée de la complexité classique correspondant).